

REQUEST FOR QUOTATION (THIS IS NOT AN ORDER)		THIS RFO <input type="checkbox"/> IS <input checked="" type="checkbox"/> IS NOT A SMALL BUSINESS SET ASIDE		PAGE OF PAGES 1 300
1 REQUEST NO. HSHQDC-07-R-00094	2 DATE ISSUED 06/19/2007	3 REQUISITION/PURCHASE REQUEST NO.	4 CERT. FOR NAT. DEF UNDER BDSA REG 2 AND/OR DMS REG. 1	RATING
5a. ISSUED BY U.S. Dept. of Homeland Security Office of Procurement Operations ITAC IT Support Services Branch 245 Murray Lane, SW Building 410 Washington DC 20528			6 DELIVERY BY (Date) Multiple	
5b. FOR INFORMATION CALL (No collect calls)			7 DELIVERY <input type="checkbox"/> FOB DESTINATION <input type="checkbox"/> OTHER (See Schedule)	
8 TO			9 DESTINATION	
a NAME Charles Conrad			a NAME OF CONSIGNEE	
b COMPANY			b STREET ADDRESS	
c STREET ADDRESS			c CITY	
d CITY	e STATE	f ZIP CODE	d STATE	e ZIP CODE
10. PLEASE FURNISH QUOTATIONS TO THE ISSUING OFFICE IN BLOCK 5a ON OR BEFORE CLOSE OF BUSINESS (Date) 07/10/2007 1500 ES		IMPORTANT This is a request for information, and quotations furnished are not offers. If you are unable to quote, please so indicate on this form and return it to the address in Block 5a. This request does not commit the Government to pay any costs incurred in the preparation of the submission of this quotation or to contract for supplies or services. Supplies are of domestic origin unless otherwise indicated by quote. Any representations and/or certifications attached to this Request for Quotations must be completed by the quoter.		

11. SCHEDULE (Include applicable Federal, State and local taxes)

ITEM NO (a)	SUPPLIES/SERVICES (b)	QUANTITY (c)	UNIT (d)	UNIT PRICE (e)	AMOUNT (f)
	Request for Technical Qualifications & Preliminary Price Estimate A copy of the RFP Enclosed for Planning Purposes. Questions regarding the RFP will only be entertained from the successful offerors of the down-select after July 31, 2007. If this date changes, offerors will be notified via FedConnect. Note: Attachment 1 and Section J- Attachment J-1 refer to the same PWS/Section C document. Therefore, the document is attached only once, in Attachment 1.				

12. DISCOUNT FOR PROMPT PAYMENT	a. 10 CALENDAR DAYS (%)	b. 20 CALENDAR DAYS (%)	c. 30 CALENDAR DAYS (%)	d. CALENDAR DAYS	
				NUMBER	PERCENTAGE

NOTE: Additional provisions and representations are are not attached

13. NAME AND ADDRESS OF QUOTER			14. SIGNATURE OF PERSON AUTHORIZED TO SIGN QUOTATION	15. DATE OF QUOTATION
a. NAME OF QUOTER			16. SIGNER	b. TELEPHONE
b. STREET ADDRESS				
c. COUNTY				AREA CODE
d. CITY	e. STATE	f. ZIP CODE	c. TITLE (Type or print)	NUMBER

DRIZED FOR LOCAL REPRODUCTION
us edition not usable

STANDARD FORM 18 (REV. 6-95)
Prescribed by GSA - FAR (48 CFR) 53.215-1(a)

RFP

**IT-NOVA
Operations and Maintenance**

TABLE OF CONTENTS

B.1	GENERAL	2
B.2	BASE AND OPTION PERIODS	2
B.3	TASK ORDER PRICING	2
B.3.1	TIME AND MATERIAL LABOR.....	2
B.3.2	DEPLOYMENT ORDERS.....	3
B.4	UPDATED SECTION B.5 LABOR RATE TABLE	3
B.5	LABOR RATE TABLE	4
C.1	PERFORMANCE WORK STATEMENT	5
D.1	PACKAGING AND MARKING	6
D.2	MARKINGS	6
D.3	EQUIPMENT REMOVAL	6
E.1	GENERAL	7
E.2	CLAUSES INCORPORATED BY REFERENCE	7
E.3	INSPECTION AND ACCEPTANCE	7
E.4	SCOPE OF INSPECTION	8
E.5	BASIS OF ACCEPTANCE	8
E.6	REVIEW OF DELIVERABLES	9
E.7	WRITTEN ACCEPTANCE/REJECTION BY THE GOVERNMENT	9
F.1	TASK ORDER TERM	10
F.2	OPTION TO EXTEND THE TERM OF THE CONTRACT	10
F.3	EVALUATION OF OPTIONS (FAR 52.217-5) (JUL 1990)	10
F.4	OPTION TO EXTEND SERVICES (FAR 52.217-8) (NOV 1999)	10
F.5	PLACE OF PERFORMANCE	11
F.6	DELIVERY OF REPORTS	11
G.1	TO CONTRACTING OFFICER (TO CO)	12
G.2	TO ADMINISTRATIVE CONTRACTING OFFICER (TO ACO)	12
G.3	CONTRACTING OFFICER’S TECHNICAL REPRESENTATIVE (COTR)	13

IT-NOVA
Operations and Maintenance

G.3.1	COTR (HSAR 3052.242-72)(DEC 2003).....	13
G.3.2	COTR DESIGNATION	13
G.3.3	CHANGES IN COTR DESIGNATION(S).....	14
G.4	ORDERING.....	14
G.4.1	ORDERING PROCEDURES.....	14
G.4.2	DEPLOYMENT ORDER CONTENT	15
G.4.3	MODIFICATION OF ORDERS	16
G.4.4	DEPLOYMENT ORDER PERIOD OF PERFORMANCE	16
G.5	ACCOUNTABILITY OF COSTS/SEGREGATION OF TASKS/DEPLOYMENT ORDERS.....	16
G.6	INVOICE REQUIREMENTS	17
G.6.1	PAYMENT UNDER TIME-AND-MATERIALS AND LABOR-HOUR CONTRACTS.....	17
	(FAR 52.232-7) (FEB 2007).....	17
G.6.2	INVOICE APPROVAL	22
G.6.3	INVOICE ATTACHMENTS.....	22
G.6.4	INVOICE REQUIREMENT DATA ELEMENTS	22
G.6.5	MATERIAL ORDER STATUS REPORT.....	24
G.7	ELECTRONIC INVOICE SUBMISSION	24
G.8	TRAVEL AND PER DIEM.....	24
G.9	PURCHASE AGENT AUTHORITY	25
G.10	GOVERNMENT-FURNISHED FACILITIES AND EQUIPMENT	25
H.1	GENERAL.....	26
H.2	TYPE OF TASK ORDER	26
H.3	SUBCONTRACTING.....	26
H.4	FAIR OPPORTUNITY FOR FUTURE TASK ORDER COMPETITION.....	27
H.5	WARRANTY PERIOD	28
H.6	INTERRELATIONSHIP OF ASSOCIATE CONTRACTORS.....	28
H.7	NON-PERSONAL SERVICES.....	28
H.8	QUALIFICATIONS OF EMPLOYEES.....	29
H.9	PERSONNEL ACCESS.....	30
H.10	NON-DISCLOSURE AGREEMENTS	30
H.11	DHS REQUIREMENTS AND DUTIES FOR HANDLING SENSITIVE SECURITY INFORMATION (SSI).....	30
H.12	DHS DATA PROTECTED BY THE PRIVACY ACT.....	31
H.13	ORDER OF PRECEDENCE	31
I.1	FAR CLAUSES INCORPORATED BY REFERENCE	32

**IT-NOVA
Operations and Maintenance**

I.2	HSAR CLAUSES INCORPORATED BY REFERENCE	32
I.4	CONTINUITY OF SERVICES (FAR 52.237-3) (JAN 1991).....	33
I.5	OFFICIALS NOT TO BENEFIT	34
I.6	WHISTLEBLOWER PROTECTION FOR CONTRACTOR EMPLOYEES	34
I.7	NOTICE OF DELAY	35
I.8	STOP WORK (FAR 52.242-15) (AUG 1989)	35
I.9	SENSITIVE UNCLASSIFIED INFORMATION	36
I.10	ORGANIZATIONAL CONFLICT OF INTEREST (HSAR 3052.209-72).....	37
	(JUN 2006)	37
I.11	KEY PERSONNEL OR FACILITIES (HSAR 3052.215-70) (DEC 2003).....	38
I.12	AVAILABILITY OF FUNDS (FAR 52.232-18) (APR 1984)	39
	PART II – PART III – LIST OF DOCUMENTS, EXHIBITS AND OTHER ATTACHMENTS	41
	SECTION J – LIST OF ATTACHMENTS	41
K.1	REPRESENTATION – RELEASE OF CONTRACT INFORMATION	42
L.1	TYPE OF AWARD.....	43
L.2	SOLICITATION AMENDMENTS.....	43
L.3	DUE DILIGENCE/EXCHANGES OF INFORMATION	43
L.4	GENERAL INSTRUCTIONS.....	44
L.5	GENERAL INFORMATION	45
L.6	ORGANIZATION/PROPOSAL FORMAT/PAGE LIMITS.....	46
L.7	PROPOSAL CONTENT	48
	L.7.1 VOLUME 1 - TECHNICAL PROPOSAL	48
	L.7.1(A) SECTION 1 - EXECUTIVE SUMMARY (10 PAGES, NOT INCLUDED IN PAGE COUNT)	48
	L.7.1(B) SECTION 2 – TECHNICAL CAPABILITY	49
	L.7.2 VOLUME 2 - MANAGEMENT PROPOSAL	50
	L.7.3 VOLUME 3 - PRICE PROPOSAL.....	52
	L.7.4 VOLUME 4 – ORAL PRESENTATIONS AND DISCUSSIONS	56
L.8	SOLICITATION PROVISIONS INCORPORATED BY REFERENCE	58
L.9	EVALUATION OF COMPENSATION FOR PROFESSIONAL EMPLOYEES	60
M.1	GENERAL.....	62
M.2	BASIS FOR AWARD	62

**IT-NOVA
Operations and Maintenance**

M.3 EVALUATION FACTORS..... 62

M.4 RELATIVE IMPORTANCE OF EVALUATION FACTORS..... 63

M.5 EVALUATION CRITERIA..... 63

M.6 EVALUATION..... 66

 M.6.1 RATING SCALE FOR NON-PRICE FACTORS 67

 M.6.2 RATING SCALE FOR NON-PRICE FACTOR 4 – PROPOSAL RISK..... 67

 M.6.3 EXTENT OF SMALL BUSINESS PARTICIPATION..... 68

 M.6.4 PRICE PROPOSAL EVALUATION..... 68

M.7 EVALUATION OF OPTIONS 69

M.8 USE OF NON-GOVERNMENT ADVISORS 69

**IT-NOVA
Operations and Maintenance**

PART I - THE SCHEDULE

SECTION B—SUPPLIES AND SERVICES AND PRICES/COSTS

B.1 General

The Contractor shall provide all of the contract line items (CLINs) incorporated herein. These CLINs specify pricing for each of the services, deliverables, and data items within the scope and performance work statement described in Section C of this Task Order. The Government expects to procure most or all of these CLINs on a time and materials basis. Deployment Projects (Performance Work Statement Section C.5.2) will be initiated and activated in accordance with the procedures set forth in Section G for the identified CLIN(s).

B.2 Base and Option Periods

The term of this task order is a one year base period and four (4) one year option periods.

B.3 Task Order Pricing

B.3.1 Time and Material Labor

All work will be priced in accordance with the pricing set forth in the EAGLE contract, Section B.5 and Section J, Attachment J-5, Pricing Model. The labor rates in this section reflect the fully-burdened rates for each labor category and will apply to all direct labor hours.

(a) Labor. The Section B.5 Labor Rate Table and Section J, Attachment J-5, Pricing Model shall represent fully-loaded hourly rates for each skill classification. The fully-burdened labor rates include all direct, indirect, general and administrative costs and profit associated with providing the required skill for performance at specified Government sites. The use of uncompensated overtime is not encouraged.

(b) Government Site Rates. When performing at Government sites, the Government will provide only office space, furniture, and office equipment and supplies, as described in Section C.3 herein.

(c) Contractor Site Rates. When performing at a Contractor site, the Contractor shall furnish fully-burdened labor rates which include loads for office space and all normal supplies and services required to support the work, as described in Section C.4 herein.

IT-NOVA Operations and Maintenance

(d) ODCs. During the life of the task order, the Government may order Other Direct Costs (ODCs) in an amount not to exceed \$74 million for each 12 month performance period. Each ODC Contract Line Item Number (CLIN) and dollar amount represents a quarterly allocation and is optional. It is anticipated that ODCs will be funded quarterly using Working Capital Funds; hence, ODCs under this task order are subject to FAR 52.232.18-Availability of Funds. ODCs shall be reimbursed unless otherwise negotiated prior to issuance of any work order. ODCs consist of materials, subcontractor (other than labor) and task order-related travel costs, i.e., relocation and temporary duty (TDY) to include travel, lodging and meals. The ODC percentages are indicated on the Section B.5 Labor Rate Table under the ODC rates. Deployment orders will include quantity of hours required at the proposed rates herein for each labor category, plus materials (ODCs) and the fixed ODC markup percentages. The cost of general-purpose items required for the conduct of the Contractor's normal business operations will not be considered an allowable ODC in the performance of work under this task order. See also Section G and Section H for limitations on materials and mandatory support documentation. Profit is not allowed on ODCs under this task order. All travel costs associated with this task order, if applicable, shall be in accordance with the Federal Travel Regulations (see Section G).

B.3.2 Deployment Orders

For deployment orders, the quantity of hours ordered from each labor category will be specified as deliverable hours billable at the rates specified in the Section B.5 Labor Rate Table. Travel and ODCs will be estimated for each deployment order and burdened with the ODC markup percentage specified in the Section B.5 Labor Rate Table. Profit on travel and ODCs is not allowable. The cumulative extended total of all labor categories ordered plus travel and ODCs will define the deployment order ceiling price. Deployment orders may authorize adjustments between labor category quantities of up to 10%, within the established task labor ceiling price, without a change order. The government will not reimburse the Contractor for costs incurred beyond the ceiling price, for hours not delivered, for hours delivered but in excess of the quantities ordered for a particular labor category, or for travel and ODCs exceeding the ordered pool amount. Labor dollars will not be used to pay for ODCs nor ODC dollars used to pay for labor without a change order. Additional information on Deployment Order Requirements is provided in PWS Section C.1.11.1.7.

B.4 UPDATED SECTION B.5 LABOR RATE TABLE

The Contractor shall provide an updated, electronic Section B.5 labor rate table on an as needed basis to the Contracting Officer. The Section B.5 Labor Rate Table contains the labor categories and labor rates as well as any applicable information regarding the T&M rates. The updated Section B.5 table will be incorporated into the task order via task order modification as required.

**IT-NOVA
Operations and Maintenance**

B.5 LABOR RATE TABLE

Fixed loaded labor rates shall include all direct labor costs, indirect costs, overhead, general and administrative (G&A) expenses, and profit.

CLIN	DESCRIPTION	RATE
X1XX	Government Site Rates	(to be inserted at task order award)
X2XX	Contractor Site Rates	(to be inserted at task order award)
ODC Rates		
X3XX	Travel Markup Percentage	0.00%
X4XX	Materials or Subcontracts Markup Percentage	0.00%
OPTIONAL ODCs*		
X5XX	Travel Costs-Quarter 1 or 2 or 3 or 4	(to be determined when travel required)
X6XX	Materials/Subcontracts (other than labor) Quarter 1 or 2 or 3 or 4	(to be determined when required)

* Subject to Availability of Funds

(End of Section B)

**IT-NOVA
Operations and Maintenance**

**SECTION C—DESCRIPTION/SPECIFICATIONS/PERFORMANCE WORK
STATEMENT**

C.1 PERFORMANCE WORK STATEMENT

See Attachment J-1, Section J for the Performance Work Statement.

(End of Section C)

**IT-NOVA
Operations and Maintenance**

SECTION D—PACKAGING AND MARKING

D.1 PACKAGING AND MARKING

The EAGLE contract clause D.1 – *Packing, Packaging, Marking and Storage of Equipment* is incorporated by reference and has the same force and effect as if it were restated in this task order.

D.2 MARKINGS

The EAGLE contract clause D.2 – *Markings* is incorporated by reference and has the same force and effect as if it were restated in this task order.

D.3 EQUIPMENT REMOVAL

Task order requirements for equipment removal are detailed in Performance Work Statement (PWS) Sections C.3 and C.5.

(End of Section D)

**IT-NOVA
Operations and Maintenance**

SECTION E—INSPECTION AND ACCEPTANCE

E.1 GENERAL

This section sets forth requirements for inspection and acceptance of all equipment, systems, and services acquired under this Task Order and installed/performed by the Contractor. It establishes inspection and acceptance testing requirements that must be met before any systems, equipment or services, ordered under this contract are accepted by the Government. This section also applies to all replacement systems and equipment, substitute equipment, or other individual items of equipment ordered throughout the term of the Task Order.

E.2 CLAUSES INCORPORATED BY REFERENCE

This Task Order, as applicable, incorporates by reference one or more provisions or clauses listed below with the same force and effect as if they were given in full text. Upon request, the Contracting officer will make their full text available. Also, the full text can be accessed electronically at this internet address:

<http://acquisition.gov/far/index.html>. The full text of the HSAM clause can be accessed electronically at this internet address:

<https://dhsonline.dhs.gov/portal/jhtml/dc/sf.jhtml?doid=45071>.

FAR Clause No.	Title	Date
52.246-6	Inspection of Services – Time and Material or Labor-Hour	May 2001
HSAM Clause No.	Title	Date
3046.672	Inspection, Acceptance and Receiving Report	Dec 2006

E.3 INSPECTION AND ACCEPTANCE

(a) Inspection and acceptance of all work and services performed under this TO will be in accordance with the FAR and HSAM clauses incorporated in Section E.2, *Clauses Incorporated by Reference* as applicable, and Section C of this RFP.

(b) Final acceptance of all deliverables and/or services performed as specified under this Task Order will be made in writing, at destination by the TO COTR.

IT-NOVA
Operations and Maintenance

E.4 SCOPE OF INSPECTION

(a) All deliverables will be inspected for content, completeness, and accuracy and conformance to task order requirements by the TO COTR. Inspection may include validation of information or software through the use of automated tools and/or testing of the deliverables, as specified in Section C of this RFP. The scope and nature of this testing will be sufficiently comprehensive to ensure the completeness, quality and adequacy of all deliverables and services.

(b) The government requires a period not to exceed ten (10) business days after receipt of services and final deliverable items for inspection and acceptance or rejection unless otherwise specified in Section C of this RFP.

E.5 BASIS OF ACCEPTANCE

(a) The basis for acceptance shall be in compliance with the requirements set forth in the task order Section C, the deployment order, the Contractor's proposal, the Contractor's EAGLE contract and other terms and conditions of this Task Order. Services and/or deliverable items rejected shall be corrected in accordance with the applicable clauses.

(b) Commercial and non-developmental hardware items, software items, pre-packaged solutions, and maintenance and support solutions will be accepted within ten (10) business days of delivery when performance is in accordance with delivery requirements.

(c) Custom services and cost reimbursable items such as travel and ODCs will be accepted upon receipt of proper documentation as specified in Section G.8 for Travel and/or Section C of this RFP. If custom services are required such as software development, the final acceptance of the services or product, e.g., software program will occur when all discrepancies, errors or other deficiencies identified in writing by the government have been resolved, either through documentation updates, program correction, or other mutually agreeable methods.

(d) Reports, documents and narrative type deliverables will be accepted when all discrepancies, errors or other deficiencies identified in writing by the government have been corrected.

IT-NOVA
Operations and Maintenance

(e) Non-conforming products or services will be rejected or revised as directed by the COTR. Unless otherwise agreed by the parties, deficiencies will be corrected within ten (10) business days of the rejection notice. If the deficiencies cannot be corrected within the specified period, the Contractor will immediately notify the TO Contracting Officer of the reason for the delay and provide a proposed corrective action plan within ten (10) business days.

E.6 REVIEW OF DELIVERABLES

(a) The government will provide written acceptance, comments and/or change requests, if any, within ten (10) business days from receipt by the Government of the initial deliverable, as indicated in Section C of this RFP.

(b) Upon receipt of the Government comments, the Contractor shall have fifteen (15) business days to incorporate the government's comments and/or change requests and to resubmit the deliverable in its final form.

(c) If written acceptance, comments and/or change requests are not issued by the Government within 10 business days of submission, the draft deliverable shall be deemed acceptable as written and the Contractor may proceed with the submission of the final deliverable product.

E.7 WRITTEN ACCEPTANCE/REJECTION BY THE GOVERNMENT

The Government shall provide written notification of acceptance or rejection of all final deliverables within 10 business days. Absent written notification, final deliverables will be construed as accepted. All notifications of rejection will be accompanied with an explanation of the specific deficiencies causing the rejection.

(End of Section E)

IT-NOVA
Operations and Maintenance

SECTION F—DELIVERIES OR PERFORMANCE

F.1 TASK ORDER TERM

The term of this T&M task order is a one-year base period from effective date of award with four (4) one-year option periods.

**F.2 OPTION TO EXTEND THE TERM OF THE CONTRACT
(FAR 52.217-9) (Mar 2000)**

(a) The Government may extend the term of this task order by written notice to the Contractor at any time within the term of the EAGLE contract, provided that the Government gives the Contractor a preliminary written notice of its intent to extend at least thirty (60) days before the contract expires. The preliminary notice does not commit the Government to an extension.

(b) If the Government exercises this option, the extended task order shall be considered to include this option clause.

(c) The total duration of this contract, including the exercise of any options under this clause, shall not exceed sixty (60) months.

F.3 EVALUATION OF OPTIONS (FAR 52.217-5) (JUL 1990)

Except when it is determined in accordance with FAR 17.206(b) not to be in the Government's best interests, the Government will evaluate offers for award purposes by adding the total price for all options to the total price for the basic requirement. Evaluation of options will not obligate the Government to exercise the option(s).

F.4 OPTION TO EXTEND SERVICES (FAR 52.217-8) (NOV 1999)

The Government may require continued performance of any services within the limits and at the rates specified in the contract. These rates may be adjusted only as a result of revisions to prevailing labor rates provided by the Secretary of Labor. The option provision may be exercised more than once, but the total extension of performance hereunder shall not exceed 6 months. The Contracting Officer may exercise the option by written notice to the Contractor within thirty (30) days prior to the end of the performance period.

**IT-NOVA
Operations and Maintenance**

(End of Clause)

F.5 PLACE OF PERFORMANCE

The contractor shall perform the work under this task order at locations specified in:

- Section C of the Performance Work Statement,
- Technical Exhibit C.1.2-002-01, Locations Supported Summary (Sensitive but Unclassified),
- And at such other locations as may be approved in writing by the TO Contracting Officer, e.g., Help Desk – as specified in PWS Section C.5.5, must be on contractor's facilities located 50 miles outside of the Washington, DC metropolitan area and within the continental United States of America; and, Test Laboratory – as specified in PWS section C.5.4, if DHS chooses to provide Government furnished facility.

F.6 DELIVERY OF REPORTS

Unless otherwise specified in Section C, all reports shall be addressed to the COTR marked with the task order number, to the attention of the appropriate TO COTR recipient or as specified by the CO.

(End of Section F)

**IT-NOVA
Operations and Maintenance**

SECTION G—CONTRACT ADMINISTRATION DATA

G.1 TO CONTRACTING OFFICER (TO CO)

The TO Contracting Officer (TO CO) is the only person authorized to make any changes, approve any changes in the requirements of this Task Order, obligate funds and authorize the expenditure of funds, and notwithstanding any provisions contained elsewhere in this task order, the said authority remains solely in the TO CO. In the event, the contractor makes any changes at the direction of any person other than the TO CO, the change will be considered to have been without authority and no adjustment will be made in the task order price to cover any increase in costs occurred as a result thereof. It is incumbent on the Contractor to make sure that this requirement is enforced, or work performed will be performed at the Contractor's own risk.

The following TO Contracting Officer is assigned to this Task Order:

TO Contracting Officer:

NAME:	Charles Conrad
PHONE NO.:	(202) 447-5554
EMAIL:	charles.conrad@dhs.gov

G.2 TO ADMINISTRATIVE CONTRACTING OFFICER (TO ACO)

The TO Administrative Contracting Officer(s) (TO ACOs) is the person authorized to administer the requirements of this Task Order. In the event, the contractor makes any changes to the requirements at the direction of any person other than the TO ACO or the TO CO, the change will be considered to have been without authority and no adjustment will be made in the task order price to cover any increase in costs occurred as a result thereof. It is incumbent on the Contractor to make sure that this requirement is enforced, or work performed will be performed at the Contractor's own risk.

**IT-NOVA
Operations and Maintenance**

The following TO Administrative Contracting Officer(s) are assigned to this Task Order:

TO Administrative Contracting Officer:

NAME:	TBD
PHONE NO.:	TBD
EMAIL:	TBD

G.3 CONTRACTING OFFICER'S TECHNICAL REPRESENTATIVE (COTR)

G.3.1 COTR (HSAR 3052.242-72)(DEC 2003)

(a) The Contracting Officer may designate Government personnel to act as the Contracting Officer's Technical Representative (COTR) to perform functions under the contract such as review or inspection and acceptance of supplies, services, including construction, and other functions of a technical nature. The Contracting Officer will provide a written notice of such designation to the Contractor within five working days after contract award or for construction, not less than five working days prior to giving the contractor the notice to proceed. The designation letter will set forth the authorities and limitations of the COTR under the task order.

(b) The Contracting Officer cannot authorize the COTR or any other representative to sign documents, such as contracts, contract modifications, etc., that require the signature of the Contracting Officer.

G.3.2 COTR Designation

The TO Contracting Officer hereby designates the individual(s) named below as the Contract Officer's Technical Representative(s). Such designations(s) shall specify the scope and limitations of the authority so delegated.

COTR:

NAME:
ADDRESS: TBD
PHONE NO.: TBD

IT-NOVA
Operations and Maintenance

G.3.3 Changes in COTR Designation(s)

The COTR may be changed at any time by the Government without prior notice to the Contractor. Notification of the change, including the name and phone number of the successor COTR, will be promptly provided to the Contractor by the TO Contracting Officer in writing.

G.4 ORDERING

G.4.1 Ordering Procedures

Certain services to be furnished under this task order (as specified by CLIN(s)) shall be ordered by issuance of Deployment Orders. Such Deployment Orders may be issued from date of task order award up to sixty (60) months from date of task order award (if all options are exercised). Each *designated* Deployment Project shall be initiated only by issuance of a TO ACO approved Deployment Order. The work to be performed under these Deployment Orders must be within the scope of the task order. The Government is only liable for labor hours expended under the terms and conditions of this task order to the extent that a TO ACO approved Deployment Order has been issued and covers the required work. Charges for any work not authorized shall be disallowed.

The COTR shall initiate the Deployment Order implementation process by preparing a statement of requirements or objectives to be achieved by completion of the Deployment Order in the form of a Deployment Order Request (DOR). The DOR will contain a detailed description of the functional or other objectives to be achieved, a schedule for completion of the Deployment Order, funding sources, and deliverables to be provided by the Deployment Order as well as a statement of work, independent government cost estimate or rough order of magnitude, other direct costs, anticipated labor mix/hours and location and any special requirements.

The Contractor shall acknowledge receipt of each DOR and shall develop and forward to the COTR within ten (10) business days a Deployment Project Plan for accomplishing the assigned task within the period specified. The Deployment Project Plan shall define the scope, specific tasks and actions which are proposed to be taken by the Contractor to complete the Deployment Order, resumes of key personnel (as applicable), and a price estimate. The Deployment Project Plan shall provide the Contractor's interpretation of the scope of work, a description of the technical approach, work schedule and deliverables. The Contractor shall also identify all the

Source Selection Information – See FAR 2.101 and 3.104

Page 14 of 70

IT-NOVA
Operations and Maintenance

responsibilities of the Government which will affect the Deployment Order and any dependencies which may exist. The COTR will evaluate the Deployment Project Plan for consistency with the DOR and budget. Then, the COTR will submit recommendations to the TO ACO for approval/disapproval of the Deployment Project Plan. The TO ACO will approve (or reject) and send the Deployment Project Plan to the Contractor for further action.

Based upon the contents of the Deployment Project Plan, the Contractor and the Government shall negotiate a ceiling price for the Deployment Project Plan, any changes in the scope of the work to be performed, the schedule or the deliverables to be provided in the Deployment Order.

Within two (2) working days following the conclusion of the final negotiations related to the Deployment Project Plan, the Contractor shall submit a revised Deployment Project Plan which reflects the negotiated agreement. A revised Deployment Project Plan is then approved by the TO ACO who issues the Deployment Order.

The Contractor shall begin work on the Deployment Order in accordance with the effective date indicated in the TO ACO approved Deployment Project Plan.

G.4.2 Deployment Order Content

Deployment Orders issued shall include, but not be limited to the following information, when applicable):

- (a) Date of order;
- (b) Task Order and Deployment Order numbers;
- (c) Task Order Reference/WBS;
- (d) Appropriation and accounting data;
- (e) Description of the services to be performed;
- (f) Description of end item(s) to be delivered;
- (g) DD Form 254 (Contract Security Classification Specification);
- (h) Contract Data Requirements List;
- (i) The individual responsible for inspection/acceptance;
- (j) Period of performance/delivery date;
- (k) Estimated number of labor hours for each applicable labor category;
- (l) The fixed price or ceiling price for the order;
- (m) List of Government furnished equipment, material, and information; and
- (n) Signature/Concurrence lines for Contractor and TO ACO.

Source Selection Information – See FAR 2.101 and 3.104

Page 15 of 70

IT-NOVA
Operations and Maintenance

All orders are subject to the terms and conditions of this task order. In the event of conflict between a Deployment Order and this Task Order, the Task Order shall control.

If mailed, a Deployment Order is considered "issued" when the Government deposits the Deployment Order in the mail (electronic and/or postal/delivery service).

G.4.3 Modification of Orders

Following execution of the Deployment Order, the COTR shall notify the TO ACO of any need to change the Deployment Order which will impact the cost, schedule or deliverables content of the baseline work plan. In cases where technical instructions or other events may dictate a change from the baseline, Deployment Orders may be formally amended in writing by the TO ACO to reflect modifications to tasking. The Contractor is responsible for revising the work plan to reflect Deployment Order amendments within five (5) business days following negotiation or issuance of a change order.

The ceiling price for each Deployment Order may not be changed except when authorized by a fully executed change order issued by the TO ACO. The Contractor shall not exceed the ceiling price established in each Deployment Order. When the Contractor has reason to believe that the total cost will exceed 15 percent of the projected cost specified in the Deployment Order, the Contractor shall notify the TO ACO and COTR. Such notification shall include an estimate of the additional amount and, if necessary, additional time required for completion of the ordered work.

G.4.4 Deployment Order Period of Performance

Deployment Orders may be placed during the period of performance of the task order, as identified in clause F.1. Agreed upon labor rates awarded for the task order shall prevail throughout the entire period of performance. Work performed on such orders after the end of the task order's period of performance will continue to be charged at the last effective rates.

G.5 ACCOUNTABILITY OF COSTS/SEGREGATION OF TASKS/DEPLOYMENT ORDERS

IT-NOVA
Operations and Maintenance

All costs incurred by the Contractor under this task order shall be segregated by task/deployment order. The Contractor shall, therefore, establish separate job order accounts and numbers for each task/deployment order and shall record all incurred costs in the appropriate job order account assigned each task/deployment order. There shall be no commingling of costs between options.

G.6 INVOICE REQUIREMENTS

**G.6.1 Payment Under Time-and-Materials and Labor-Hour Contracts
(FAR 52.232-7) (FEB 2007)**

The Government will pay the Contractor as follows upon the submission of vouchers approved by the Contracting Officer or the authorized representative:

(a) *Hourly rate.*

(1) *Hourly rate* means the rate(s) prescribed in the contract for payment for labor that meets the labor category qualifications of a labor category specified in the contract that are—

- (i) Performed by the Contractor;
- (ii) Performed by the subcontractors; or
- (iii) Transferred between divisions, subsidiaries, or affiliates of the Contractor under a common control.

(2) The amounts shall be computed by multiplying the appropriate hourly rates prescribed in the Schedule by the number of direct labor hours performed.

(3) The hourly rates shall be paid for all labor performed on the contract that meets the labor qualifications specified in the contract. Labor hours incurred to perform tasks for which labor qualifications were specified in the contract will not be paid to the extent the work is performed by employees that do not meet the qualifications specified in the contract, unless specifically authorized by the Contracting Officer.

(4) The hourly rates shall include wages, indirect costs, general and administrative expense, and profit. Fractional parts of an hour shall be payable on a prorated basis.

(5) Vouchers may be submitted once each month (or at more frequent intervals, if approved by the Contracting Officer), to the Contracting Officer or authorized representative. The Contractor shall substantiate vouchers (including any subcontractor hours reimbursed at the hourly rate in the schedule) by evidence of actual payment and by—

- (i) Individual daily job timekeeping records;
- (ii) Records that verify the employees meet the qualifications for the labor categories specified in the contract; or
- (iii) Other substantiation approved by the Contracting Officer.

Source Selection Information – See FAR 2.101 and 3.104

Page 17 of 70

IT-NOVA
Operations and Maintenance

(6) Promptly after receipt of each substantiated voucher, the Government shall, except as otherwise provided in this contract, and subject to the terms of paragraph (e) of this clause, pay the voucher as approved by the Contracting Officer or authorized representative.

(7) Unless otherwise prescribed in the Schedule, the Contracting Officer may unilaterally issue a contract modification requiring the Contractor to withhold amounts from its billings until a reserve is set aside in an amount that the Contracting Officer considers necessary to protect the Government's interests. The Contracting Officer may require a withhold of 5 percent of the amounts due under paragraph (a) of this clause, but the total amount withheld for the contract shall not exceed \$50,000. The amounts withheld shall be retained until the Contractor executes and delivers the release required by paragraph (g) of this clause.

(8) Unless the Schedule prescribes otherwise, the hourly rates in the Schedule shall not be varied by virtue of the Contractor having performed work on an overtime basis. If no overtime rates are provided in the Schedule and overtime work is approved in advance by the Contracting Officer, overtime rates shall be negotiated. Failure to agree upon these overtime rates shall be treated as a dispute under the Disputes clause of this contract. If the Schedule provides rates for overtime, the premium portion of those rates will be reimbursable only to the extent the overtime is approved by the Contracting Officer.

(b) *Materials*.

(1) or the purposes of this clause—

(i) *Direct materials* means those materials that enter directly into the end product, or that are used or consumed directly in connection with the furnishing of the end product or service.

(ii) *Materials* means—

(A) Direct materials, including supplies transferred between divisions, subsidiaries, or affiliates of the Contractor under a common control;

(B) Subcontracts for supplies and incidental services for which there is not a labor category specified in the contract;

(C) Other direct costs (*e.g.*, incidental services for which there is not a labor category specified in the contract, travel, computer usage charges, etc.); and

(D) Applicable indirect costs.

(2) If the Contractor furnishes its own materials that meet the definition of a commercial item at 2.101, the price to be paid for such materials shall not exceed the Contractor's established catalog or market price, adjusted to reflect the—

(i) Quantities being acquired; and

(ii) Actual cost of any modifications necessary because of contract requirements.

Source Selection Information – See FAR 2.101 and 3.104

Page 18 of 70

IT-NOVA
Operations and Maintenance

- (3) Except as provided for in paragraph (b)(2) of this clause, the Government will reimburse the Contractor for allowable cost of materials provided the Contractor—
- (i) Has made payments for materials in accordance with the terms and conditions of the agreement or invoice; or
 - (ii) Ordinarily makes these payments within 30 days of the submission of the Contractor's payment request to the Government and such payment is in accordance with the terms and conditions of the agreement or invoice.
- (4) Payment for materials is subject to the Allowable Cost and Payment clause of this contract. The Contracting Officer will determine allowable costs of materials in accordance with Subpart 31.2 of the Federal Acquisition Regulation (FAR) in effect on the date of this contract.
- (5) The Contractor may include allocable indirect costs and other direct costs to the extent they are—
- (i) Comprised only of costs that are clearly excluded from the hourly rate;
 - (ii) Allocated in accordance with the Contractor's written or established accounting practices; and
 - (iii) Indirect costs are not applied to subcontracts that are paid at the hourly rates.
- (6) To the extent able, the Contractor shall—
- (i) Obtain materials at the most advantageous prices available with due regard to securing prompt delivery of satisfactory materials; and
 - (ii) Take all cash and trade discounts, rebates, allowances, credits, salvage, commissions, and other benefits. When unable to take advantage of the benefits, the Contractor shall promptly notify the Contracting Officer and give the reasons. The Contractor shall give credit to the Government for cash and trade discounts, rebates, scrap, commissions, and other amounts that have accrued to the benefit of the Contractor, or would have accrued except for the fault or neglect of the Contractor. The Contractor shall not deduct from gross costs the benefits lost without fault or neglect on the part of the Contractor, or lost through fault of the Government.
- (7) Except as provided for in 31.205-26(e) and (f), the Government will not pay profit or fee to the prime Contractor on materials.
- (c) If the Contractor enters into any subcontract that requires consent under the clause at 52.244-2, Subcontracts, without obtaining such consent, the Government is not required to reimburse the Contractor for any costs incurred under the subcontract prior to the date the Contractor obtains the required consent. Any reimbursement of subcontract costs incurred prior to the date the consent was obtained shall be at the sole discretion of the Government.
- (d) *Total cost.* It is estimated that the total cost to the Government for the performance of this contract shall not exceed the ceiling price set forth in the Schedule, and the

Source Selection Information – See FAR 2.101 and 3.104

Page 19 of 70

IT-NOVA
Operations and Maintenance

Contractor agrees to use its best efforts to perform the work specified in the Schedule and all obligations under this contract within such ceiling price. If at any time the Contractor has reason to believe that the hourly rate payments and material costs that will accrue in performing this contract in the next succeeding 30 days, if added to all other payments and costs previously accrued, will exceed 85 percent of the ceiling price in the Schedule, the Contractor shall notify the Contracting Officer giving a revised estimate of the total price to the Government for performing this contract with supporting reasons and documentation. If at any time during performing this contract, the Contractor has reason to believe that the total price to the Government for performing this contract will be substantially greater or less than the then stated ceiling price, the Contractor shall so notify the Contracting Officer, giving a revised estimate of the total price for performing this contract, with supporting reasons and documentation. If at any time during performing this contract, the Government has reason to believe that the work to be required in performing this contract will be substantially greater or less than the stated ceiling price, the Contracting Officer will so advise the Contractor, giving the then revised estimate of the total amount of effort to be required under the contract.

(e) *Ceiling price.* The Government will not be obligated to pay the Contractor any amount in excess of the ceiling price in the Schedule, and the Contractor shall not be obligated to continue performance if to do so would exceed the ceiling price set forth in the Schedule, unless and until the Contracting Officer notifies the Contractor in writing that the ceiling price has been increased and specifies in the notice a revised ceiling that shall constitute the ceiling price for performance under this contract. When and to the extent that the ceiling price set forth in the Schedule has been increased, any hours expended and material costs incurred by the Contractor in excess of the ceiling price before the increase shall be allowable to the same extent as if the hours expended and material costs had been incurred after the increase in the ceiling price.

(f) *Audit.* At any time before final payment under this contract, the Contracting Officer may request audit of the vouchers and supporting documentation. Each payment previously made shall be subject to reduction to the extent of amounts, on preceding vouchers, that are found by the Contracting Officer or authorized representative not to have been properly payable and shall also be subject to reduction for overpayments or to increase for underpayments. Upon receipt and approval of the voucher designated by the Contractor as the "completion voucher" and supporting documentation, and upon compliance by the Contractor with all terms of this contract (including, without limitation, terms relating to patents and the terms of paragraph (g) of this clause), the Government shall promptly pay any balance due the Contractor. The completion voucher, and supporting documentation, shall be submitted by the Contractor as promptly as practicable following completion of the work under this contract, but in no event later

IT-NOVA
Operations and Maintenance

than 1 year (or such longer period as the Contracting Officer may approve in writing) from the date of completion.

(g) *Assignment and Release of Claims.* The Contractor, and each assignee under an assignment entered into under this contract and in effect at the time of final payment under this contract, shall execute and deliver, at the time of and as a condition precedent to final payment under this contract, a release discharging the Government, its officers, agents, and employees of and from all liabilities, obligations, and claims arising out of or under this contract, subject only to the following exceptions:

(1) Specified claims in stated amounts, or in estimated amounts if the amounts are not susceptible of exact statement by the Contractor.

(2) Claims, together with reasonable incidental expenses, based upon the liabilities of the Contractor to third parties arising out of performing this contract, that are not known to the Contractor on the date of the execution of the release, and of which the Contractor gives notice in writing to the Contracting Officer not more than 6 years after the date of the release or the date of any notice to the Contractor that the Government is prepared to make final payment, whichever is earlier.

(3) Claims for reimbursement of costs (other than expenses of the Contractor by reason of its indemnification of the Government against patent liability), including reasonable incidental expenses, incurred by the Contractor under the terms of this contract relating to patents.

(h) *Interim payments on contracts for other than services.*

(1) Interim payments made prior to the final payment under the contract are contract financing payments. Contract financing payments are not subject to the interest penalty provisions of the Prompt Payment Act.

(2) The designated payment office will make interim payments for contract financing on the not applicable [Contracting Officer insert day as prescribed by agency head; if not prescribed, insert "30th"] day after the designated billing office receives a proper payment request. In the event that the Government requires an audit or other review of a specific payment request to ensure compliance with the terms and conditions of the contract, the designated payment office is not compelled to make payment by the specified due date.

(i) *Interim payments on contracts for services.* For interim payments made prior to the final payment under this contract, the Government will make payment in accordance with the Prompt Payment Act (31 U.S.C. 3903) and prompt payment regulations at 5 CFR part 1315.

IT-NOVA
Operations and Maintenance

G.6.2 Invoice Approval

It is the responsibility of the Contracting Officer Technical Representative (COTR) to ensure that all services/products have been delivered by the Contractor prior to invoice acceptance and payment. The Contractor shall submit all invoices in accordance with the address listed in section G.7.

G.6.3 Invoice Attachments

A separate invoice should be provided each month for the support billed to DHS. In addition, a fully completed Standard Form (SF) 1034, Public Voucher for Purchases and Services Other Than Personal, shall accompany each separate contractor invoice. Invoice content requirements are outlined in Table G-1 below. Each separate contractor invoice shall be accompanied by a cover sheet with the dollar amount billed, the cumulative dollar amount billed to date and the balance remaining for the task order. The contractor shall prepare and submit individual vouchers to DHS using the same criteria employed to obligate funding on the Task Order and individual Work Orders. The invoice shall have a valid Material Inspection and Receiving Report (DHS 700-21) signed by an authorized DHS government representative for all materials contained in the invoice. A copy of each signed DHS 700-21 shall be sent to the designated COTR authorized to evaluate contractual obligations on behalf of DHS.

G.6.4 Invoice Requirement Data Elements

A detailed list of invoice requirements is included in Table G-1 below. The list provides DHS required data elements for all invoices as well as individual requirements by a specific type of invoice (i.e. T&M or FFP). Details and format of invoices shall be consistent with structure specified by COTR.

**IT-NOVA
Operations and Maintenance**

Invoice Requirements—Table G-1

All invoices submitted to DHS shall include:	Time and Materials invoices shall (additionally) include:	Firm Fixed Price invoices shall (additionally) include:
<ol style="list-style-type: none"> 1. Vendor Name 2. Invoice Number 3. Invoice Date 4. Date of Service/Equipment Provided 5. Payment/Vendor Address, Telephone Number, Other Contact Information 6. Contract Month 7. Fiscal Year 8. Payment Due Date 9. Contract Number 10. Task Order Number 11. Work Order Number (if applicable) 12. DHS Functional/Budget Code/Accounting Data 13. Cumulative Value to Date 14. Total Amount Invoiced 15. Vendor Point-of-Contact 16. DHS Point-of-Contact 17. Grand Total per Invoice 18. Page Numbers 19. Shipping and payment terms 	<ol style="list-style-type: none"> 1. Labor Categories 2. Contractors Name 3. Number of Hours and FTE Billed 4. Cost per Hour for Each Consultant 5. Cost per Period for Each Labor Category 6. Site Location of Deliverables 7. Contract Line Item Number (CLIN)/ PWS for each Labor Category 8. Description of Equipment 9. Unit Cost of Equipment) 10. Quantity 11. Total Direct Labor Charges 12. Total Other Direct Costs 13. Subtotal per Deliverable 	<ol style="list-style-type: none"> 1. Cost per period 2. Number of Periods 3. Site location of Deliverables 4. Description of Billed Services/Equipment 5. Contract Line Item Number (CLIN)/PWS for each CLIN, if applicable 6. Total Other Direct Costs

IT-NOVA
Operations and Maintenance

G.6.5 Material Order Status Report

A report of all material/labor billed to DHS is required each month to track outstanding equipment in the "field" or residing at DHS HQ. The report shall include a status of the DHS 700-21, a government Point-of-Contact (POC), the equipment delivery location, equipment operational location, cost of each unit, lease duration/useful life, date of acquisition, type of equipment, system capabilities/specifications, and the bureau the equipment is supporting. The data must be provided in an application that is consistent with DHS approved software, preferably Microsoft Excel or Microsoft Access format.

G.7 ELECTRONIC INVOICE SUBMISSION

Electronic invoices must be submitted to:
www.DOB-Invoice@DHS.GOV within thirty (30) days of services rendered.

G.8 TRAVEL AND PER DIEM

(a) Contractor personnel may be required to travel to support the requirements of this task order and as stated in individual tasks/Work Orders. Long distance and local travel will be required in the Continental United States (CONUS). For those work orders requiring travel, the Contractor shall include estimated travel requirements in the price estimate(s). The Contractor shall then coordinate specific travel arrangements with the individual TO COTR to obtain advance, written approval for the travel about to be conducted. The Contractor shall obtain advanced written approval for travel from the COTR prior to making specific travel arrangements. The Contractor's request for travel shall be in writing and contain the dates, locations and estimated costs of the travel. See PWS Section C.1.11.3 – Travel for additional information.

(b) If any travel arrangements cause additional costs to the task/work order that exceed those previously negotiated, written approval by change order issued by the CO is required, prior to undertaking such travel.

(c) The Contractor is expected to have a facility within the Washington, DC metropolitan area. Local travel reimbursement within a 50-mile radius from the contractor's facility or the Contractor's assigned duty station is not authorized. This includes travel, subsistence, and associated labor charges for travel time. Travel performed for personal convenience or daily travel to and from work at the Contractor's

Source Selection Information – See FAR 2.101 and 3.104

Page 24 of 70

**IT-NOVA
Operations and Maintenance**

facility or local Government facility (i.e., designated work site) shall not be reimbursed hereunder. Travel, subsistence, and associated labor charges for travel time for travel beyond a 50-mile radius of the Contractor's facility or assigned duty station are authorized; HOWEVER, all travel outside the Washington, DC metropolitan area must be previously approved by the COTR.

(d) The Contractor shall, to the maximum extent practicable, minimize overall travel costs by taking advantage of discounted airfare rates available through advance purchase. Charges associated with itinerary changes and cancellation under nonrefundable airline tickets are reimbursable as long as the changes are driven by the work requirement. Costs associated with Contractor travel shall be in accordance with FAR Part 31.205-46, Travel Costs and applicable Federal Travel Regulation. No travel will be reimbursed without prior approval from the COTR.

G.9 PURCHASE AGENT AUTHORITY

The Contracting Officer may issue the Contractor a purchase agent authorization to use Government supply sources or other Government-issued contract vehicles in the performance of this task order. Title to all property acquired by the Contractor under such an authorization shall vest in the Government unless otherwise specified in the contract. Such property shall be considered Government Property.

G.10 GOVERNMENT-FURNISHED FACILITIES AND EQUIPMENT

DHS will provide administrative supplies and onsite office facilities for Contractor support personnel, to include, but not limited to, a workspace, workstation, desk, and phone. Dedicated DHS-provided laptops(s) and telephone(s) will be provided for the HQ support personnel. Refer to Section C.3 and C.4 for additional information.

The contractor shall use the Government-furnished facilities and equipment only in connection with this task order.

(END OF SECTION G)

**IT-NOVA
Operations and Maintenance**

SECTION H—SPECIAL TASK ORDER REQUIREMENTS

H.1 GENERAL

The Contractor shall comply with the terms and conditions of the EAGLE contract.

H.2 TYPE OF TASK ORDER

This is a Time and Materials type Task Order as defined in FAR Subpart 16.6.

H.3 SUBCONTRACTING

(a) The subcontracting plan small business subcontracting goals for large businesses under this Task Order are as follows:

Type of Business	Goal % of Total Planned Subcontracting Dollars
Small Business (SB)	40%
Small Disadvantaged Businesses (SDB)	05%
Women-Owned Small Businesses (WOSB)	05%
Service-Disabled Veteran Owned Small Business (SDVOSB)	03%
Veteran-Owned Small Business (included in SDVOSB)	03%
HUBZone	03%

(b) A subcontracting plan is required for this task order as prescribed in FAR 52.219-9 and in accordance with Section L, Instructions herein.

(c) The Contractor may add or delete subcontractors without the express written consent of the Government. Although the Contractor has the ability to add or delete Subcontractors without express written consent of the CO, in accordance with FAR 52.244-2 – Subcontracts, if the Contractor does not have an approved purchasing system, the Contractor shall obtain written contract level Contracting Officer consent prior to subcontracting under a:

Source Selection Information -- See FAR 2.101 and 3.104

Page 26 of 70

IT-NOVA
Operations and Maintenance

- (1) Cost-reimbursement, T&M or labor hour type contract; or
- (2) Firm fixed price contract that exceeds \$75 million.

In such instances, contract level CO approval must be received prior to subcontracting. Any new T&M Subcontractor approved for addition to the task order shall be reimbursed via the labor rates set forth in Section B. No addition or adjustments will be made to account for added Subcontractors.

(d) The subcontracting plan, dated [insert date], in response to the Task Order solicitation, and submitted in accordance with FAR 52.219-9, is hereby approved and incorporated herein.

H.4 FAIR OPPORTUNITY FOR FUTURE TASK ORDER COMPETITION

All EAGLE contractors under the applicable Functional Category will be provided a "Fair Opportunity" to be considered for award of the Task Order (IT-NOVA O&M) resulting from this competition. However, the government reserves the right to issue logical follow-on orders on a sole source basis subject to the Fair Opportunity exceptions to the successful offeror of this competition.

Fair opportunity competitions will be conducted for future task orders unless an exception is allowed in accordance with the Fair Opportunity exceptions under FAR 16.505, Ordering. For task orders with a value expected to exceed \$3,000, the FAR 16.505 statutory exceptions consist of:

- (d) The agency need for the supplies or services is so urgent that providing a fair opportunity would result in unacceptable delays.
- (ii) Only one awardee is capable of providing the supplies or services required at the level of quality required because the supplies or services ordered are unique or highly specialized.
- (iii) The order must be issued on a sole-source basis in the interest of economy and efficiency because it is a logical follow-on to an order already issued under the contract, provided that all awardees were given a fair opportunity to be considered for the original order.
- (iv) It is necessary to place an order to satisfy a minimum guarantee.

IT-NOVA
Operations and Maintenance

H.5 WARRANTY PERIOD

The warranty for all labor and materials furnished by the Contractor under this contract shall be for a period of ninety (90) days or if equipment is involved, the Original Equipment Manufacturer's warranty (OEM), or whichever is greater.

H.6 INTERRELATIONSHIP OF ASSOCIATE CONTRACTORS

DHS may enter into contractual agreements with other contractors (i.e., "Associate Contractors") in order to provide information technology requirements separate from the work to be performed under this task order, yet having links and interfaces to this task order. The Contractor may be required to coordinate with other such contractor(s) through the cognizant CO and/or designated representative in providing suitable, non-conflicting technical and/or management interfaces and in avoidance of duplication of effort. Information on deliverables provided under separate contracts/task orders may, at the discretion of the DHS and/or other Government agencies, be provided to such other contractor(s) for the purpose of such work.

Where the contractor and an associate contractor fail to agree upon action to be taken in connection with their respective responsibilities, the contractor shall notify the COTR in writing of unresolved disputes in receiving support from or providing support to customers or other third party contractors within two business days from the time the dispute occurs, unless otherwise specified in Section C. The contractor shall not be relieved of its obligations to make timely deliveries or be entitled to any other adjustment because of failure of the contractor and its associate to promptly refer matters to the CO or because of failure to implement CO directions.

Compliance with this Special Contract Requirement is included in the task order price and shall not be a basis for equitable adjustment. Refer to Section C.1.8 for additional information.

H.7 NON-PERSONAL SERVICES

In accordance with FAR Subpart 7.5, Inherently Governmental Functions, no personal services shall be performed under this task order. No Contractor employee will be directly supervised by a Government employee. All individual contractor employee assignments, and daily work direction, shall be given by the applicable employee supervisor. If the Contractor believes any Government action or

Source Selection Information – See FAR 2.101 and 3.104

Page 28 of 70

IT-NOVA
Operations and Maintenance

communication has been given that would create a personal services relationship between the Government and any Contractor employee, the Contractor shall promptly notify the Contracting Officer of this communication or action.

The Contractor shall not perform any inherently governmental actions as defined by FAR Subpart 7.5. No Contractor employee shall hold him or herself out to be a Government employee, agent, or representative. No Contractor employee shall state orally or in writing at any time that he or she is acting on behalf of the Government. In all communications with third parties in connection with this task order, Contractor employees shall identify themselves as Contractor employees and specify the name of the company for which they work. In all communications with other Government contractors in connection with this task order, the Contractor employee shall state that they have no authority to in any way change the task order and that if the other contractor believes this communication to be a direction to change their task order, they should notify the Contracting Officer for the task order and not carry out the direction until a clarification has been issued by the Contracting Officer.

The Contractor shall ensure that all of its employees working on this task order are informed of the substance of this clause. Nothing in this clause shall limit the Government's rights in any way under any other provision of the task order, including those related to the Government's right to inspect and accept the services to be performed under this task order. The substance of this clause shall be included in all subcontracts at any tier.

H.8 · QUALIFICATIONS OF EMPLOYEES

The Contracting Officer may require dismissal from work of those employees which he/she deems incompetent, careless, insubordinate, unsuitable or otherwise objectionable, or whose continued employment he/she deems contrary to the public interest or inconsistent with the best interest of national security. The Contractor shall fill out, and cause each of its employees on the task order work to fill out, for submission to the Government, such forms as may be necessary for security or other reasons. Upon request of the Contracting Officer, the Contractor's employees shall be fingerprinted. Each employee of the Contractor shall be a citizen of the United States of America. Refer to Section C.1.7 for additional information.

IT-NOVA
Operations and Maintenance

H.9 PERSONNEL ACCESS

All Contractor personnel requiring access to the Government's sites will be subject to the security clearance procedures set forth in Attachment J-3, Implementing Instructions for Compliance with HSAR clause 3052.204-71, "Contractor Employee Access" and Section C of this Task Order.

H.10 NON-DISCLOSURE AGREEMENTS

Non-Disclosure Agreements are required to be signed by all Contractor personnel when their role requires them to come into contact with Government procurement sensitive information, other sensitive information, or proprietary business information from other contractors (e.g., cost data, plans, and strategies). The recipient certifies in writing that they will take the necessary steps to prevent the unauthorized disclosure and use of information. The Contractor shall maintain the file of the signed Non-Disclosure Agreements which will be made available to the Government upon request. Please refer to Section J, Attachment J-6, Non-Disclosure Agreement.

H.11 DHS REQUIREMENTS AND DUTIES FOR HANDLING SENSITIVE SECURITY INFORMATION (SSI)

Requirements for Safeguarding and Control of SSI—For purposes of this Contract, all information that the DHS provides or causes to be provided to the Contractor as SSI in connection with its duties under this contract shall be covered by DHS policies and procedures for safeguarding and control of SSI until DHS specifically authorizes the Contractor in writing to treat any such information as public. This requirement shall be applicable to all subcontracting on the contract.

Definition of Confidential Information—In addition to the SSI defined by DHS, SSI on this contract shall also include: (1) any specifications, know-how, strategies or technical data, processes, business documents or information, marketing research and other data, customer or client lists, or sources of information which are owned, used or possessed exclusively by or for the benefit of the DHS and based on SSI; (2) SSI-derived work product(s); (3) all SSI obtained by the Contractor from a third party in connection with performance under this contract.

Duty to Maintain SSI—Except as required by any law, court order, subpoena, or by the DHS, or as required to perform Contractor's duties under this Contract, neither Contractor nor its related entities shall disclose SSI to anyone without a valid need to

**IT-NOVA
Operations and Maintenance**

know, nor shall they use or allow the use of SSI to further any private interest other than those within the scope of this Contract. The Contractor shall immediately notify the DHS Contracting Officer in writing of any subpoena or court order requiring disclosure of SSI.

H.12 DHS DATA PROTECTED BY THE PRIVACY ACT

Data collected under this task order that pertains to individuals will belong solely to the Government and the Contractor shall have no property rights to this data whatsoever. In addition, information pertaining to individuals gathered under any resulting contract shall only be disclosed in accordance with the terms of the Privacy Act, 5 U.S.C.552a.

H.13 ORDER OF PRECEDENCE

This Task Order incorporates by reference EAGLE contract clauses under (c) Contract Clauses below. The Contractor's proposal dated [TBD] is hereby incorporated into the task order as Attachment [x] to Section J. Any inconsistency in this task order with the Government's requirements and the Contractor's proposal and EAGLE contract clauses shall be resolved by giving precedence in the following order:

ORDER OF PRECEDENCE—UNIFORM CONTRACT FORMAT (OCT 1997)

Any inconsistency in this solicitation or contract shall be resolved by giving precedence in the following order:

- (a) The Schedule (excluding the specifications).
- (b) Representations and other instructions.
- (c) Contract clauses.
- (d) Other documents, exhibits, and attachments.
- (e) The specifications.

(END OF SECTION H)

IT-NOVA
Operations and Maintenance

PART II – TASK ORDER CLAUSES

SECTION I – TASK ORDER CLAUSES

I.1 FAR CLAUSES INCORPORATED BY REFERENCE

This RFP or Task Order, as applicable, incorporates by reference one or more provisions or clauses from the EAGLE contract sections H and I, with the same force and effect as if they were restated in this task order. Upon request, the TO Contracting officer will make their full text available. Also, the full text can be accessed electronically at this internet address: <http://www.arnet.gov>.

I.2 HSAR CLAUSES INCORPORATED BY REFERENCE

This RFP or task order, as applicable, incorporates by reference one or more provisions or clauses listed below with the same force and effect as if they were given in full text. The full text may be accessed electronically at the Internet address: <http://www.farsite.hill.af.mil/HSAR>.

HSAR Clause No.	Title	Date
3052.204-70	Security	DEC 2003
3025.209-72	Organizational Conflicts of Interest	JUN 2006
3052.222-71	Strikes or Picketing Affecting Access to a DHS Facility	DEC 2003
3052.223-70	Removal or Disposal of Hazardous Substance-Applicable Licenses and Permits	JUN 2006
3052.228-70	Insurance	DEC 2003
3052.242-71	Dissemination of Contract Information	DEC 2003
3052.242-72	Contracting Officer's Technical Representative	DEC 2003
3052.245-70	Government Property Reports	JUN 2006

I.3 52.204-2 Security Requirements (Aug 1996)

- (a) This clause applies to the extent that this contract involves access to information classified "Confidential," "Secret," or "Top Secret."
- (b) The Contractor shall comply with—

**IT-NOVA
Operations and Maintenance**

- (1) The Security Agreement (DD Form 441), including the *National Industrial Security Program Operating Manual* (DOD 5220.22-M); and
- (2) Any revisions to that manual, notice of which has been furnished to the Contractor.

(c) If, subsequent to the date of this contract, the security classification or security requirements under this contract are changed by the Government and if the changes cause an increase or decrease in security costs or otherwise affect any other term or condition of this contract, the contract shall be subject to an equitable adjustment as if the changes were directed under the Changes clause of this contract.

(d) The Contractor agrees to insert terms that conform substantially to the language of this clause, including this paragraph (d) but excluding any reference to the Changes clause of this contract, in all subcontracts under this contract that involve access to classified information.

I.4 52.204-9 Personal Identity Verification of Contractor Personnel (Nov 2006)

(a) The Contractor shall comply with agency personal identity verification procedures identified in the contract that implement Homeland Security Presidential Directive-12 (HSPD-12), Office of Management and Budget (OMB) guidance M-05-24, as amended, and Federal Information Processing Standards Publication (FIPS PUB) Number 201, as amended.

(b) The Contractor shall insert this clause in all subcontracts when the subcontractor is required to have routine physical access to a Federally-controlled facility and/or routine access to a Federally-controlled information system.

(End of clause)

I.5 CONTINUITY OF SERVICES (FAR 52.237-3) (JAN 1991)

(a) The Contractor recognizes that the services under this contract are vital to the Government and must be continued without interruption and that, upon contract expiration, a successor, either the Government or another contractor, may continue them. The Contractor agrees to—

- (1) Furnish phase-in training; and
- (2) Exercise its best efforts and cooperation to effect an orderly and efficient transition to a successor.

IT-NOVA
Operations and Maintenance

(b) The Contractor shall, upon the Contracting Officer's written notice, (1) furnish phase-in, phase-out services for up to 90 days after this contract expires and (2) negotiate in good faith a plan with a successor to determine the nature and extent of phase-in, phase-out services required. The plan shall specify a training program and a date for transferring responsibilities for each division of work described in the plan, and shall be subject to the Contracting Officer's approval. The Contractor shall provide sufficient experienced personnel during the phase-in, phase-out period to ensure that the services called for by this contract are maintained at the required level of proficiency.

(c) The Contractor shall allow as many personnel as practicable to remain on the job to help the successor maintain the continuity and consistency of the services required by this contract. The Contractor also shall disclose necessary personnel records and allow the successor to conduct on-site interviews with these employees. If selected employees are agreeable to the change, the Contractor shall release them at a mutually agreeable date and negotiate transfer of their earned fringe benefits to the successor.

(d) The Contractor shall be reimbursed for all reasonable phase-in, phase-out costs (*i.e.*, costs incurred within the agreed period after contract expiration that result from phase-in, phase-out operations) and a fee (profit) not to exceed a pro rata portion of the fee (profit) under this contract.

I.6 OFFICIALS NOT TO BENEFIT

No member of or delegate to Congress, or resident commissioner, shall be admitted to any share or part of this contract, or to any benefit arising from it. However, this clause does not apply to this contract to the extent that this contract is made with a corporation for the corporation's general benefit.

I.7 WHISTLEBLOWER PROTECTION FOR CONTRACTOR EMPLOYEES

The contractor agrees not to discharge, demote or otherwise discriminate against an employee as a reprisal for disclosing information to a Member of Congress, or an authorized official of an agency or of the Department of Justice, relating to a violation of law related to this contract (including the competition for or negotiation of a contract). Definitions: (1) "Authorized official of the agency" means an employee responsible for contracting, program management, audit, inspection, investigation, or enforcement of any law or regulation relating to DHS procurement or the subject matter of the contract. (2) "Authorized official of the Department of Justice" means any person responsible for the investigation, enforcement, or prosecution of any law or regulation.

IT-NOVA
Operations and Maintenance

I.8 NOTICE OF DELAY

If the Contractor becomes unable to complete the task order work at the time(s) specified because of technical difficulties, notwithstanding the exercise of good faith and diligent efforts in the performance of the work called for hereunder, the Contractor shall give the Contracting Officer written notice of the anticipated delay and the reasons therefore. Such notice and reasons shall be delivered promptly after the condition creating the anticipated delay becomes known to the Contractor, but in no event less than forty-five (45) days before the completion date specified in this task order, unless otherwise directed by the Contracting Officer. When the notice is required, the Contracting Officer may extend the time specified in the Schedule for the period determined in the best interest of the Government.

I.9 STOP WORK (FAR 52.242-15) (AUG 1989)

(a) The Contracting Officer may, at any time, by written order to the Contractor, require the Contractor to stop all, or any part, of the work called for by this contract for a period of 90 days after the order is delivered to the Contractor, and for any further period to which the parties may agree. The order shall be specifically identified as a stop-work order issued under this clause. Upon receipt of the order, the Contractor shall immediately comply with its terms and take all reasonable steps to minimize the incurrence of costs allocable to the work covered by the order during the period of work stoppage. Within a period of 90 days after a stop-work is delivered to the Contractor, or within any extension of that period to which the parties shall have agreed, the Contracting Officer shall either—

(1) Cancel the stop-work order; or

(2) Terminate the work covered by the order as provided in the Default, or the Termination for Convenience of the Government, clause of this contract.

(b) If a stop-work order issued under this clause is canceled or the period of the order or any extension thereof expires, the Contractor shall resume work. The Contracting Officer shall make an equitable adjustment in the delivery schedule or contract price, or both, and the contract shall be modified, in writing, accordingly, if—

(1) The stop-work order results in an increase in the time required for, or in the Contractor's cost properly allocable to, the performance of any part of this contract; and

(2) The Contractor asserts its right to the adjustment within 30 days after the end of the period of work stoppage; provided, that, if the Contracting Officer decides the facts justify the action, the Contracting Officer may receive and act upon the claim submitted at any time before final payment under this contract.

IT-NOVA
Operations and Maintenance

(c) If a stop-work order is not canceled and the work covered by the order is terminated for the convenience of the Government, the Contracting Officer shall allow reasonable costs resulting from the stop-work order in arriving at the termination settlement.

(d) If a stop-work order is not canceled and the work covered by the order is terminated for default, the Contracting Officer shall allow, by equitable adjustment or otherwise, reasonable costs resulting from the stop-work order.

I.10 SENSITIVE UNCLASSIFIED INFORMATION

(a) Sensitive information shall be restricted to specific contractors who:

- (1) Have a need to know to perform contract tasks;
- (2) Meet personnel suitability security requirements to access sensitive information; and
- (3) Successfully complete a non-disclosure agreement (NDA).

(b) The contractor shall develop and implement procedures to ensure that sensitive information is handled in accordance with DHS requirements and at a minimum, will address:

- (1) Steps to minimize risk of access by unauthorized persons during business and non-business hours to include storage capability;
- (2) Procedures for safeguarding during electronic transmission (voice, data, fax) mailing or hand carrying;
- (3) Procedures for protecting against co-mingling of information with general contractor data system/files;
- (4) Procedures for marking documents with both the protective marking and the distribution limitation statement as needed;
- (5) Procedures for the reproduction of subject material;
- (6) Procedures for reporting unauthorized access; and
- (7) Procedures for the destruction and/or sanitization of such material.

Source Selection Information -- See FAR 2.101 and 3.104

Page 36 of 70

**IT-NOVA
Operations and Maintenance**

**I.11 ORGANIZATIONAL CONFLICT OF INTEREST (HSAR 3052.209-72)
(JUN 2006)**

(a) Determination. The Government has determined that this effort may result in an actual or potential conflict of interest, or may provide one or more offerors with the potential to attain an unfair competitive advantage. The nature of the conflict of interest and the limitation on future contracting:

The contractor, under the terms of this task order, or through the performance of the Performance Work Statement/Section C made a part of this task order, is neither obligated nor expected to deliver or provide material or perform work, which will place the contractor in an organizational conflict of interest, which could serve as a basis for excluding the contractor from supplying products or services to the Department of Homeland Security. Further, during the course of this task order, the Contracting Officer will not knowingly unilaterally direct the contractor to perform work, in contravention of the above understanding. The contractor is required to provide information regarding any situation in which the potential for an organizational conflict of interest exists. However, if the Contracting Officer discerns the potential for an organizational conflict of interest prior to the execution of any task or amendment thereto, the Contracting Officer shall notify the contractor per FAR 9.5, and the parties shall mutually take action to resolve any potential organizational conflict of interest. For the purposes of this clause, an organizational conflict of interest is understood to include tasking which involves the preparation of a complete specification of materials leading directly and predictably to competitive procurement of a system.

(b) If any such conflict of interest is found to exist, the Contracting Officer may (1) disqualify the offeror, or (2) determine that it is otherwise in the best interest of the United States to contract with the offeror and include the appropriate provisions to avoid, neutralize, mitigate, or waive such conflict in the contract awarded. After discussion with the offeror, the Contracting Officer may determine that the actual conflict cannot be avoided, neutralized, mitigated or otherwise resolved to the satisfaction of the Government, and the offeror may be found ineligible for award.

(c) Disclosure: The offeror hereby represents, to the best of its knowledge that:

___ (1) It is not aware of any facts which create any actual or potential organizational conflicts of interest relating to the award of this contract, or

IT-NOVA
Operations and Maintenance

___ (2) It has included information in its proposal, providing all current information bearing on the existence of any actual or potential organizational conflicts of interest, and has included a mitigation plan in accordance with paragraph (d) of this provision.

(d) Mitigation. If an offeror with a potential or actual conflict of interest or unfair competitive advantage believes the conflict can be avoided, neutralized, or mitigated, the offeror shall submit a mitigation plan to the Government for review. Award of a contract where an actual or potential conflict of interest exists shall not occur before Government approval of the mitigation plan. If a mitigation plan is approved, the restrictions of this provision do not apply to the extent defined in the mitigation plan.

(e) Other Relevant Information: In addition to the mitigation plan, the Contracting Officer may require further relevant information from the offeror. The Contracting Officer will use all information submitted by the offeror, and any other relevant information known to DHS, to determine whether an award to the offeror may take place, and whether the mitigation plan adequately neutralizes or mitigates the conflict.

(f) Corporation Change. The successful offeror shall inform the Contracting Officer within thirty (30) calendar days of the effective date of any corporate mergers, acquisitions, and/or dive stures that may affect this provision.

(g) Flow-down. The contractor shall insert the substance of this clause in each first tier subcontract that exceeds the simplified acquisition threshold.

(End of provision)

I.12 KEY PERSONNEL OR FACILITIES (HSAR 3052.215-70) (DEC 2003)

(a) The personnel or facilities specified below are considered essential to the work being performed under this contract and may, with the consent of the contracting parties, be changed from time to time during the course of the contract by adding or deleting personnel or facilities, as appropriate.

(b) Before removing or replacing any of the specified individuals or facilities, the Contractor shall notify the Contracting Officer, in writing, before the change becomes effective. The Contractor shall submit sufficient information to support the proposed action and to enable the Contracting Officer to evaluate the potential impact of the change on this contract. The Contractor shall not remove or replace personnel or facilities until the Contracting Officer approves the change.

The Key Personnel or Facilities under this Contract:

Source Selection Information – See FAR 2.101 and 3.104

Page 38 of 70

IT-NOVA
Operations and Maintenance

Refer to Section C, Technical Exhibit 1.7-001 for Key Personnel Listing.

I.11.1 All substitutes must have at least equal qualifications to those of the individual being replaced.

I.13.2 All appointments of key personnel shall be approved by the Contracting Officer, and no substitutions of such personnel shall be made without the advance written approval of the Contracting Officer.

I.11.3 Except as provided otherwise in this clause, at least thirty (30) days (sixty (60) days if security clearance is required) in advance of the proposed substitution, all proposed substitutions of key management personnel must be submitted in writing to the Contracting Officer, including the information required otherwise in this provision.

I.11.4 Where individuals proposed as key management personnel become unavailable between the submission of the final proposal revisions and contract award, within five (5) days following task order award, the Contractor shall notify the Contracting Officer in writing of such unavailability and who will be performing, if required, as the temporary substitute. Within fifteen (15) days following task order award, the Contractor shall submit in writing to the Contracting Officer proposed substitutions for the unavailable individuals.

I.11.5 Request for substitution of key management personnel must provide a detailed explanation of the circumstances necessitating substitution, a resume of the proposed substitute, and any other information requested by the Contracting Officer to make a determination as to the appropriateness of the proposed substitute's qualifications. All resumes shall be signed by the proposed substitute and his/her formal direct supervisor or higher authority.

I.11.6 The Contracting Officer shall promptly notify the Contractor in writing of his/her approval or disapproval of all requests for substitution of key management personnel. All disapprovals will require resubmission of another substitution by the Contractor within fifteen (15) days.

I.13 AVAILABILITY OF FUNDS (FAR 52.232-18) (APR 1984)

Funds are not presently available for portions of this contract. The Government's obligation under this contract is contingent upon the availability of appropriated funds

IT-NOVA
Operations and Maintenance

from which payment for contract purposes can be made. No legal liability on the part of the Government for any payment may arise until funds are made available to the Contracting Officer for this task order and until the Contractor receives notice of such availability, to be confirmed in writing by the Contracting Officer.

**I.14 3052.242-71 DISSEMINATION OF CONTRACT INFORMATION
(DEC 2003)**

The Contractor shall not publish, permit to be published, or distribute for public consumption, any information, oral or written, concerning the results or conclusions made pursuant to the performance of this contract, without the prior written consent of the Contracting Officer. An electronic or printed copy of any material proposed to be published or distributed shall be submitted to the Contracting Officer.

(End of clause)

(END OF SECTION I)

**IT-NOVA
Operations and Maintenance**

**PART II – PART III – LIST OF DOCUMENTS, EXHIBITS AND OTHER
ATTACHMENTS**

SECTION J – LIST OF ATTACHMENTS

The following attachments are available as shown in the table below:

Attachment Number	Title
Attachment J-1	Performance Work Statement
Attachment J-2	DHS Form 700-21
Attachment J-3	Implementing Instructions for Compliance with HSAR Clause 3052.204-71, "Contractor Employee Access"
Attachment J-4	DHS Form 11000-6 – Non-Disclosure
Attachment J-5	Pricing Model
Attachment J-6	DD Form 254 Contract Security Classification Specification
Attachment J-6A	DHS HSDN – Security Classification Guide
Attachment J-6B	DHS – National Security IT Systems Certification and Accreditation Security Classification Guide

IT-NOVA
Operations and Maintenance

PART IV – REPRESENTATIONS AND INSTRUCTIONS

**SECTION K – REPRESENTATIONS, CERTIFICATIONS AND OTHER STATEMENTS
OF OFFERORS**

K.1 REPRESENTATION – RELEASE OF CONTRACT INFORMATION

This Task Order incorporates the representation from the original proposal submitted by the Contractor in accordance with EAGLE contract.

IT-NOVA
Operations and Maintenance
SECTION L
INSTRUCTIONS, CONDITIONS AND NOTICES TO OFFERORS

L.1 TYPE OF AWARD

This task order competition will be conducted consistent with FAR Part 16.5 and the Government contemplates award of two (2) time and materials (T&M) type task orders from this solicitation.

The offeror shall submit a price proposal by completing the CLIN structure/ pricing model provided in Section B with the hourly labor (T&M) rates and Other Direct Costs (ODC) markup percentages provided in its EAGLE contract. The offeror may propose an alternative price proposal in addition to the price proposal required above.

L.2 SOLICITATION AMENDMENTS

Any Amendments or other information issued by the Department will be made available via FedConnect.

L.3 DUE DILIGENCE/EXCHANGES OF INFORMATION

(a) The Government intends to conduct a due diligence process to allow the successful offerors from the down-selection competition to survey the unclassified DHS locations and exchange information with DHS Office of the Chief Information Officer (OCIO) technical representatives. This process will allow the offerors to gain a better understanding of the DHS mission objectives, operations and existing conditions. These exchanges will also significantly increase the likelihood that the offerors will submit superior solutions. Exchanges will occur prior to the receipt of proposals. A major objective of this due diligence process is to provide each offeror and/or teaming partners one-on-one sessions with the OCIO and Task Order Contracting Officer (TOCO) and the ability to ask questions which will be treated as proprietary/confidential and will not be released or made available to their competitors.

(b) Requests for clarification that result in specific information necessary to submit proposals will be provided to all offerors. The Government will provide competing contractors equal access to data and information. However, the Government assumes no responsibility for any representation made by any of its officers or agents during due diligence. Contractor questions and Government responses furnished during due diligence are unofficial.

Source Selection Information – See FAR 2.101 and 3.104
Page 43 of 70

IT-NOVA
Operations and Maintenance
SECTION L
INSTRUCTIONS, CONDITIONS AND NOTICES TO OFFERORS

L.4 GENERAL INSTRUCTIONS

(a) RFP and Section C - PWS Compliance

The offeror shall ensure that technical and price proposals meet all requirements in the Request for Proposal and Section C, Performance Work Statement (PWS), i.e., instructions, terms and conditions, representations and certifications, performance and/or data requirements, etc. in addition to those items identified as evaluation factors and subfactors to be eligible for award. Any exceptions to the solicitation's terms and conditions must be fully explained and justified. Additionally, the proposal shall be clear, concise, and shall include sufficient detail for effective evaluation and for substantiating the validity of stated claims. Elaborate brochures or documentation, binding, detailed artwork, or other embellishments are unnecessary and are not desired.

The Government will award a separate six month task order for Transition Ramp-Up. The Transition Ramp-Up shall be priced separately in Volume 3, Price Proposal. Due to the number of contracts being transitioned over a 12 month period, the Government anticipates a subset of the Transition Ramp-Up tasks may be accomplished during both the transition ramp-up and the base year of the Task Order award.

All Offerors must comply with the "Instructions for Compliance with HSAR clause 3052.204-71, "Contractor Employee Access" provided as attachment J-3.

(b) Point of Contact

The TOCO is the **sole** point of contact for this acquisition. Address any questions or concerns you may have to the TOCO. Requests for clarification may be provided to the TOCO during the due diligence phase of this acquisition.

(c) Proposal Acceptance and Validity Dates

Proposal due date is specified in block 9 of the Standard Form 33, Solicitation, Offer and Award. Proposal Validity: The offeror agrees to hold its prices in its offer firm for at least 120 calendar days from the date specified for receipt of offers. The offeror shall make a clear statement in the proposal Volume III that the proposal is valid for no less than 120 calendar days from the date of its offer.

IT-NOVA
Operations and Maintenance
SECTION L
INSTRUCTIONS, CONDITIONS AND NOTICES TO OFFERORS

L.5 GENERAL INFORMATION

(a) Debriefings

If a non-selected offeror has questions as to why it was not selected for task order award, the offeror should contact the TOCO. The TOCO and non-selected offeror may discuss the reasons why that offeror was not selected, however, the TOCO may not (1) discuss other contractors' proposals, (2) compare contractors' proposals, or (3) allow the non-selected offeror access to the award decision documentation.

(b) Protests

In accordance with FAR Part 16.505 (a)(9), no protests are authorized in connection with the issuance or proposed issuance of a task order, except for protest on grounds that the order increases the scope, period, or maximum value of the contract. However, under FAR 16.505(b)(4), prime contractors may contact the customer-designated contract ombudsman with complaints on specific task orders on this contract. The designated DHS ombudsman for this contract is:

Acting Director, Office of Procurement Policy and Oversight
Department of Homeland Security
Office of the Chief Procurement Officer
245 Murray Lane, Bldg 410
Washington, DC 20528
(202) 447-5594

(c) Discrepancies

If an offeror believes that the requirements in these instructions contain an error, or omission, the offeror shall immediately notify the TOCO in writing with supporting rationale.

(d) IT-NOVA Reference Library

An IT-NOVA Reference Library will be made available to all prospective offerors that will provide select documents that were referenced but not available in the RFP. These documents will be made available via DHS Interactive, an agency intranet web site. Only one individual from each EAGLE prime contractor will be

Source Selection Information – See FAR 2.101 and 3.104

Page 45 of 70

IT-NOVA
Operations and Maintenance
SECTION L
INSTRUCTIONS, CONDITIONS AND NOTICES TO OFFERORS

provided access to this web site to review the select RFP information. The Prime EAGLE contractor must provide the TOCO the name and Social Security Number of the person designated by their organization to access the RFP online technical exhibits and documents. The designated person must possess an active suitability security clearance to be considered for access to the DHS interactive web site and prior to an account assignment by DHS.

L.6 ORGANIZATION/PROPOSAL FORMAT/PAGE LIMITS

Offerors shall submit proposals as set forth in the Proposal Organization Table below. The titles and contents of the volumes shall be defined in this table, all of which shall be within the required page limits indicated in the table below. The contents of each proposal volume are described in these instructions. Volumes I and II may be combined into one document but Volume III (Small Business Subcontracting Plan and Price Proposal) **must** be a submitted in a separate document. The Offeror shall submit a written hard copy of its Price Proposal and submit an electronic copy in MS Excel. Excel® files submitted by the Offeror shall include the formatting as provided in the sample model shown in Section B. The cells within the submitted files should contain all necessary functional formulas necessary for the Government to evaluate completeness, reasonableness, and realism. Volume IV, Oral Presentation slides shall be provided to the government on the date scheduled for presentation.

**IT-NOVA
Operations and Maintenance
SECTION L
INSTRUCTIONS, CONDITIONS AND NOTICES TO OFFERORS**

PROPOSAL VOLUME	SECTIONS	FORMAT	COPIES	PAGE LIMIT
I: Technical Proposal	Section 1: Executive Summary Section 2: Technical Capability	MS Word and MS PowerPoint	Electronic Submission via FedConnect	50 pages plus 25 slides Executive Summary shall not exceed 10 pages and will not be included in page count
II: Management Proposal	Section 1: Management Approach	MS Word and MS PowerPoint	Electronic Submission via FedConnect	100 pages plus 35 slides
II: Management Proposal	Section 2: Staffing Approach Section 3: (a) Overall Transition Plan (b) Transition Ramp-Up	MS Word and MS PowerPoint	Electronic Submission via FedConnect; 2 page limit per key personnel resume	Page Limit included in Management Approach (not to exceed 100 pages and 35 slides for both Management and Staffing Approach); Resumes and Section 3- Transition Plan (a) and (b) not included in page count
III: Price Proposal	Section 1: Exceptions and Deviations Section 2: Contract Documents (Small Business Subcontracting Plan for Large Businesses) Section 3: CLIN Rate Table and Hourly Labor Rates	MS Word and MS Excel 2003	Electronic Submission via FedConnect	No page limit MS Word and MS Excel Worksheets
IV: Oral Presentation	Volume 4 – Oral Presentation Slides	MS PowerPoint	15 copies submitted to DHS at Oral Presentation session	60 Slides Hard copy and electronic copy in MS PowerPoint in compliance with Volumes I and II above

Table L.6.1

- a) An official authorized to bind your organization must sign the proposal.
- b) Paper size shall be 8.5" by 11.0", except if the pricing and/or WBS spreadsheet pages required landscape printing on 8.5" by 14.0" paper.

Source Selection Information – See FAR 2.101 and 3.104

IT-NOVA
Operations and Maintenance
SECTION L
INSTRUCTIONS, CONDITIONS AND NOTICES TO OFFERORS

c) All page limitations are based on single sided pages, 8.5 X 11 inch paper, single spaced, Arial or Times New Roman typeface no smaller than 12-point (smaller fonts are acceptable for graphics, figures, tables, footnotes and legends), and "1 inch margins.

d) Proposals shall be received via FedConnect no later than (Time TBD) local time (Washington, DC) on (Date TBD). (Please note: The Government will not accept proposals sent by mail or fax.)

L.7 PROPOSAL CONTENT

L.7.1 VOLUME 1 - TECHNICAL PROPOSAL (50 pages plus 25 slides for Volumes 1, Section 1)

COVER LETTER, TABLE OF CONTENTS, AND STANDARD FORM-33 (SF-33) (not included in page count)

Volume 1 will consist of the completed and signed SF-33 with a cover letter delineating any exceptions taken to the RFP terms and conditions. However, offerors are cautioned that any noncompliance with the terms and conditions of the RFP may cause their proposal to be determined unacceptable. A Table of Contents may also be included to facilitate review and evaluation of the proposal content.

L.7.1(a) SECTION 1 - EXECUTIVE SUMMARY (10 pages, not included in page count)

The offeror shall provide a concise summary of the entire proposal, including significant approach tradeoffs and risks, and highlight any key or unique features, excluding cost/price. Any summary material presented here shall not be considered as meeting the requirements for any portions of other sections or volumes of the proposal.

NOTE: The evaluators will not take any information contained in the Executive Summary into consideration in the evaluation of any of the evaluation factors. Offerors should ensure that all information required for the evaluation of factors and sub factors in Section M are contained within other sections or volumes of the proposal.

The offeror shall fill out a Cross Reference Matrix (CRM) indicating where the proposal addresses the solicitation requirements. An example format is shown below. The

Source Selection Information – See FAR 2.101 and 3.104

Page 48 of 70

**IT-NOVA
Operations and Maintenance
SECTION L
INSTRUCTIONS, CONDITIONS AND NOTICES TO OFFERORS**

purpose of the CRM is to show critical interrelationships and dependencies among the documents. The matrix ensures that all requirements are addressed, requirements do not conflict and proposal sections are internally consistent.

Example Format:

SOLICITATION CROSS REFERENCE MATRIX	
Solicitation Section/Paragraph	Proposal Volume/Section/Paragraph
Solicitation Section/Paragraph	Proposal Volume/Section/Paragraph
Solicitation Section/Paragraph	Proposal Volume/Section/Paragraph

L.7.1(b) SECTION 2 – TECHNICAL CAPABILITY (50 pages, 25 slides, Technical Proposal) (Non-Price Factor 1)

The offeror shall sufficiently describe its technical understanding and approach to performing all technical objectives as delineated in Section C, Performance Work Statement (PWS) in its written proposal and oral presentation under this task order. The following items shall be addressed:

- a) Non-Price Factor 1 – Technical Capability has three subfactors, as follows:
 Subfactor 1: Understanding of Requirements;
 Subfactor 2: Integrator Expertise; and
 Subfactor 3: Implementation.

Subfactor 1: Understanding of Requirements: The offeror shall demonstrate an understanding of the Section C/PWS requirements and inherent complexity in meeting all the technical objectives of this procurement. The offeror must provide a comprehensive summary and narrative identifying how the full range of services in the task order PWS (Section C) shall be provided. The offeror shall also demonstrate an understanding of the services required in the PWS and its relationship to achieving the mission of the agency.

Subfactor 2: Integrator Expertise: Offeror shall demonstrate its capability to integrate separate IT service requirements into a consolidated effort, resulting in advantages such as reductions in project overlaps, realized economies of scale, improved efficiency and service delivery, standardized support services, increased customer satisfaction, and meeting or exceeding industry standards.

IT-NOVA
Operations and Maintenance
SECTION L
INSTRUCTIONS, CONDITIONS AND NOTICES TO OFFERORS

Subfactor 3: Implementation: Offeror must provide an implementation approach that encompasses the anticipated logical sequence of tasks, methodology, techniques, and any other areas of consideration the offeror deems necessary to implement/execute Section C/PWS requirements and related deliverables.

L.7.2 VOLUME 2 - MANAGEMENT PROPOSAL (100 pages plus 35 slides)

The offeror shall describe its management approach to include management structure and division of responsibility to control the full range of support services to be provided under this task order in its written proposal and oral presentation. The management approach shall specifically address all aspects of program and performance management, including plans to manage deployment, transition, cost controls, governance structure, teaming arrangements/subcontractors, change and risk management, management tools, reporting systems, quality assurance, and performance metrics. Key management personnel shall be identified by position, skill type, overall qualifications and experience. The following items shall be addressed:

L.7.2(a) SECTION 1 – MANAGEMENT APPROACH (Non-Price Factor 2)

- a) Non-Price Factor 2 – Management Approach
 - Subfactor 1: Organization;
 - Subfactor 2: Management Methodology;
 - Subfactor 3: Transition Plan and Transition Ramp-Up; and
 - Subfactor 4: Quality Control

Subfactor 1: Organization. The offeror's proposed organizational approach delineates a coordinated, flexible and efficient workflow management and provides an organizational control and communication plan to accomplish the requirements in Section C including clearly defined roles, responsibilities and direct lines of control and communication; Project Manager's responsibility and authority to effectively control, monitor and manage the project.

Subfactor 2: Management Methodology. Proposed methodology demonstrates proficiency in managing multiple IT services/requirements and meeting performance metrics under this task order and how the selected approach will

IT-NOVA
Operations and Maintenance
SECTION L
INSTRUCTIONS, CONDITIONS AND NOTICES TO OFFERORS

generate efficient services and increase customer satisfaction; plan to collect, analyze and maintain workload data per Section C.1.6.

Subfactor 3: Transition Plan and Transition Ramp-Up. Section 3 of the Management Plan shall be divided into two sections - A: Overall Transition Plan and B: Transition Ramp-up.

Section 3A: Overall Transition Plan shall provide a comprehensive transition plan that minimizes impacts on continuity of operations and identifies key issues and overcomes barriers to transition; plan shall establish feasible and timely transition schedule, milestones, measurable commitments, and estimated costs for transition (include in Price Proposal) and other tasks necessary to conduct and complete the transition during the designated time period.

Section 3b: Transition Ramp-up shall address PWS Section C.1.12.1.1.3 Transition Ramp-up. The Transition Ramp-Up Plan shall identify critical tasks and implementation strategies for expediently vetting and obtaining employees for security clearances, employee recruiting and/or staffing for required positions, conducting joint inventory of GFP and assets, establishing management processes and controls and other tasks the offeror deems necessary to initiate pre-transition and transition activities within the first six (6) months of task order award.

Subfactor 4: Quality Control. Quality Control Plan to meet Section C/PWS requirements to ensure quality in the delivery of services from the transition of current contracts throughout the entire contract period of performance; plans must demonstrate proficiency, efficiency and cost effectiveness.

L.7.2(b) SECTION 2 – STAFFING APPROACH (Non-Price Factor 3)

The staffing approach shall describe the offeror's proposed processes, procedures and controls to recruit, train, and retain a qualified/certified workforce including key personnel capable of supporting the scope of Section C/PWS as well as contingency plans to meet surge /emergency requirements and/or unforeseen personnel shortages in its written proposal and oral presentation. The offeror shall also describe its approach to obtaining personnel with the appropriate security clearances and the vetting process of proposed employees to facilitate the DHS clearance process during

**IT-NOVA
Operations and Maintenance
SECTION L
INSTRUCTIONS, CONDITIONS AND NOTICES TO OFFERORS**

the transition phase and task order period of performance. The following items shall be addressed:

- a) Non-Price Factor 3 – Staffing Approach:
 - Subfactor 1: Staffing methods; and
 - Subfactor 2: Key personnel qualifications

Subfactor 1: Staffing Methods. Proposed approach to recruit, train and retain qualified/certified contractor personnel and ensure adequate staffing to perform the task order requirements from contract transition throughout the contract period of performance; accommodate varying staffing requirements over the life of the task order, including both long term ongoing tasks and special or emergency efforts of lesser duration to ensure continuous contractor support; approach to obtaining personnel with the appropriate security clearances and the vetting process of proposed employees to facilitate the DHS clearance process during the transition phase and task order period of performance.

Subfactor 2: Key Personnel Qualifications. Describe proposed approach for ensuring each proposed key personnel position possesses the experience, education, training, technical expertise and certification required to sufficiently and/or proficiently perform the duties described in Section C (i.e., scope, complexity, technical tasks and expertise, leadership, anticipated workload, etc.) Correlate or map proposed key personnel to the experience and education requirements provided in the EAGLE contract. Provide resumes for Key Personnel meeting the above requirements.

L.7.3 VOLUME 3 - PRICE PROPOSAL

The price proposal shall be separate from the technical proposal. The price proposal must not contain technical information as described in Section L.3 and Section L.5. The price proposal shall be divided into the distinct sections identified below. Price information requested under this RFP is considered information other than cost and pricing data as defined in FAR 15.4. The price proposal shall include the information identified below. The Government intends to make an award without discussions. A Table of Contents may also be included to facilitate review and evaluation of the proposal content.

L.7.3.1 SECTION 1 – EXCEPTIONS AND DEVIATIONS (5 pages)

Source Selection Information – See FAR 2.101 and 3.104

Page 52 of 70

**IT-NOVA
Operations and Maintenance
SECTION L
INSTRUCTIONS, CONDITIONS AND NOTICES TO OFFERORS**

Section 1 of Volume 3 will consist of the completed and signed SF-33 with a cover letter delineating any exceptions taken to this section of the RFP's terms and conditions. However, offerors are cautioned that any noncompliance with the terms and conditions of the RFP may cause their proposal to be determined unacceptable.

L.7.3.2 SECTION 2 - SMALL BUSINESS PARTICIPATION (for Large Businesses only)
(No page limit)

a) Subcontracting Plan

As a part of its proposal, all offerors (other than small businesses) shall prepare and submit an acceptable small business and small disadvantaged business subcontracting plan, as prescribed in FAR 52.219-9. In accordance with FAR 19.702(a)(1), an otherwise apparently successful offeror may become ineligible for award if such offeror fails to negotiate a subcontracting plan acceptable to the TOCO within the time limit prescribed by the TOCO. The goals stated in this RFP are applicable to this procurement and should be utilized for developing a subcontracting plan in response to this RFP. The offeror's subcontracting plan should be realistic, challenging and attainable. Offerors shall also provide a record of previous performance in carrying out the goals of subcontracting plans by including a copy of its FY2006 SF-294 and 295 subcontract reports. If the offeror has had no previous contracts requiring a subcontracting plan, please include a statement to that effect in the proposal. Provide a subcontracting plan to meet or exceed small business participation goals as set forth below.

Offeror's are reminded that the approved subcontracting plan will be incorporated into the task order. The offeror must provide details, percentages, performance incentives, and evidence of corporate commitment for each business category addressed.

TYPE OF BUSINESS	Goal % of Total Planned Subcontracting Dollars
Total Small Business	40%
Small Disadvantaged Business	5%
Women-Owned Small Business	5%
HUBZone Business	3%
Service Disabled Veteran-Owned Small Business	3%

Source Selection Information – See FAR 2.101 and 3.104

Page 53 of 70

**IT-NOVA
Operations and Maintenance
SECTION L
INSTRUCTIONS, CONDITIONS AND NOTICES TO OFFERORS**

(SDVOSB)

Veteran-Owned Small Business (included in SDVOSB) 3%

b) The above goals are separate and independent goals, all of which offerors should assertively pursue to meet in the submission of their offer. For example: A woman-owned small business (WOSB) that subcontracts to a small disadvantaged business (SDB) contributes to the WOSB, SDB and Total Small Business goals.

c) Liquidated damages for failure to achieve small business goals provided in your small business subcontracting plan will be determined in accordance with FAR 52.219-16, Liquidated Damages – Subcontracting Plan (See EAGLE contract - Section I).

L.7.3.3 SECTION 3 – PRICE REASONABLENESS, AND COMPLETENESS

L.7.3.3.1 These instructions are to assist the offeror in submitting their price proposal in a manner that facilitates the government's evaluation of its offer for reasonableness, realism and completeness of the proposed prices. Compliance with these instructions is mandatory and failure to comply may render the offeror's price proposal ineligible for award. Offers should be sufficiently detailed to demonstrate their reasonableness. The burden of proof for credibility of proposed prices rests with the offeror. Offerors are strongly encouraged to propose more favorable terms/T&M rates than currently provided in its EAGLE contract. Each offeror shall provide price proposals based upon its current EAGLE contract T&M rates for each labor category, ODCs and any proposed discount offered. Offerors are reminded that the range of FTEs provided in the Pricing Model are applicable to their Section J, Attachment J-5, Pricing Model.

L.7.3.3.2 The Offeror shall submit pricing for the total life-cycle for the 5-year performance period. Prices shall be provided in accordance with the format included in Section J, Attachment J-5 and the proposal shall include other basis of estimate (BOE) information used to calculate the total life-cycle price. The Contract Line Item Number (CLIN) Structure, Schedule B Prices, Section J, Attachment J-5 and BOE should be consistent and clearly relate to the Technical Proposal and Section C – PWS. Any limitations and assumptions in the price proposal shall be included by the offeror.

L.7.3.3.2(a) **Assumptions:** All assumptions derived by the offeror relating to estimated prices shall be separately identified in the price section and shall reference applicable paragraph and page number in the technical and management sections of the proposal

Source Selection Information – See FAR 2.101 and 3.104

Page 54 of 70

IT-NOVA
Operations and Maintenance
SECTION L
INSTRUCTIONS, CONDITIONS AND NOTICES TO OFFERORS

that provides corresponding discussion of the particular assumption. During the life of the task order, the Government may order Other Direct Costs (ODCs) in an amount not to exceed \$74 million for each 12 month performance period. Each ODC Contract Line Item Number (CLIN) and dollar amount represents a quarterly allocation and is optional. It is anticipated that ODCs will be funded quarterly using Working Capital Funds; hence, ODCs under this task order are subject to FAR 52.232.18-Availability of Funds.

IT-NOVA
Operations and Maintenance
SECTION L
INSTRUCTIONS, CONDITIONS AND NOTICES TO OFFERORS

L.7.3.3.2(b) **Price Realism:** A proposal is presumed to represent an offeror's best effort to respond to the solicitation. Any inconsistency, whether real or apparent, between promised performances and price, shall be explained in the proposal. For example, if the intended use of new and innovative techniques is the basis for an abnormally low estimate, the nature of these techniques and their impact on price should be explained. Any significant inconsistency, if unexplained, raises a fundamental issue of the offeror's understanding of the nature and scope of work required and maybe grounds for rejection of the proposal or grounds for adjusting the proposed price.

L.7.3.3.2(c) **Non-Required Data:** Data beyond that required by this instruction shall not be submitted, unless the offeror considers it essential to document or support the price position. All information relating to the proposed price, including all required documentation, must be included in the section of the proposal designated as the Price Volume. Under no circumstances shall this information and documentation be included elsewhere in the proposal.

L.7.3.3.2(d) **Price Volume Submission Requirements:** The offeror shall submit pricing for the total life-cycle of the 5-year performance period for the IT-NOVA O&M requirement. Prices shall be provided in accordance with the Pricing Model/format included in Schedule B of this RFP and will be incorporated into the subsequent task order award.

L.7.3.3.2(e) **Transition Ramp-Up:** Offerors shall submit a separate pricing section in their Price Proposal identifying proposed prices for the six (6) month Transition Ramp-Up tasks under Management Approach-Transition Plan. This portion of the Price Proposal shall provide the price details for Section 3(b) Transition Ramp-Up of the Volume II proposal.

L.7.3.3.2(f) **Alternate Price Proposals:** Offerors may submit an alternative price proposal in addition to the price proposal required under this section. An alternative price proposal must comply with the CLIN structure/Pricing Model provided in Section B and the requirements indicated under RFP Section L.3.3 and Section M.6.4.

L.7.4 VOLUME 4 – Oral Presentations and Discussions (Non-Price Factors 1, 2 and 3) (60 slides)

a. The purpose of the oral presentations is to allow the Government to better understand the offeror's proposed technical solution and management approach as well as other aspects of the proposal. As such, Government participants may ask questions

IT-NOVA
Operations and Maintenance
SECTION L
INSTRUCTIONS, CONDITIONS AND NOTICES TO OFFERORS

throughout the presentation. Offerors will also be given the opportunity to ask the Government questions during this time. These exchanges will enhance the Government's understanding of the proposal, allow reasonable interpretation of the proposal, and/or facilitate the Government's evaluation process. The information obtained during the question and answer exchanges may be used by the offeror to cure proposal weaknesses or material omissions, materially alter the technical requirements of the proposal and/or otherwise revise the technical and price proposals.

b. Each Offeror shall address the Technical Capability - Non-Price Factor 1, Management Approach – Non-Price Factor 2, Staffing Approach – Non-Price Factor 3 in an oral presentation. The Offeror is required to submit oral presentation charts (slides) on the day of Oral Presentation as indicated in Table L.6.1 above. The Offeror shall be required to respond to three (3) scenarios during oral presentations. The topics for these scenarios are 1) Blackberry Problems; 2) Wireless Networking; and 3) Emergency/COOP Operations. There will be no reference to rates or prices in Volume 4 – Oral Presentation.

Oral Presentations slides shall be clear, concise, and include sufficient detail for effective evaluation. The presentation/slides should not simply rephrase or restate the Government's requirements, but rather shall provide convincing rationale to address how the Offeror intends to meet these requirements. Offerors shall assume that the Government has no prior knowledge of their facilities and experience, and will base its evaluation on the information provided in the Offeror's oral presentation.

c. The oral presentation will be held at 301-7th and D Streets, S.W.-Washington, DC on September 9 and 10, 2007. Oral presentations and discussions will be conducted with the offerors selected under the down-selection phase of this competition as most highly qualified to perform the DHS O&M requirement and invited to submit a technical and price proposal in response to the RFP. The contracting officer will schedule oral presentations and discussions based on an estimated four (4) hour time frame. While the oral presentations are scheduled for 4 hours, they may continue beyond that time estimate to allow Government participants to gain a through understanding of the proposal. At the conclusion of oral presentations, discussions will commence. Offerors will be provided the opportunity to submit proposal revisions, due at 2:00 pm, EDT, the second calendar day following the conclusion of oral presentations and discussions.

d. Contractor participating in oral presentations must provide all necessary audio-visual materials. Presenting prime contractors and their team member may use the 4-

**IT-NOVA
Operations and Maintenance
SECTION L
INSTRUCTIONS, CONDITIONS AND NOTICES TO OFFERORS**

hour period as they deem most advantageous to describe their proposed technical solution, management approach, staffing and pricing structures.

e. The oral presentation shall be given by key personnel responsible for project performance such as program/project managers and supervisors. Prior to the oral presentation of the Offeror's proposal, each Offeror is permitted to present an optional 10-minute corporate introduction; this portion of the presentation will not have any impact on evaluation of the technical capability or risk assessment. The 10-minute corporate introduction may be presented by an individual or team of not more than three (3) representatives at any level in the corporate structure, and will not count toward the representative or time limitations specified herein. Corporate introduction briefers may remain in the briefing room during the oral presentations as a non-participant. It is required that individuals presenting be those identified as key personnel and/or senior management. It is important to the Government that the individuals responsible for performance of this task order are the ones representing the offeror at the oral presentations. Due to space limitation, 10 people are allowed to attend each presentation; 15 copies of the oral presentation in hard copy should be presented to the Government team on the day of the presentation. Oral presentations will be video taped by the Government.

L.8 SOLICITATION PROVISIONS INCORPORATED BY REFERENCE

This solicitation incorporates one or more solicitation provisions by reference, with the same force and effect as if they were given in full text. Upon request, the TOCO will make their full text available. The full text of a provision may be accessed electronically at: <http://www.arnet.gov/far/>

PROVISION NO.	DATE	TITLE
52.216-29	FEB 2007	TIME AND MATERIALS/LABOR-HOUR PROPOSAL REQUIREMENTS – NON-COMMERCIAL ITEM ACQUISITION WITH ADEQUATE PRICE COMPETITION
52.204-6	OCT 2003	DATA UNIVERSAL NUMBERING SYSTEM (DUNS) NUMBER

IT-NOVA
Operations and Maintenance
SECTION L
INSTRUCTIONS, CONDITIONS AND NOTICES TO OFFERORS

PROVISION NO.	DATE	TITLE
52.222-24	FEB 1999	PREAWARD ON-SITE EQUAL OPPORTUNITY COMPLIANCE EVALUATION

IT-NOVA
Operations and Maintenance
SECTION L
INSTRUCTIONS, CONDITIONS AND NOTICES TO OFFERORS

L.9 EVALUATION OF COMPENSATION FOR PROFESSIONAL EMPLOYEES
(FAR 52.222-46) (FEB 1993)

(a) Recompensation of service contracts may in some cases result in lowering the compensation (salaries and fringe benefits) paid or furnished professional employees. This lowering can be detrimental in obtaining the quality of professional services needed for adequate contract performance. It is therefore in the Government's best interest that professional employees, as defined in 29 CFR 541, be properly and fairly compensated. As part of their proposals, offerors will submit a total compensation plan setting forth salaries and fringe benefits proposed for the professional employees who will work under the contract. The Government will evaluate the plan to assure that it reflects a sound management approach and understanding of the contract requirements. This evaluation will include an assessment of the offeror's ability to provide uninterrupted high-quality work. The professional compensation proposed will be considered in terms of its impact upon recruiting and retention, its realism, and its consistency with a total plan for compensation. Supporting information will include data, such as recognized national and regional compensation surveys and studies of professional, public and private organizations, used in establishing the total compensation structure.

(b) The compensation levels proposed should reflect a clear understanding of work to be performed and should indicate the capability of the proposed compensation structure to obtain and keep suitably qualified personnel to meet mission objectives. The salary rates or ranges must take into account differences in skills, the complexity of various disciplines, and professional job difficulty. Additionally, proposals envisioning compensation levels lower than those of predecessor contractors for the same work will be evaluated on the basis of maintaining program continuity, uninterrupted high-quality work, and availability of required competent professional service employees. Offerors are cautioned that lowered compensation for essentially the same professional work may indicate lack of sound management judgment and lack of understanding of the requirement.

(c) The Government is concerned with the quality and stability of the work force to be employed on this contract. Professional compensation that is unrealistically low or not in reasonable relationship to the various job categories, since it may impair the Contractor's ability to attract and retain competent professional service employees, may be viewed as evidence of failure to comprehend the complexity of the contract requirements.

IT-NOVA
Operations and Maintenance
SECTION L
INSTRUCTIONS, CONDITIONS AND NOTICES TO OFFERORS

(d) Failure to comply with these provisions may constitute sufficient cause to justify rejection of a proposal.

(END OF SECTION L)

IT-NOVA
Operations and Maintenance
SECTION M
EVALUATION FACTORS FOR AWARD

M.1 GENERAL

(a) The Government is conducting this source selection in accordance with the fair opportunity ordering procedures contained in FAR Part 16.

(b) The Government intends to award two (2) Time and Materials (T&M) task orders to the responsible offeror whose proposal represents the best value. Best value is defined in FAR Part 2, as the expected outcome of an acquisition that, in the Government's estimation, provides the greatest overall benefit in response to the requirement. The Government will select the best overall offer based on an integrated assessment of the evaluation factors listed in Section M.3.

(c) When conducting the evaluation, the Government may use data included by Offers in their proposals, as well as data obtained from other sources. Each offeror is responsible for ensuring that the information provided is through, accurate, and complete.

M.2 BASIS FOR AWARD

The Government will award two (2) Time and Materials Task Order to the responsible offeror whose proposal is the most advantageous to the Government, price and other factors considered. The task orders will be awarded to the offeror who is deemed responsible in accordance with the FAR, whose proposal conforms to the solicitation requirements (including all stated terms, conditions, representations, certifications, and all other information required by Section L of this solicitation), and is judged, based on the evaluation factors, to represent the best value to the Government, considering both cost and non-cost factors. This may result in awards to a higher-price offeror where the decision is consistent with the evaluation factors and the Selection Official reasonably determines that the proposal represents the best value to the Government. While the Government Best Value Evaluation Team and the Selection Official will strive for maximum objectivity, the procurement selection process, by its nature, is subjective and, therefore, professional judgment is implicit throughout the entire process.

M.3 EVALUATION FACTORS

The Government will use the following factors to evaluate proposals and make a best value determination.

Non-Price Factors:

1. Technical Capability
 1. Understanding of Requirements
 2. Integrator Expertise
 3. Implementation

**IT-NOVA
Operations and Maintenance
SECTION M
EVALUATION FACTORS FOR AWARD**

- 2. Management Approach
 - 1. Organization
 - 2. Management Methodology
 - 3. Transition Plan and Transition Ramp-up
 - 4. Quality Control

 - 3. Staffing Approach
 - 1. Staffing Methods
 - 2. Key Personnel Qualifications

 - 4. Proposal Risk
- Price Factor
- 1. Price

M.4 RELATIVE IMPORTANCE OF EVALUATION FACTORS

- a) Non-Price factors in Section M.3 above are of equal importance. Sub-factors under each Non-Price factor are of equal importance.

- b) The non-price factors in Section M.3, when combined, are significantly more important than the price factor.

M.5 EVALUATION CRITERIA

An evaluation of all proposals will be conducted in accordance with the criteria set forth below. Evaluation criteria consist of factors and sub-factors. The members of the evaluation panels will evaluate each proposal in relation to the price and non-price factors and sub-factors, then the evaluation panels will determine consensus ratings for each proposal. The evaluation panels will present their ratings and findings to the Selection Official (SO), whose sole authority it will be to make the final award decision.

M.5.1 Factor 1 - Technical Capability

- a. Each Offeror's technical proposal and oral presentation will be evaluated to determine if the offeror provides a sound, compliant approach that meets the requirements of the IT-NOVA O&M Support Services function and demonstrates a thorough knowledge and understanding of those requirements and their associated risks.

IT-NOVA
Operations and Maintenance
SECTION M
EVALUATION FACTORS FOR AWARD

i. Subfactor 1: Understanding of Requirements.

This sub-factor is met when the offeror's response to "understanding of requirement", demonstrates to the extent applicable, a sound and proficient understanding and application of this knowledge to:

Section C/PWS requirements and the inherent complexity in meeting all the technical objectives of the procurement; comprehensive summary identifying how the full range of services in the task order PWS (Section C) shall be accomplished; services required in the PWS and its relationship to achieving the mission of the agency.

ii. Subfactor 2: Integrator Expertise

This sub-factor is met when the offeror's response to "integrator expertise", demonstrates to the extent applicable, a sound and proficient understanding and viable approach to:

Capability to integrate separate IT service requirements into a consolidated effort, resulting in advantages such as reductions in project overlaps, realized economies of scale, improved efficiency and service delivery, standardized support services, increased customer satisfaction, and meeting or exceeding industry standards.

iii. Subfactor 3: Implementation

This sub-factor is met when the offeror's response to "implementation", demonstrates to the extent applicable, a sound and proficient understanding and viable approach to:

Implementing activities/tasks that encompasses the anticipated logical sequence of tasks, methodology, techniques, and any other areas of consideration the offeror deems necessary to implement/execute Section C/PWS requirements and related deliverables.

M.5.2 Management Approach

The offeror's management proposal and oral presentation will be evaluated to determine the extent to which it demonstrates a comprehensive, sound, and reasonable approach to accomplish and manage the requirements as described in Section C of this solicitation.

IT-NOVA
Operations and Maintenance
SECTION M
EVALUATION FACTORS FOR AWARD

Subfactor 1: Organization.

This sub-factor is met when the offeror's response to "organization", demonstrates to the extent applicable, a sound and proficient understanding and viable approach to:

Delineating a coordinated, flexible and efficient workflow management and provide an organizational control and communication plan to accomplish the requirements in Section C including clearly defined roles, responsibilities and direct lines of control and communication; Defining Project Manager's responsibility and authority to effectively control, monitor and manage the project.

Subfactor 2: Management Methodology.

This sub-factor is met when the offeror's response to "management methodology", demonstrates to the extent applicable, a sound and proficient understanding and viable approach to:

Managing multiple services/requirements and meeting performance metrics under this task order and identifying how the selected approach will generate efficient services and increase customer satisfaction; collecting, analyzing and maintaining workload data per Section C.1.6;

Subfactor 3: Transition Plan.

This sub-factor is met when the offeror's response to "transition plan", demonstrates to the extent applicable, a sound and proficient understanding and viable approach to:

Minimizing impacts on continuity of operations, identifying key issues and overcoming barriers to transition; transition schedule, milestones, measurable commitments, estimated price for transition (include in Price Proposal) and other tasks the offeror deems necessary to conduct and complete the transition during the designated time period.

Subfactor 4: Quality Control Plan.

This sub-factor is met when the offeror's response to "quality control plan", demonstrates to the extent applicable, a sound and proficient understanding and viable approach to:

IT-NOVA
Operations and Maintenance
SECTION M
EVALUATION FACTORS FOR AWARD

Meeting Section C/PWS requirements and ensuring quality in the delivery of services from the transition of current contracts throughout the entire contract period of performance; plans demonstrate proficiency, efficiency and cost effectiveness.

M.5.3 Staffing

The offeror's proposal, oral presentation and scenarios will be evaluated to determine the extent to which it offers qualified and sufficient staffing to accomplish Section C requirements in the DHS dynamic IT environment while simultaneously maintaining the service level requirements as described in Section C of this solicitation.

Subfactor 1: Staffing Methods.

This sub-factor is met when the offeror's response to "staffing methods", demonstrates to the extent applicable, a sound and proficient understanding and viable approach to:

Recruiting, training and retaining qualified/certified contractor personnel and ensuring adequate staffing to perform the task order requirements from contract transition throughout the contract period of performance; accommodating varying staffing requirements over the life of the task order, including both long term ongoing tasks and special or emergency efforts of lesser duration to ensure continuous contractor support; obtaining personnel with the appropriate security clearances and the vetting process of proposed employees to facilitate the DHS clearance process during the transition phase and task order period of performance.

Subfactor 2: Key Personnel Qualifications.

This sub-factor is met when the offeror's response to "key personnel qualifications", demonstrates to the extent applicable, a sound and proficient understanding and viable approach to:

Providing key personnel possessing qualifications to meet Section C/PWS requirements and who demonstrates the necessary experience to perform the tasks required under the scope and complexity of the task order.

M.6 EVALUATION

**IT-NOVA
Operations and Maintenance
SECTION M
EVALUATION FACTORS FOR AWARD**

M.6.1 Rating Scale for Non-Price Factors

The Government will rate non-price factors 1 through 3 using the adjectival ratings below. Narrative descriptions of the proposal evaluation findings will accompany the adjectival rating designations.

Evaluation Rating Scale for Non-Price Factors

ADJECTIVAL RATINGS	
RATING	DEFINITION
Exceptional (E)	Exceeds specified minimum performance or capability requirements in a way beneficial to the government; proposal must have one or more strengths and no deficiencies to receive an exceptional.
Acceptable (A)	Meets specified minimum performance or capability requirements delineated in the Request for Proposal; proposal rated Acceptable must have no major deficiencies but may have one or more strengths.
Marginal (M)	Does not clearly meet some specified minimum performance or capability requirements delineated in the Request for Proposal, but these weaknesses may be correctable.
Unacceptable (U)	Fails to meet specified minimum performance or capability requirements; proposal has one or more deficiencies. Proposals with an unacceptable rating are not awardable.

M.6.2 Rating Scale for Non-Price Factor 4 – Proposal Risk

The Government will rate the proposal risk assessed by the evaluation of non-price factors 1 through 3 using the adjectival ratings below. Narrative descriptions of the proposal risk evaluation findings will accompany the proposal risk rating designations.

PROPOSAL RISK ADJECTIVAL RATINGS	
RATING	DESCRIPTION
High	Likely to cause significant disruption of schedule, increased cost or degradation of performance. Risk may be unacceptable even with special contractor emphasis and close Government monitoring.
Moderate	Can potentially cause disruption of schedule, increased cost, or degradation of performance. Special contractor emphasis and close Government monitoring will likely be able to overcome difficulties.
Low	Has little potential to cause disruption of scheduled, increased cost or degradation of performance. Normal contractor effort and normal Government monitoring will likely be able to overcome any difficulties.

IT-NOVA
Operations and Maintenance
SECTION M
EVALUATION FACTORS FOR AWARD

M.6.3 Extent of Small Business Participation

(a) Subcontracting plans (other than small business) that do not meet the requirements of H.3 will be rejected. The Government will consider the methodology used to incorporate small business, percentages, performance incentives, evidence of corporate commitment, and the extent to which small businesses are included in areas of performance that are integral to RFP Section C.

(b) The Small Business Subcontracting Plan will not be rated. It will be assessed a finding of Acceptable or Not Acceptable in accordance with the criteria set forth below.

Acceptable. The Small Business Subcontracting Plan developed to meet criteria stated in (a) above is acceptable.

Not Acceptable. The Small Business Subcontracting Plan developed to meet the criteria stated in (a) above is NOT acceptable.

M.6.4 Price Proposal Evaluation

M.6.4(a) The government will not rate or score price, but will evaluate each offeror's price proposal for realism, reasonableness, and completeness. This evaluation will reflect the offeror's understanding of the solicitation requirements and the validity of the offeror's approach to performing the work. Alternative price proposals, if considered by the Government will be evaluated on contract type risk, potential savings, other advantages or disadvantages to the government, and the discretion of the government.

M.6.4(b) Realism. The government will evaluate the realism of the proposed price by assessing the compatibility of proposed price with proposal scope and effect. In the evaluation the government will consider the following:

- i. Do the proposed prices reflect a clear understanding of the requirements?
- ii. Do the proposed prices for performing various functional service requirements reflect the likely costs to the offeror in performing the effort with reasonable economy and efficiency?
- iii. Are proposed prices unrealistically high or low?
- iv. Are the proposed prices consistent with the technical and management/staffing approach (e.g., if the offeror proposes a staff of x people, the price proposal must account for x people)?

M.6.4(c) Reasonableness. In evaluating reasonableness, the government will determine if the offeror's proposed prices, in nature and amount, do not exceed those which would be incurred by a prudent contractor in the conduct of competitive business. The assessment of reasonableness will take into account the context of the source

IT-NOVA
Operations and Maintenance
SECTION M
EVALUATION FACTORS FOR AWARD

selection, including current market conditions and other factors that may impact price. In the evaluation the government will consider the following:

- i. Is the proposed price(s), ODCs and number of FTEs comparable to the prices and staffing requirements anticipated in the independent government cost estimate (IGCE)?
- ii. Is the level of effort or estimated number of T&M hours for each service functional area in Section C and the complete five year performance period comparable to the effort anticipated by the IGCE?
- iii. Is the proposed labor/skill mix comparable to the projected IGCE skill mix and/or sufficient to meet the Section C requirements based upon the offeror's technical and management/staffing approach?
- iv. Are the proposed price(s) and ODCs for separate functional service areas and the full five year performance period comparable to competitor's prices under this solicitation?

M.6.4(d) Completeness. In evaluating completeness, the government will determine if the offeror's provides pricing data of sufficient detail to fully support the offer and permit the government to evaluate the proposal thoroughly. In the evaluation the government will consider the following:

- i. Do the proposed prices include all price elements the offeror is likely to incur in performing the effort?
- ii. Is there a labor listing/schedule that includes labor category and skill levels, to cover the 12 month base period and four (4) 12 month options?
- iii. Are proposed prices traceable to requirements?
- iv. Do proposed prices account for all requirements?
- v. Are all proposed prices, including subcontract costs, fully supported with adequate data to permit a thorough evaluation?

M.7 EVALUATION OF OPTIONS

For award purposes, in addition to an offeror's response to the base period requirements, the Government will evaluate the offeror's technical, management, staffing, and price response to all contract option periods. Evaluation of the option periods will not obligate the Government to exercise the options.

The maximum quantities/amounts for each optional ODC CLIN is \$14.5 million for three months (one quarter) of the 12-month performance period. The maximum aggregate amount of all ODCs issued under this task order shall not exceed **\$74,000,000** for each 12-month period of performance of the task order.

M.8 USE OF NON-GOVERNMENT ADVISORS

IT-NOVA
Operations and Maintenance
SECTION M
EVALUATION FACTORS FOR AWARD

The Government will use the following non-Government advisors in the evaluation process:

PMC
Management Analysis, Incorporated
Acquisition Solutions, Inc.

These non-Government advisors will be authorized access to only that data and those discussions that are necessary to enable them to provide specific guidance on specialized matters on particular problems. As advisors they are not authorized to be voting members of any panel, or to make final decisions. Each non-Government advisor will sign a nondisclosure certificate.

**IT-NOVA
Operations and Maintenance**

**PART II – PART III – LIST OF DOCUMENTS, EXHIBITS AND OTHER
ATTACHMENTS**

SECTION J – LIST OF ATTACHMENTS

The following attachments are available as shown in the table below:

Attachment Number	Title
Attachment J-1	Performance Work Statement
Attachment J-2	DHS Form 700-21
Attachment J-3	Implementing Instructions for Compliance with HSAR Clause 3052.204-71, "Contractor Employee Access"
Attachment J-4	DHS Form 11000-6 – Non-Disclosure
Attachment J-5	Pricing Model
Attachment J-6	DD Form 254 Contract Security Classification Specification
Attachment J-6A	DHS HSDN – Security Classification Guide
Attachment J-6B	DHS – National Security IT Systems Certification and Accreditation Security Classification Guide

U.S. DEPARTMENT OF HOMELAND SECURITY

TASK ORDER

For

**Information Technology Network Operations Virtual Alliance
(IT-NOVA)**

Operations and Maintenance (O&M)



August 17, 2007

TABLE OF CONTENTS

C.1	GENERAL INFORMATION	1
C.1.1	Introduction.....	1
C.1.2	Background	1
C.1.3	Span of Support	2
C.1.3.1	Service Model	2
C.1.3.2	Information Technology Services.....	2
C.1.3.3	Network Services	3
C.1.3.4	Network Interfaces	4
C.1.4	General Requirements	4
C.1.4.1	Contractor Responsibilities.....	4
C.1.4.2	Function-Specific Contractor Requirements.....	6
C.1.5	Layout of Section C	8
C.1.5.1	Section C Contents	8
C.1.5.2	Document Information.....	9
C.1.6	Required Reports and Meetings.....	9
C.1.6.1	Task Order Administration.....	9
C.1.6.2	Required Reports	10
C.1.6.3	Required Meetings	11
C.1.6.4	Function Specific Reports and Documents	13
C.1.7	Contractor Personnel	14
C.1.7.1	Key Personnel.....	14
C.1.7.2	Personnel Staffing	15
C.1.7.3	Personnel Training	15
C.1.7.4	Personnel Security Requirements.....	16
C.1.8	Contractor Interfaces.....	17
C.1.8.1	Personnel Performing Security/Continuity/Quality	17
C.1.9	Quality Assurance and Quality Control	18
C.1.9.1	Quality Assurance	18
C.1.9.2	Quality Control	18
C.1.10	Property Control	19
C.1.11	Operating Environment	19
C.1.11.1	Operating Hours.....	19

PROCUREMENT SENSITIVE

- C.1.11.2 Operations Under Adverse Conditions 21
- C.1.11.3 Travel 22
- C.1.12 Contract Transition 22
 - C.1.12.1 Transition and Phase In 22
 - C.1.12.2 Phase Out 23
- C.2 DEFINITIONS AND ACRONYMS..... 25**
 - C.2.1 Definitions..... 25
 - C.2.2 Acronyms 37
- C.3 GOVERNMENT – FURNISHED PROPERTY (GFP) AND SERVICES 47**
 - C.3.1 Scope 47
 - C.3.1.1 Government-Furnished Property 47
 - C.3.1.2 Government-Furnished Services..... 47
 - C.3.1.3 Supplies and Materials 48
 - C.3.1.4 Government-Furnished Equipment (GFE) 48
- C.4 CONTRACTOR – FURNISHED PROPERTY AND SERVICES 51**
 - C.4.1 Scope 51
 - C.4.1.1 Contractor-Furnished Facilities (CFF) 51
- C.5 SCOPE OF WORK 52**
 - C.5.1 Applications Management, Support, and Development 52
 - C.5.1.1 Application Management Services 52
 - C.5.1.2 Status and Availability of Major Applications on the Network..... 53
 - C.5.1.3 Application Maintenance and Operation Documentation 53
 - C.5.1.4 Application Database and Systems Maintenance 53
 - C.5.1.5 Performance Trends of Major Applications on the Network 54
 - C.5.1.6 Enterprise Desk Application Licensing 54
 - C.5.1.7 Collaborative Applications 54
 - C.5.1.8 Application Development..... 54
 - C.5.1.9 Ensure New Acquisitions Include Common Security Configurations 54
 - C.5.2 Deployment Support..... 55
 - C.5.2.1 Provide Deployment Support 55
 - C.5.2.2 Develop Deployment Plan Template 56
 - C.5.2.3 Site Activation 56
 - C.5.2.4 Facilities Modifications 56
 - C.5.2.5 Installation and Checkout..... 56

C.5.2.6	Transition to O&M	57
C.5.2.7	Engineering and Project Management	57
C.5.3	Infrastructure Engineering Services	57
C.5.3.1	On-site Engineering Team	57
C.5.3.2	Systems Engineering Support.....	57
C.5.3.3	Engineering Projects	58
C.5.3.4	Engineering Process and Methodology.....	59
C.5.4	Testing.....	60
C.5.4.1	Test Support and Documentation.....	60
C.5.4.2	Test and Development Lab	61
C.5.5	Operations and Maintenance For End User Support	62
C.5.5.1	End User and Desk Side Support	62
C.5.5.2	Maintenance.....	64
C.5.6	Video Conferencing.....	65
C.5.6.1	Video Conferencing (VTC).....	65
C.5.7	Satellite/Cable Television Operations	65
C.5.7.1	Operations.....	65
C.5.8	Voice Communications and Messaging	66
C.5.8.1	Private Branch Exchange (PBX) Infrastructure	66
C.5.8.2	Telephone Switchboard Operations Center	67
C.5.8.3	Voice Over Internet Protocol (VOIP)	68
C.5.8.4	Unified Messaging.....	68
C.5.9	Network Management Center (NMC).....	68
C.5.9.1	NMC Operations.....	68
C.5.10	Security Management Center (SMC)	71
C.5.10.1	SMC Operations.....	71
C.5.10.2	Vulnerability Assessment	72
C.5.10.3	Security Information Management (SIM) & Security Management Capability ...	73
C.5.10.4	Security Systems Administration.....	73
C.5.10.5	Security Change Management.....	74
C.5.10.6	Security Log Access, Retention and Review.....	74
C.5.10.7	System Security Administrators	74
C.5.10.8	Data Spills and Response	74
C.5.10.9	Incident Response.....	74

PROCUREMENT SENSITIVE

C.5.10.10 Information Condition (INFOCON) Management	75
C.5.11 Communications Security (COMSEC) Management	75
C.5.11.1 COMSEC Security.....	75
C.5.12 Other Communications Operations	76
C.5.12.1 Emergency Notification System	76
C.5.12.2 Executive Telecommunications Support	76
C.5.13 Training	77
C.5.13.1 System Administrator Training	77
C.5.13.2 Security Training	78
C.5.13.3 End-User Training	78
C.5.14 Wireless Management.....	78
C.5.14.1 Wireless Communication Architecture Development	78
C.5.14.2 Systems Engineering Support.....	79
C.5.14.3 Working Group Support.....	80
C.5.14.4 Enterprise Architecture Governance Support.....	80
C.5.14.5 Frequency Management Support.....	80
C.5.14.6 Spectrum Planning	80
C.5.15 IT Continuity Management	81
C.5.15.1 Continuity Assessment.....	81
C.5.15.2 Continuity Planning	82
C.5.15.3 Continuity Reviews and Coordination	82
C.5.15.4 Continuity Program Administration.....	82
C.5.15.5 Testing and Exercises	83
C.5.15.6 Electronic Records	83
C.6 APPLICABLE LAWS, PUBLICATIONS, AND FORMS	85
C.6.1 General Information.....	85
C.6.1.1 Applicable Publications and Forms	85
C.6.1.2 Publication Conflict Resolution.....	85
C.6.2 Federal Publications.....	85
C.6.2.1 Federal Regulation and Guidelines	85
C.6.3 Other Publications	86
C.6.3.1 U.S. Congress-Public Law (PL) and United States Code (U.S.C.)	86
C.6.3.2 Executive Orders–Office of Management and Budget (OMB), Homeland Security Presidential Directive (HSPD) and Presidential Decision Directive	86

PROCUREMENT SENSITIVE

C.6.3.3 DHS Management Directive (MD)..... 87

C.6.3.4 DHS Regulations..... 89

C.6.3.5 DHS Guides 90

C.6.3.6 National Institute of Standards and Technology (NIST), Special Publications ... 90

C.6.3.7 Federal Information Processing Standards Publications (FIPS PUBS) 91

C.6.4 Forms 91

C.7 TECHNICAL EXHIBITS..... 92

C.8 CONTRACT DATA REQUIREMENTS LISTING (CDRL)..... 93

C.1 GENERAL INFORMATION

C.1.1 INTRODUCTION

The contractor shall provide Information Technology (IT) support services to the Department of Homeland Security (DHS) headquarters, the department's Associate Components, select field offices of the department's Major Components and to other federal, state, and local level government organizations through this Information Technology Networking Operations Virtual Alliance (IT-NOVA) Operations & Maintenance (O&M) Task Order under the Enterprise Acquisition Gateway for Leading Edge Solutions (EAGLE) Information Technology Support Services Contract. The support services include all network components, services, and monitoring; network and internet access; infrastructure transformation and support; applications management, delivery, and development; wireless communications systems management; communications and messaging; communications security (COMSEC); Continuity of Operations (COOP) planning; and IT operations disaster management. The contractor shall provide all labor to complete the services herein in accordance with the terms, conditions, and specifications of this Task Order. The contractor shall assume total responsibility for all requirements performed by incumbent contractors whose period of performance expires on or by the commencement date of this Task Order. In those instances where incumbent contractor periods of performance expire after the commencement date of this task order, the contractor shall assume responsibility of those requirements based upon the Government approved transition plan.

C.1.2 BACKGROUND

In March 2003, Congress passed the Homeland Security Act of 2003 (Public Law 107-296) creating a single department from 22 components that had previously resided in other agencies. One primary reason for the establishment of the Department of Homeland Security (DHS) was to provide the unifying core for the vast national network of organizations and institutions involved in efforts to secure our nation.

To comply with the new legislative requirement, the President directed the DHS Secretary to integrate the 22 legacy components into one organization and the DHS Secretary stated the objective to centrally manage services, including Information Technology (IT).

The DHS components are as follows:

- Associate Components
 - Office of the Secretary
 - Citizenship and Immigration Services, Ombudsman (CISOMB)
 - Civil Rights and Civil Liberties (CRCL)
 - Counternarcotics Enforcement (CNE)
 - Domestic Nuclear Detection Office (DNDO)
 - Executive Secretariat (ESEC)
 - Federal Emergency Management Agency (FEMA)
 - Office of the General Counsel (OGC)
 - Gulf Coast Region (GCR)
 - Office of Health Affairs (OHA)
 - Office of Intelligence and Analysis (I&A)

- Military Advisor's Office (MIL)
- National Protection and Programs Directorate (NPPD)
- Office of Inspector General (OIG)
- Office of Legislative Affairs (OLA)
- Office of Operations Coordination (OPS)
- Office of Policy (PLCY)
- Chief Privacy Officer (PRIV)
- Office of Public Affairs (OPA)
- Science and Technology (S&T)
- Major Components
 - Federal Law Enforcement Training Center (FLETC)
 - Transportation Security Administration (TSA)
 - United States Citizenship and Immigration Services (USCIS)
 - United States Coast Guard (USCG)
 - United States Customs and Border Protection (CBP)
 - United States Immigration and Customs Enforcement (ICE)
 - United States Secret Service (USSS)

TE C.1.2-001 is a chart of the DHS organizational structure. TE C.1.2-002 is a Sensitive But Unclassified listing of the locations supported by this Task Order.

The DHS Management Directorate is responsible for budgets and appropriations, expenditure of funds, accounting and finance, procurement, human resources, information technology systems, facilities and equipment, and the identification and tracking of performance measurements. Their mission is to ensure the DHS's more than 170,000 employees have well-defined responsibilities and those managers and their employees have effective means of communicating with one another, with other governmental and nongovernmental bodies, and with the public, they serve.

The DHS Office of the Chief Information Officer (OCIO) falls under the Management Directorate. Within the OCIO is the Information Technology Services Office whose mission is to provide IT services to the department. The contractor shall provide IT Support Services to the Information Technology Services Office throughout the duration of this Task Order. TE C.1.2-003 is a chart of the OCIO organizational structure.

C.1.3 SPAN OF SUPPORT

C.1.3.1 Service Model

The DHS uses the Information Technology Service Library (ITIL) version 2 framework as the basis for its service model. The contractor shall adopt the ITIL version 3 service model framework (Service Strategies, Service Design, Service Transition, Service Operation, and Continual Service Improvement) for the execution of the DHS IT System Development Life Cycle (SDLC).

C.1.3.2 Information Technology Services

C.1.3.2.1 The Contactor shall provide the DHS a full line of Information Technology (IT), telecommunications, and related services to manage the baseline requirements defined in this Task Order. The contractor shall provide IT

PROCUREMENT SENSITIVE

infrastructure services that conform to specified standards for reliability, readiness, sustainability, supportability, availability, stability, security, flexibility, responsiveness and cost effectiveness. DHS Headquarters and DHS Associate Components shall receive the entire range of support and monitoring as described in this Task Order. DHS Major Components and other Federal/State/Local/Tribal Government organizations that have connectivity to at least one of the three DHS networks shall receive the entire range of support and monitoring as described in this Task Order with the exception of Desk Side Support. However, these entities may require Desk Side Support in emergency situations facilitated through logical follow-on Task Orders. IE C.1.3-002 identifies the number of supported users by network for the FY06 to FY13 time frame.

C.1.3.2.2 The contractor shall demonstrate a proactive and technologically aggressive methodology to identify and pursue new IT advancements, forecast IT trends and provide a comprehensive system of support. The support shall include conducting frequent and thorough market research of new or updated IT technologies, equipment, and data acquisition and availability including software based reporting and performing subjective and comparative analysis to existing DHS technology. If authorized by the COTR, the contractor shall perform and conduct operational and theoretical performance evaluations of current IT capabilities and propose recommended IT advancements.

C.1.3.2.3 To effectively meet their mission objectives, DHS requires a robust, reliable, scalable, integrated, secure, and flexible IT Infrastructure support Task Order that employs methodologies to achieve mission and business-critical systems and applications in accordance with the DHS business critical system reliability levels identified in Table 1 below. An integrated IT infrastructure Task Order will provide for a more cohesive IT support structure for DHS. Improved information sharing via a consolidated, enterprise wide IT infrastructure support will achieve DHS' strategic goals and business objectives that consist of: awareness, prevention, protection, response, recovery, service, and organizational excellence.

C.1.3.2.3.1 IT Support Services shall be governed by the DHS reliability levels for critical and non-critical systems identified in Table 1.

Table 1 – Reliability for Critical and Non-Critical Systems

Minimum Reliability Level	Hours of Unscheduled Downtime	Minutes of Unscheduled Downtime	Seconds of Unscheduled Downtime
99%	Up to 87.6	Up to 5,256	Up to 315,360
99.9%	Up to 8.76	Up to 525.6	Up to 31,536
99.99%	Up to .876	Up to 52.559	Up to 3,153.6
99.999%	Up to .0876	Up to 5.256	Up to 315.36

C.1.3.3 Network Services

The contractor shall provide IT Support Services for Unclassified, Classified, and Top Secret Networks. The extent of the support services for each of the networks is as follows:

PROCUREMENT SENSITIVE

- Unclassified and Top Secret Networks: The Headquarters and Associate Component locations identified in TE C.1.2-002 receive all the services described in this Task Order
- Classified Network – referred to as Homeland Security Data Network (HSDN): Certain Major Component field office locations, certain other Federal government organizations and select State and Local government organizations identified in TE C.1.2-002 receive all the services described in this Task Order with the exception of Desk-Side Support; however, Desk-Side Support may be required on an exception basis or in emergency cases only. For security the field office locations are not named and their information is provided in an aggregated manner by state.

C.1.3.4 Network Interfaces

The contractor shall provide, and maintain operability, of interfaces to multiple networks such as the following:

- DHS National Capital Region Metropolitan Area Network (MAN)
- DHS National Capital Region Wide Area Network (WAN)
- Homeland Security Information Network (HSIN)
- Homeland Security Information Network – Secret (HSIN-S)
- Director of National Intelligence – Secret (DNI-S)
- Secret Internet Protocol Router Network (SIPRnet)
- Joint Worldwide Intelligence Communications System (JWICS)

C.1.4 GENERAL REQUIREMENTS**C.1.4.1 Contractor Responsibilities**

The Government requires that the contractor adhere to and follow all applicable executive orders, presidential directives, other federal and DHS laws, federal orders management policies, handbooks, guidelines, processes, and procedures provided in section C-6. The contractor shall take initiative to identify, respond to problems, and propose solutions for issues that have a potential negative impact to the mission environment. The contractor shall analyze the operational environment, identify and propose solutions to improve the efficiency and effectiveness of the Information Technology Services Office.

C.1.4.1.1 Administrative Services: The contractor shall perform all related administrative services required to perform services such as, material requisitioning, Quality Control (QC), financial control (cost control and savings), status and tracking reports, and correspondence. The contractor shall also maintain accurate and complete records, files, and libraries of or access to documents to such as Federal, state, and local regulations, codes, laws, technical manuals, manufacturer's instructions, Standard Operating Procedures (SOPs), and recommendations, which are necessary and related to the functions being performed. The contractor shall support DHS during audits and inspections, and provide support and responses to audit and inspection items (internal and external).

C.1.4.1.2 Submittal of Reports and Information: The contractor shall compile data, prepare required reports, and submit information as specified by the Contract Data Requirements Lists (CDRLs), Section C.8, and as presented in this Task

PROCUREMENT SENSITIVE

Order. The reports include daily, weekly, monthly and annual reports the contractor shall submit at the specified time. The COTR will forward the approved reports to the proper Government element.

- C.1.4.1.3 Ad hoc Requirements: Upon notification from the Government, the contractor shall provide management and technical information to the Government such as: (CDRL C.1.4-1, Ad hoc Requirements)
- Technical evaluation of suggestions
 - Input for staff studies
 - Fact sheets
 - Audits
 - Congressional inquiries
 - One-time reports
 - Material, equipment, facilities, and other property listings or inventories
 - Equipment maintenance records
 - Recommendations for amending, revising, or originating Government regulations or policies within the scope of this Task Order
 - Information requested by the CO/COTR on other interfacing Task Orders that support this effort
- C.1.4.1.4 Paper File Archiving. The contractor shall prepare all correspondence in and maintain all files using DHS specific, and generally accepted commercial industry standards in accordance with the appropriate current National Archives and Record Administration (NARA), and General Records Schedule (36 Code of Federal Regulations (CFR) 122014 and 44 U.S.C. 3301). The website at <http://www.archives.gov/records-mgmt/ardor/records-schedules.html> contains the index of NARA schedules. All contractor files, records, and documents maintained in the performance of this Task Order are Government property and the contractor shall return them upon completion or termination of the work. However, internal proprietary contractor business files are not Government property.
- C.1.4.1.5 Electronic File Archiving: The contractor shall provide daily, weekly, and monthly electronic file and system backups with copies provided at both an on site and off site storage location, per Government established processes and procedures.
- C.1.4.1.6 Document Management: For all deliverables within this Task Order, the contractor shall implement document management to include version control and comment resolution such that each release has clear inventory of comments accepted/rejected as part of the version.
- C.1.4.1.7 Enterprise Architecture Compliance: All solutions and services shall meet DHS Enterprise Architecture policies, standards, and procedures as it relates to this Task Order. Specifically, the contractor shall comply with the following Homeland Security Enterprise Architecture (HLSEA) requirements:
- All developed solutions and requirements shall comply with the HLSEA
 - All IT hardware or software shall comply with the HLSEA Technical Reference Model (TRM) Standards and Products Profile

- The contractor shall submit all data assets, information exchanges and data standards, whether adopted or developed to the DHS Enterprise Data Management Office (EDMO) for review and insertion into the DHS Data Reference Model.

C.1.4.2 Function-Specific Contractor Requirements

- C.1.4.2.1 Project Support: The purpose of this task is to provide project management support, monitoring, and lifecycle systems development methodologies for all DHS IT projects.
- C.1.4.2.1.1 The contractor shall provide project management support to include executive level Information Assurance (IA), planning, implementation, reporting and other services as required or directed.
- C.1.4.2.1.2 The contractor shall support projects by providing services such as: Development, coordination, scheduling, design validation, documentation, migration planning, writing service delivery guidance and other references, and weekly status reporting.
- C.1.4.2.1.3 The contractor shall attend the Weekly Project Team Meeting and provide a summary of the Weekly Status Report. The contractor shall prepare support documentation for the Weekly Project Team Meeting (e.g. project issue updates, action issue updates, and project plan/status updates) to support the summary presentation.
- C.1.4.2.2 Systems Security: The contractor shall ensure systems security for network environments, applications, databases, Internet, Portal and Intranet that allows access only by authorized users, prevention of unauthorized release of information, prevention of degradation due to circumstances such as unauthorized internal use and external intrusion, maintenance of data integrity, and authorized utilization by the user community.
- C.1.4.2.3 Change Management Requirements: The contractor shall manage the Change Management process in accordance with the DHS Change Management Policy Process and Procedures and will maintain the Change Management Database. The Government will provide detailed Configuration Management Database information after Task Order award. The contractor shall comply with the DHS Change Management requirements for all equipment, hardware, system software, applications software (both source and executable), data files, and control-language.
- C.1.4.2.4 Deliverables
- C.1.4.2.4.1 Any change to the Task Order list of deliverables or the scheduled delivery date shall be coordinated with the COTR with a written copy to the CO for Task Order modification if required.
- C.1.4.2.4.2 The contractor shall notify the appropriate project and DHS personnel when a deliverable is ready for review and provide the document online.
- C.1.4.2.4.3 The contractor shall post, store and maintain all deliverables and all documentation produced pursuant to this Task Order on the DHS SharePoint Portal. The Project Management Office (PMO) shall be provided access to the Portal.

PROCUREMENT SENSITIVE

- C.1.4.2.4.4 The contractor shall review deliverables at appropriate points in the development process to verify accuracy, completeness, and timeliness of each deliverable product.
- C.1.4.2.5 Enterprise Architecture (EA) Compliance: The contractor shall perform work in compliance with the EA Plan. The contractor shall support and comply with the standards and technologies of the DHS target architecture as described in the DHS EA Blueprint. The source website for the DHS EA Blueprint is provided in Section C-6.
- C.1.4.2.6 Maintenance and Outages: The contractor shall perform maintenance and other related activities that degrade or may degrade the performance of network environments, operating systems, databases and applications during outage periods that occur on weekends, federal holidays, or between the hours of 10:00 pm ET and 6:00 am ET on weekdays. The contractor shall avoid performing these maintenance and other activities during periods of the year that require continuous availability 24 hours each day. The COTR will notify the contractor a minimum of five business days prior to periods requiring continuous availability.
- C.1.4.2.7 Program Development: The contractor shall establish and maintain a program for the enhancement and improvement of information technology services. (CDRL C.1.4-2, Information Technology Improvement Program) The contractor shall baseline the existing systems and infrastructure for items such as configuration and performance metrics. As part of the baseline the contractor shall submit a plan defining timelines and operations, improvements based upon findings and supported by and compared to industry standards and metrics. The Plan shall be re-baselined every year. The contractor shall conduct an analysis every six months or as required of future programmatic and cost requirements for information technology services for the DHS. A written analysis and recommendations shall be provided to the COTR within five business days of completing the analysis (CDRL C.1.4-3, Future Programmatic and Cost Requirements for IT Services) The contractor must base the analysis upon an assessment of the current information technology capabilities, evaluations of the operations efficiency of information technology, considerations regarding the adequacy of information technology, market surveys of new and emerging technologies, and technological developments that could improve the cost effectiveness of the delivery of information technology services. The contractor shall also consider the following factors in the analysis:
- Known future requirements and program requirements established or stated by the DHS authorization language contained in Congressional Committee bills.
 - Appropriation language
 - Programs and directives received from the Department of Labor and Office of Management and Budget
 - Budgetary information
 - Information and requests received from other sources that utilize information technology services

PROCUREMENT SENSITIVE

- C.1.4.2.7.1 The contractor shall conduct an analysis that results in the identification of projects and initiatives necessary to support the needs of the DHS. The analysis shall also identify projects and initiatives that represent "State-of-the-Art" advancements in the capability supporting the DHS.
- C.1.4.2.8 Standard Operating Procedures: The contractor shall, within 30 business days after award of the Task Order, prepare and submit separate Standard Operating Procedures (SOPs) for each of the Functional Areas listed in paragraph C.1.5.1.2. (CDRL C.1.4-4, Standard Operating Procedures for Each Functional Area) The SOPs shall describe, at a minimum, the organization, methodology, approach, procedures, monitoring, auditing, problem escalation, documentation and reporting used by the contractor to accomplish the work required for the Functional Area. The COTR will review the Standard Operating Procedures and provide written comments to the contractor within ten business days following plan delivery to the COTR. The contractor shall address Government comments and deliver the final Standard Operating Procedures within five business days.
- C.1.4.2.9 Plans and Standard Operating Procedures: The contractor shall maintain and update all Plans and Standard Operating Procedures throughout the life of the Contract as changes occur or as directed by the COTR. The contractor shall submit in writing to the COTR changes in Plans and Standard Operating Procedures not less than 45 days prior to the desired date of implementation. The contractor shall not implement any changes until authorized in writing by the COTR. The contractor shall notify the Contracting Officer (CO) in writing of any changes that affect Task Order cost, Task Order requirements or terms and conditions and not implement these changes until receiving written approval from the CO.

C.1.5 LAYOUT OF SECTION C**C.1.5.1 Section C Contents**

- C.1.5.1.1 Section C Structure: The following bullets identify the structure of Section C in this Task Order:
- C-1 General Information
 - C-2 Definitions and Acronyms
 - C-3 Government-Furnished Property (GFP) and Services
 - C-4 Contractor-Furnished Property and Services
 - C-5 Scope of Work
 - C-6 Applicable Laws, Publications, and Forms
 - C-7 Technical Exhibits
 - C-8 Contract Data Requirements List (CDRL)

Paragraphs in Section C-1 all begin with the number "1," paragraphs in Section C-2 all begin with the number "2," and the pattern continues for the other sections.

- C.1.5.1.2 Functional Areas: Section C-5, Scope of Work, contains the Functional Areas which are organized into the following broad work categories:
- 5.1 Applications Management and Support Services
 - 5.2 Deployment Support

- 5.3 Infrastructure Engineering Services
- 5.4 Testing
- 5.5 Operations and Maintenance for End User Support
- 5.6 Video Teleconferencing
- 5.7 Satellite/Cable TV Operations
- 5.8 Phone and PBX Operations
- 5.9 Network Management Center (NMC)
- 5.10 Security Management Center (SMC)
- 5.11 Communications Security Management
- 5.12 Other Communications Operations
- 5.13 Wireless Management
- 5.14 Training
- 5.15 IT Continuity Management

C.1.5.2 Document Information

- C.1.5.2.1 **Pagination:** Pagination for all parts of the document is sequential with the prefix of "C" designating this as the Task Order Section of a Request for Proposal (RFP). Technical Exhibits have page numbers in relation to their TE title. For example, page three of TE C.5.2.-001 is shown as page number TE C.5.2.-001-03 to indicate that it is the third page of TE C.5.2.-001.
- C.1.5.2.2 **Technical Exhibits:** Technical Exhibits provide supplementary information in forms of text, tables, graphs, or maps. Any part of the Task Order may reference Technical Exhibits. Technical Exhibits for Section C have a 5-digit number that links them to a designated Task Order Section. For example, Technical Exhibit 5.3-002 is the second Technical Exhibit referenced from Sub-Functional Area 5.3. Section C-7 contains all Technical Exhibits except those maintained on the DHS Interactive website.
- C.1.5.2.3 **Contract Data Requirements List (CDRL):** The contractor shall compile historical data, prepare required reports, and submit information as specified by CDRLs in this Task Order. CDRLs may be referenced from any part of the Task Order. CDRLs for Section C have a two-digit number, which links them to a designated Task Order Section, e.g., CDRL C.5.3-1, is the first CDRL referenced in Section C.5.3. A listing of all CDRLs is located in Section C-8 of this Task Order.
- C.1.5.2.4 **Other Document Information:** As a rule, the term "contractor" refers to the contractor who is contracted to provide service on this Task Order. The term "third party contractor" refers to all other contractors with whom the contractor may interact with in the performance of their duties on this Task Order.

C.1.6 REQUIRED REPORTS AND MEETINGS

C.1.6.1 Task Order Administration

Workload Data Collection and Analysis: The contractor shall collect, analyze, maintain and provide to the COTR on a monthly basis and upon request workload data for all of the specific requirements identified in the Performance Requirements Summary (PRS) identified in TE C.1.6-001. The contractor shall provide to the COTR for approval a proposed format indicating workload data within 20 business days of Task Order award.

PROCUREMENT SENSITIVE

The contractor shall track all workload data by functional service area from Task Order start date, throughout the life of the Task Order, and provide a monthly report of the data to the COTR. The contractor shall analyze monthly data and determine the level and frequency of data necessary to capture, and provide recommended initiation or adjustments of systems and methods to accurately capture the necessary detail of workload data. In addition, the contractor shall provide the COTR an annual workload data report that summarizes the monthly workload data, identifies trends and statistical variations, and provides a logistical forecast for future years, by the last business day of each fiscal year. (CDRL C.1.6-1, Monthly and Annual Workload Data Reports)

C.1.6.1.1 Performance Requirements: The contractor shall attain the performance requirements depicted in TE C.1.6-001, the PRS. The contractor can provide suggestions to the COTR for refinement and adjustment of the performance requirements during the transition period. The COTR will evaluate the suggestions and notify the contractor in writing of any changes to the performance requirements, at least 20 business days prior to implementing the adjusted performance requirements.

C.1.6.2 Required Reports

C.1.6.2.1 Weekly Status Report: The contractor shall submit a Weekly Status Report to the COTR no later than 9:00 am each Tuesday, including one hard copy and an electronic file of the report. The Weekly Status Report shall include the following: (CDRL C.1.6-2, Weekly Status Report)

- Activities and accomplishments in each functional area during the previous week
- Task Order status (e.g., completed activities, current activities, activities planned for the following two weeks, issues or problems anticipated or encountered and proposed or implemented resolution) review of any associated project plan
- Project related issues/problems by functional area and actions taken/planned to resolve those issues/problems, and cost impact, if any
- Summary of any actual, planned or anticipated staffing changes
- Summary of any actual, planned or anticipated changes to procedures
- Summary of any actual or potential problems with procurement, asset management, and IT Infrastructure Library activities
- Summary of any issues regarding the achievement of performance standards
- Projected date when funds will be exhausted, if applicable
- Activities planned for the next week
- Actions required of DHS

C.1.6.2.2 Monthly Performance Summary Report: The contractor shall provide the COTR with a Monthly Performance Summary Report evaluating their performance in terms of the Performance Standards. The contractor shall submit the report no later than the fifth business day of each month and must include the quantitative data and calculations. The report must provide sufficient detail to allow auditing to the databases and other performance records maintained by the contractor. The report must provide the results of monitoring and simulations including the number of occurrences, the number of

PROCUREMENT SENSITIVE

successful occurrences and the calculated percentage of successful occurrences. The report must list the date, time and duration of outages interruptions or periods of degradation for applications, network environments, and databases. (CDRL C.1.6-3, Monthly Performance Summary Report)

C.1.6.2.3 Monthly Quality Control Report: The contractor shall submit a Quality Control Report to the COTR no later than the 10th business day of each month. The report shall summarize the information included in the Monthly Performance Summary Report and include a list of the tasks inspected, the number of completed tasks sampled, and the number of tasks determined by the Government as acceptably performed. The contractor shall provide a copy of the metrics data along with analysis to the COTR as part of the report. The contractor shall also include a summary of customer evaluations including the number received, a description of any evaluations with negative comments or complaints and the corrective actions taken. The contractor shall identify any tasks that fail to meet the performance standards specified in the Contract and shall describe the actions taken to correct performance. (CDRL C.1.6-4, Monthly Quality Control Report)

C.1.6.2.4 List of Plans: TE C.1.6-002 contains a comprehensive list of plans that the contractor shall develop, maintain, and update.

C.1.6.3 Required Meetings

The contractor's key staff shall attend meetings and provide status reports as outlined below. Status reports are due even in the event of the cancellation of meetings. Due to the parties' geographical locations, status meetings may be accomplished via telephone conferencing with the agreement of the Government.

C.1.6.3.1 Contract Administration Review (Monthly): The objective of the Contract Administration Review (CAR) is for DHS and the contractor to provide management consultation and assistance when resolving task order performance issues that will enhance efficiency and effectiveness and mission performance component-wide. Furthermore, the CAR will also ensure that O&M Task Order standards conform to DHS expectations.

C.1.6.3.1.1 The contractor's key staff (e.g., Program Manager and Project Managers) shall attend a monthly Contract Administration Review Status Meeting with representatives from the OCIO and Office of Procurement Operations – Information Technology Acquisition Center (OPO-ITAC). The contractor shall brief attendees on contractual issues that may impact Task Order performance or schedule. Action items from previous meetings (e.g., open action items, long-term action items, and action items closed during period) shall be addressed at meetings. The contractor shall prepare and deliver the monthly meeting agenda by close of business at least two business days prior to the scheduled meeting. The CAR agenda shall contain the following items: (CDRL C.1.6-5, Monthly Contract Administration Review Status Meeting Agenda)

- Action items from previous status meetings
- Open action items
- Long-term action items
- Action items closed during the period

PROCUREMENT SENSITIVE

- Items for discussion regarding status of funds expended
 - Items for discussion regarding leadership, services, process compliance and general assessments/comments
 - Items for discussion regarding customer service and performance evaluation
- C.1.6.3.1.2 The contractor shall prepare and distribute meeting minutes that document issues, decisions, assignments, and pending matters from the status meeting. (CDRL C.1.6-6, Monthly Contract Administration Review Status Meeting Minutes)
- C.1.6.3.2 Program Management Review and Report (Quarterly): The objective of the Program Management Review (PMR) is to determine the state of the O&M program in a systematic on-going manner to manage risks. The health of the O&M program will consist of assessments in the following subject areas:
- Leadership
 - Customer Support
 - Sound Business Judgment
 - Implementation of High Priority Actions
 - Policy Initiative
 - Statutory Compliance
 - Accuracy and Responsiveness Data Collection
- C.1.6.3.2.1 The contractor shall attend a quarterly Program Management Review (PMR) with representatives from the Office of the Chief Information Officer (OCIO) and the OPO-ITAC. The contractor shall prepare and deliver a meeting agenda. The contractor shall brief attendees on issues that may impact on-time completion of project milestones and deliverables. (CDRL C.1.6-7, Quarterly Program Management Review Agenda)
- C.1.6.3.2.2 The contractor shall provide a status report for each meeting. The report will provide highlights of the accomplishments for the reporting period, activities anticipated for the next reporting period, outstanding issues and recommendations for resolution, and resolved issues since the previous reporting period. (CDRL C.1.6-8, Quarterly Program Management Review Status Report)
- C.1.6.3.2.3 The contractor shall prepare and distribute a PMR status report with accompanying agenda documenting the status of issues, decisions, assignments, and pending matters from the PMR. The contractor shall prepare and deliver the quarterly status report and agenda by close of business at least two business days prior to the scheduled PMR. Each PMR status report and agenda shall contain a heading with the following information at a minimum:
- Contract number
 - Task order number
 - Contractor name, PM name and phone number
 - Date of Award
 - Period of Performance

- Award Amount

C.1.6.3.2.4 To assist DHS in compiling useful data on work performed under this contract, each status report shall contain the following support items:

- A brief, factual summary description of system operations activities
- A brief, factual summary of technical progress made for each task during the reporting period
- Customer support metrics (general user queries, FOIA requests received, completed, and in progress)
- Number of help-desk tickets opened, closed, and in progress
- Level of Effort Metrics (for each task/activity performed include Level of Effort, Available Range of Hours, Actual Hours Used, Contract Occurrences, and Occurrences Remaining) Any significant problems and their impacts, causes, proposed corrective actions, and the effect that such corrective actions will have on the accomplishments of the contract/task order objectives
- A status of overall project schedule and/or degree of completion of tasks/activities by time intervals
- Status of user support activities
- Significant concerns/risks/mitigation options and recommendations
- Summary of Change Requests, Problem Reports, responses, and solutions

C.1.6.3.2.5 The contractor shall prepare and distribute meeting minutes that document issues, decisions, assignments, and pending matters from the PMR. (CDRL C.1.6-9, Program Management Review Meeting Minutes)

C.1.6.4 Function Specific Reports and Documents

C.1.6.4.1 Security Violation Report: The contractor shall prepare and submit a Security Violation Report to CIO Management and the Information Systems Security Manager (ISSM) within one hour of determining the occurrence of a security violation. The report must include a description of the security violation, the name and telephone number of the point-of-contact, the time of the security violation, the extent of the security violation, the potential threat that could arise from the violation. It must also include any potential or real data compromise or system degradation resulting from the security violation, and recommendations regarding resolution or resolution actions undertaken to address the impact of the security violation. (CDRL C.1.6-10, Security Violation Report)

C.1.6.4.2 Architectural Compliance Plan: The contractor shall prepare and submit to the COTR no later than 30 business days after Task Order award an Architectural Compliance Plan that demonstrates that the technologies utilized by the contractor conform to the target architecture. The contractor shall update and submit the Architectural Compliance Plan no later than the first business day of May and November in subsequent performance periods. (CDRL C.1.6-11, Architectural Compliance Plan)

C.1.6.4.3 Program Development Report: The contractor shall submit a Program Development Report to the COTR on the last business day of April and

October. The contractor shall base the report upon the program for the enhancement and improvement of information technology services. The report shall identify projects and initiatives recommended to support the needs of the DHS. The report shall also identify projects and initiatives that represent "State-of-the-Art" advancements in the capability to support the DHS. (CDRL C.1.6-12, Program Development Report)

C.1.6.4.4 Network and Application Diagrams: The contractor shall maintain the Network and Application Diagrams. The contractor shall submit updated diagrams to the COTR semi-annually no later than the first business day in June and December. The submission shall consist of a separate electronic file for each network, entity relationship and application. The name of the network or application shall appear in the filename and the tab of the worksheet. (CDRL C.1.6-13, Network and Application Diagrams)

C.1.7 CONTRACTOR PERSONNEL

C.1.7.1 Key Personnel

C.1.7.1.1 Project Manager/Alternate(s): The contractor shall provide an on-site Project Manager (PM) who shall be responsible for the performance of the work and provide overall direction to the personnel working under this EAGLE Task Order. The name and resume of this person and of an alternate(s), who shall act for the manager when the on-site manager is absent, shall be designated in writing to the CO for approval prior to Task Order start date. The contractor shall provide a PM succession plan and keep it updated throughout the life of the Task Order. (CDRL C.1.7-1, Project Manager Succession Plan)

C.1.7.1.1.1 The PM shall be the contractor's authorized representative for the technical and administrative performance of all services required under this Task Order. The PM shall be the first Point of Contact (POC) for Task Order or administrative questions or difficulties that arise related to this Task Order. The PM shall be the primary point through which communications, work assignments, and technical direction flow between the Government and the contractor.

C.1.7.1.1.2 The PM, or designated alternate, shall be available during normal work hours to meet with the DHS, in person or as otherwise agreed upon by the DHS, to discuss problem areas within 30 minutes. After normal duty hours, the manager or alternate shall be available in accordance with DHS approved escalation protocol procedures and in the event of disaster recovery or Continuity of Operations event.

C.1.7.1.1.3 The PM shall be available during normal hours of operation, and during periods of no-notice emergencies, including localized acts of nature, accidents, and military or terrorist attacks, to plan, direct, and control the overall management and operational functions specified herein. The PM shall provide the necessary level of Task Order management and administrative oversight to achieve the quantitative and qualitative requirements of this Task Order.

C.1.7.1.1.4 The PM or alternate shall have full authority to act for the contractor on all matters relating to daily operation of this Task Order.

C.1.7.1.2 Other Key Personnel: The contractor shall provide key personnel as defined in TE C.1.7-001. In the event of key personnel departures, the contractor shall ensure support for all DHS requirements until permanent replacements are available. These replacements, on an acting or permanent basis, are required within 20 business days after the departure of a key individual. Final approval of key personnel is the responsibility of the DHS. The contractor shall provide a current succession plan for the key personnel positions. (CDRL C.1.7-2, Key Personnel Succession Plan)

C.1.7.2 Personnel Staffing

C.1.7.2.1 Employees: The contractor shall ensure that employees (other than managers) are competent in Operation and Maintenance of Information Technology systems to include project management, engineering, end user services, application services, infrastructure services, IT Continuity Management and security services.

C.1.7.2.2 Staffing Roster: The contractor shall submit a staffing roster to the COTR monthly, no later than the 15th business day of each month. The staffing roster shall list the names of each employee working on the Task Order. The roster shall include as a minimum, the Contract Number, contractor Name, Employee Primary User ID, Employee Last Name, Employee First Name, Current DHS Security Classification, Work Location, Office Number, Phone Number, Emergency Point of Contact, Emergency Point of Contact Phone Number, Primary Project Number, and Secondary Project Number for each employee. The contractor shall notify the COTR of any additions, deletions, or changes within one business day after the change(s). (CDRL C.1.7-3, Staffing Roster)

C.1.7.2.2.1 If the Contracting Office identifies an employee to the contractor as a potential threat to the health, safety, security, general well being, or operational mission of the DHS, the contractor shall not employ persons for work on this Task Order. The Government reserves the right to remove such persons. Where reading, understanding, and discussing safety and environmental warnings are an integral part of a contract employee's duties, that employee must be able to understand, read, write, and speak English.

C.1.7.2.2.2 The contractor shall not employ any person who is an employee of the United States (U.S.) Government if employing that person would create a conflict of interest. Contractor personnel shall meet relevant DHS security requirements as identified in DHS regulations and orders. The contractor shall provide a sufficient number of personnel possessing the skills, knowledge, training, and security clearance to perform the services required by this Task Order for each specific functional area.

C.1.7.2.2.3 The contractor shall maintain agreed upon staffing levels at or above 95% for the life of the Task Order.

C.1.7.2.3 Subcontractor Personnel: Subcontractors must comply with all employee provisions identified in the Task Order.

C.1.7.3 Personnel Training

C.1.7.3.1 Personnel Proficiency: All contractor Personnel shall be trained, competent, and skilled in the performance of their assigned work. The contractor shall ensure they provide any necessary refresher training to their

PROCUREMENT SENSITIVE

employees in order to maintain required certification levels and proficiency to perform assigned duties.

C.1.7.3.2 **Employee Training:** The contractor shall be responsible for all new and recurring training of contractor personnel in such a manner as to ensure performance of all tasks required by this Task Order. The contractor shall provide the Government an employee-training plan, identifying both initial and recurring training, including any DHS required training the contractor envisions to ensure personnel remain current in their areas of responsibility. (CDRL C.1.7-4, Employee Training Plan)

C.1.7.3.2.1 The contractor shall conduct or provide to their employees detailed instruction on Government statutes, regulations, policies, and guidelines in areas such as employee conduct ethics, safety, security, health, fire prevention, and the environment as they pertain to the operations specified in this Task Order. This contractor shall conduct or provide this training upon initial employee hire, annually, and as directed by the Government. The contractor shall ensure all new employees attend DHS Security Education, Training, and Awareness training as described in DHS Management Directive (MD) 11053.

C.1.7.3.2.2 The contractor shall develop, implement, and maintain written guidelines or standard procedures necessary for effective accomplishment of Task Order requirements. The contractor shall comply with all Privacy Act and other regulations governing personal and private information.

C.1.7.3.2.3 The contractor shall conduct any remediation training necessary to ensure competency of contractor employees. The contractor shall conduct remediation training in a manner to minimize adverse impact on contract performance and interruption of normal business processes.

C.1.7.3.3 **Knowledge Management:** The contractor shall develop, maintain, update, and implement a knowledge management system for retention and referencing of processes, procedures, best practices, lessons learned, and any other information that can be used to enhance IT operations. The knowledge management system shall reside on the DHS intranet and be accessible to DHS IT management and the contractor's personnel.

C.1.7.4 Personnel Security Requirements

C.1.7.4.1 **Access Requirements:** The Government has the right to restrict and control access to its facilities, property, and data, including those identified in this Task Order. The contractor shall ensure all contractor employees pass DHS suitability screening requirements, and receive an Entry on Duty (EOD) date from the DHS Office of Security, prior to beginning performance. Personnel requiring clearances under the task order will not be eligible for billing to the Government prior to EOD determination. Contractor administrative/support staff personnel not requiring EOD determinations are available for billing to the government upon task order award. The Government will be the final authority in determining access privileges. The Government's exercise of its right to grant and revoke the access of particular individual(s) to its facilities, or parts thereof, shall not constitute a breach or change to the Task Order. Regardless of whether the contractor employs said individual(s), and regardless of whether

it precludes said individual(s) from performing work under the resulting Task Order.

- C.1.7.4.2 **Personnel Security Clearances:** Much of the scope of work required within the Task Order requires access to classified data and/or classified areas. Personnel requiring access to classified data and/or classified areas are required to have a current Secret, Top Secret, or Top Secret/Sensitive Compartmentalized Information (TS/SCI) access authorization clearance prior to the commencement of the work. All access authorization clearances must be active and in place prior to the start of any work on any tasking within this Task Order which requires a clearance. DHS has final authority on determining an individual's security clearance eligibility. The contractor shall submit requests for security clearances for staff. All personnel assigned to functions described in this document must be U.S. Citizens. Contractor administrative or technical personnel who will not require access to classified areas or information will not require access authorizations. The contractor shall identify, on the contractor Employee Roster, those employees who require access to restricted areas or classified information, and shall obtain and maintain the appropriate security clearances as identified in this solicitation.
- C.1.7.4.3 **Personnel Access Badges:** The contractor shall ensure all contractor personnel requiring access authorization have valid badges and shall collect and return badges for employees: 1) who are no longer working on the Task Order; 2) who no longer require access; 3) upon expiration of badges; or 4) when the Task Order expires or terminates. The contractor shall return badges to the appropriate DHS security office. The contractor shall notify the COTR by e-mail within one hour of any of these occurrences and return the badges to the appropriate DHS security office.
- C.1.7.4.4 **Personnel Separation:** The contractor shall ensure all contractor personnel who are no longer working on the Task Order, or when the Task Order expires or terminates, shall comply with DHS established contract employee separation procedures.

C.1.8 CONTRACTOR INTERFACES

C.1.8.1 Personnel Performing Security/Continuity/Quality

- C.1.8.1.1 **Coordination with Other Performing Activities:** The contractor shall coordinate with Government and third party contractor personnel performing required services in areas associated with the requirements of this Task Order. Some examples of the required services are personnel performing security and continuity functions, audits, inspections, delivery services, construction, and telecommunication services.
- C.1.8.1.1.1 The DHS COTR will facilitate initial contact between the contractor and other third party contractors performing work for DHS, as necessary. The contractor shall provide support services to other third party contractors within the scope of this Task Order as required by the Government.
- C.1.8.1.1.2 The contractor shall notify the COTR in writing of unresolved disputes in receiving support from or providing support to customers or other third party contractors within two business days from the time the dispute occurs, unless otherwise specified in SLAs. (CDRL C.1.8-1 Unresolved Dispute Information)

PROCUREMENT SENSITIVE

C.1.8.1.2 Inspection by Government Agencies: Per FAR 52.246-6 the contractor shall provide access to and cooperate with Government personnel conducting official inspections and surveys. Government personnel other than CO or Quality Assurance Personnel may periodically observe contractor operations. However, the CO is the only person that may obligate the Government or direct contractor operations. The following list identifies agencies performing inspections:

- Quality Assurance Evaluators
- Property Inspectors
- The Inspector General (IG)
- Other offices in the DHS such as the Facilities and Services Department
- Other federal agencies such as the Occupational Safety and Health Administration (OSHA)
- Environmental Protection Agency (EPA)
- Government Accountability Office (GAO)
- General Services Administration (GSA)
- Defense Contracting Audit Agency (DCAA)
- DHS Office of Security

C.1.9 QUALITY ASSURANCE AND QUALITY CONTROL**C.1.9.1 Quality Assurance**

C.1.9.1.1 Quality Assurance: The Government will evaluate the contractor's performance under this Task Order. For those tasks listed in the Performance Requirements Summary (PRS), TE C.1.6-001, the Quality Assurance Personnel (QAP) or evaluators will follow the methods of surveillance specified in this Task Order. The Government will conduct surveillance according to standard inspection procedures or other Task Order provisions. Any action taken by the CO because of surveillance will be according to the terms and conditions of this Task Order.

C.1.9.1.1.1 The COTR will record the results of surveillance. The COTR will provide copies of surveillance reports to the contractor. The contractor shall sign the surveillance reports and return them to the COTR within two business days. The contractor shall annotate on the signed copy any exceptions or disagreement with the surveillance report.

C.1.9.2 Quality Control

C.1.9.2.1 Quality Control: The contractor shall provide a revision to the Quality Control Plan submitted as part of the Contractor's proposal, to the COTR for approval within 20 business days of Task Order award. The plan shall include a detailed description of the processes used during performance to ensure the services meet or exceed the requirements of the Task Order and contract. The plan shall address each mission essential objective of the PRS, and all others considered necessary to meet the Task Order requirements. The plan shall systematically provide for early identification of nonconforming services, develop, maintain, update and implement metrics to track performance trends, detail corrective action plans including milestones. (CDRL C.1.9-1, Quality Control Plan)

PROCUREMENT SENSITIVE

- C.1.9.2.1.1 Revisions to the Quality Control Plan may be required at any time. The contractor shall make appropriate revisions and obtain acceptance of the revised plan from the COTR. The contractor shall provide revised copies of the Quality Control Plan to the COTR and Quality Assurance Personnel (QAP) upon approval from the COTR.
- C.1.9.2.1.2 The contractor shall maintain records of the work sampled and the results of the inspection for each discrete sample. The records shall allow the COTR to review each discrete sample and validate the determinations made during the performance of Quality Control.
- C.1.9.2.2 Customer Evaluation: The contractor shall create, maintain, and update a customer evaluation plan to include identifying and implementing customer satisfaction improvements, as part of the Quality Control Plan. The contractor's plan shall adhere to the ITIL framework for Service Delivery and Service Support. The contractor shall submit the final plan to the COTR for approval no later than 20 business days after Task Order award. The COTR may require changes to the plan at any time during the life of the Task Order. The contractor shall submit their changes within 20 business days of the requested change. (CDRL C.1.9-2, Customer Evaluation Plan)

C.1.10 PROPERTY CONTROL

The contractor's property control procedures shall comply with FAR 52.245-5, Government Property (Cost-Reimbursement, Time-and-Material, or Labor-Hour Contracts).

C.1.11 OPERATING ENVIRONMENT**C.1.11.1 Operating Hours**

- C.1.11.1.1 Hours of Operation and Government Holidays: The normal hours of operation are 8:00 A.M. to 5:00 P.M. Various functions within the Information Technology Services Office require 7X24X365 (366 for leap years) coverage as addressed in Table 2 below and in section C.5.

Table 2 – Operating Hours

Functional Service Area	Work Hours	Required Security Clearances
Application and Management Support Services	8 A.M to 5 P.M. ¹	Suitability, Secret, Top Secret, Top Secret/SCI
Deployment Support	8 A.M to 5 P.M.	Suitability, Secret, Top Secret, Top Secret/SCI
Infrastructure Engineering	8 A.M to 5 P.M.	Suitability, Secret, Top Secret, Top Secret/SCI
Testing	8 A.M to 5 P.M.	Suitability, Secret, Top Secret, Top Secret/SCI
Operations and Maintenance for End User Support: Help Desk	7X24X365 (366 for leap years) 5x12 desk side support operations,	Suitability, Secret, Top Secret, Top Secret/SCI

¹ Monitoring is 24X7X365 (366 for leap years)

PROCUREMENT SENSITIVE

Functional Service Area	Work Hours	Required Security Clearances
Desk Side Support	with provision that designated VIPs are entitled to on call support	
Video Teleconferencing	8 A.M to 5 P.M. ²	Suitability, Secret, Top Secret, Top Secret/SCI
Satellite/Cable TV Operations	8 A.M to 5 P.M.	Suitability, Secret, Top Secret, Top Secret/SCI
Phone and PBX Operations	8 A.M to 5 P.M. ³	Suitability, Secret, Top Secret, Top Secret/SCI
Network Management Center	7X24X365 (366 for leap years)	Suitability, Secret, Top Secret, Top Secret/SCI
Security Management Center	7X24X365 (366 for leap years)	Suitability, Secret, Top Secret, Top Secret/SCI
Communications Security (COMSEC) Management	7X24X365 (366 for leap years)	Suitability, Secret, Top Secret, Top Secret/SCI
Continuity Management	8 A.M to 5 P.M.	Suitability, Secret, Top Secret, Top Secret/SCI

C.1.11.1.2 The days specified in Table 3 below are the legal public holidays. The contractor will adhere to the Government holiday schedule. If the holiday falls on a Saturday, the recognized Federal holiday is the preceding Friday. If the holiday falls on a Sunday, the recognized Federal holiday is the following Monday.

Table 3 – Federal Holidays

Holiday	Date
New Year's Day	1st day of January
Martin Luther King's Birthday	3rd Monday in January
President's Day	3rd Monday in February
Memorial Day	Last Monday in May
Independence Day	4th of July
Labor Day	1st Monday in September
Columbus Day	2nd Monday in October
Veteran's Day	11th of November
Thanksgiving Day	4th Thursday in November
Christmas Day	25th of December

² Limited coverage required 24X7X365 (366 for leap years)

³ Limited support required 24X7X365 (366 for leap years)

C.1.11.1.3 Hours of Operation Other Than Normal: There will be mission situations that require the contractor to work other than normal hours. Such scheduling may require accomplishment of contractor work at times other than normal operation hours; the CO, or appropriate Government representative, will approve in writing work outside normal operation hours when required. Overtime shall only be permitted when approved in writing by the CO.

C.1.11.2 Operations Under Adverse Conditions

C.1.11.2.1 Emergencies and Special Events: The contractor shall respond to emergencies as governed by procedures prescribed by the DHS in accordance with its applicable statutes, regulations, orders, policies, and guidelines. The DHS may have the need to extend contractor tour of duties, hours, and bringing on additional cleared contractor personnel in the event of a major emergency. The contractor shall provide surge personnel support, as directed by the CO, in response to emergencies or special events. Emergencies may consist of natural disasters, terrorist threats or events, elevation of the DHS threat level or as designated by the Department. In the event of any emergency, the CO may initiate contractor action by a verbal authorization. The CO will define a task order in a timely manner or as time permits after the emergency is contained or resolved.

C.1.11.2.1.1 Extreme weather conditions and natural disasters (such as tornados, flooding, snow, and ice) may warrant temporary office evacuation or office closure. The contractor shall respond to extreme weather conditions according to DHS direction, and shall inform all employees of these instructions. During normal duty hours, the normal chain of management will provide notification of facility closures. During non-duty hours, local radio and television channels will provide notification. Facility closings shall in no way interfere with the contractor operation and maintenance of the critical systems. All contractor employees identified as essential personnel shall remain on duty or report for duty in accordance with the Emergency Situations and relevant Continuity of Operations (COOP), IT Contingency, IT Disaster Recovery/Business Continuity Plan.

C.1.11.2.1.2 The contractor shall participate in all scheduled and unscheduled fire drills, Shelter in Place, and other scheduled safety and emergency-training exercises, which may necessitate interrupted services unless directed otherwise. The Government will consider such interruptions when assessing contractor performance for the affected period.

C.1.11.2.2 Building Occupant Emergency Plan Compliance: Contractor personnel shall comply with all building occupant emergency plan activities such as building evacuations and shelter in place.

C.1.11.2.3 Personnel Response to IT Continuity Events: Key contractor personnel and contractor personnel with critical skills shall report to and perform duties at alternate sites during IT continuity events, as directed by the Government. The contractor shall provide personnel resources to respond to IT continuity events. The contractor should consider such things as cross-training and providing personnel who would be able to respond from outside the metropolitan area (i.e. individual with appropriate skill sets who would be unaffected by issues in the Baltimore-Washington metropolitan area).

PROCUREMENT SENSITIVE

C.1.11.2.4 Performance of Services during Crisis: The following services are essential during crises declared by the DHS Secretary or the President of the United States. All basic services and operations will continue as directed by the COTR. The contractor shall submit an essential personnel list, to include designated emergency POCs, to the COTR within ten business days after Task Order start and shall update monthly for changes throughout the life of the Task Order. The list shall contain the individual's name, address, home phone number, beeper number or cell phone number, security clearance, and duty title. Upon notification of a crisis by the COTR, the contractor shall perform the essential services identified in the CIO COOP Implementation Plan. The COTR will direct implementation of Services under this provision at any time as required to meet mission requirements. (CDRL C.1.11-1, Essential Personnel Contact List)

C.1.11.3 Travel

C.1.11.3.1 Authorization and Restrictions: Contractor personnel may be required to travel to support the requirements of this Task Order. Long distance and local travel may be required in the Continental United States (CONUS). The Government expects the contractor to have a facility within the Washington DC Metropolitan area. The Government will not reimburse local travel within a 50-mile radius from the contractor's facility or the contractor's assigned duty station. This includes travel, subsistence, and associated labor charges for travel time. The Government will not reimburse travel performed for personal convenience and daily travel to and from work at the contractor's facility. The Government will authorize travel, subsistence, and associated labor charges for travel beyond a 50-mile radius of the contractor's facility or assigned duty station; HOWEVER, the COTR shall previously approve all travel outside the Washington DC Metropolitan area. The Government will reimburse authorized travel in accordance with the Federal Travel Regulation. The Government will not reimburse travel without prior approval from the COTR. The contractor's request for travel shall be in writing or electronic as directed by the COTR and contain the dates, locations and estimated costs of the travel.

C.1.11.3.2 Costs: The contractor shall, to the maximum extent practicable, minimize overall travel costs by taking advantage of discounted airfare rates available through advance purchase. Charges associated with itinerary changes and cancellations under nonrefundable airline tickets are reimbursable as long as the changes are driven by the work requirement. Costs associated with Contractor travel shall be in accordance with FAR Part 31.205-46, Travel Costs and applicable Federal Travel Regulation. If any travel arrangements cause additional costs to the contract that exceed those previously negotiated, written approval by contract modification issued by the CO is required prior to undertaking such travel. (CDRL C.1.11-2 Travel Requests)

C.1.12 CONTRACT TRANSITION**C.1.12.1 Transition and Phase In**

C.1.12.1.1 Transition Plan: The contractor shall provide a revision to the Transition and Phase-In Plan submitted as part of the Contractor's proposal, to the COTR for approval within 20 business days of Task Order award. The Transition Plan shall include milestones, which will indicate how the contractor plans to migrate all existing services from the current providers, add new services, and

PROCUREMENT SENSITIVE

minimizing operational and project impacts, and when properly trained, qualified, and certified personnel will accomplish full assumption of all requirements identified in the Task Order by the completion of the transition period. The transition plan shall include start up, mobilization schedule, and transition depicting the chronological sequence of events, which the contractor shall accomplish beginning on Task Order start date. The contractor shall incorporate termination dates of existing contractor performance periods and DHS planned major project dates into the transition plan. (See TE C.1.12-001, Phased Termination Dates and TE C.1.12-002, DHS Projects). The contractor shall demonstrate the ability to quickly staff the requirement in order to meet the transition schedules dictated by the expiring Task Orders. The contractor shall demonstrate the ability to ensure proposed personnel are vetted to ensure they meet DHS suitability and security clearance process (See paragraphs C.1.7.4.1 and C.1.7.4.2) thus aiding in a more expedient process. The contractor shall perform analyses and planning to develop the plans for transitioning the DHS services and sites to their operations. The guiding principle for this will be the use of innovation in developing and providing functionality to include transition and consolidation strategies for DHS assets both present and future, and the use of COTS application whenever advantageous to the Government. The Transition Plan shall include the plans for migrating assets, data, and services. The overall transition period shall not exceed 12 months. (CDRL C.1.12-1, Contract Transition Plan)

C.1.12.1.2 Transition Tasks: Starting the first day of the transition period, the contractor shall ensure necessary personnel actions, appropriate training, (including any required certifications), as well as non-personnel considerations such as materials and supplies, equipment, facilities, sub-contracts, leases, environmental issues, safety and security, etc. are accomplished in accordance with the accepted transition plan. The contractor shall perform relocations of equipment as directed by the COTR.

C.1.12.1.3 Transition Ramp-up: The contractor shall fulfill the requirements (as applicable) in sections C.1.12.1.1 and C.1.12.1.2 within the first six months of the Task Order award. During this timeframe the contractor shall identify an implementation strategy and perform critical tasks to expediently obtain employee security clearances; recruit and staff required positions; conduct a joint inventory of Government Furnished Equipment (GFE) and IT assets; establish management processes and controls; and other tasks the contractor deems necessary to initiate pre-transition and transition tasks within the first six months of Task Order award. A subset of these tasks may be accomplished during both the transition ramp-up and the base year of the Task Order award.

C.1.12.2 Phase Out

C.1.12.2.1 Inventory: At the Phase-out of this Task Order the contractor and Government shall conduct a joint inventory assessment of property accounts for the contractor's staff (i.e. hand receipts of cell phones, blackberries, etc.) to ensure a full accounting of all Government property. The Government will hold the contractor liable for any damaged or lost equipment, and the contractor shall ensure all other Government equipment is in working order.

C.1.12.2.2 Observations: The contractor shall permit the successor contractor (and the successor contractor's employees) to observe and become familiar with

any and all operations specified in this Task Order for a minimum of 90 business days, or for a COTR specified timeframe, prior to the expiration or termination of the Task Order.

- C.1.12.2.3 Maintenance of Systems, Files, and Data: The contractor shall maintain the full operational status of all Government systems and equipment, and continue all current work in progress until the successor contractor assumes full operational responsibility. The contractor shall not destroy, delete, or otherwise dispose of any files or data upon expiration or termination of the Task Order, without prior permission from the COTR.
- C.1.12.2.4 Cooperation: The contractor shall fully cooperate with the successor contractor and the Government so as not to interfere with their work or duties.

C.2 DEFINITIONS AND ACRONYMS

C.2.1 DEFINITIONS

The definitions set forth below are those unique or used in this Task Order. Definitions for technical terms or words which are included in this Task Order can be found in the technical documents referenced in the individual functional areas of the Task Order. The definitions provided below are oriented to DHS's Task Order. In many cases definitions are specific by situation. The total listing of definitions is not all-inclusive, but it has been derived from official publications (e.g., regulations and technical manuals and industry standards) when available.

Note: In the event of a conflict between any definition in this section and a comparable definition in the Federal Acquisition Regulation, the latter shall prevail.

A LAN: The DHS unclassified network

Acceptance, Approved (as Directed, as Permitted, as Required): Where these words or words of similar import are used, it shall be understood that the direction, requirement, permission, approval, or acceptance of the Contracting Officer (CO) or Contracting Officer's Technical Representative (COTR) is intended, unless stated otherwise.

Acceptable Quantity Level (AQL): Represents the required success rate for each output that comprises the total workload. The AQL is reasonable to allow for the possibility of unexpected problems that prevent some outputs from meeting the requirements of the performance standards. The AQL is a percentage value of the number of performances of each output that must adhere to the performance standard set for that output. AQLs are determined based on agency directives or historical records of Government performance.

Accountability: The obligation of both the contractor and the Government to fulfill the requirements of this Task Order. This includes item such as the contractor's responsibility to maintain accurate and complete records of documents, funds and property.

Accreditation: The formal declaration by a Designated Approving Authority (DAA) that an information system (IS) is approved to operate in a particular security mode using a prescribed set of safeguards to an acceptable level of risk.

Approval: The process through which the Government provides authorization to the contractor to proceed with an action. An approved authorization must be in writing.

Availability: A measure of the degree to which an item is in an operable and committable state at the start of any task or mission, when the task or mission is called for at an unknown (random) point in time.

Authentication: A security process designed to establish the validity of a transmission, message or originator or to verify an individual's eligibility to receive specific categories of information.

Authorization: The process of granting or denying access to system objects based on an individual or entities identities, roles or other qualifying characteristics (e.g. clearance level).

Availability period: The amount of time the system(s), or the total system, is functioning so that the customer can get work done.

PROCUREMENT SENSITIVE

Baseline: A specification or product that has been formally reviewed and agreed upon, and thereafter serves as the basis for further development and can be changed only through formal change-control procedures or a type of procedure such as configuration management (CM).

Basic Rate Interface (BRI): A level of service within the Integrated Services Digital Network (ISDN). The BRI includes a number of B-channels and a D-channel; B-channels carry data, voice, and other services and the D-channel carries control and signaling information.

Biennially: One time every two years

Bi-monthly: One time every two months

Bi-weekly: One time every two weeks

C LAN: The DHS Top Secret network

Certificate: Digital documents attesting to the binding of a public key to an individual or other entity. They allow verification of the claim that a given public key does in fact belong to a given individual. Certificates, also called digital certificates, are issued by a Certificate Authority and contain the public key and other identification information relating to the certificate requester.

Certification: Certification is the comprehensive evaluation of the technical and non-technical security features of an Information System (IS) and other safeguards, made in support of the accreditation process, to establish the extent to which a particular design and implementation meets a set of specified security requirements.

Certified Information Systems Security Professional (CISSP): A professional certification in information systems security administered by the International Information Systems Security Certification Consortium (ISC)²®

Channel Service Unit/Data Service Unit (CSU/DSU): A digital-interface device used to connect a router to a digital circuit such as a T1 or T3 line.

Classified: Documents, data, information, systems, products, services, items, etc for which access is limited to those persons having a "need to know" and appropriate security clearance.

Clearance: Authority permitting individuals cooperating in DHS work, and having a legitimate interest therein, access to classified technical information, material, or equipment or admission to restricted areas or facilities where such information or material is located.

Commercial Off The Shelf (COTS): Describes software or hardware products that are ready-made and available for sale to the general public.

Common Operating Environment (COE): A listing of components (hardware and software) that captures the concept of a common or shared operating environment across an enterprise or organization; provides a standard for the organization to be common operating environment (COE) compliant.

Common Vulnerabilities and Exposures (CVE): An index of standardized names for vulnerabilities and other information security exposures. CVE aims to standardize the names for all publicly known vulnerabilities and security exposures. The CVE database is operated by the MITRE corporation, and is sponsored by the Department of Homeland Security.

PROCUREMENT SENSITIVE

Confidentiality: Assurance that information is not disclosed to unauthorized entities or processes.

Configuration Management (CM): A discipline applying technical and administrative direction and surveillance to: (a) identify and document the functional and physical characteristics of a particular item, system, etc; (b) control changes of those characteristics; and (c) record and report changes to processing and implementation status.

Conflict of Interest (COI): According to DHS Clause 1337, "Conflict of interest means that because of other activities or relationships with other persons or organizations, a person or organization is unable or potentially unable to render impartial assistance or advice to the Government, that the person's or organization's objectivity in performing the Task Order is or might be otherwise impaired, or that the person or organization has or might acquire an unfair competitive advantage."

Configuration: The functional or physical characteristics of equipment, systems, hardware or software set forth in technical documentation and achieved in a product.

Conservation: The protection, improvement, and use of natural resources according to principles that will provide optimum public benefit and support of DHS's mission.

Continuity of Operations (COOP). The COOP focuses on restoring and organization's (usually headquarters element) essential functions at an alternate site and performing those functions for up to 30 days before returning to normal operations. Because a COOP addresses headquarters-level issues, it is developed and executed independently from the Business Continuity Plan (BCP). Implementation of a viable COOP capability is mandated by PDD 67, Enduring Constitutional Governmental and Continuity of Government Operations. FEMA, the Federal Government's executive agent for COOP, provides COOP guidance in FPC 65, Federal Executive Branch Continuity of Operations. Standard elements of a COOP include Delegation of Authority statements, Orders of Succession, and Vital Records and Databases. Because the COOP emphasizes the recovery of an organization's operational capability at an alternate site, the plan does not necessarily include IT operations. In addition, minor disruptions that do not required relocation to an alternate site are typically not addressed. However, COOP may include the BCP, Business Resource Plan (BRP), and disaster recovery plan as appendices. (Source: NIST 800-34, Contingency Planning for Information Systems)

Contract Data Requirements List (CDRL). Data required to be submitted by the contractor to the Government. A proper and correct submission of a CDRL is evidenced by the following criteria: completeness, accuracy of data, preparation in accordance with applicable mandatory publication or other prescribing document, signature or initials by the certifying official, and correct and timely turn-in or distribution.

Contract Modification: Any written alteration in the terms and conditions of the contract or Task Order, such as specifications, delivery point, rate of delivery, Task Order period, price, quantity, or other Task Order provisions.

Contracting Officer (CO): An individual appointed in accordance with procedures prescribed by the Federal Acquisition Regulation with the authority to enter into, administer, and terminate contracts and make related determinations and findings.

Contracting Officer's Technical Representative (COTR): The individual or individuals appointed by the Contracting Officer to act as the authorized Government representative and to oversee contractor performance.

Contractor: The term contractor, as used herein, refers to the principle/prime contractor.

Contractor Furnished Equipment (CFE): That equipment that the contractor includes in its offer in order to perform the requirements of the Task Order, and that is not covered under Government-Furnished Property (GFP).

Contractor-Furnished Property (CFP): Equipment and facilities provided by the Contractor to perform the Task Order requirements.

Corrective Action: Consists of those efforts required to correct reported deficiencies and mitigate reoccurrence of defects.

Critical Design Review (CDR): The CDR is a multi-disciplined technical review to ensure that the system under review can proceed into system fabrication, demonstration, and test; and can meet the stated performance requirements within cost (program budget), schedule (program schedule), risk, and other system constraints. Generally this review assesses the system final design as captured in product specifications for each configuration item in the system, and ensures that each product in the product baseline has been captured in the detailed design documentation.

Customer: Any recipient of a service described in Section 5, Specific Work Requirements of the Task Order.

Damage: A condition that impairs either value or utility of an article; may occur in varying degrees. Property may be damaged in appearance or in expected useful life without rendering it unserviceable or less useful. Damage also shows partial non-serviceability. Usually implies that damage is the result of some act or omission.

Data Integrity: Condition that exists when data is unchanged from its source and has not been accidentally or maliciously modified, altered or destroyed.

Database: A collection of records, in one or more files, which are often coded for rapid search and retrieval via computer.

Defense Message System (DMS): The system of record for organizational messaging used by the Department of Defense. It is a modified commercial-off-the-shelf (COTS) application that provides multimedia messaging, directory, and security services. DMS uses the underlying Defense Information Infrastructure (DII) network and security services in conjunction with National Security Agency (NSA) security products.

Degauss: Destroy information contained in magnetic media by subjecting that media to high-intensity alternating magnetic fields, following which the magnetic fields slowly decrease.

Degausser: Electrical device or hand-held permanent magnet that can generate a high intensity magnetic field to sanitize magnetic storage media.

Denial of Service: Any action or series of actions that prevent any part of a system from functioning in accordance with its intended purpose. This includes any action that causes unauthorized destruction, modification or delay of service.

Desktop Administration: Services provided in the operation and maintenance of an individual's desktop computer. This includes services such as installation of a new system, hardware upgrades, relocation and removal of hardware, installation and upgrade of software applications and operating system. It also includes configuration of hardware and software, backup and restore, performance monitoring and tuning, problem tracking and error detection, needs assessment, procurement, disposal, and inventory management.

PROCUREMENT SENSITIVE

Desktop Computer: Distributed computing resource, either networked or standalone, consisting of a CPU, keyboard, monitor, and a screen manipulation device, such as a mouse. This typically includes PCs, Apple Macintoshes, UNIX based workstations, X-terminals and other terminals. This definition excludes mainframes, supercomputers and midrange computers.

Desktop Configuration: The hardware and software characteristics associated with a desktop computer (UNIX, PC, Macintosh, and X-Terminal). Hardware characteristics include: CPU, RAM, amount of disk storage, size of monitor, cards installed in the system unit, and devices attached directly to the system unit. Software characteristics include: identification of COTs application software in use on the workstation, operating system, and a description of any commonly distributed custom applications.

Digital Video Disk (DVD): An optical disc storage media format that can be used for data storage.

Discrepancy: A variance between contractually required and actual performance.

Disposal: The disposition of excess assets (including intellectual and real property, industrial and personal property) by the Government in accordance with DHS regulations and the FAR.

Document Type Definition (DTD): A DTD defines the legal building blocks of an XML document. It defines the document structure with a list of legal elements.

Downtime: The amount of time when an end user's access to network services is impaired. Downtime for each incident shall be the period between the time of failure and the time that the system is returned to the Government fully operational.

Due Diligence: The purpose of Due Diligence is for the contractor to validate the inventory and environment portrayed during the master Task Order award and account for any changes that have occurred between Task Order award and the Task Order start. If there is a discrepancy found which exceeds parameters, then a due diligence price adjustment will be submitted. The Due Diligence period shall be limited to not more than 20 business days unless a longer period is granted by the CO.

E-Government: One of the five key elements of the President's Management Agenda designed to make better use of information technology (IT) investments to eliminate billions of dollars of wasteful Federal spending, reduce Government's paperwork burden on citizens and businesses, and improve Government response time to citizens. A key goal is for citizens to be able to access Government services and information within three "clicks," when using the Internet.

Electronic Signatures In Global and National Commerce Act (ESIGN): A U.S. Code that facilitates the use of electronic records and signatures in interstate and foreign commerce by ensuring the validity and legal effect of contracts entered into electronically.

Emergency: The reporting of sudden, usually unforeseen, occurrences where life or property are in immediate danger and require immediate action.

Employee: An employee includes both contractor employees and subcontract employees.

Enterprise Acquisition Gateway for Leading Edge Solutions (EAGLE): The DHS contracts for Information Technology (IT) support services that will enable DHS business and program units to accomplish their mission objectives.

PROCUREMENT SENSITIVE

Enterprise Architecture (EA): A description including graphics of the systems and interconnections providing for or supporting various functions. EA defines the physical connection, location, and identification of such key nodes as circuit and network platforms, and allocates system and component performance parameters. Shows how multiple systems within a domain or an operational scenario link and interoperate, and may describe the internal construction or operations of particular systems in the systems architecture.

Enterprise Change Control Board (ECCB): The board responsible for reviewing any incoming change requests, including both enhancements and defects. The first step focuses on triage, where high severity defects are assigned to the support team so that they can be dealt with by a hot fix. Lower severity defects and all enhancement requests will be evaluated by the board in order to determine which change requests are to be acted upon and which systems will be affected so that the change request may be assigned appropriately.

Facilities: Property used for production, maintenance, research, development or testing. It includes plant equipment and real property. It does not include material, special test equipment, special tooling or agency peculiar property.

FAR: Federal Acquisition Regulation.

FASTLANE: FASTLANE is a high speed asynchronous transfer mode (ATM) encryptor for local and wide area network multimedia applications (i.e., voice, video, data, and imagery). FASTLANE supports permanent and switched virtual circuits, point-to-point and point-to-multi-point, simplex and duplex connections. It provides authentication and end-to-end protection of user information up to the Top Secret/Sensitive Compartmented Information level.

Fiscal Year (FY): A period of 12 months beginning 1 October and ending 30 September of the following year. Fiscal year is designated by the calendar year in which it ends.

Government Furnished Equipment (GFE): A term used in this Task Order to mean equipment in the possession of, or directly acquired by, the Government and subsequently made available for the use by the contractor solely in the performance of this Task Order.

Government Furnished Property (GFP): A term used in this Task Order to mean property in the possession of, or directly acquired by, the Government and subsequently made available for the sole use of the contractor in the performance of this Task Order. Facilities, equipment, and materials in possession of, or acquired directly by the Government, and subsequently provided to the contractor.

Government Off The Shelf (GOTS): Software developed for and owned by the Government.

Guidance: A statement of direction such as, rules, laws, regulations, guidelines, and directives.

Heterogeneous: Environment in which platform architectures may differ.

Homogenous: Environment in which platform architecture is the same.

HSDN LAN: The Homeland Secure Data Network that transmits classified information

Information Technology Management (ITM): Activities related to management support of IT related policy development, strategic planning, capital planning, resource management, and special projects.

PROCUREMENT SENSITIVE

Infrastructure: Identifies the top-level design of communications, processing, and operating system (OS) software and describes the performance characteristics needed to meet database and application requirements. It includes processors, OS, service software, and standards profiles that include network diagrams showing communication links with bandwidth, processor locations, and capacities to include hardware builds versus schedule and costs. The active and passive components used to transfer information between two points. Infrastructure includes items such as cable plant, premise wiring, phone switch, routers, hubs, concentrators, Ethernet switches, and antennae.

Inspection: Determination and identification of the condition of equipment, facilities, services, systems and all other work output, with reference to contractual requirements.

Integration: The result of an effort that seamlessly joins two or more similar products (for example, individual system elements, components, modules, processes, databases, or other entities) to produce a new product. The new product functions as a replacement for two or more similar entities or products within a framework or architecture.

Integrator: A public or private sector entity that develops, assembles, and executes a comprehensive solution to complex information technology requirements.

Interoperability: The condition achieved when information can be exchanged directly and satisfactorily between two or more systems or components. The concept of having free and open methods to share data and IT services among different products of a similar functional capability. Interface standards are adhered to for the maintenance of service availability and consistent access methods. The use of proprietary features is discouraged. Functional categories for interoperability standards include: desktop systems; server systems; printing; network communications; word processing, spreadsheet and presentation applications; calendar and scheduling applications; application serving and license management.

Intrusion Detection System: Provides an additional layer of assurance through the monitoring of network activity to detect and report suspicious, unauthorized, or harmful activities.

Inventory Control: The process of managing, cataloging, and accounting for property provided under this Task Order.

Inverse Multiplexor (IMUX): A device that breaks up a high-speed transmission into several low-speed transmissions, and vice versa. It is used to transmit LAN and videoconferencing traffic over lower-speed digital channels.

Joint Inventory: A physical count of assets conducted by the contractor and the Government for establishing the quantity and condition of property accountable to the Contract.

Key Management: The process of managing keys. This includes ensuring that key values generated have the necessary properties and making keys known in advance to the parties that will use them. The process also ensures that keys are protected as necessary against disclosure and/or substitution.

Knowledge Management: The systematic process of finding, selecting, securing, organizing, distilling, and presenting information in a way that maintains an ongoing corporate knowledge.

Local: Policy or information pertaining to a particular DHS facility. For example, local facility policy refers to the specific policies of each of the DHS facility locations.

PROCUREMENT SENSITIVE

Local Area Network (LAN): Data network system used to provide connectivity within a logical boundary. In most cases, the extent of a logical boundary can be defined by the service area associated with an assigned TCP/IP address space. This includes inter- and intra-building cable plant or fiber plant, Metropolitan Area Network connections, backbones, and any active or passive components required to provide service from the desktop up to a LAN or WAN/ISP interface.

Lot Size: Number of units or product of output from which a sample is derived.

Maintenance: The work required to preserve and maintain a real property facility or piece of equipment in such condition that it may be effectively used for its designated functional purpose. Maintenance includes activities such as preventing damage that would be more costly to repair than to prevent, diagnosing failures, and performing corrective actions to ensure proper operation.

Mission Critical Systems: The systems used to support critical functions such as: Emergency Warning Systems, Operational Voice Systems, Operational LAN Systems, Operational Intercommunication Systems, Operational Fire and Security Systems, Secure Voice Systems (COMSEC).

Multiplexor: A device that merges several low-speed signals into one high-speed transmission and vice versa

Network: A collection of Local Area Networks (LAN)s under the administrative control of one organization. Networks typically use backbone technology to interconnect LANs and are themselves interconnected with the transmission system.

Network Interface: A network interface consists of the physical, logical and management connections where there is a distinct change in management responsibility or technical implementation. This can occur between two distinct networks or between a user device and its supporting network.

National Institute of Standards and Technology (NIST): The Federal technology agency that works with industry to develop and apply technology, measurements, and standards.

Normal Wear and Tear: Loss or impairment of appearance, effectiveness, worth, or utility of an item that has occurred solely because of normal and customary use of the item for its intended purpose.

On-Site: Repairs or services performed at a customer's location.

Organization: An administrative structure with a mission. The term is used in a very broad sense throughout this document.

Other Direct Costs (ODC): Costs not previously identified as a direct material cost, direct labor cost, or indirect cost; a cost that can be identified specifically with a final cost objective that the Offeror does not treat as a direct material cost or a direct labor cost.

Personal Computer (PC): Desktop and notebook computers.

Personal Digital Assistant (PDA): A small, portable, hand held computing device. PDAs offer communications capabilities to include voice, e-mail, SMS, text messaging, and web access.

Performance Requirements Summary (PRS): The portion of the Task Order which documents Task Order requirements, the component requirements related to each Task Order requirement, and the standards and measures of performance.

PROCUREMENT SENSITIVE

Performance Standard: A selected characteristic of an output of a work process that can be measured in order to evaluate performance.

Personally Identifying Information (PII): Any piece of information which can potentially be used to uniquely identify, contact, or locate a single person.

Personal Peripherals: Peripheral devices attached directly to individual desktops or workstations. These devices include printers, scanners, plotters, modems, external hard disks, etc.

Phase-In Period: The period(s) during which the contractor contends with the transfer of performance responsibility from the existing provider to the contractor. During this period the contractor shall organize, plan, recruit personnel, train, mobilize, develop procedures, and accomplish all actions necessary to commence performance of the services at the end of the transition period.

Phase-out Period: The approximately 90 business day period prior to completion of the Task Order.

Preventive Maintenance: Systematic and cyclic check, inspection, servicing and repairs of deficiencies, as well as reporting of deficiencies beyond scope of preventative maintenance. Preventative maintenance includes accomplishment of routine maintenance and repair.

Primary Rate Interface (PRI): A telecommunications standard for carrying multiple DSO voice and data transmissions between two physical locations.

Program: An organized set of activities directed toward a common purpose, objective, or goal undertaken or proposed by an Agency to carry out assigned responsibilities. The term is generic and may be applied to many types of activities. Acquisition programs are programs whose purpose is to deliver a capability in response to a specific mission need. Acquisition programs may comprise multiple acquisition projects and other activities necessary to meet the mission need.

Program Manager: The contractor representative who acts as the point of contact (POC) with the Government and coordinates Task Order management.

Project: A single undertaking or task involving maintenance, repair, construction, or equipment-in-place, in which a facility or group of similar facilities are treated as an entity with a finite scope.

Protocols: Protocols are conventions and algorithms for the transmittal of information over the network. Protocols exist at various layers of the stack and are often used to perform a specific function, a unique network service or application. Service protocols work in conjunction with the transport protocols to complete the required function(s). Examples of service protocols are the Simple Mail Transfer Protocol (SMTP), File Transfer Protocol (FTP), and Hypertext Transfer Protocol (HTTP).

Quality Assurance (QA): Actions taken by the Government to inspect or check goods and services to determine that they meet or do not meet requirements of the Task Order. See Quality Assurance Surveillance Plan for further detail.

Quality Assurance Personnel (QAP): The personnel responsible for surveying the contractor's performance.

Quality Assurance Surveillance Plan (QASP): An organized written document used by Government for quality assurance surveillance. Document contains sampling/evaluation guides, checklists, and the Performance Requirements Summary (PRS).

PROCUREMENT SENSITIVE

Quality Control (QC): Those actions taken by a contractor to control the performance of services so they meet the requirements of the Task Order. See Quality Control Plan for further detail.

Quality Control (QC) Plan: The contractor's system to control the equipment, systems, or services so that they meet the requirements of the Task Order.

Random Sample: A sampling method whereby each service output in a lot has an equal chance of being selected.

Remote Access: Logging into a computer system through a network or modem to execute a command or manipulate data on that system.

Remote Communication: The services that allow a remote user to connect with an address assigned out of the DHS's internal assigned address space. Typical examples of this type of connectivity include: asynchronous modem/terminal server/dial-in service, HSDN and ISDN service, and some wireless modem services.

Reportable Incident: Any event, suspected event, or vulnerability that could pose a threat to the integrity, availability, or confidentiality of systems, applications or data. Incidents may result in the possession of unauthorized knowledge, the wrongful disclosure of information, the unauthorized alteration or destruction of data or systems and violation of Federal or state laws. If such violations are detected or suspected, they are to be reported immediately to a security manager.

Requirement: Effort mandated by this Task Order, issued by a DHS contracting officer (CO) and performed as directed by the CO or their representative (COTR) within the scope of the resulting Task Order.

Restricted Area: Those areas designated by DHS that require control of personnel for security reasons and/or equipment for protection of personnel, property and information.

Return to Service: The time taken to resolve the user's problem to the state that the end user has full functionality restored as specified in the Service Level Agreements and performance metrics.

Routine Call: A request for service with a response time as defined in the Technical Exhibits.

Sample: A sample consists of one or more service outputs drawn from a lot, the outputs being chosen at random.

Scheduled Outage: The maintenance, testing, or other contractor-initiated activity that impacts the user's ability to access network services. A scheduled outage is not considered downtime if the outage is not during business hours and occurs during the COTR approved maintenance window timeframe.

Secure Telephone Equipment (STE): STE is the U.S. Government's current encrypted telephone communications system for wired or "landline" communications. It is intended to replace the older STU-III system. STE is designed to use ISDN telephone lines which offer higher speeds of up to 128k bits per second and are all digital. The greater bandwidth allows higher quality voice and can also be utilized for data and fax transmission. STE sets are backwards compatible with STU-III phones.

Secure Telephone Unit, Third generation (STU III): STU III are a line of secure telephones.

PROCUREMENT SENSITIVE

Security Systems: Defined to be only those that directly support a given communication service. Examples of systems that would be included are: policy enforcement points or PEP security systems, phone or fax encryption systems, authentication or certification systems, and World Wide Web or e-mail proxy systems.

Sensitive: Documents, data, information, systems, products, services, items, etc requiring protection and control because of statutory requirements or regulations.

Server Administration: Services provided in the operation and maintenance of servers. This includes services such as installation of a new server and additional hardware, installation and upgrade of software applications and network operating system, and configuration of hardware and software. This also includes account management, backup and restore, performance monitoring and tuning, security monitoring, problem tracking and error detection.

Service Call: Any notification or request for service as defined in the Technical Exhibits.

Service Category: A classification for a group of services associated with a specific functional use of a desktop computer. This is comprised of service characteristics for the type of support needed by an individual performing a specific desktop computer function. A suite of services will be packaged into a service category to define a service level agreement.

Service Delivery Model: A Service Delivery Model places total responsibility on the contractor for all component services and products needed to meet the customer's requirements. The customer then comes to the single contractor and selects from a menu of services that best meet their needs. All services provided are governed by a Service Level Agreement between the contractor and the customer that stipulates service quality measures, pricing, and customer recourse for poor performance.

Service Level: A unit used to identify characteristics and metrics that define a particular type of support to be provided by the Contractor. Multiple service levels may be needed for a type of service, such as hardware maintenance, to provide various degrees of support needed by a computer user.

Service Level Agreement (SLA): An agreement between the CIO's Office and its supported customer to provide services at stated performance level.

Shall: The word "Shall" is used in connection with the contractor and specifies that the provisions are mandatory as defined by the FAR.

Site Offices/Locations: Those support locations, offices, and facilities listed in IE C.1.3-002.

Software Categories: Desktop software is divided into three types: operating system, utilities, and applications. Operating system software includes Windows XP, Windows VISTA, and their successors. Utility programs perform functions such as disk management, file backup/recovery, file compression, memory management, security, and virus protection. Application programs encompass a wide variety of programs required by the end users to perform their work. Examples of programs in this category are word processors, spreadsheets, email, groupware, desktop publishing, programming languages, compilers, data base managers, and engineering tools.

Software Release: The date that a software developer makes their software product publicly available. This date is often used in determining when a software product is deployed to the computer desktop.

Standard Operating Procedure (SOP): A comprehensive narrative description of methods prepared by either the Government or contractor. A set of instructions covering those features of operations that lend themselves to a definite or standardized procedure without loss of effectiveness. The procedure is applicable unless ordered otherwise.

Supplies: Items needed to equip, maintain, operate, and support the requirements of this Task Order and the resulting Task Order

System: Any entity that has input, process, output and feedback.

Tactical FASTLANE (TACLANE): Tactical FASTLANE® was developed by the National Security Agency (NSA) to provide network communications security on Internet Protocol (IP) and Asynchronous Transfer Mode (ATM) networks for the individual user or for enclaves of users at the same security level.

Task Order: An order placed for services by the CO in accordance with the terms and conditions of the contract.

Task Order Start Date: Effective date of the Task Order and beginning of the Phase-In Period as authorized by the CO at or following Task Order award.

Test Readiness Review (TRR): TRR is a multi-disciplined technical review to ensure that a subsystem or system under review is ready to proceed into formal test. The TRR assesses test objectives, test methods and procedures, scope of tests, and safety and confirms that required test resources have been properly identified and coordinated to support planned tests.

Throughput Capability: The rate at which data can be transferred over a network. The physical connection point into the operating network is able to support transferring information at this rate. It does not necessarily mean that the computer is powerful enough to transfer information at this rate. The performance requirements will correspond to the slower of either the sender or the receiver of the data transfer. The throughput is to be verified with a standard set of hardware and software. The validation procedure of throughput capability shall be performed at any time during the day. If the specifications are not met, the network shall be considered down.

Transport Protocols: Protocols used specifically to provide the data transfer mechanisms necessary to establish and maintain a reliable communications link to transmit data across a network. These protocols are independent of the media and topology of the underlying sub networks.

User: A person, organization, or other entity that employs IT related services provided under this Task Order and the resulting Contract.

Utilities: Electricity, gas, water, sewage disposal, and steam are types of utilities used under the performance of this Task Order.

Vulnerability Assessment/Risk Analysis: Identifying, characterizing, and testing potential security exposures.

Wireless LAN Systems: The components and systems used to provide network connectivity without requiring 100% physical cable plant connectivity. Examples of these are Bluetooth, infrared, laser, and radio based interconnection services.

Workstation: This is a networked or standalone computer. This computer is normally used for calculation or graphics intensive applications. It includes the CPU, monitor, keyboard, and a mouse or other screen manipulation devices.

C.2.2 ACRONYMS

ACRONYM	TITLE
ACD	Automatic Call Directory
ADPE	Automated Data Processing Equipment
AIS	Automated Information System
AMHS	Automated Message Handling System
APO	Accountable Property Officer
ATO	Authorization to Operate
AV	Audio Visual
BA	Bachelor of Arts
BMO	Budget Management Office
BOM	Bill of Materials
BPA	Blanket Purchase Agreement
BRI	Basic Rate Interface
BS	Bachelor of Science
C&A	Certification and Accreditation
CAP	Contractor Acquired Property
CAR	Contract Administration Review
CATV	Cable Television
CBP	Customs and Border Protection
CBT	Computer-based Training
CCB	Change Control Board
CCI	COMSEC Controlled Items
CDR	Critical Design Review
CDRL	Contract Data Requirements List
CFE	Contractor Furnished Equipment

ACRONYM	TITLE
CFF	Contractor Furnished Facilities
CFO	Chief Financial Officer
CFR	Code of Federal Regulations
CIA	Central Intelligence Agency
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CISSP	Certified Information Systems Security Professional
CM	Configuration Management
CMM	Capabilities Maturity Model
CND	Computer Network Defense
CNPPD	Chemical and Nuclear Preparedness and Protection Division
CO	Contracting Officer
COCO	Contractor Owned, Contractor Operated
COMSEC	Communications Security
CONOPS	Concept of Operations
COOP	Continuity of Operations Plan
COTR	Contracting Officer's Technical Representative
COTS	Commercial Off The Shelf
CPIC	Capital Planning and Investment Control
CSIRT	Computer Security Incident Response Team
CSU/DSU	Channel Service Unit/Data Service Unit
CVAM	Controlled Vulnerability Assessment Methodology
CVE	Common Vulnerabilities and Exposures
DAA	Designated Accrediting Authority

ACRONYM	TITLE
DAC	Discretionary Access Control
DCAA	Defense Contracting Audit Agency
DCID	Director of Central Intelligence Directive
DHS	Department of Homeland Security
DISA	Defense Information Systems Agency
DITSCAP	DoD Information Technology Security Certification and Accreditation Process
DMS	Defense Message System
DR	Disaster Recovery
DoD	Department of Defense
DoS	Denial of Service
DSN	Database Source Networks
DSS	Digital Satellite Service
DTD	Document Type Definition
DVD	Digital Video Disk
EA	Enterprise Architecture
EACOE	Enterprise Architecture Center of Excellence
EAGLE	Enterprise Acquisition Gateway for Leading Edge Solutions
ECCB	Enterprise Change Control Board
ECR	Engineering Change Request
EDI	Electronic Data Interchange
EDMO	Enterprise Data Management Office
EF	Essential Functions
EIWG	Enterprise Interconnection and Policy Working Group
EML	Environmental Measurement Lab

ACRONYM	TITLE
EOD	Entry on Duty
EPA	Environmental Protection Agency
ERG	Engineering Review Group
ESIGN	Electronic Signatures in Global and National Commerce Act
ESM	Enterprise System Management
ET	Eastern Time
EVM	Earned Value Management
FAR	Federal Acquisition Regulation
FDCC	Federal Desktop Core Configuration
FEMA	Federal Emergency Management Agency
FIPS	Federal Information Processing Standards
FFMS	Federal Financial Management System
FISMA	Federal Information Security Management Act
FITSAF	Federal Information Technology Security Assessment Framework
FOIA	Freedom of Information Act
FY	Fiscal Year
FYHSP	Future Years Homeland Security Program
GAO	Government Accountability Office
GFE	Government-Furnished Equipment
GFF	Government-Furnished Facilities
GFP	Government-Furnished Property
GFS	Government-Furnished Services
GISRA	Government Information Security Reform Act
GOGO	Government Owned – Government Operated

ACRONYM	TITLE
GOTS	Government Off The Shelf
GPEA	Government Paperwork Elimination Act
GPO	Group Policy Office
GSA	General Services Administration
HAZMAT	Hazardous Material
HLSEA	Homeland Security Enterprise Architecture
HQ	Headquarters
HSDN	Homeland Secure Data Network
HSHR	Homeland Security Presidential Directive
HSRD	Hot Standby Router Protocol
I&A	Identification and Authentication
IATO	Interim Authorization to Operate
IAVA	Information Assurance & Vulnerability Assessment
IAW	In Accordance With
IC	Intelligence Community
ICE	Immigration and Customs Enforcement
ID	Identification
IDS	Intrusion Detection System
IG	Inspector General
IMAC	Installation, Move, Add, Change
IMAP	Internet Message Access Protocol
IMEI	International Mobile Equipment Identity
IMUX	Inverse Multiplexor
INFOCON	Information Condition

ACRONYM	TITLE
IP	Internet Protocol
IRB	Investment Review Board
IS	Information Systems
ISA	Interconnection Security Agreement
ISDN	Integrated Services Digital Network
ISO	International Standards Organization
ISSM	Information System Security Manager
ISSO	Information System Security Officer
IT	Information Technology
ITAC	Information Technology Acquisition Center
ITIL	Information Technology Infrastructure Library
JRC	Joint Requirements Council
KDP	Key Decision Points
KPI	Key Performance Indicator
LAN	Local Area Network
LRU	Lowest Replaceable Units
MAN	Metropolitan Area Network
MCSE	Microsoft Certified Systems Engineer
MD	Management Directive
MOM	Microsoft Operations Management
NAC	Nebraska Avenue Complex
NARA	National Archives and Record Administration
NCS	National Communications System
NIST	National Institute of Standards and Technology

ACRONYM	TITLE
NMC	Network Management Center
NSA	National Security Agency
O&M	Operations and Maintenance
OCA	Office of Chief Administrative Officer
OCIO	Office of the Chief Information Officer
OEM	Original Equipment Manufacturer
OIM	Office of Infrastructure Management
OMB	Office of Management and Budget
OPO	Office of Procurement Operations
ORR	Operational Readiness Review
OSHA	Occupational Safety and Health Administration
OST	Order Ship Time
OTAR	Over-The-Air Rekey
OTAT	Over-The-Air Transfer
P3I	Pre-planned Product Improvement
PBX	Private Branch Exchange
PCO	Property Control Officer
PDA	Personal Digital Assistant
PDD	Presidential Decision Directive
PDR	Preliminary Design Review
PEP	Policy Enforcement Point
PII	Personally Identifying Information
PL	Public Law
PRS	Performance Requirements Summary

ACRONYM	TITLE
PM	Project Manager
PMO	Program Management Office
PMP	Project Management Plan
PMR	Program Management Review
POAM	Plan of Action and Milestones
POC	Point of Contact
PRI	Primary Rate Interface
RAM	Responsibilities Assignment Matrix
RFID	Radio Frequency Identification
ROM	Rough Order of Magnitude
S&T	Science and Technology
QAE	Quality Assurance Evaluator
QAP	Quality Assurance Personnel
QASP	Quality Assurance Surveillance Plan
QC	Quality Control
SBU	Sensitive but Unclassified
SCI	Sensitive Compartmentalized Information
SDLC	System Development Life Cycle
SEC DHS	Secretary of the Department of Homeland Security
SIM	Security Information Management
SIPRNET	Secure Internet Protocol Router Network
SLA	Service Level Agreement
SNMP	Simple Network Management Protocol
SMTP	Simple Mail Transfer Protocol

ACRONYM	TITLE
SMC	Security Management Center
SME	Subject Matter Expert
SMS	Systems Management Server
SOP	Standard Operating Procedure
SP	Special Publication
SRR	System Requirements Review
SSA	System Security Administrator
SSAA	Systems Security Authorization Agreement
STE	Secure Telephone Equipment
STU III	Secure Telephone Unit, Third generation
TACLANE	Tactical FASTLANE
TCP/IP	Transmission Control Protocol/Internet Protocol
TDA	Table of Distribution and Allowances
TE	Technical Exhibit
TRM	Technical Reference Model
TRR	Test Readiness Review
TS	Top Secret
TS/SCI	Top Secret Sensitive Compartmented Information
TSA	Transportation Security Administration
TSS	Technical Source Selection
URL	Uniform Resource Locator
U.S.	Unites States
U.S.C.	United States Code
USM	Undersecretary of Management

ACRONYM	TITLE
VIP	Very Important Person
VOIP	Voice Over Internet Protocol
VTC	Video Teleconference
WBS	Work Breakdown Structure
WCMS	Web Content Management System
WSE	Web Services Environment

C.3 GOVERNMENT – FURNISHED PROPERTY (GFP) AND SERVICES

Government Furnished Property (GFP) is applicable to the performance of this Task Order. The contractor is authorized to use GFP at the Department of Homeland Security for the duration of this Task Order in accordance with the requirements of this Task Order. The Government shall provide, without cost to the contractor, facilities (office space with desk and chair), equipment (computer, access to printer, copier, and fax), materials (all related office supplies), and/or other services necessary to perform the requirements in the Task Order.

C.3.1 SCOPE

This Section describes the property and services the Government will furnish to the contractor for performance of the requirements of this Task Order. The Government will provide to the contractor the following access for use: (1) Government Furnished Property (GFP) for which the contractor is responsible and accountable; and (2) property only made available to the contractor, as listed below in this section. The contractor shall take all reasonable precautions and such other actions as may be directed by the Government, or in the absence of such direction, in accordance with sound business practice to safeguard and protect Government property in the contractor's possession or custody listed in this section. The contractor shall accept Government-provided automated information systems (AIS) hardware and software without exception. Government Furnished Equipment (GFE) may include Government-leased equipment or Government-owned equipment. Refusal to accept some or all of the GFP offered by the Government shall not relieve the contractor from Task Order performance, but will relieve the Government from the obligation of providing the same or similar GFP at a future date.

The contractor shall not use GFP or services for any other purpose than those described in this Task Order. The contractor shall not remove GFP from DHS facilities or other supported areas without review and written approval of the CO or authorized representative. The provisions affecting GFP under this section shall be IAW FAR 52.245-5. The Government may direct the contractor to develop and /or revise milestones for joint inventory and transfer of GFP.

C.3.1.1 Government-Furnished Property

C.3.1.1.1 The Government intends to share space with the contractor personnel in the Government facilities indicated in TE C.3.1-002 or as designed by the Government for the duration of this Task Order and only for the performance of this Task Order. This is not considered Government Furnished Property (GFP) requiring property administration IAW FAR 45 plus Supplements.

C.3.1.1.2 Marking Property: The contractor shall not mark or affix any decals, emblems or signs portraying the contractor's name or logo to Government Equipment, Facilities, or Property except as directed by the COTR.

C.3.1.2 Government-Furnished Services

C.3.1.2.1 Telephone Service: The Government will furnish telephone service at contractor-occupied Government sites to include local and long-distance calls.

C.3.1.2.1.1 The contractor shall comply with DHS rules and regulations regarding telephone use. The contractor shall reimburse the Government the cost of unofficial telephone service (e.g., telephone service not incidental to performance of the Task Order).

PROCUREMENT SENSITIVE

- C.3.1.2.1.2 The contractor shall obtain prior Government review and written approval before connecting or disconnecting any Contractor Furnished Equipment (CFE) to Government-furnished communications systems or equipment.
- C.3.1.2.2 Local Area Network (LAN): The Government will provide limited access to the existing LAN at contractor-occupied Government facilities to include E-Mail capability. The contractor shall not use the LAN for purposes other than for work required under this Task Order.
- C.3.1.2.3 Paper Products: The Government will make available containers in shared Government facilities for the collection of recyclable paper.
- C.3.1.2.4 Reporting Discrepancies in Performance of Government Furnished Service Contracts: The contractor shall report discrepancies in performance of Government-provided services to the CO or COTR. (CDRL C.3.1-1, Government Furnished Service Discrepancy Report)
- C.3.1.3 Supplies and Materials**
- C.3.1.3.1 Existing Levels of Supplies and Materials: The Government will make available existing Government owned parts, supplies and material to the contractor for use in the performance of the requirements of this Task Order. The Government will furnish the existing levels of Government supplies and materials to the contractor following joint inventory during phase-in and the contractor shall provide existing levels of Government supplies and materials to the Government during phase-out. The Government will furnish replacement materials required to maintain the serviceability of production equipment on a time and materials basis. The government will furnish all items to the contractor as GFE to use under this Task Order. DHS purchases all hardware, software, warranties and parts using the FirstSource contract.
- C.3.1.4 Government-Furnished Equipment (GFE)**
- The Government will provide GFE (such as telecommunications, computers, network components, storage devices, software, and peripherals) to the contractor to complete the duties of this Task Order with the exception of equipment for the Help Desk and unclassified Test Lab.
- C.3.1.4.1 Equipment Offered for Contractor Use: The Government will furnish property from the Product Guide provided at TE C.3.1-001. Original Equipment Manufacturer (OEM) Software is provided at TE C.3.1-002. The result of the last inventory of equipment in the metropolitan Washington D.C. area and other select locations is provided at TE C.3.1-003.
- C.3.1.4.2 Contractor Accountability
- C.3.1.4.2.1 Transfer of Accountability: The contractor shall become accountable for GFE when assigned.
- C.3.1.4.2.2 Property Administration: The contractor shall perform property administration in accordance with FAR Part 45.
- C.3.1.4.2.3 Report of Government Property: The contractor shall prepare and submit to the COTR an annual Report of Government Property as directed by the COTR. (CDRL C.3.1-2, Government Property Report – Annual)
- C.3.1.4.3 Turn-In and Replacement

PROCUREMENT SENSITIVE

- C.3.1.4.3.1 Turn-In of GFE: The contractor shall prepare a recommendation for excess when GFE is no longer required or suitable for its intended use, or has reached the end of its technical life. The contractor shall provide these recommendations to the COTR who will make the final determination of the disposition of the equipment. Upon approval, the contractor shall process the items in accordance with applicable Federal regulations, and Department of Homeland Security policies and regulations. All Government furnished property and IT equipment identified in this Task Order shall remain the property of the Government.
- C.3.1.4.3.2 Replacement of GFE: The contractor shall coordinate with the CO for replacement of GFE. Upon approval by the CO, the item(s) of equipment to be replaced will be deleted from the GFE listing. If required to maintain performance standards, the Government will provide comparable GFE replacement. The contractor shall contact the Help Desk for problems regarding computers and peripherals. The Government will replace computers and peripherals.
- C.3.1.4.4 Initial Inventory Assessment and Accountability
- C.3.1.4.4.1 Initial Inventory Procedures: The contractor shall attend a phase-in GFP transfer and inventory meeting with the Government. The COTR will schedule the meeting prior to performance period start date.
- C.3.1.4.4.2 The contractor shall conduct a phase-in 100% joint inventory within ten business days prior to Task Order start date. This inventory shall items such as facilities, to include keys; property received from the designated property control officers; and materiel items of work in progress; e.g., items in various stages of repair. This provision does not preclude prior inspection of GFP by the contractor. The operational or conditional status of all GFF and on-site GFE shall be determined during the joint inventory. The contractor shall record any item found to be broken or not suitable for its intended purpose. The CO and the contractor shall certify as accurate the joint inventory. The contractor shall keep the inventory listing current. (CDRL C.3.1-3, Government Property Inventory – Initial)
- C.3.1.4.4.3 The contractor and the COTR shall jointly inspect all GFE at the time of the inventory. The contractor shall note all valid discrepancies, and the Government may correct the discrepancies by one or more of the following methods at the Government's option. The Government may elect not to provide equipment to the contractor; or may correct noted discrepancies prior to performance period start date; or may require the contractor to repair discrepancies subject to reimbursement by the Government. The COTR will determine validity.
- C.3.1.4.5 Withdrawal of GFE: The Government retains the right to withdraw any GFE at any time during the performance of the Task Order. When possible, the Government will provide at least 30 business days notice of the impending withdrawal of GFE when deemed necessary or appropriate.
- C.3.1.4.6 Equipment and Software Manuals: After conducting a joint inventory, the Government will turn over to the contractor equipment operating manuals presently maintained by the Government. The contractor shall update these

documents as new issues are published. Updated manuals are the property of the Government upon completion or termination of this Task Order.

C.4 CONTRACTOR – FURNISHED PROPERTY AND SERVICES

C.4.1 SCOPE

The contractor shall furnish all materials, supplies, tools, services, temporary work places, and equipment required to perform this Task Order, except for the items specifically identified as Government-Furnished in Section C.3 of this Task Order.

C.4.1.1 Contractor-Furnished Facilities (CFF)

The Government will provide those facilities and installed equipment as listed and identified in Section C.3 of this Task Order. The contractor shall not place, construct, or otherwise provide additional buildings or facilities on DHS premises without prior CO approval. The contractor shall provide the Help Desk facility. The contractor may provide Test Lab facilities and the associated hardware and software via a separate logical follow-on Task Order for the Test Lab requirements specified in this Task Order.

C.4.1.1.1 CFF Listing: The contractor shall provide to the CO or COTR an initial and updated list of Contractor Owned, Contractor Operated (COCO) facilities/real property used in performance of this Task Order. The contractor shall provide the location of the Help Desk and Test Lab used in performance of this Task Order to the CO or COTR. (CDRL C.4.1-1, Contractor Owned, Contractor Operated Facilities List (used in Task Order performance)).

C.4.1.1.2 Keys, Ciphers, Combinations, and Security Clearances: The contractor shall maintain records identifying those members of the contractor's workforce at Government facilities who shall be authorized the use of keys, codes, ciphers, combinations and security access.

C.4.1.1.3 The contractor may be required to provide additional storage space for IT equipment and services associated with this Task Order.

C.5 SCOPE OF WORK

The Information Technology Services Office provides support for DHS operations at various facilities and locations in, and around, the Metropolitan Washington D.C. area and at locations throughout the U.S. The number of supported locations is projected to increase throughout the U.S. TE C.1.2-002 provides facility locations and TE C.1.3-002 provides the projected number of seats by Fiscal Year (FY) for each of the three Local Area Networks (LANs).

In performing the Scope of Work identified herein, the contractor shall conduct all operations support for Information Technology Services Office with a proactive and technologically aggressive methodology. The methodology shall identify more effective, efficient or alternative forms of new IT advancements that would provide a heightened level of performance for DHS operations. The contractor shall forecast new IT trends and update, brief, and coordinate with DHS management to provide a comprehensive system of knowledge disclosure. The contractor shall use information from market research and market analysis findings to identify new or updated IT technologies, equipment, and data acquisition and availability as well as advancements in hardware, software and supporting system infrastructure. The contractor, as part of full knowledge transfer and disclosure shall perform subjective and comparative analysis to existing DHS technology identifying advancements and efficiencies. If authorized by the COTR, the contractor shall perform and conduct operational and theoretical performance evaluations of current IT capabilities with contractor identified, proposed or updated IT advancements.

C.5.1 APPLICATIONS MANAGEMENT, SUPPORT, AND DEVELOPMENT

The contractor shall manage and maintain all deployed applications for full functionality and continuous availability on all Department of Homeland Security (DHS) systems. The Government defines continuous availability as full functionality of all applications from the desktop client. All applications are run on DHS Data Center Servers. The contractor shall maintain full functionality of file and data storage and retrieval, printing, remote access, and messaging services to authorized users. A list of the supported applications is provided in the Product Guide Software Section at TE C.3.1-001, Government Furnished Equipment.

C.5.1.1 Application Management Services

- C.5.1.1.1 The contractor shall manage and support required applications, provide reporting and documentation deliverables, and a single-point of accountability. The nature of applications maintenance for COTS operating systems and software is to provide patches, pushes, and OEM updates.
- C.5.1.1.2 The contractor shall provide software development/tailoring services as required to facilitate the creation and/or migration of applications into enterprise environments to include the Web Services Environment (WSE) for DHSOnline and DHSInteractive, the Department's intranet and extranet portals. A list of the current custom applications is provided at TE 5.1-001.
 - C.5.1.1.2.1 Requirement Analysis: The contractor shall provide requirement elicitation, analysis and management services in support of applications/databases/systems. The products of this effort are requirement documentation.
 - C.5.1.1.3 Functionality Enhancement: The contractor shall provide the support effort of application development. Activities include defect correction, software tailoring to develop functionality enhancements and activities such as user profile management and training.

C.5.1.1.4 The contractor shall develop a proposed applications consolidation and rationalization plan to provide a utility computing platform. The contractor shall submit the plan to the COTR for approval. (CDRL C.5.1-1, Applications Consolidation and Rationalization Plan)

C.5.1.1.4.1 The contractor's plan shall comply with DHS enterprise configuration and change management requirements.

C.5.1.2 Status and Availability of Major Applications on the Network

C.5.1.2.1 As required for determining network status, the contractor shall provide DHS an Up/Down Status Report of Major Applications on the Network indicating the availability and functionality of applications for end users (CDRL C.5.1-2 Up/Down Status Report). Up/Down Status refers to network and server applications and not to desktop-resident applications. This report shall include an up/down status of all network and server applications.

C.5.1.2.2 The contractor shall provide the COTR access to NMC systems for real-time status of all major applications integral to the network at all times.

C.5.1.3 Application Maintenance and Operation Documentation

C.5.1.3.1 The contractor shall provide on a weekly basis, status reports for DHS applications that cover the following data points (CDRL C.5.1-3, Application Maintenance and Operation Reports – Weekly)

- Funding level
- Significant Events/Outages
- Summary of O&M activity

C.5.1.3.1.1 The contractor shall also provide a root cause analysis report (within 48 hours of the incident) to the Government following any outages on DHS Applications. (CDRL C.5.1-4, Root Cause Analysis Report) The report shall include the following:

- Root cause of outage
- Remediation activities
- Mitigation activities
- Recommendation for platform enhancement to prevent recurrence

C.5.1.4 Application Database and Systems Maintenance

The contractor shall establish and maintain an application maintenance schedule. The contractor shall coordinate with the Government to schedule any application maintenance downtime sufficiently in advance to enable smooth operations during maintenance windows. Any scheduled jobs, any automated processes (Chronologic Jobs that operate at predefined time intervals or that occur following notifications), or periodically timed or batched tasks shall also be considered applications.

C.5.1.4.1 The contractor shall identify the requirements for and install upgrades, updates, service packs, and patches.

C.5.1.4.2 The contractor shall maintain security protection and reliability updates on operating systems.

C.5.1.4.3 The contractor shall identify and notify the COTR of any upgrades, updates, service packs, and patches determined to be incompatible with system or application specifications and proceed as directed by the COTR.

C.5.1.4.4 The contractor shall provide recommendation for preempting and/or resolving any system performance issues.

C.5.1.5 Performance Trends of Major Applications on the Network

C.5.1.5.1 When requested by the Government, the contractor shall provide DHS a Performance Trend of Major Applications on the Network Report. (CDRL C.5.1-5, Performance Trend of Major Applications on the Network Report)

C.5.1.5.2 The contractor shall also maintain and provide historical data on the performance of each application to DHS in the form of trend reports. DHS will use these reports to assess the performance of each application. Data for trend reports shall be maintained in the knowledge database.

C.5.1.5.3 The contractor shall collect, maintain and update this data, along with all other knowledge that can be used to enhance IT operations, in a COTR accessible knowledge database; data shall include date and time.

C.5.1.6 Enterprise Desk Application Licensing

C.5.1.6.1 The contractor shall evaluate the available and pre-existing DHS enterprise software license agreements and shall make use of them to the extent possible and practical.

C.5.1.6.2 The contractor shall track and deploy all software licenses required to perform the DHS mission and provide a list of the licenses to the COTR. The COTR may direct the contractor to administer the purchase of software on behalf of the Government off of DHS designated licensing Task Order vehicles.

C.5.1.7 Collaborative Applications

C.5.1.7.1 The contractor shall make recommendation on purchases to support collaborate applications and functionality. The DHS will consider the recommendations and purchase approved collaborative applications through FirstSource and provide the applications as GFE

C.5.1.7.2 The collaborative applications are items such as the following:

- Secure e-mail for authorized users
- A comprehensive suite of software tools to improve authorized users' abilities to share and collaborate on secure data both on DHS systems and on authorized, interconnected networks

C.5.1.8 Application Development

The contractor shall provide Application Development services as directed by the COTR. Application Development services shall be accomplished in response to Logical Follow-On Task Orders on a case by case basis.

C.5.1.9 Ensure New Acquisitions Include Common Security Configurations

The contractor shall comply with Office of Management and Budget policy memorandum M-07-11, "Implementation of Commonly Accepted Security Configurations for Windows Operating Systems" which states: "agencies with these operating systems (Windows XP

and VISTA) and/or plans to upgrade to these operating systems must adopt these standard security configurations by February 1, 2008.” The standards are as follows:

- The contractor shall certify applications are fully functional and operate correctly as intended on systems using the Federal Desktop Core Configuration (FDCC). This includes Internet Explorer 7 configured to operate on Windows XP and Vista (in Protected Mode on Vista).
 - For the Windows XP settings see http://csrc.nist.gov/itsec/guidance_WinXP.html
 - For the Windows Vista settings see http://csrc.nist.gov/itsec/guidance_vista.html
- The standard installation, operating, maintenance, update, and/or patching of software shall not alter the configuration settings from the approved FDCC configuration. The information technology should also use the Windows Installer Service for installation to the default “program files” director and should be able to silently install and uninstall
- Application designed for normal end user shall run in the standard user context without elevated system administration privileges.

C.5.2 DEPLOYMENT SUPPORT

C.5.2.1 Provide Deployment Support

The Government shall require deployment support services for short-term and long-term deployment projects. The contractor shall provide deployment support for all DHS sites, including sites requiring Sensitive but Unclassified (SBU), Homeland Secure Data Network (HSDN), and Top Secret access, with seamless conversion from any existing network assets, failover capability, high availability during transition and operation, and temporary relocation support. The contractor shall perform installation planning and scheduling, site documentation preparation (e.g. configuration drawings), equipment staging, installation, and checkout for DHS sites. The Government will provide a technical project manager for each deployment project.

- C.5.2.1.1 The contractor shall apply and adhere to IT Project Management policies and procedures for all deployment projects.
- C.5.2.1.2 The contractor shall collect and document customer requirements, review the scope of the effort with the customer, and determine the required equipment and mutually agreed upon pricing for delivery of those services.
- C.5.2.1.3 The contractor shall develop a Deployment Project Plan for each project and submit to the COTR for approval. (CDRL C.5.2-1, Deployment Project Plan)
- C.5.2.1.4 The contractor shall develop a Rough Order of Magnitude (ROM) for the proposed services as part of the Deployment Project Plan, which the Government will use to develop additional task orders for build-out and deployment services under this Task Order. This initial tasking or the specific build-out task establishes the performance levels for subsequent task orders.
- C.5.2.1.5 The contractor shall conduct site surveys, prepare site reports, network diagrams, develop bill of materials (BOM), and any other required documentation associated with the completed site survey.
- C.5.2.1.6 The contractor shall evaluate, complete, and submit to the COTR for approval, a review and report on proposed workspace to determine if the

existing facilities infrastructure can adequately support the communications and information technology equipment. (CDRL C.5.2-2, Proposed Workspace Report)

C.5.2.1.7 The contractor shall provide the COTR and the customer organization with a trip report. (CDRL C.5.2-3, Trip Report)

C.5.2.1.8 The contractor shall prepare a detailed site report for each site that identifies equipment, internal and external interconnects, site integration plan, and site drawings and submit it to the COTR for approval when requested. (CDRL C.5.2-4, Site Report)

C.5.2.1.9 The contractor shall install new, enhanced, or replacements of hardware and/or software and the physical infrastructure, as required (e.g., wiring, cable plant) for DHS and other federal agencies systems and facilities as directed by the COTR.

C.5.2.2 Develop Deployment Plan Template

The contractor shall develop the DHS Deployment Plan Template and submit to the COTR for approval. (CDRL C.5.2-5, DHS Deployment Plan Template) Using the approved template, the contractor shall develop, maintain, update and implement specific Deployment Project Plans.

C.5.2.2.1 The contractor Deployment Plan shall, at a minimum, address the following:

- Deploy and maintain a stable and highly available system in accordance with appropriate performance standards
- Utilize highly trained maintenance technicians and systems engineers to minimize repair calls and promote minimal user disruption
- Demonstrate the availability to support geographically dispersed deployments.
- Provide special support for reviewing of cabling plans throughout current and potential locations

C.5.2.3 Site Activation

Upon COTR direction, the contractor shall execute the Government approved solution identified in accordance with the Deployment Project Plan to ensure seamless installation/integration. The contractor shall develop a formal acceptance process and submit to the COTR for approval. (CDRL C.5.2-6, Site Acceptance Process) The contractor shall provide Test Plans and Test Results to the COTR. (CDRL C.5.2-7, Test Plans and Test Results Report)

C.5.2.4 Facilities Modifications

The contractor shall provide facility modification services, when requested by the COTR, in accordance with all applicable executive orders, presidential directives, other federal and DHS laws, federal orders, management policies, handbooks, guidelines, processes, and procedures. All facility modifications shall be integral to and necessary for the successful performance of the IT services provided under this Task Order.

C.5.2.4.1 The contractor shall identify and coordinate complete facilities infrastructure modifications according to the approved plan(s).

C.5.2.5 Installation and Checkout

C.5.2.5.1 The contractor shall perform installations and checkouts in accordance with the Deployment Project Plan.

C.5.2.5.2 To provide seamless transition services and promote high system availability, the contractor shall perform onsite installation checks for all deployed equipment. These checks shall verify system and network operation and capability and be completed with results provided within ten days of system move or transition.

C.5.2.5.3 The contractor shall provide to the COTR, a summary of results in accordance with the Deployment Project Plan or as requested in a Status Report (CDRL C.5.2-8, Deployment Project Plan/Status Report).

C.5.2.6 Transition to O&M

C.5.2.6.1 The contractor shall transition to O&M processes in accordance with DHS policy and procedure.

C.5.2.7 Engineering and Project Management

C.5.2.7.1 The contractor shall provide engineering and project management support for DHS deployment projects.

C.5.2.7.2 The contractor shall attend and participate at project related meetings to resolve operational problems and issues as directed.

C.5.3 INFRASTRUCTURE ENGINEERING SERVICES

C.5.3.1 On-site Engineering Team

The contractor shall provide a dedicated on-site engineering team that performs services to support DHS projects (e.g., new architecture or infrastructure designs, new deployments of network/systems, etc.), and provide support for operation and maintenance activities (maintenance of infrastructure, maintain stability of environment, monitoring, and technology refreshment etc.).

C.5.3.1.1 The contractor Engineering Team Leader, and other technical personnel as appropriate, shall attend all meetings as directed by the COTR and contribute to specific technical working groups, change control boards and change management boards set up to address engineering operations and issues with DHS Components and other Government agencies. The contractor shall structure the technical requirements/knowledge base of the team based on the current needs of DHS.

C.5.3.2 Systems Engineering Support

The contractor shall perform the design, testing, implementation, configuration validation, operation, maintenance, administration, management, backup, and recovery of DHS IT infrastructure systems, to include servers and storage devices, with an overarching system engineering function used to guide and direct the overall value and effectiveness of the system. This function shall provide support to further refine and improve on the solution as technology, business needs, and the DHS IT infrastructure mission evolve.

Projects may consist of the building and deployment of new networks and infrastructure components such as databases, servers of many types, network storage devices, other network components, and desktops/workstations, as well as the removal of existing network features and infrastructure components. Projects may include features, which require the installation and removal of hardware such as switches, servers and routers,

databases, servers of many types, storage devices, desktops/workstations and installation and un-installation of infrastructure components. Projects also may include addition and removal of security features such as antivirus, auditing tools, and policy enforcement points (PEP)s. The contractor shall complete all work in each DHS environment classification: Unclassified, Secret and Top Secret.

Engineering projects include tasks such as the following:

- E-mail and messaging services
- File share services
- Active directory services
- Storage area network services
- Backup and archive technologies
- Blackberry and wireless technologies
- Management, configuration and utility servers
- Network configuration and planning
- Client platform designs including software images and hardware configurations
- New infrastructure designs and user rollout support
- Network and server enhancements based on recommended best practices, and technical assessments

C.5.3.3 Engineering Projects

The contractor can expect to perform the following types of engineering projects:

C.5.3.3.1 The contractor shall provide network engineering services associated with the replacement of infrastructure components or the implementation of improvements to the deployed network infrastructure planned or initiated by DHS.

C.5.3.3.2 The contractor shall engineer, all telecommunication, Local Area Network (LAN), Wide Area Network (WAN) circuits and connectivity to DHS systems with Government organizations and designated DHS business partners.

C.5.3.3.3 The contractor shall perform Client Configuration Management Engineering, develop and manage the approved images and overlays on those devices managed by the contractor including engineering, building, deploying and maintaining DHS approved images for all LANs.

C.5.3.3.4 The contractor shall provide Engineer and Build Solutions for deployments and engineering project management support for deployments of new facilities and upgrades of existing facilities throughout the DHS. Possible deployment projects include both new facilities and upgrades to existing facilities.

C.5.3.3.5 The contractor shall conduct technology refreshment projects in accordance with DHS guidance and upon approval of the COTR.

C.5.3.3.5.1 The contractor shall recommend new products and technology for supporting all layers of the IT infrastructure architecture.

C.5.3.3.6 The contractor shall perform the engineering design for the Security Management Center (SMC) and design all systems to ensure positive authentication of each user before granting system access. The SMC in this

form does not exist today, and the contractor shall propose a solution for this requirement.

- C.5.3.3.6.1 The contractor shall perform support for sustaining forensics within the SMC.
- C.5.3.3.7 The contractor shall provide Video Tele-Conferencing Engineering Support to include design, conduct market research and document video capabilities needed in accordance with their assigned engineering support duties.
- C.5.3.3.7.1 The contractor shall make recommendations to the Government for acquiring video conferencing system hardware and software and for improvements to existing systems.
- C.5.3.3.8 The contractor shall perform Satellite/Cable TV Engineering including design, implement, and document facility and individual television infrastructure.
- C.5.3.3.9 The contractor shall perform Phone and Private Branch Exchange (PBX) Engineering including design, implement, and document the telephony infrastructure.
- C.5.3.3.10 The contractor shall provide engineering support for implementing and integrating applications developed by external DHS Contractors or internal DHS employees into DHS data centers.
- C.5.3.3.11 The contractor shall provide engineering support for Continuity of Operations (COOP) and Disaster Recovery (DR) to ensure DHS functions and capabilities are not lost or diminished during periods when services or components are unavailable.
- C.5.3.3.12 The contractor shall provide Security Architecture Engineering Support. The DHS security architecture provides policy enforcement support for all network enclaves. The contractor shall abide by and follow all Government and DHS directives regarding the selection of security products, the configuration and hardening of operating systems, and for all cryptographic devices.
- C.5.3.3.12.1 The contractor shall assist the Government in continuously updating and enhancing the DHS security architecture throughout the life of the Task Order.
- C.5.3.3.12.2 The contractor shall implement an Identification and Authentication (I&A) system for all users and shall implement a strong capability for administrative and remote users.
- C.5.3.3.12.3 The contractor shall implement a Discretionary Access Control (DAC) capability providing need-to-know based access for each COTR specified user of the applicable systems.

C.5.3.4 Engineering Process and Methodology

- C.5.3.4.1 The contractor shall use an engineering development lifecycle methodology consistent with ITIL framework to support projects initiated by DHS. The contractor's methodology shall include the following as a minimum:
- Requirements Definition

- Detailed Systems Design Document
- DHS Enterprise Configuration Board Review
- System Testing
- Operational instructions
- Train operations personnel in new processes or activities as required
- Implementation Instructions and Document Delivery to Deployment and Operations
- Engineering Change Request (ECR) as required
- Obtain Operations Sign-off on Change and Deliver Documentation
- Concept of Operations (CONOPS)
- Project Implementation
- O&M Assistance

C.5.3.4.2 Configuration Management (CM)

C.5.3.4.2.1 The contractor shall support CM Boards and Project Teams through activities and deliverables such as project status reports, design documents, design validation, migration planning, service delivery guidance, and implementation support documents.

C.5.3.4.2.2 The contractor shall develop, maintain, update, and implement CM plans and procedures; control configuration baselines and conduct functional and physical configuration audits and formal qualifications reviews.

C.5.3.4.2.3 The contractor shall submit proposed changes to DHS systems or to project baselines, to the Change Control Board (CCB) and the Engineering Review Group (ERG), maintain a record of all submitted and approved changes, and maintain a schedule of deliverables showing both the scheduled and actual delivery dates.

C.5.3.4.2.4 The contractor shall develop, maintain, update, and implement a Configuration Management Data Base (CMDB), an engineering release system, a configuration item development record (including the configuration index and change status listing), configuration status accounting, and support the CCB.

C.5.3.4.2.5 The contractor shall maintain configuration management of all images and provide Gold Copy images to the Government as a deliverable to this task within five business days of any approved changes. (CDRL C.5.3-1, Gold Copy Images)

C.5.4 TESTING

C.5.4.1 Test Support and Documentation

The contractor shall establish and operate a test environment to perform hardware, software and systems testing. The test environment shall include testing for engineered systems including networks, video, and phone systems. The contractor shall supply systems engineering oversight, identification of readiness criteria for all system milestones, and verification and validation oversight to include test success criteria, test plans, and requirements verification traceability to demonstrate that all implementations meet requirements as stated in the requirements database. The contractor shall propose a test environment architecture and a standardized test template that supports DHS

PROCUREMENT SENSITIVE

engineering projects. This support shall also include the development of individual test plans for each individual test project approved by the COTR. (CDRL C.5.4-1, Individual Test Plans)

C.5.4.1.1 The contractor's test template shall define the scope and approach for testing and acceptance. At a minimum, the template shall address the following: initial receipt of hardware and software, unit level testing of software components for any developed software, hardware and software integration and installation testing, and system end-to-end testing in a simulated operational environment.

C.5.4.1.1.1 The contractor's test template shall also include methodology and a systematic approach for testing external interfaces to agencies and entities.

C.5.4.1.1.2 The test template shall describe the roles and responsibilities of the contractor, the DHS program office, users, stakeholders, and external systems, the test facilities used for each testing event, and the data and sources used during testing events. The template shall describe the test plans and procedures developed for each testing event, the testing events and sequences (schedule) in which they will occur, and the integration of the testing events and the security certification and accreditation activities. The contractor performing IT-NOVA O&M shall complete all of the documentation required for C&A. IT-NOVA Program Management Office personnel shall accomplish the actual C&A.

C.5.4.2 Test and Development Lab

The contractor may be required to establish, operate and maintain a test laboratory, using CFE, to support the DHS IT Infrastructure Systems. The contractor may provide its' own existing test lab to support this effort. The test lab shall be located in the Washington DC Metro area, and a segment of the test lab shall be capable of handling tests of Top Secret information. The Government will determine the exact requirements of this facility after the Task Order is awarded. The contractor shall provide personnel to operate and maintain a Government provided classified test lab in an undetermined Government facility. The Government will provide more information on the location and requirements of the classified test lab as it becomes available.

C.5.4.2.1 The contractor shall provide support to developers and customers performing integration and test activities. The contractor shall provide support during the hours of 8:00 am ET to 5:00 pm ET, Monday – Friday, excluding Federal holidays. The contractor shall also provide support after hours, on weekends and on Federal holidays for purposes such as deployments, maintenance and extended testing support as directed by the COTR.

C.5.4.2.2 The contractor shall make configuration changes in the test laboratory and production environments at the direction of the COTR. The contractor shall plan for future configuration changes and production deployments in coordination with the COTR. The contractor shall make configuration changes in compliance with security policies and procedures and change control procedures. Configuration changes shall be in accordance with controlled and repeatable procedures established by the contractor and approved by the COTR.

C.5.4.2.3 The contractor shall document test procedures and configurations performed by the contractor relating to the support of testing activities.

PROCUREMENT SENSITIVE

- C.5.4.2.4 The contractor shall track the status of actions and tasks performed by them in support of testing activities.
- C.5.4.2.5 The contractor shall notify the COTR regarding any issues or risks that affect the performance of current or scheduled test activities. The contractor shall notify the COTR within three business days of discovery of an identified issue or risk that could affect performance of the test activities. The contractor shall provide the COTR a complete description of the issue, diagnosis, resolution actions undertaken, and the impact on the timeframe for test activities. (CDRL C.5.4-2, Test Lab Issues and Risks Report)
- C.5.4.2.6 The contractor shall perform Microsoft Exchange and Active Directory Configurations activities such as configuring Exchange and Active Directory; installing software; verifying currency of installed software; and configuring security settings, databases, and user accounts and permissions.
- C.5.4.2.7 The contractor shall install communications and network infrastructure components to support test requirements.
- C.5.4.2.8 The contractor shall create, update and maintain standard workstation images, commonly referred to as ghosts, to support deployment to the desktop. The images shall meet all stated standards for "as-is" current production environment and "to-be" production environment. The contractor shall provide the Integration and Testing with the standard mechanism for delivery of the application to the desktop.
- C.5.4.2.9 The contractor shall maintain web based applications in the test environment by performing activities such as installing upgrades, patches and service packs, assigning user names and passwords, and assigning user permissions.
- C.5.4.2.10 The contractor shall provide support to the Testing Lab by performing activities such as reviewing new application architecture, verifying that the application architecture supports the current DHS environment, and submitting findings to the COTR. (CDRL C.5.4-3, Testing Lab Findings Report)
- C.5.4.2.11 The contractor shall perform a production readiness review in order to determine whether a system is ready for deployment into the production environment.

C.5.5 OPERATIONS AND MAINTENANCE FOR END USER SUPPORT**C.5.5.1 End User and Desk Side Support**

The contractor shall provide a detailed End User and Desk Side Support Concept of Operations that includes elements such as a detailed description of processes, procedures, policies, WBS, organization chart, work flow, detailed performance metrics, and evaluation criteria for the entire Help Desk operations including Tier 1, 2 and 3, and field site support (CDRL C.5.5-1, End User and Desk Side Support Concept of Operations).

The End User and Desk Side Support Concept of Operations Plan shall demonstrate a proactive and aggressive methodology to pursue new IT technological advancements and trends applicable to help desk and desk side support such as conducting frequent and thorough market research and analysis of new IT technologies and equipment including software based upon a subjective and comparative analysis to existing DHS technology. If authorized by the COTR, the contractor shall perform and conduct

PROCUREMENT SENSITIVE

operational and theoretical performance evaluations of current IT capabilities with contractor proposed IT advancements.

The contractor's Concept of Operations Plan shall meet the following minimum requirements: Provide continuous operation 7X24X365 (366 for leap years) helpdesk and 5x12 desk side support operations, with provision that designated VIPs are entitled to on call support, that includes call center support, Network Systems Monitoring, Tier 1 (Help Desk Services) including remote desktop management for Commercial Off The Shelf (COTS) and Government Off The Shelf (GOTS) applications and Tier 2 (Desk Side Support) services as well as Tier 3 Engineering support for diagnosing and resolving end user problems unresolved by the second-level analysts. The Government reserves all rights stated for review and personnel disposition. TE C.5.5-001 provides one year's monthly Help Desk Ticket Data workload. The Following represents a portion of the workload for 2006 O&M services:

Category	Workload
LAN – A E-mail Messages	72,335,644
LAN – A Support Requests	86,565
LAN – A Active Accounts	5,976
LAN – HSDN E-mail Message	1,105,254
LAN – HSDN Support Requests	3,104
LAN – HSDN Active Accounts	1,894
LAN – C E-mail Messages	767,307
LAN – C Support Requests	11,029
LAN – C Active Accounts	1,350
VTC Sessions	2,292
Unclassified Voice Conference Bridge	21,628
DMS Messages	228,413
AMHS Messages	517,611
Secure Fax	18,988
PBX Support	16,059
Total E-mail Messages	74,208,205
Support Requests	100,698

C.5.5.1.1 Help Desk Operations through Tier 3 Engineering Support: The contractor shall design the Help Desk to act as the primary interface to the end users of various COTS and custom-developed applications. DHS currently has email

PROCUREMENT SENSITIVE

and telephonic help desk contact capabilities. The contractor shall propose the contact methods (e.g. phone, fax, web, e-mail, chat) for contacting the help desk. The contractor shall provide seamless call distribution and call management support. In accomplishing this function, the DHS requires the contractor to provide a comprehensive, state-of-the-art, Help Desk solution that aligns with industry best practices, and that represents the best value to the Department and the Government.

- C.5.5.1.1.1 The contractor shall provide the help desk facility and its associated IT infrastructure at a location(s) that is located at least 50 miles outside of the metropolitan Washington D.C. area and inside the continental U.S.
- C.5.5.1.2 The contractor shall design, implement, and maintain a DHS approved COTS enterprise help desk system capable of interfacing and reporting to DHS systems as required. Additionally, this system shall provide a knowledge base for use by Tier 2, and 3 technicians and provide self-help for end users. All data generated, stored, and maintained in the system remains the property of the Government.
- C.5.5.1.3 The contractor shall provide on-site and field office support comprised of personnel with appropriate level of security clearances who will resolve complex technical problems of laptops, desktops, network peripheral devices, network components, storage devices, and troubleshooting of various software- and hardware-related issues.
- C.5.5.1.4 The contractor shall provide infrastructure advanced operational support and infrastructure services to DHS. The contractor shall perform troubleshooting to isolate the source of, diagnose and/or resolve, or assist in the resolution of IT and telecommunications problems (end-to-end).

C.5.5.2 Maintenance

- C.5.5.2.1 The contractor shall develop a Preventative Maintenance Plan, Preventative Maintenance Policies and Preventative Maintenance Procedures for all DHS IT and telecommunications fixed and mobile systems/equipment. The contractor shall provide to the COTR the plan within 40 business days of Task Order start, the policies within 60 business days and the procedures within 120 business days. (CDRL C.5.5-2, Preventative Maintenance Plan, Policies and Procedures)
- C.5.5.2.2 The contractor shall perform preventative maintenance on DHS system components in accordance with the DHS approved Preventative Maintenance Plan, policies and procedures. This includes personnel to perform the support and maintenance of data center assets, except for OEM warranty and maintenance agreements. For all new installations, system upgrades or routine maintenance the contractor shall complete all requested administrative requirements and reports to the CCB for approval prior to implementation. All information shall be presented to the COTR.
 - C.5.5.2.2.1 The contractor shall coordinate with the Government to schedule any system maintenance downtime sufficiently in advance to enable smooth operations during maintenance windows.
- C.5.5.2.3 The contractor shall maintain the Microsoft Systems Management Server (SMS) Deployment solution, or newer equivalent technology, to support the

PROCUREMENT SENSITIVE

management and distribution of changes to the DHS computing environment. Using this technology the contractor shall:

- C.5.5.2.3.1 Perform software pushes and security patch management; provide an accurate account of software usage; and inventory network devices.
- C.5.5.2.3.2 Create, maintain and update application packages.
- C.5.5.2.3.3 If system changes are required the contractor shall follow the established DHS Change Control and Security Review processes prior to implementation.

C.5.6 VIDEO TELECONFERENCING**C.5.6.1 Video Teleconferencing (VTC)**

The contractor shall engineer, operate, and maintain Video teleconferencing and multimedia services and equipment. The contractor shall support customers who receive core services and customers who receive enterprise-level service as depicted in TE C.1.2-002. Conferencing and multimedia equipment includes support for secure and non-secure bridging systems, display and projection systems, electronic whiteboards, audio systems, DVD and video recording and replay, video switching systems, control systems, and video cameras. A list of the type of VTC equipment supported is provided at TE C.3.1-001, Government Furnished Equipment.

- C.5.6.1.1 The contractor shall provide 7X24X365 (366 for leap years) support for set up and operation of VTC and multimedia systems for DHS buildings, provide user level maintenance support for VTC and multi-media systems, and operate video conferences at multiple locations.
- C.5.6.1.2 The contractor shall maintain, setup, monitor, and troubleshoot video equipment for users. The contractor shall assist customers with the use of video conferencing systems by providing personal instruction in the use of control interfaces and procedures.
- C.5.6.1.3 The contractor shall schedule and monitor all video teleconferencing sessions.
- C.5.6.1.4 The contractor shall maintain an inventory of video conferencing equipment owned and leased by DHS.
- C.5.6.1.5 The contractor shall maintain a DHS video conferencing contact list.
- C.5.6.1.6 The contractor shall maintain and operate a VTC management platform.
- C.5.6.1.7 The contractor shall install/replace and configure video conferencing equipment required by DHS Component customers.
- C.5.6.1.8 The contractor shall complete all work in each DHS environment classification: Unclassified, Secret and Top Secret.

C.5.7 SATELLITE/CABLE TELEVISION OPERATIONS

The contractor shall engineer, operate, and maintain satellite/cable television services and equipment.

C.5.7.1 Operations

- C.5.7.1.1 The contractor shall complete all work in each DHS environment classification, Unclassified, Secret, Top Secret, and Top Secret/SCI.

PROCUREMENT SENSITIVE

- C.5.7.1.2 The contractor shall perform periodic testing to ensure system operations.
- C.5.7.1.3 The contractor shall set up and maintain channel alignment of the head-in systems, coordinate system expansion and reconfiguration, interface and coordinate with the Digital Satellite Service (DSS) and cable contractors as necessary for maintenance and system reconfiguration.
- C.5.7.1.4 The contractor shall maintain, setup, monitor, and troubleshoot satellite and/or cable TV equipment for users, assist customers with the use of satellite and/or cable TV systems by providing personal instruction in the use of control interfaces and procedures.
- C.5.7.1.5 The contractor shall maintain and update an inventory of satellite and/or cable TVs and associated peripheral, connectivity and installation components and make available for COTR review upon request.
- C.5.7.1.6 The contractor shall develop, maintain, update and implement a DHS satellite and/or cable TV contact list.
- C.5.7.1.7 The contractor shall install/replace and configure satellite and/or cable TV equipment as directed by the COTR or DHS Component customers.

C.5.8 VOICE COMMUNICATIONS AND MESSAGING

The contractor shall engineer, operate, and maintain voice communications, messaging services and equipment.

C.5.8.1 Private Branch Exchange (PBX) Infrastructure

The contractor shall provide administrative, operational, and management support for the DHS headquarters and associate component telecommunications. The contractor shall install, maintain and support the PBX Infrastructure within the Washington DC metropolitan area. This infrastructure includes components such as an Integrated Services Digital Network (ISDN), Voice over Internet Protocol (VOIP), analogue, digital and other communication devices at specified levels of classification. The contractor shall use FTS 2001 currently and transition to Network for Phone and PBX operations.

- C.5.8.1.1 The contractor shall manage, update and make changes to systems.
- C.5.8.1.2 The contractor shall install, maintain, setup, monitor, and troubleshoot phone and PBX equipment for users, assist customers with the use of phone systems by providing personal instruction in the use of control interfaces and procedures, and install/replace and configure phone and PBX equipment required by DHS Headquarters and Component customers.
- C.5.8.1.3 The contractor shall maintain an inventory of phone and PBX equipment owned and leased by DHS.
- C.5.8.1.4 The contractor shall perform management and scheduling for conference bridges at unclassified and secure levels
- C.5.8.1.5 The contractor shall complete all work in each DHS environment classification: Unclassified, Secret and Top Secret.
- C.5.8.1.6 The contractor shall provide handset installation and configuration.
- C.5.8.1.7 The contractor shall develop, maintain, update, implement and report on phone and PBX services such as providing the following: A DHS Dial Plan, Telephone Infrastructure Cabling plant (infrastructure) documentation, port

PROCUREMENT SENSITIVE

utilization reports, load balancing reports, route pattern reports. (CDRL C.5.8-1, Phone and PBX Services Report)

- C.5.8.1.7.1 The contractor shall maintain all documentation and records of telephony infrastructure.
- C.5.8.1.7.2 The contractor shall ensure all telephony infrastructure components conform to a standardized set-up and design and provide redundancy.
- C.5.8.1.8 The contractor shall continuously (or as directed) refresh the PBX, conference bridges and all tools and technologies for providing this support so that the Government is ensured the best value for its investment, to include all systems upgrades and patches to current release levels.

C.5.8.2 Telephone Switchboard Operations Center

The contractor shall provide contiguous hours 24X7X365 Telephone Switchboard Operation Center services for the DHS headquarters to The Secretary of the DHS, executive staff, employees, DHS contractors, and the public. The monthly call volume for the last year is provided at TE C.5.8-001.

- C.5.8.2.1 The Switchboard shall be maintained and operated within the Washington, DC area in proximity to the switch.
- C.5.8.2.2 The contractor shall develop, maintain, update and implement an organizational reference and automatic call directory (ACD).
 - C.5.8.2.2.1 The contractor shall create a knowledge base reference for operators that identifies DHS organizational elements, their responsibilities/services, and anticipated issues and/or keywords that may be used by members of the public when contacting the DHS. The contractor shall coordinate with each and every DHS Headquarters organization and create a proposed reference within 20 business days of Task Order start. The proposed reference shall be submitted to the COTR for review and approval prior to use of the reference. The contractor shall update the reference within five business days of DHS announcement of functional realignments or organizational moves and as directed by the COTR. (CDRL C.5.8-2, Switchboard Knowledgebase Reference)
 - C.5.8.2.2.2 The contractor shall create a proposed ACD and submit it to the COTR within 40 days of Task Order start. The contractor shall make changes to the proposed ACD as directed by the COTR and make the ACD operational within 10 business day of final approval. The ACD shall be subject to COTR directed changes throughout the life of the Task Order. (CDRL C.5.8-3, Automatic Call Directory)
- C.5.8.2.3 The contractor shall provide an employee and office call directory service to DHS or DHS agency callers and connect callers who are members of the public to the requested/appropriate office or individual (phone extensions shall not be provided to the public).
 - C.5.8.2.3.1 The contractor shall develop, maintain, update and implement an office and personnel directory.
 - C.5.8.2.3.2 The contractor shall use the current office and personnel directory and the DHS Personal Profile data in Microsoft Outlook to identify phone extensions.

PROCUREMENT SENSITIVE

- C.5.8.2.4 The contractor shall operate the teleconference bridge and will schedule teleconferences as requested and provide confirmation of scheduling to the requesters.
- C.5.8.2.5 The contractor shall assign an operations center project manager who will report to the Director of the DHS Executive Service Center. The contractor shall have a supervisor for the switchboard.
- C.5.8.2.6 The contractor shall provide automated reports monthly to the COTR on call pattern statistics. (CDRL C.5.8-4, Call Pattern Statistics Report – Monthly) The reports shall include the following:
- Call volume by day of week and duty hours (8:00 am to 7:00 pm ET) and non-duty hours.
 - Aggregate monthly call volume from internal (DHS) and external (public) sources
 - Aggregate monthly call volume of external calls and the specific ACD option selected
- C.5.8.2.7 The contractor shall develop, maintain, update and implement a Continuity of Operations (COOP) Plan for Switchboard Operations. (CDRL C.5.8-5, Switchboard COOP Plan)
- C.5.8.2.8 The contractor shall train its staff on switchboard operations.
- C.5.8.2.8.1 The training shall cover DHS call handling policy, equipment use, use and maintenance of references, and routing of calls to the appropriate office or person.
- C.5.8.2.8.2 The contractor shall develop, maintain, update and implement a training lesson plan and materials for the handling of calls in a professional manner and tone of voice. The contractor shall submit the initial and all updated lesson plans to the COTR for review and approval prior to using for training. (CDRL C.5.8-6, Switchboard Training Lesson Plan)
- C.5.8.2.9 The contractor shall make recommendations necessary for upgrading the switchboard operation.

C.5.8.3 Voice Over Internet Protocol (VOIP)

The contractor shall facilitate the DHS transition and implementation of VOIP.

C.5.8.4 Unified Messaging

The contractor shall facilitate the DHS transition and implementation of unified messaging.

C.5.9 NETWORK MANAGEMENT CENTER (NMC)**C.5.9.1 NMC Operations**

The contractor shall monitor, manage, and perform problem resolution support of all DHS HQ components, which consist of network circuits and devices, computer systems, applications, and databases/file servers. The purpose of the Network Management Center is to monitor systems 7X24X365 (366 for leap years). The NMC/SMC facility is not currently built and the Government anticipates completion at the Nebraska Avenue Complex located in Washington, DC, Building 100, second floor during the second

PROCUREMENT SENSITIVE

quarter of FY08. The NMC/SMC will be located and maintained in a SCIF environment. The contractor shall use the NMC/SMC to monitor and manage all three network enclaves using industry standard applications and shall segregate; both logically and physically, maintain and operate NMC systems by security classification level. The contractor shall ensure that the NMC interfaces with the DHS Network Operations Center (NOC), including escalation procedures. The NOC is managed by Customs and Border Protection (CBP) and it is responsible for the the enterprise level issues that affect all components of the Department. The contractor shall operate and maintain the primary and backup NMC to monitor the following functions on a 7X24X365 (366 for leap years) basis:

- Network operations
- Security operations
- Help Desk operations

- C.5.9.1.1 The contractor shall respond to network related problems and notify the COTR as specified in the DHS Escalation Policy. The contractor shall work in conjunction and cooperate with other LAN personnel and contractors supporting other IT infrastructure areas in order to respond to alarms, diagnose problems, and escalate issues to DHS NMC for fast, effective response before they cause costly unscheduled downtime or poor performance.
- C.5.9.1.2 The contractor shall monitor all network devices, environmental systems or peripheral devices which are managed or monitored using Simple Network Management Protocol (SNMP) and diagnostics tools currently in place, and to include any future additions to the hardware configuration to quickly detect, track, isolate, and resolve problems.
- C.5.9.1.3 The contractor shall perform troubleshooting techniques to isolate the source of, diagnose and/or resolve, or assist in the resolution of network problems (end-to-end) and root cause analysis.
- C.5.9.1.4 The contractor shall develop and submit the NMC Standard Operating Procedures (SOP) to the COTR for review and approval. (CDRL C.5.9-1, NMC Standard Operating Procedures)
- C.5.9.1.5 The contractor shall operate the NMC and support DHS COOP exercises. The contractor shall perform tests as requested by the COTR quarterly, at a minimum and as required by the DHS COOP Policy to verify failover from primary to backup NMC without any disruption of operational capability.
- C.5.9.1.6 The contractor shall identify the requirements for and install upgrades, updates, service packs, and patches.
- C.5.9.1.7 The contractor shall maintain security protection and reliability updates on operating systems.
- C.5.9.1.8 The contractor shall identify and notify the COTR of any upgrades, updates, service packs, and patches determined to be incompatible with system or application specifications and proceed as directed by the COTR.
- C.5.9.1.9 The contractor shall monitor system operability and functionality, identify abnormal performance and degradation and complete resolution actions and return the system to normal performance.

PROCUREMENT SENSITIVE

- C.5.9.1.10 The contractor shall monitor system capacity, maintain normal performance, and prevent system degradation resulting from usage exceeding system capacity.
- C.5.9.1.11 The contractor shall operate the NMC to respond to changes in loads on the network as necessary, in response to higher threat levels.
- C.5.9.1.12 The contractor shall report on the network and systems infrastructure using a GFE Enterprise Management Tool. The contractor shall report on network and system status as directed by COTR to include Network Diagrams that identify enterprise building, floor, room, rack and system for HQ and field sites. (CDRL C.5.9-2, Network and Systems Infrastructure Report)
- C.5.9.1.13 The contractor shall notify and update the Help Desk of any network or system infrastructure issue or problem detected or managed by the NMC.
- C.5.9.1.14 The contractor shall manage status, errors, and inbound and outbound traffic statistics of all routing interfaces, bandwidth utilization, and errors of all inbound and outbound LAN /WAN circuits.
- C.5.9.1.15 The contractor shall manage the LAN/WAN routing protocol between the routers; perform port management, network capacity management (including planning and trending), and configuration management.
- C.5.9.1.16 The contractor shall maintain configuration LAN/WAN change documentation, and continually update schematics to reflect current network architectures.
- C.5.9.1.17 The contractor shall support terminal equipment associated with special circuits as required and shall maintain and monitor connections to LAN tail sites.
- C.5.9.1.18 The contractor shall maintain and monitor the secure wide area network connection to existing and/or future connections to other Intelligence Community's networks.
- C.5.9.1.19 NMC/SMC management shall provide Network Metrics Reports to the COTR. (CDRL C.5.9-3, Network Metrics Reports)
- C.5.9.1.20 The contractor shall maintain the outbound and inbound Internet access to ensure full operational capability for internal and external user contiguous hours access to the Internet 24X7X365 (366 for leap years) except during periods of Government approved planned outage. The contractor shall provide outbound access connectivity for the DHS staff to the Internet. The contractor shall provide In-bound public access connectivity to the DHS Public Website.
- C.5.9.1.21 The contractor shall monitor Internet access, identify, and resolve interruptions to the Internet service. The contractor shall perform upgrades, implement changes, and install patches to components on the Internet servers. These shall include middleware updates, new Database Source Networks (DSNs), application updates, application additions, patches and hot fixes.
- C.5.9.1.21.1 The contractor shall perform upgrades, implement changes and install patches to components of the Web Content Management System (WCMS), which publishes finished web site updates to the public web site.

PROCUREMENT SENSITIVE

- C.5.9.1.21.2 The contractor shall perform all maintenance that will disrupt or could disrupt the availability of Internet services only during planned outage periods.
- C.5.9.1.21.3 The contractor shall maintain logs of Internet activity and make available for review as requested by the COTR.
- C.5.9.1.22 The contractor shall develop and utilize a system to receive, respond and resolve technical inquiries from the public regarding access to the DHS Website (currently <http://www.dhs.gov>). The DHS Webmaster receives inquiries from the public and will forward those requiring technical assistance to the contractor. The DHS Webmaster will provide the requirements for technical assistance and establish a timeline, in conjunction with the contractor, for completion of the development, set-up and operation of the Public Interface Activities technical assistance system.
- C.5.9.1.22.1 The contractor shall post Internet notices alerting those accessing the DHS Website of interruptions or other problems causing degradation of access.
- C.5.9.1.23 The contractor shall provide Web page content assistance for authorized users, developers or content providers. The contractor assistance shall include verifying approval of the request for assistance, preparation of the content, complying with the requirements of Section 508, and deploying the content.
- C.5.9.1.24 The contractor shall adhere to the DHS perspective in Enterprise Interconnection and Policy Working Group (EIWG) with the DOD to facilitate the technical issues and governance processes related to the interconnection between the Secure Internet Protocol Router Network (SIPRNET) and DHS secure networks, address operational problems and assist in extending capabilities to federal information sharing initiatives.
- C.5.9.1.24.1 The contractor shall attend meetings of and contribute to specific technical operational working groups set up to address engineering and operations issues with DoD and other Governmental agencies, and leverage the contractor knowledge and resources with the Intelligence Community (IC) to ensure that DHS is aligned with emerging IC systems engineering and technology solutions.

C.5.10 SECURITY MANAGEMENT CENTER (SMC)

The DHS SMC shall provide continuous security monitoring to detect all potential adverse events within all DHS network and computer systems. The SMC shall provide day-to-day operations and maintenance of the DHS defense-in-depth security infrastructure. At Contract award, GFE will be provided to assist in Security structure build-out. The SMC in this form does not exist today, and the contractor shall propose a solution for this requirement. (See paragraph C.5.9.1 for the location and status of the NMC/SMC.)

C.5.10.1 SMC Operations

The contractor shall centrally manage DHS Information Technology Services Office Security Management. The SMC shall be co-located with the NMC to provide a fully integrated operations and security management function.

- C.5.10.1.1 The contractor shall provide security system administration, key management, security audit and analysis, security incident reporting and response, security intrusion detection, system vulnerability assessment,

PROCUREMENT SENSITIVE

responding to Information Security Vulnerability Notices (ISVMs), the most recent anti-virus signature updates, and end-user support to resolve security issues.

- C.5.10.1.2 The contractor shall prepare a DHS Information Technology Services Office Security Management Approach and SOPs, Checklists and a DHS Information Technology Services Office Security Plan, for operations within the SMC, and submit to the COTR for approval. (CDRL C.5.10-1, Information Technology Services Office Security Management Approach and SOPs, Checklists and DHS Information Technology Services Office Security Plan)
- C.5.10.1.3 The contractor shall staff the SMC with subject matter experts to act as analysts to support 7X24X365 (366 for leap years) monitoring and response capability.
- C.5.10.1.4 The contractor shall identify the requirements for and install upgrades, updates, service packs, and patches.
- C.5.10.1.5 The contractor shall maintain security protection and reliability updates on operating systems.
- C.5.10.1.6 The contractor shall identify and notify the COTR of any upgrades, updates, service packs, and patches determined to be incompatible with system or application specifications and proceed as directed by the COTR.
- C.5.10.1.7 The contractor shall monitor system operability and functionality, identify abnormal performance and degradation and complete resolution actions to return the systems to normal performance.
- C.5.10.1.8 The contractor shall monitor system capacity, maintain normal performance, and prevent system degradation resulting from usage exceeding system capacity.

C.5.10.2 Vulnerability Assessment

- C.5.10.2.1 The contractor shall perform threat and vulnerability assessments on all information system assets, including Public Facing operational IT systems, as part of its sustaining Security Systems Administration. The contractor shall generate a Vulnerability Assessment Report following each assessment that lists the vulnerabilities discovered, and their impact/threat to the network (high, medium, and low). (CDRL C.5.10-2, Vulnerability Assessment Report) The contractor's security team shall present high threat vulnerabilities and suggested mitigations to the Government prior to leaving the sites. The report shall include mitigation recommendations for all other vulnerabilities identified. The SMC shall report the status of actions to correct the high threat vulnerabilities to the System Security Administrators (SSAs), security manager, and the ISSO/ISSM on a monthly basis.
- C.5.10.2.2 The contractor shall identify specific security weaknesses on target systems, and provide recommended techniques and/or improvements to strengthen the security of the target system.
- C.5.10.2.3 The contractor shall scan DHS systems using GFE or vulnerability tools approved by the Government.
- C.5.10.2.4 The contractor's vulnerability assessment capability shall identify unauthorized access points or potential implementation weaknesses.

PROCUREMENT SENSITIVE

C.5.10.2.5 The contractor shall define and audit PEP policy and determine how the PEP handles application(s) traffic such as web, email, or telnet. Additionally, the integrated security team's DHS PEP Management Policy shall describe PEP updates and management.

C.5.10.2.6 The contractor shall identify, review and analyze the vulnerabilities associated with each application and the cost-benefits associated with the methods used for securing the applications and provide the findings to the COTR. (CDRL C.5.10-3, Application Vulnerability Cost-Benefit Analysis)

C.5.10.2.7 The contractor shall develop a DHS PEP policy that identifies the necessary network applications, vulnerabilities associated with these applications, creation of applications traffic matrices identifying protection methods, and PEP rule-sets based on applications traffic matrices.

C.5.10.3 Security Information Management (SIM) & Security Management Capability

SIM is an automated capability that provides for the collection, analysis, alerting, reporting, and trending for all of the system components within a computing environment.

C.5.10.3.1 The contractor shall establish, operate, and maintain an Information Technology Services Office security management capability suitable for the real-time monitoring and assessment of all assigned assets in accordance with DHS MD 4300 and Security Architecture Volume 2. Examples of these assets are PEPs, virtual private networks, routers, switches, server and end system computing elements. Additionally, the system shall collect event input from the IDS, anti-virus, and network management systems. DHS HQ shall procure initial GFE for all LAN environments. The contractor should propose tools to address capabilities that may not be either fully procured or implemented by the government prior to the award of IT NOVA. DHS determined that the ESM and other enterprise security management products manufactured by ArcSight will form the nucleus of the DHS HQ SIM.

C.5.10.3.2 The SMC shall be responsible for day-to-day operations and maintenance of the defense-in-depth security infrastructure. The SMC shall be co-located with the Information Technology Services Office NMC to provide a fully integrated operations and security management functions.

C.5.10.4 Security Systems Administration

The contractor shall manage and monitor all DHS security components including intrusion detection systems (IDSs) and PEPs. Security systems shall use an automated delivery function to the maximum extent possible to push anti-virus software signature updates to the desktops and provide the results to Information Technology Services Office NMC/SMC management for analysis. Security systems administration shall include the following:

C.5.10.4.1 The contractor shall monitor DHS systems for intrusion activity, and be prepared to take appropriate steps to mitigate any suspected intrusion while maintaining the availability of the system for all authorized users.

C.5.10.4.2 The contractor shall conduct computer forensics, law enforcement evidence collection and preservation efforts in support of the system.

C.5.10.4.3 The contractor shall conduct assessments quarterly (or as directed) at all major nodes, such as gateways and regional centers where data is stored and report the results of such findings to the COTR.

C.5.10.4.4 The contractor shall perform anti-virus scans of the entire DHS networks in accordance with the proscribed procedures in DHS Approved Maintenance Downtime as described in Section C.5.6.4.

C.5.10.5 Security Change Management

The contractor shall centrally manage and control the implementation of corrective patches and service packs.

C.5.10.5.1 For all new installations, system upgrades or routine maintenance, the contractor shall complete all requested administrative requirements and testing prior to submission to CCB for approval.

C.5.10.5.2 The contractor shall assess DHS directed security patches or service packs before implementation to verify the need to implement and the impact upon the system.

C.5.10.5.3 The contractor, in coordination with DHS, shall determine the schedule for deploying Information Assurance and Vulnerability Alerts (IAVAs), patches, and service packs.

C.5.10.5.4 The contractor shall provide monthly reports to the appropriate COTR on the success of the patch/service pack deployment, and any issues preventing completion. (CDRL C.5.10-4, Patch/Service Pack Deployment Report)

C.5.10.6 Security Log Access, Retention and Review

C.5.10.6.1 In accordance with applicable DHS directives, the contractor shall maintain all security logs for the required retention period. Access to these logs shall be restricted to ISSM approved personnel.

C.5.10.6.2 The contractor shall record all accesses to these logs, including an audit history of reads, changes, and deletions.

C.5.10.6.3 The contractor shall protect logs under these restrictions to include all security logs (PEP, IDS, anti-virus), as well as domain controller, and all management systems as directed by the ISSM/ISSO.

C.5.10.6.4 The contractor shall perform reviews and provide monthly reports (or as directed) on all system logs. (CDRL C.5.10-5, System Log Security Review Report)

C.5.10.7 System Security Administrators

The contractor shall provide all System Security Administrators (SSA). Each SSA is an extension of the SMC in providing security oversight, monitoring, and reporting for DHS and is the principal POC for all security issues and support of Government ISSMs and ISSOs.

C.5.10.8 Data Spills and Response

The contractor shall employ guards and gateways to monitor, prevent, detect, respond, report and correct the unauthorized release of Secret or TS/SCI data.

C.5.10.9 Incident Response

The contractor shall create and maintain the capability to respond rapidly to any network event that could affect the Information Assurance /Information Protection posture of DHS. The contractor shall create and maintain SOPs and checklists to cover events such as network intrusions, data spills, introduction of malicious software, Denial of Service (DoS)

PROCUREMENT SENSITIVE

incidents, inappropriate network use, etc. The contractor shall base these SOPs and checklists upon existing DHS directives and guidance.

C.5.10.9.1 The contractor shall maintain a trained Computer Security Incident Response Team (CSIRT), which may include systems administrators and other personnel. The contractor shall develop policy and processes related to the establishment and generation of the CSIRT. The CSIRT shall maintain a digital forensics capability that establishes and maintains an evidentiary chain of custody.

C.5.10.9.2 The contractor shall utilize all available audit logs to support forensics activities, and shall develop SOPs for the conduct of forensics investigations that shall be submitted to the COTR for approval. (CDRL C.5.10-6, Forensic Investigation SOPs)

C.5.10.9.3 The contractor shall follow established reporting procedures when providing initial notification to the SSAs, Security Manager, ISSO, and Information System Security Manager (ISSM) of any network event or incident.

C.5.10.9.4 The contractor shall provide Event and Incident Reports to the Government as directed in the DOD-Dir.8500 Series Computer Network Defense (CND). (CDRL C.5.10-7, Event and Incident Reports) The Continuity of Operations Plan shall detail non-IT incident response, as identified in HSPD-5 and the DHS Initial National Response Plan.

C.5.10.10 Information Condition (INFOCON) Management

In response to potential threats to the DHS (and U.S. infrastructure assets in general), the Secretary of the DHS (SEC DHS) may direct the elevation of the protection levels of the network and IT assets through the implementation of INFOCON levels. The INFOCON level is determined based upon an assessment of risk to the DHS networks. When directed by DHS, the Designated Accrediting Authority (DAA) will approve specific measures of protection for the networks.

C.5.10.10.1 The contractor shall implement INFOCON conditions within the DHS, and will track the attainment of the directed INFOCON level across the networks.

C.5.10.10.2 The contractor shall assist in the coordination of DHS INFOCON levels and that of external entities such as DOD as directed by the COTR.

C.5.10.10.3 The contractor shall develop, submit to the COTR for approval and follow SOPs and checklists to track the changes in INFOCON level and the attainment of the directed INFOCON. (CDRL C.5.10-8, INFOCON Level SOPs and Checklists)

C.5.10.10.4 The Information Technology Services Office SMC shall create SOPs based upon DHS policies to support the DHS Computer Network Defense Continuity of Operations Plan.

C.5.11 COMMUNICATIONS SECURITY (COMSEC) MANAGEMENT

C.5.11.1 COMSEC Security

C.5.11.1.1 The contractor shall provide on-site 7X24X365 (366 for leap years) COMSEC Support for services such as installation maintenance and administration of messaging systems (e.g., DMS, AMHS, receipt, transmission and/or distribution of all forms of communication media such as: faxes, messages, correspondence, etc).

PROCUREMENT SENSITIVE

- C.5.11.1.2 The contractor shall operate encryption systems to support secure voice and video systems as required and assist Government personnel with receipt, inventory control, deployment, and securing of encryption systems. The contractor shall assist users in the operations of secure facsimile systems, and perform user level maintenance.
- C.5.11.1.3 The contractor shall receive, distribute, inventory and administrator COMSEC account material.
- C.5.11.1.4 The contractor shall perform COMSEC technical tasks such as maintaining and updating messaging systems, installation and maintenance of all cryptographic equipment (e.g., TACLANE, FASTLANE, and KIV-7).
- C.5.11.1.5 The contractor shall provide a COMSEC Plan to address implementation and operational details in accordance with DHS and NSA policies and procedures and provide to the COTR. (CDRL C.5.11-1, COMSEC Plan)
- C.5.11.1.6 The contractor shall establish and manage a COMSEC account in accordance with DHS guidelines and procedures.
- C.5.11.1.7 The contractor shall manage, update and maintain the Information Technology Services Office SMC COMSEC account and COMSEC controlled items (CCI) and all keying material.

C.5.12 OTHER COMMUNICATIONS OPERATIONS**C.5.12.1 Emergency Notification System**

The contractor shall program and operate Emergency Notification System (Communicator) and:

- C.5.12.1.1 The contractor shall provide user training as required.
- C.5.12.1.2 The contractor shall interface and coordinate with the vendor for maintenance and software upgrades.
- C.5.12.1.3 The contractor shall provide data entry and system backup as required.

C.5.12.2 Executive Telecommunications Support

The contractor shall provide contiguous hours 24x7x365 secure and non-secure IT and communications services and support for the Secretary of the Department of Homeland Security (DHS), the Deputy Secretary and other designated DHS executive staff while they are traveling outside of the National Capital Area (NCA).

- C.5.12.2.1 The contractor shall provide daily operations support for fixed and mobile IT/Telecom equipment such as the following tasks:
- Manage and control inventory
 - Operate, test, troubleshoot, and maintain equipment
 - Operate and ensure capability of mobile IT/Telecom vehicle
 - Maintain proficiency on existing and future IT/Telecom systems
 - Assist in design, development, analysis, integration, and evaluation of IT/Telecom systems
 - Plan and perform preventive maintenance inspections on IT/Telecom equipment that is installed at the ETS NAC facility, installed in secure mobile vehicle platforms, and used while traveling

- Perform equipment lifecycle management
 - Perform COMSEC and project management support
 - Synthesize customer needs with commercially available IT products into requirements that will allow the implementation of engineered IT/Telecom systems and processes
 - Provide operational assistance to DHS Senior Executives and staff
- C.5.12.2.2 The contractor shall provide travel operations support such as:
- Coordinate with DHS staff advance arrival personnel at the travel sites
 - Transport IT/Telecommunications equipment to and from travel sites
 - Conduct site survey(s) for installation of travel systems
 - Install and remove IT/Telecom equipment from trip site
 - Provide point-to-point telecom support to travel teams
 - Coordinate their own travel logistics arrangements

C.5.13 TRAINING

The contractor shall provide professional, technical and end-user training. The contractor shall provide the training support for DHS IT operations to include user applications and network access, system administration, and security. The contractor shall develop training plans for DHS personnel, system users, and contractor personnel. The training plans shall be submitted to the COTR for approval prior to implementation. (CDRL C.5.13-1, Training Plan) The contractor shall maintain an electronic record of all training courses conducted and who attended.

C.5.13.1 System Administrator Training

The contractor shall provide appropriate training, training materials, and help desk support for the applications provided for DHS. The contractor shall work with the Government to develop a Training Plan that addresses the delivery of training to supervisors, and system administrators. The plan shall be in conformance with the SOPs and SLAs.

C.5.13.1.1 The contractor shall provide the training curriculum and training materials for DHS applications and desktops. The training materials shall be suitable for both users and system administrators, and adopted from existing training materials for legacy applications integrated into DHS service.

C.5.13.1.2 The contractor shall provide the delivery of the user training through a "train-the-trainer" approach to the maximum extent possible. The contractor shall provide training directly to the users at either contractor facilities or Government facilities.

C.5.13.1.2.1 The contractor shall provide DHS training through training delivery methods such as the following:

- Direct delivery of the training to user and system administrators at DHS facilities or other locations as directed by the Government
- Direct delivery of special user training to personnel who will then act as trainers in the field

- Delivery of training to user through computer-based training (CBT) or other distance learning techniques that the contractor has found effective

C.5.13.1.3 The contractor shall provide documentation and manuals for COTS products that have them.

C.5.13.2 Security Training

The contractor shall develop, document, and administer a Security Training Plan and Curriculum providing annual required security awareness and operational security refresher training. Delivered training elements shall comply with DHS and other relevant external agency directives and policies for enforcement of Government security provisions. The appropriate COTR will review and approve the training curriculum prior to implementation. Implementation of the training may be either through instructed sessions or via computer-based self-paced training. The contractor may elect to provide this training in incremental elements depending upon component usage, and the training may be delivered via computer-based training, help files or instructed sessions following Government approval.

C.5.13.2.1 The contractor shall provide training to users and operators to facilitate the usage of security components within the network and on the desktop.

C.5.13.3 End-User Training

The contractor shall develop, document, and conduct end-user training on all COTS, GOTS, and unique software. The appropriate COTR will review and approve the training curriculum prior to implementation. Implementation of the training may be either through instructed sessions or via computer-based self-paced training. The contractor may elect to provide this training in incremental elements depending upon component usage, and may be delivered via computer-based training, help files or instructed sessions following Government approval.

C.5.14 WIRELESS MANAGEMENT

The contractor shall provide services to the Wireless Management Office (WMO) to develop Wireless Communications Architecture (WCA) and Enterprise Architecture Governance. The contractor shall also provide Support Systems Engineering, support to Working Groups, Frequency Management and Spectrum Planning.

The contractor shall provide support to the WMO in the following manner:

- Work as an integrated member of the WMO team, and in close coordination and cooperation with the representatives of the DHS components, members of the Wireless Working Group (WWG), Enterprise Architecture (EA), and other DHS participants designated by the WMO or the WWG
- Maintain a strategic mission focus on the overarching strategic priorities of the WMO as they work to meet the needs and obligations of DHS' WCA and EA programs
- Perform specific actions and produce results that meet the goals of the WMO as coordinated and evaluated by the members of the WMO, WWG, EA, and the DHS CIO

C.5.14.1 Wireless Communication Architecture Development

C.5.14.1.1 The contractor shall enhance the pilot architecture and concept of operations that support deployable wireless communications, for use in the

PROCUREMENT SENSITIVE

event of a disaster, terrorist attack, or other crisis, and can be tested against past events (e.g., Hurricane Katrina, Los Angeles earthquakes, 9/11).

- C.5.14.1.2 The contractor shall integrate and reflect the relevant aspects of the following programs, where applicable and relevant: IWN, SAFECOM, Rescue 21, Command 2010, Deepwater, NAIS, FNARS, CBP Modernization, SBI.net, HSARPA, 25 Cities, Gulf Coast, and others as appropriate.
- C.5.14.1.3 The contractor shall integrate critical interoperability standards into the Wireless Communications Enterprise Architecture Technical Reference Model (TRM) spanning all DHS wireless programs and infrastructure.
- C.5.14.1.4 The contractor shall identify infrastructure and assets that can be leveraged in support of the overall WCA, and realize synergies from shared resources during all phases of the system lifecycle.

C.5.14.2 Systems Engineering Support

The contractor shall support Systems Engineering initiatives along with the affiliated work products through the following tasks:

- C.5.14.2.1 Ensure tactical communications investment meet common and unique mission needs.
- C.5.14.2.2 Improve interoperability while facilitating long-term investment goals.
- C.5.14.2.3 Develop models of existing and desired future frameworks.
- C.5.14.2.4 Provide analysis, decision support, risk mitigation and system engineering processes for migrating to the desired future framework.
- C.5.14.2.5 Develop a Systems Engineering (SE) framework for the WMO, its Programs and Projects. The initial framework shall be created and submitted to the COTR within 40 business days of Task Order start and update as changes occur. (CDRL C.5.14-1 Wireless Systems Engineering Framework)
- C.5.14.2.6 Define and maintain Systems Engineering Gold Standards and best practices for all aspects of wireless and general communications systems engineering and the associated software-based or other tools.
- C.5.14.2.7 Employ, maintain, improve and verify practices against Systems Engineering Gold Standards upon Government approval of the standards.
- C.5.14.2.8 Develop the definition and specification of Systems Engineering documents such as the Systems Engineering Management Plan (SEMP), Concept of Operations (CONOPS), Functional Baseline, System Specifications, System Development Specifications, and other applicable requirement documents to maintain Requirements traceability. (CDRL 5.14-2, Wireless SEMP, Wireless CONOPS, Functional Baseline, System Specifications, System Development Specifications)
- C.5.14.2.9 Write statements of work and specifications for the development, deployment and maintenance of the IWN program and other DHS programs.
- C.5.14.2.10 Evaluate technical performance, develop verification strategies and perform Independent Verification & Validation, review/critique of deliverables of other contractors.

- C.5.14.2.11 Employ WMO's existing Metis (brand) toolset and the WCA Framework to create architecture based on the DoDAF to capture WMO program and project objectives, CONOPS, and requirements.
- C.5.14.2.12 Provide technical direction and administrative support for the development of interoperability standards, such as the Wireless Inter-System Interface (WISI), Software Defined Radio (SWR), and other standards in support of DHS wireless interoperability objectives.
- C.5.14.2.13 Provide a full range of on-site engineering, technical, acquisition, and logistics support to ensure that fully integrated multimedia (e.g., voice, data, video) cable and wireless based tactical and strategic command, control, sensor, communication, security, and surveillance systems are properly developed, fielded by, and effectively operated in support of the DHS.
- C.5.14.2.14 Design, implement, and support private and public alerting systems, including AM, FM, TV, and satellite system broadcast capabilities and the appropriate subscriber devices.

C.5.14.3 Working Group Support

- C.5.14.3.1.1 The contractor shall support the Wireless Working Group, Project 25, Project 34, Push-to-Talk on Cellular (POC), Standards Working Sessions, RFID summit meetings, and various conferences through meeting attendance, providing subject matter expertise, providing documents, developing materials for presentation and performing follow-up actions.

C.5.14.4 Enterprise Architecture Governance Support

The contractor shall support the DHS WMO to ensure that the wireless investments and other wireless projects brought before the EACOE comply with WMO's policies and strategic direction.

C.5.14.5 Frequency Management Support

The contractor shall perform frequency management functions as follows

- C.5.14.5.1 Assist with the daily selection, coordination, and processing of all radio frequency authorizations in support of DHS components. The selected frequencies shall be selected from the frequencies in the Government Master File.
- C.5.14.5.2 Develop frequency plans that meet new communications requirements and improve methodologies for interoperability among the DHS components and key federal, state, and local partners.
- C.5.14.5.3 Perform detailed frequency planning for DHS' migration to new wireless systems, utilizing 12.5 kHz channel bandwidth in accordance with the NTIA Manual of Regulations and Procedures for Federal Radio Frequency Management.
- C.5.14.5.4 Ensure that systems will neither cause nor receive harmful interference to or from other authorized users when placed in their intended operational environments.
- C.5.14.5.5 Ensure accuracy of all frequency assignments by conducting "five-year-reviews" of records for all locations with installed narrowband equipment.

C.5.14.6 Spectrum Planning

PROCUREMENT SENSITIVE

The contractor shall support Spectrum Planning as follows:

- C.5.14.6.1 Develop channel plans for implementations of DHS wireless systems, including DHS OneNet-Wireless, which feeds into a nationwide channel plan.
- C.5.14.6.2 Review current frequency plans and those under development to support the implementations of DHS OneNet-Wireless.
- C.5.14.6.3 Develop recommended frequency changes to eliminate technical incompatibilities, improve interoperability, and reduce and/or minimize harmful interference.
- C.5.14.6.4 Refine the nationwide channel plan with the support of the WWG Spectrum Management Working Group (SMWG) to include identifying frequencies and developing a logical structure for nationwide channels (e.g., component specific channels, DHS common channels, interoperability channels).
- C.5.14.6.5 Develop a nationwide strategy to define optimal geographic spacing for frequency reuse zones; identify the number of frequencies needed for a successful regional/zone system design, use temporary transition frequencies (if required), and use permanent narrowband frequencies of the new wireless systems.
- C.5.14.6.6 Prepare equipment and system certification documentation as required.
- C.5.14.6.7 Coordinate new, proposed frequencies within DHS and with other federal departments and government agencies.
- C.5.14.6.8 Prepare spectrum Planning analyses and documentation as directed.

C.5.15 IT CONTINUITY MANAGEMENT

The contractor shall perform continuity management actions affecting the Information Technology Service Office and all of its functions including the Network Management Center, Security Management Center, Front Office, Enterprise Business Management Office, Infrastructure Information Systems Security Manager (ISSM), Mission Critical Infrastructure Operations (MCIO), Enterprise Application Delivery and Operations, IT Continuity Management, Business Office Operations, Infrastructure Transformation Office, Wireless Management Office, and all network and telecommunications components. The contractor shall also provide continuity management and redundancy capability of the Help Desk.

These programs/offices have 46 recoverable essential functions (EFs) with alternate site operations occurring at two sites as a minimum. The sites, to include redundant NMC, and SMC, are provided by DHS. EFs concern DHS, state/local Governments, law enforcement, and other executive branch directorates, and agencies. The DHS Continuity Planning framework is provided at [TE C.5.15-001](#).

The contractor shall provide IT integration capability for all departmental, intergovernmental, and non-governmental organizations (NGO) applications used on the LANs.

C.5.15.1 Continuity Assessment

- C.5.15.1.1 The contractor shall perform an initial baseline analysis of existing IT continuity plans and programs. (CDRL C.5.15-1, Business Continuity Initial Assessment)

PROCUREMENT SENSITIVE

C.5.15.1.2 After completing the baseline analysis, and its approval by the COTR, the contractor shall evaluate the baseline against the Business Continuity Framework to determine operational gaps. The contractor shall document the findings of the gap analysis and submit the findings to the COTR within 60 business days of the baseline analysis approval by the COTR. (CDRL C.5.15-2, Business Continuity Framework Gap Analysis)

C.5.15.2 Continuity Planning

C.5.15.2.1 The contractor shall facilitate strategic planning with programs and offices annually, or as directed by the COTR. The outcome of the strategic planning is the Multi-Year Strategic Program Management Plan containing continuity planning goals and objectives to include performance measures for the period. (CDRL C.5.15-3, Multi-Year Strategic Program Management Plan)

C.5.15.2.2 The contractor shall update and maintain annually, or as directed by the COTR, the CIO COOP Implementation Plan. The contractor shall provide the document to the COTR for approval. (CDRL C.5.15-4, CIO COOP Implementation Plan)

C.5.15.2.3 The contractor shall develop, maintain, update and implement the Incident Response and Management Plan, containing management activist and emergency response and escalation procedures. The contractor shall update the plan annually or as directed by the COTR, based on threat/exposure/business continuity strategy. (CDRL C.5.15-5, Incident Response and Management Plan)

C.5.15.2.4 The contractor shall develop, maintain, update and implement the CIO Operational Recovery Plan and IT Disaster Recovery/Business Continuity Plans, at least annually for offices/programs. (CDRL C.5.15-6, CIO Operational Recovery Plan and IT Disaster Recovery/Business Continuity Plan)

C.5.15.3 Continuity Reviews and Coordination

C.5.15.3.1 The contractor shall participate in Enterprise Architecture Center of Excellence (EACOE) reviews, Enterprise Change Control Board (ECCB) reviews, and other compliance activities to identify the impact of these bodies' decisions and actions on IT continuity planning and advise these bodies' on continuity planning considerations. The contractor shall document the reviews continuity planning impacts and provide comments in accordance with the guidelines provided by the appropriate board.

C.5.15.3.2 The contractor shall schedule, plan and conduct a bi-weekly meeting of designated stake holders to discuss and coordinate requirements for the development and maintenance of the Disaster Recovery and IT Contingency Plan and coordinate the plans and activities for conducting COOP Exercises. The meeting participants shall also coordinate the actions taken to address findings resulting from COOP exercises. The contractor shall provide meeting minutes to the COTR within three business days of the meeting. (CDRL C.5.15-7, Plans and Exercises Coordination Meeting Minutes)

C.5.15.4 Continuity Program Administration

C.5.15.4.1 The contractor shall develop, maintain, update and implement IT continuity policy, guidance, methodologies and tools. Updates shall occur at least

PROCUREMENT SENSITIVE

annually, in response to Homeland Security Presidential Directives (HSPDs), or as directed by the COTR. (CDRL C.5.15-8, Continuity Policy, Guidance, Methodologies and Tools)

C.5.15.4.2 The contractor shall update and maintain, at the direction of the COTR, the list of CIO essential functions and critical IT/telecommunication networks, systems, facilities, and critical positions. (CDRL C. 5.15-9, Essential Functions, Critical IT/Telecommunication Networks, Systems, Facilities, and Critical Positions List)

C.5.15.4.3 The contractor shall annually, or when significant changes occur to the essential function(s) or DHS IT infrastructure perform a continuity management review. Changes shall result in a threat and vulnerability exposure, Risk Assessment, Interdependency Analysis, Business Impact Analysis. The contractor shall ensure re-use of existing information when performing the aforementioned tasks. The contractor shall prepare a report and executive briefing identifying risk to the CIO. (CDRL C.5.15-10, Continuity Management Review)

C.5.15.4.4 The contractor shall conduct a review of the CIO COOP Implementation program, Operational Recovery/IT Contingency Plans, observe related tests, and provide feedback on program compliance in accordance with all applicable executive orders, presidential directives, other federal and DHS laws, federal orders management policies, handbooks, guidelines, processes, and procedures, as directed by the COTR.

C.5.15.4.5 The contractor shall develop executive briefings as directed by COTR. (CDRL C.5.15-11, Business Continuity Executive Briefings)

C.5.15.5 Testing and Exercises

C.5.15.5.1 The contractor shall develop test plans and provide training on the test/exercise plans annually or as directed by COTR. (CDRL C.5.15-12, Test/Exercise Plans)

C.5.15.5.2 The contractor shall participate in test/exercises and the after-action test/exercise reviews and document issues in an After Action Report. (CDRL C.5.15-13, Test/Exercise After Action Report)

C.5.15.6 Electronic Records

C.5.15.6.1 The contractor shall develop, maintain, update and implement the electronic vital records program to ensure critical records from all three networks are stored off premise. Records range from paper-based documents to the latest electronic-storage media.

C.5.15.6.2 The off-site storage location(s) shall be located at least 50 miles from the production site, outside of the impact area of the production site, and inside the continental U.S.

C.5.15.6.3 The frequency of records back-up is dependent on the record type and COTR direction.

C.5.15.6.4 The retrievable and fully operational time frames shall fulfill the performance requirements for critical and non-critical systems as identified in Table 1 of the Task Order, Continuity of Government Condition (COGCON) level activation/reconstitution timeframes, or as designated by the COTR.

C.5.15.6.5 The contractor shall test and ensure the records are retrievable and usable at least quarterly. The contractor shall provide a test report to the COTR within five business days of completing the test. (CDRL C.5.15-14, Electronic Vital Records Program Test Report.

C.6 APPLICABLE LAWS, PUBLICATIONS, AND FORMS

C.6.1 GENERAL INFORMATION

C.6.1.1 Applicable Publications and Forms

- C.6.1.1.1 Most Government publications listed are available electronically and the Government will provide the non-electronic versions at the start of the Task Order. The contractor shall maintain a copy of all required publications listed in this Section and Technical Exhibits in accordance with Section C.1. The contractor shall post supplements or amendments to listed publications from any organizational level issued during the life of the Task Order as required.
- C.6.1.1.2 The contractor shall establish continuing publication requirements with the DHS publication distribution office. The contractor shall have customer accounts for all publications listed in this Task Order.
- C.6.1.1.3 The contractor shall immediately implement changes to publications that result in a decrease or no change to the Task Order price. Prior to implementing any revision, supplement, or amendment that may result in an increase in Task Order price, the contractor shall submit a price proposal to the COTR and obtain approval. The contractor shall submit said price proposal within 20 business days from the date the contractor receives notice of the revision, supplement, or amendment-giving rise to the increase in cost of performance. Failure of the contractor to submit a price proposal within 20 business days from the date of receipt of any change shall entitle the Government to require performance in accordance with such change at no increase in Task Order price.
- C.6.1.1.4 The contractor shall ensure that all publications are posted and up-to-date. Upon completion of the Task Order, the contractor shall return to the Government all issued publications.

C.6.1.2 Publication Conflict Resolution

- C.6.1.2.1 If there is a conflict between Section C and the cited references, Section C shall control.
- C.6.1.2.2 Any task set forth in any such reference which will call for the exercise of discretionary Government authority that cannot be delegated, will be subject to the final approval of the Government official having such authority.
- C.6.1.2.3 All publications and forms will be current issue. The contractor shall use existing stocks of forms until depleted.
- C.6.1.2.4 The publications and documents listed in this Section are current with dates as of the writing of this Task Order, not necessarily date of Task Order award. The Government will not modify this section of the Task Order during the tenure of the Task Order unless a Contract Price change is required based upon a new documentary requirement.

C.6.2 FEDERAL PUBLICATIONS

C.6.2.1 Federal Regulation and Guidelines

All supplies and services provided under this Task Order shall conform to the applicable Federal Information Processing Standards Publications (FIPS PUBS) as specified on Web site <http://www.itl.nist.gov/fipspubs/>. The contractor shall also comply with

Electronic and Information Technology Standards as specified on Web site
<http://www.section508.gov/index.cfm?FuseAction=Content&ID=3>

- Government Paperwork Elimination Act (GPEA)
<http://www.whitehouse.gov/omb/fedreg/gpea2.html>
- Federal Acquisition Regulation
- Records management guidance for agencies implementing electronic signature technologies <http://www.nara.gov/records/policy/gpea.html>
- Electronic Signatures in Global and National Commerce Act (ESIGN)
<http://www.whitehouse.gov/omb/memoranda/m00-15.html>
- OMB Circular A130
<http://www.whitehouse.gov/OMB/circulars/a130/a130.html>

C.6.3 OTHER PUBLICATIONS

C.6.3.1 U.S. Congress-Public Law (PL) and United States Code (U.S.C.)

- PL 107-347 Section III, Federal Information Security Management Act (FISMA) of 2002, 2002
- PL 107-305, Cyber Security Research and Development Act of 2002
- PL 96-456, Classified Information Procedures Act of 1980
- 5 U.S.C. 552, Freedom of Information Act; Public Information; Agency Rules, Opinions, Orders, Records, and Proceedings, 1967
- 5 U.S.C. 552a, Privacy Act; Records Maintained on Individuals, 1974
- 18 U.S.C. 1029, Fraud and Related Activity in Connection with Access Devices
- 18 U.S.C. 1030, Fraud and Related Activity in Connection with Computers
- 40 U.S.C. 1401 et seq., P.L. 104-106, Clinger Cohen Act of 1996 (Information Technology and Management Reform Act of 1996)
- 44 U.S.C. 3534, Federal Agency Responsibilities
- 44 U.S.C. 3535, Annual Independent Evaluation
- 44 U.S.C. 3537, Authorization of Appropriations
- 44 U.S.C. 3541, P.L. 107-296, Federal Information Security Management Act of 2002 (FISMA)
- 44 U.S.C. 3546, Federal Information Security Incident Center

C.6.3.2 Executive Orders—Office of Management and Budget (OMB), Homeland Security Presidential Directive (HSPD) and Presidential Decision Directive

- HSPD-7, Critical Infrastructure Identification, Prioritization, and Protection, 2004
- HSPD-20 National Continuity Policy, 2007
- OMB Policy Memorandum M-07-11, Implementation of Commonly Accepted Security Configurations for Windows Operating Systems.
- OMB Memorandum M-07-18, Ensuring New Acquisitions Include Common Security Configurations
- OMB Circular A-130, Appendix III, Security of Federal Automated Information Systems, 2000

C.6.3.3 DHS Management Directive (MD)

The DHS Interactive web site contains the DHS MDs

- DHS MD 0000 Organization of the Office of the Secretary of Homeland Security
- DHS MD 0002 Operational Integration Staff
- DHS MD 0003 Acquisition Line of Business Integration and Management
- DHS MD 0004 Administrative Service Line of Business Integration and Management
- DHS MD 0005 Financial Management Line of Business Integration and Management
- DHS MD 0006 Human Capital Line of Business Integration and Management
- DHS MD 0007.1 Information Technology Integration and Management
- DHS MD 0475 Information Collection Program
- DHS MD 0480.1 Ethics/Standards of Conduct
- DHS MD 0490.1 Federal Register Notices and Rules
- DHS MD 0550.1 Record Management
- DHS MD 0560 Real Property Management Program
- DHS MD FORM 560-1 (3/05): Custody Receipt for Personal Property/Property Pass
- DHS MD FORM 560-3 (3/05): Property Transfer Receipt
- DHS MD 0565 Personal Property Management Directive
- DHS MD 0590 Mail Management Program
- DHS MD 0720.1 Small Business Acquisition Program
- DHS MD 0731 Strategically Sourced Commodities Policy and Procedures
- DHS MD 0760.1 Purchase Card Program
- DHS MD 0780 Contracting Officer's Technical Representative (COTR) Certification, Appointment & Responsibilities
- DHS MD 0782 Acquisition Certification Requirement for Program Managers
- DHS MD 0783 Ordering Official Certification
- DHS MD 0784 Acquisition Oversight Program
- DHS MD 1120 Capitalization and Inventory of Personal Property
- DHS MD 1130.1 Electronic Funds Transfer for Disbursements, Collections and Deposits
- DHS MD 1190.1 Billings and Collections
- DHS MD 1210.1 Vendor Maintenance
- DHS MD 1330 Planning, Programming, Budgeting and Execution
- DHS MD 1400 Investment Review Process
 - Enclosure 1: Definitions
 - Enclosure 2: Guiding Principles
 - Enclosure 3: Exhibit 300 Light

PROCUREMENT SENSITIVE

- Enclosure 4: Request for MRC Review
- Enclosure 5: IT Investment Review
- Enclosure 6: Business Case Scoring Template
- Enclosure 7: Phases and Business Case Elements
- DHS MD 1510.1 Travel for Official Government Business
- DHS MD 1560.2 Payment for Official Travel Expenses by Non-Federal Sources
- DHS MD 3120.2 Employment of Non-Citizens
- DHS MD 4010.2 Section 508 Program Management Office & Electronic and Information Technology Accessibility
 - Appendix A: Software Applications and Operating Systems
 - Appendix B: Web-Based Intranet and Internet Information and Applications
 - Appendix C: Telecommunications Products
 - Appendix D: Video and Multimedia Products
 - Appendix E: Self Contained, Closed Products
 - Appendix F: Desktop and Portable Computers
 - Appendix G: Functional Performance Criteria
 - Appendix H: Information, Documentation and Support
- DHS MD 4030 Geospatial Management Office
- DHS MD 4100.1 Wireless Management Office
- DHS MD 4200.1 IT Capital Planning and Investment Control (CPIC) and Portfolio Management
 - Attachment 1: Guide to Information Technology Capital Planning and Investment Control
- DHS MD 4300.1 Information Technology Systems Security
- DHS MD 4400.1 DHS Web (Internet, Intranet, and Extranet Information) and Information Systems
- DHS MD 4500.1 DHS E-Mail Usage
- DHS MD 4510 Domain Names
- DHS MD 4600.1 Personal Use of Government Office Equipment
- DHS MD 4700.1 Personal Communications Device Distribution
- DHS MD 4800 Telecommunications Operations
 - Attachment A: Frequently Asked Questions (FAQs)
 - Attachment B: Nomination and Designation of Designated Agency Representative (DAR) for Telecommunications Services
 - Attachment C: Designated Agency Representative (DAR) for Telecommunications Services Function Requirements
- DHS MD 4900 Individual Use and Operation of DHS Information Systems/ Computers
 - Attachment A: Information Systems/Computer Access Agreement

- Attachment B: Logon Screen
- DHS MD 5110.1 Environmental Compliance Program
- DHS MD 5120.1 Environmental Management Program
- DHS MD 5200.1 Occupational Safety and Health Programs
- DHS MD 8200.1 Information Quality
- DHS MD 9300.1 Continuity of Operations Programs and Continuity of Government Functions
- DHS MD 11000 Office of Security
- DHS MD 11005 Suspending Access to DHS Facilities, Sensitive Information, and IT Systems
- DHS MD 11020.1 Issuance of Access Control Media
- DHS MD 11021 Portable Electronic Devices in SCI Facilities
- DHS MD 11030.1 Physical Protection of Facilities and Real Property
- DHS MD 11041 Protection of Classified National Security Information Program Management
- DHS MD 11042.1 Safeguarding Sensitive But Unclassified (For Official Use Only) Information
- DHS MD 11043 Sensitive Compartmented Information Program Management
- DHS MD 11044 Protection of Classified National Security Information Classification Management
- DHS MD 11045 Protection of Classified National Security Information: Accountability, Control, and Storage
- DHS MD 11046 Open Storage Area Standards for Collateral Classified Information
- DHS MD 11047 Protection of Classified National Security Information Transmission & Transportation
- DHS MD 11048 Suspension, Denial, and Revocation of Access to Classified Information
- DHS MD 11049 Protection of Classified National Security Information: Security Violations and Infractions
- DHS MD 11050.2 Personnel Security and Suitability Program
- DHS MD 11051 Department of Homeland Security SCIF Escort Procedures
- DHS MD 11052 Internal Security Program
- DHS MD 11053 Security Education, Training, and Awareness Program Directive
- DHS MD 11056.1 Sensitive Security Information (SSI)
- DHS MD 11060.1 Operations Security Program
- DHS MD 11080 Security Line of Business Integration and Management

C.6.3.4 DHS Regulations

- Homeland Security Acquisition Regulation 305.242-71

C.6.3.5 DHS Guides

- DHS SCG OS-001 (IT), Security Classification Guide – Homeland Security Data Network, February 2004
- DHS SCG OS-002 (IT), Security Classification Guide – National Security IT Systems Certification and Accreditation, March 2004

C.6.3.6 National Institute of Standards and Technology (NIST), Special Publications

The web site www.nist.gov contains the NIST publications

- 800-18, Guide for Developing Security Plans for Information Technology Systems, 1998
- 800-23, Guideline to Federal Organizations on Security Assurance and Acquisition/Use of Tested/Evaluated Products, 2000
- 800-26, Revised NIST SP 800-26 System Questionnaire with NIST SP 800-53 References and Associated Security Control Mappings, 2005
- 800-27, Engineering Principles for Information Technology Security (A Baseline for Achieving Security), Revision A, 2004
- 800-30, Risk Management Guide for Information Technology Systems, 2002
- 800-31, Intrusion Detection Systems (IDS), 2001
- 800-34, Contingency Planning Guide for Information Technology Systems, 2002
- 800-35, Guide to Information Technology Security Services, 2003
- 800-36, Guide to Selecting Information Security Products, 2003
- 800-37, Guide for the Security Certification and Accreditation of Federal Information Systems, 2004
- 800-40, Procedures for Handling Security Patches, 2002
- 800-41, Guidelines on PEPs and PEP Policy, 2002
- 800-42, Guideline on Network Security Testing, 2003
- 800-45, Guidelines on Electronic Mail Security, 2002
- 800-47, Guide for Interconnecting Information Technology Systems, 2002
- 800-50, Building an Information Technology Security Awareness and Training Program, 2003
- 800-51, Use of the Common Vulnerabilities and Exposures (CVE) Vulnerability Naming Scheme, 2002
- 800-53, Recommended Security Controls for Federal Information Systems, 2005
- 800-55, Security Metrics Guide for Information Technology Systems, 2003
- 800-59, Guideline for Identifying an Information System as a National Security System, 2003
- 800-60, Guide for Mapping Types of Information and Information Systems to Security Categories, 2004

- 800-61, Computer Security Incident Handling Guide, 2004
- 800-64, Security Considerations in the Information System Development Life Cycle, 2004
- 800-65, Integrating Security into the Capital Planning and Investment Control Process, 2005
- 800-68, Draft NIST Special Publication 800-68, Guidance for Securing Microsoft Windows XP Systems for IT Professionals: A NIST Security Configuration Checklist, 2004
- 800-70, The NIST Security Configuration Checklists Program

C.6.3.7 Federal Information Processing Standards Publications (FIPS PUBS)

The web site <http://www.itl.nist.gov/fipspubs/> contains FIPS publications.

- FIPS 199, Standards for Security Categorization of Federal Information and Information Systems, 2003

C.6.4 FORMS

DHS will provide electronically a comprehensive list of all forms upon Task Order award. DHS will provide a URL address to access the DHS website for forms.

C.7 TECHNICAL EXHIBITS

Technical Exhibit Title Numbering System:

A Technical Exhibit (TE) is titled in relation to the Section from which it is first referenced and its order among TEs in that Section. For example, Section 3.1 has three Technical Exhibits titled TE C.3.1.-001, TE C.3.1-002, and TE C.3.1.-003.

TE Page Numbering System:

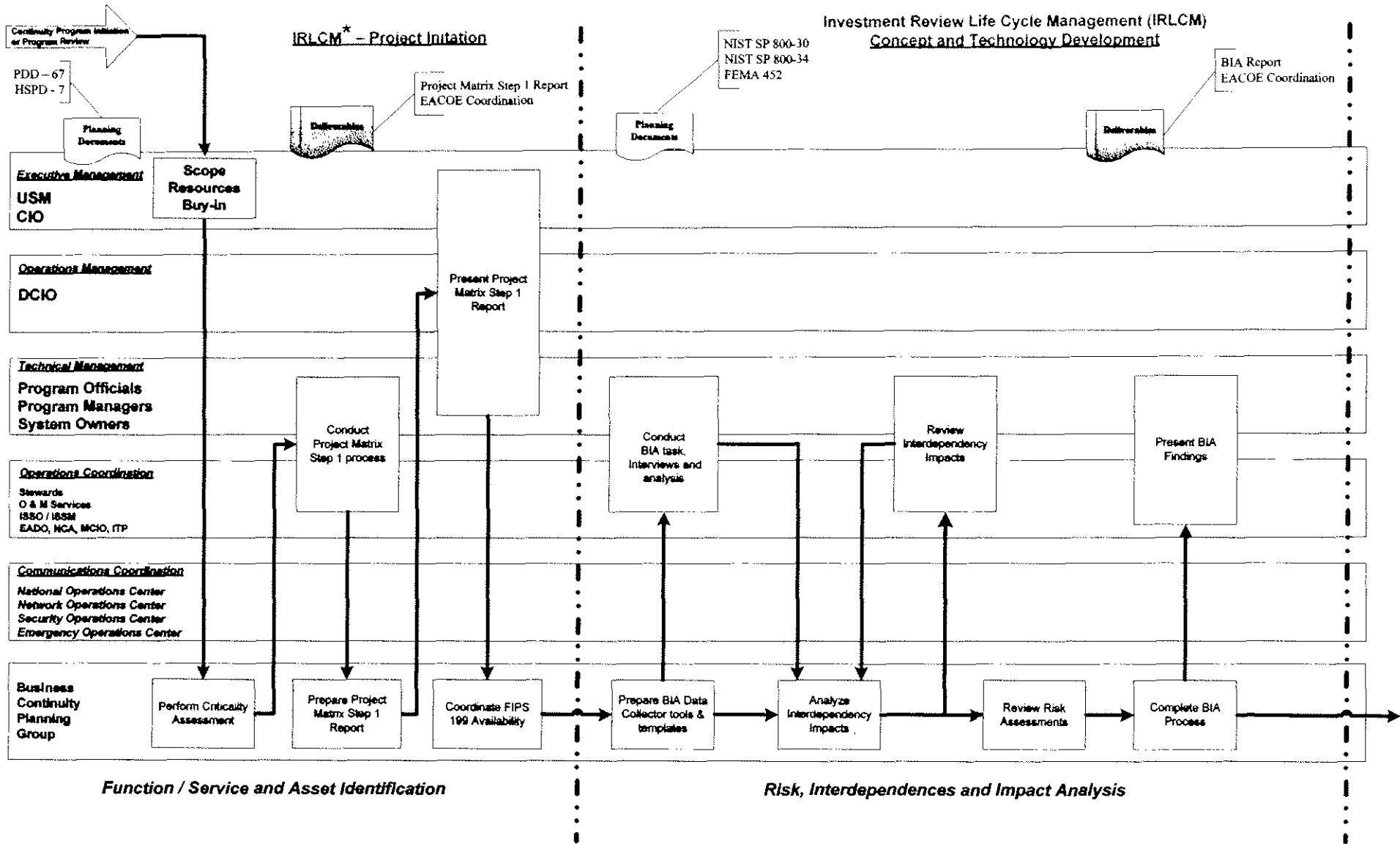
Since Section C.7 provides all Technical Exhibits except those maintained on the DHS Interactive website, all TEs are page numbered in relation to their TE title. For example, page one of TE C.5.2.-001 is shown as page number TE C.5.2.-001-01 to indicate that it is the first page of TE C.5.2.-001 from Task Order Section 5.2.

List of Technical Exhibits:

TE	Description	Task Order Paragraph
<u>C.1.2-001</u>	DHS Organization Chart	<u>C.1.2</u>
<u>C.1.2-002</u>	Locations Supported Summary (Sensitive But Unclassified)	<u>C.1.2, C.5.6.1</u>
<u>C.1.2-003</u>	DHS OCIO Organization Chart	<u>C.1.2</u>
<u>C.1.3-002</u>	Seats by Fiscal Year (FY) for LAN – A	<u>C.1.3.1.1, C.5</u>
<u>C.1.3-002</u>	Seats by Fiscal Year (FY) for LAN – HSDN	<u>C.1.3.1.1, C.5</u>
<u>C.1.3-002</u>	Seats by Fiscal Year (FY) for LAN – C	<u>C.1.3.1.1, C.5</u>
<u>C.1.6-001</u>	Performance Requirements Summary	<u>C.1.6.1, C.1.6.1.2, C.1.9.1.1</u>
<u>C.1.6-002</u>	Plans developed, maintained, and updated by Contractor	<u>C.1.6.2.4</u>
<u>C.1.7-001</u>	Key Personnel Positions and Descriptions	<u>C.1.7.1.2</u>
<u>C.1.12-001</u>	Current Contracts Period of Performance	<u>C.1.12.1.1</u>
<u>C.1.12.002</u>	Projects	<u>C.1.12.1.1</u>
<u>C.3.1-001</u>	Government Furnished Equipment Product Guide of IT Equipment & Software	<u>C.3.1.4.1, C.5, C.5.1, C.5.6.1</u>
<u>C.3.1-002</u>	Government Furnished Equipment Software	<u>C.3.1.4.1</u>
<u>C.3.1-003</u>	Government Furnished Equipment Inventory	<u>C.3.1.4.1</u>
<u>C.3.1-004</u>	Government Furnished Facilities	<u>C.3.1.4.1</u>
<u>C.5.1-001</u>	DHS Custom Applications	<u>C.5.1.1.2</u>
<u>C.5.5-001</u>	Help Desk Ticket volume	<u>C.5.5.1</u>
<u>C.5.8-001</u>	Switchboard Call Volume	<u>C.5.8.2</u>
<u>C.5.15-001</u>	Continuity Planning Framework	<u>C.5.15.1</u>

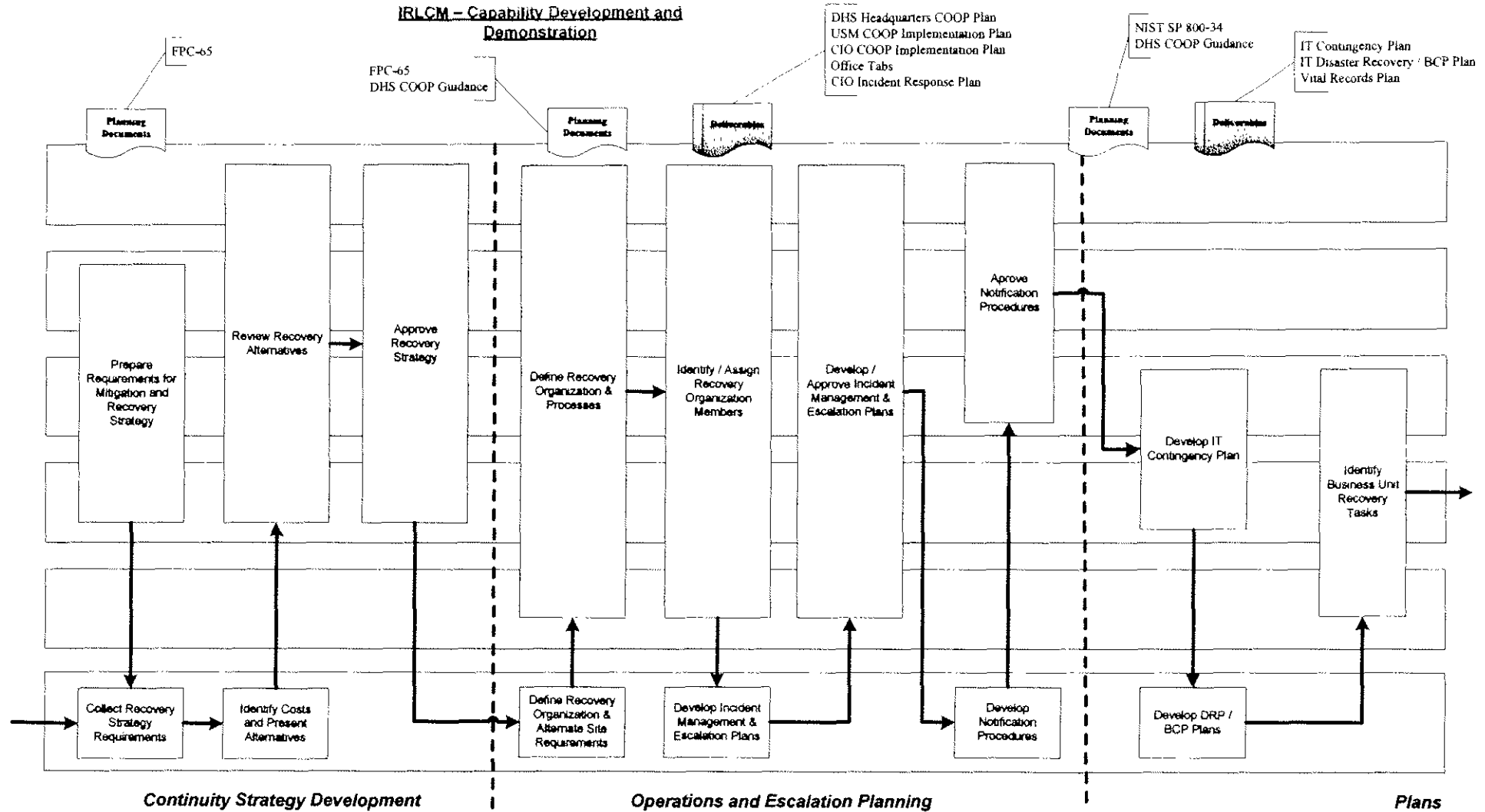
PROCUREMENT SENSITIVE

TE C.5.15-001 Continuity Planning Framework



PROCUREMENT SENSITIVE

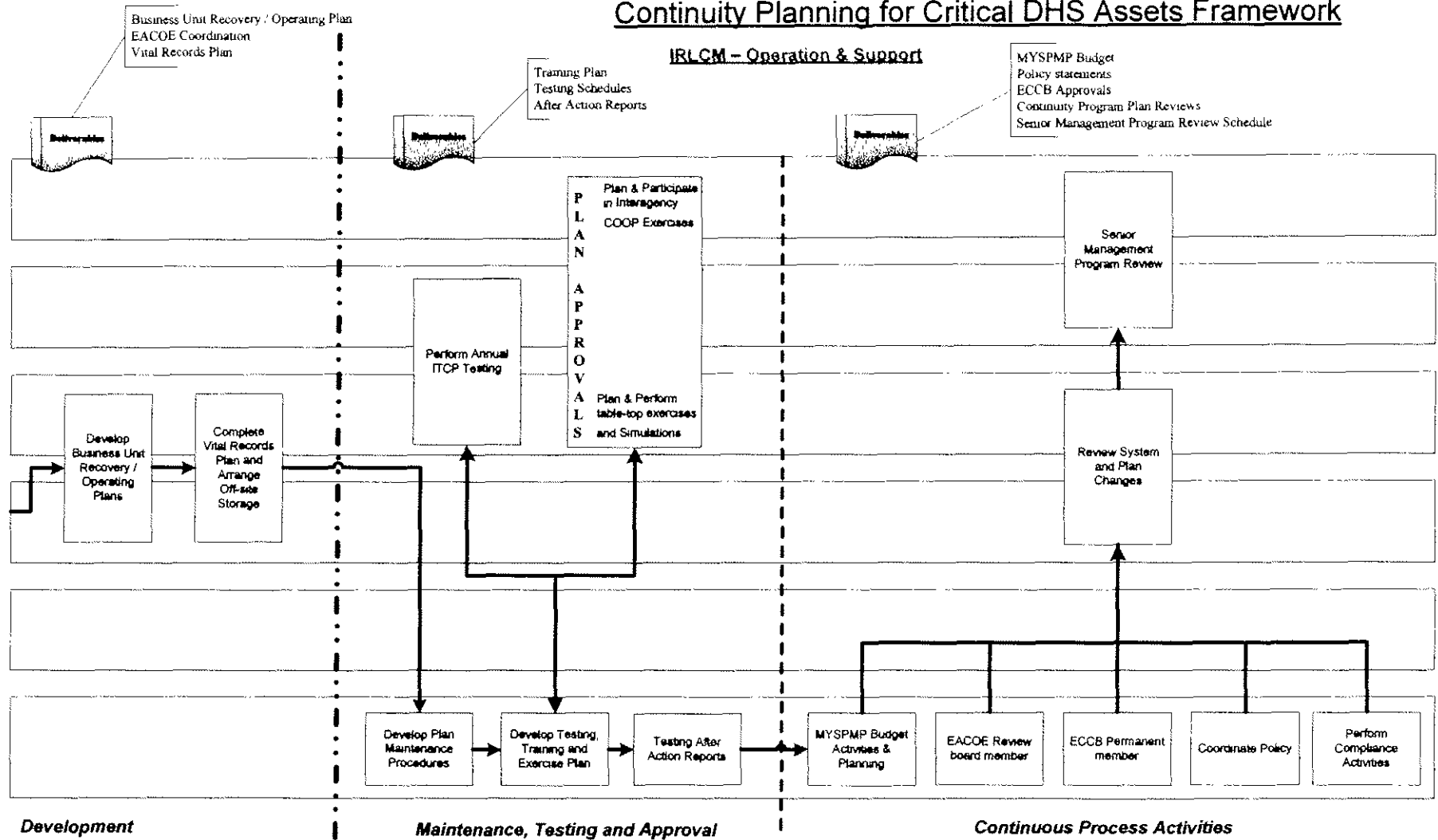
TE C.5.15-001 Continuity Planning Framework



PROCUREMENT SENSITIVE

TE C.5.15-001 Continuity Planning Framework

Continuity Planning for Critical DHS Assets Framework



Development

Maintenance, Testing and Approval

Continuous Process Activities

Comments Version	DATE	TITLE
	2/22/2007	BCP ROADMAP
	REVISED	DRAWN BY
	2/22/2007	Continuity Planning Group / Critical Assets

C.8 CONTRACT DATA REQUIREMENTS LISTING (CDRL)

CDRL Title Numbering System:

A CDRL is titled in relation to the Section and Paragraph number from which it is first referenced and its order among CDRLs in that Paragraph. For example:

Section C.4.2, Paragraph 1 (i.e., C.4.2.1) references two CDRLs. Those CDRLs are titled CDRL C.4.2-1 through CDRL C.4.2-2.

The contractor shall provide electronic submittals of CDRLS using standard Microsoft Office applications. If no format is specified in this Task Order, the contractor shall coordinate with the COTR to format style of deliverable.

List of CDRLs:

CDRL Number	Task Order Paragraph	Title
C.1.4-1	C.1.4.1.3	Ad-Hoc Requirements
C.1.4-2	C.1.4.2.7	Information Technology Improvement Program
C.1.4-3	C.1.4.2.7	Future Programmatic and Cost Requirements for IT Services
C.1.4-4	C.1.4.2.8	Standard Operating Procedures For Each Functional Area
C.1.6-1	C.1.6.1	Monthly and Annual Workload Data Reports
C.1.6-2	C.1.6.2.1	Weekly Status Report
C.1.6-3	C.1.6.2.2	Monthly Performance Summary Report
C.1.6-4	C.1.6.2.3	Monthly Quality Control Report
C.1.6-5	C.1.6.3.1.1	Monthly Contract Administration Review Status Meeting Agenda
C.1.6-6	C.1.6.3.1.2	Monthly Contract Administration Review Status Meeting Minutes
C.1.6-7	C.1.6.3.2.1	Quarterly Program Management Review Agenda
C.1.6-8	C.1.6.3.2.2	Quarterly Program Management Review Status Report
C.1.6-9	C.1.6.3.2.5	Quarterly Program Management Review Meeting Minutes
C.1.6-10	C.1.6.4.1	Security Violation Report
C.1.6-11	C.1.6.4.2	Architectural Compliance Plan
C.1.6-12	C.1.6.4.3	Program Development Report
C.1.6-13	C.1.6.4.4	Network and Application Diagrams
C.1.7-1	C.1.7.1.1	Project Manager Succession Plan
C.1.7-2	C.1.7.1.2	Key Personnel Succession Plan
C.1.7-3	C.1.7.2.2	Staffing Roster
C.1.7-4	C.1.7.3.2	Employee Training Plan

CDRL Number	Task Order Paragraph	Title
C.1.8-1	C.1.8.1.1.2	Unresolved Dispute Information
C.1.9-1	C.1.9.2.1	Quality Control Plan
C.1.9-2	C.1.9.2.2	Customer Evaluation Plan
C.1.11-1	C.1.11.2.4	Essential Personnel Contact List
C.1.11-2	C.1.11.3.2	Travel Requests
C.1.12-1	C.1.12.1.1	Contract Transition Plan
C.3.1-1	C.3.1.2.4	Government Furnished Service Discrepancy Report
C.3.1-2	C.3.1.4.2.3	Government Property Report – Annual
C.3.1-3	C.3.1.4.4.2	Government Property Inventory – Initial
C.4.1-1	C.4.1.1.1	Contractor Owned, Contractor Operated Facilities List (used in Task Order performance)
C.5.1-1	C.5.1.1.4	Applications Consolidation and Rationalization Plan
C.5.1-2	C.5.1.2.1	Up/Down Status Report
C.5.1-3	C.5.1.3.1	Application Maintenance and Operation Reports – Weekly
C.5.1-4	C.5.1.3.1.1	Root Cause Analysis Report
C.5.1-5	C.5.1.5.1	Performance Trend of Major Applications on the Network Report
C.5.2-1	C.5.2.1.3	Deployment Project Plan
C.5.2-2	C.5.2.1.6	Proposed Workspace Report
C.5.2-3	C.5.2.1.7	Trip Report
C.5.2-4	C.5.2.1.8	Site Report
C.5.2-5	C.5.2.2	DHS Deployment Plan Template
C.5.2-6	C.5.2.3	Site Acceptance Process
C.5.2-7	C.5.2.3	Test Plans and Test Results Report
C.5.2-8	C.5.2.5.3	Deployment Project Plan/Status Report
C.5.3-1	C.5.3.4.2.5	Gold Copy Images
C.5.4-1	C.5.4.1	Individual Test Plans
C.5.4-2	C.5.4.2.5	Test Lab Issues and Risks Report
C.5.4-3	C.5.4.2.10	Testing Lab Findings Report
C.5.5-1	C.5.5.1	End User and Desk Side Support Concept of Operations
C.5.5-2	C.5.5.2.1	Preventative Maintenance Plan, Policies and Procedures
C.5.8-1	C.5.8.1.7	Phone and PBX Services Report

CDRL Number	Task Order Paragraph	Title
C.5.8-2	C.5.8.2.2.1	Switchboard Knowledgebase Reference
C.5.8-3	C.5.8.2.2.2	Automatic Call Directory
C.5.8-4	C.5.8.2.6	Call Pattern Statistics Report – Monthly
C.5.8-5	C.5.8.2.7	Switchboard COOP Plan
C.5.8-6	C.5.8.2.8.2	Switchboard Training Lesson Plan
C.5.9-1	C.5.9.1.4	NMC Standard Operating Procedures
C.5.9-2	C.5.9.1.12	Network and Systems Infrastructure Report
C.5.9-3	C.5.9.1.19	Network Metrics Reports
C.5.10-1	C.5.10.1.2	Information Technology Services Office Security Management Approach and SOPs, Checklists and DHS Information Technology Services Office Security Plan
C.5.10-2	C.5.10.2.1	Vulnerability Assessment Report
C.5.10-3	C.5.10.2.6	Application Vulnerability Cost-Benefit Analysis
C.5.10-4	C.5.10.5.4	Patch/Service Pack Deployment Report
C.5.10-5	C.5.10.6.4	System Log Security Review Report
C.5.10-6	C.5.10.9.2	Forensic Investigation SOPs
C.5.10-7	C.5.10.9.4	Event and Incident Reports
C.5.10-8	C.5.10.10.3	INFOCON Level SOPs and Checklists
C.5.11-1	C.5.11.1.6	COMSEC Plan
C.5.13-1	C.5.13	Training Plan
C.5.14-1	C.5.14.2.5	Wireless Systems Engineering Framework
C.5.14-2	C.14.2.8	Wireless SEMP, Wireless CONOPS, Functional Baseline, System Specifications, System Development Specifications
C.5.15-1	C.5.15.1.1	Business Continuity Initial Assessment
C.5.15-2	C.5.15.1.2	Business Continuity Framework Gap Analysis
C.5.15-3	C.5.15.2.1	Multi-Year Strategic Program Management Plan
C.5.15-4	C.5.15.2.2	CIO COOP Implementation Plan
C.5.15-5	C.5.15.2.3	Incident Response and Management Plan
C.5.15-6	C.5.15.2.4	CIO Operational Recovery Plan and IT Disaster Recovery/Business Continuity Plan
C.5.15-7	C.5.15.3.2	Plans and Exercises Coordination Meeting Minutes
C.5.15-8	C.5.15.4.1	Continuity Policy, Guidance, Methodologies and Tools
C.5.15-9	C.5.15.4.2	Essential Functions, Critical IT/ Telecommunications

CDRL Number	Task Order Paragraph	Title
		Networks, Systems, Facilities, and Critical Positions List
C.5.15-10	C.5.15.4.3	Continuity Management Review
C.5.15-11	C.5.15.4.5	Business Continuity Executive Briefings
C.5.15-12	C.5.15.5.1	Test/Exercise Plans
C.5.15-13	C.5.15.5.2	Test/Exercise After Action Reports
C.5.15-14	C.5.15.6.1	Electronic Vital Records Program Test Report

CDRL Deliverables:

CDRL Number	Task Order Section	Title	Format	Required Date	Frequency	Distribution
	C.1.4	GENERAL REQUIREMENTS				
C.1.4-1	C.1.4.1.3	Ad-Hoc Requirements	Electronic	As directed by COTR	As required	COTR
C.1.4-2	C.1.4.2.7	Information Technology Improvement Program	Electronic	COB the fifth business day after annual review	Annually	COTR
C.1.4-3	C.1.4.2.7	Future Programmatic and Cost Requirements for IT Services	Electronic	COB the fifth business day after semi-annual review	Semi-annually	COTR
C.1.4-4	C.1.4.2.8	Standard Operating Procedures for each Functional Area	Electronic	Initial: 45 days after award Final: 5 days after DHS review	Contract start and as required	COTR
	C.1.6	REQUIRED REPORTS AND MEETINGS				
C.1.6-1	C.1.6.1	Monthly and Annual Workload Data Reports	Electronic	Monthly as directed by the COTR Annually on last business day of each fiscal year	Monthly Annually	COTR
C.1.6-2	C.1.6.2.1	Weekly Status Report	Written and Electronic	9:00 AM each Tuesday	Weekly	COTR
C.1.6-3	C.1.6.2.2	Monthly Performance Summary Report	Electronic	COB the fifth business day of each month	Monthly	COTR

CDRL Number	Task Order Section	Title	Format	Required Date	Frequency	Distribution
C.1.6-4	C.1.6.2.3	Monthly Quality Control Report	Electronic	COB the tenth business day of each month	Monthly	COTR
C.1.6-5	C.1.6.3.1.1	Monthly Contract Administration Review Status Meeting Agenda	Electronic	COB the tenth business day of each month	Monthly	COTR
C.1.6-6	C.1.6.3.1.2	Monthly Contract Administration Review Status Meeting Minutes	Electronic	COB one business day after meeting	Monthly	Meeting attendees
C.1.6-7	C.1.6.3.2.1	Quarterly Program Management Review Agenda	Electronic	COB two business days prior to scheduled meeting	Quarterly	Meeting attendees
C.1.6-8	C.1.6.3.2.2	Quarterly Program Management Review Status Report	Electronic	COB two business days after meeting	Quarterly	Meeting attendees
C.1.6-9	C.1.6.3.2.5	Quarterly Program Management Review Meeting Minutes	Electronic	COB two business days after meeting	Quarterly	Meeting attendees
C.1.6-10	C.1.6.4.1	Security Violation Report	Electronic	Within one hour of detecting violation	As required	CIO Management
C.1.6-11	C.1.6.4.2	Architectural Compliance Plan	Electronic	Initial: 30 days after Task Order award Semi-annual update: First business day of May & November	Semi-annually	COTR
C.1.6-12	C.1.6.4.3	Program Development Report	Electronic	Last business day of April & October	Semi-annually	COTR
C.1.6-13	C.1.6.4.4	Network and Application Diagrams	Electronic	First business day in June & December	Semi-annually	COTR
	C.1.7	CONTACTOR PERSONNEL				
C.1.7-1	C.1.7.1.1	Project Manager Succession Plan	Electronic	Within 20 business days of Task Order	As required	COTR

CDRL Number	Task Order Section	Title	Format	Required Date	Frequency	Distribution
				award		
C.1.7-2	C.1.7.1.2	Key Personnel Succession Plan	Electronic	Within 20 business days of Task Order award	As required	COTR
C.1.7-3	C.1.7.2.2	Staffing Roster	Electronic	No later than the 15th business day of each month	Monthly	COTR
C.1.7-4	C.1.7.3.2	Employee Training Plan	Electronic	Within 20 business days of Task Order award	As required	COTR
	C.1.8	CONTRACTOR INTERFACES				
C.1.8-1	C.1.8.1.1.2	Unresolved Dispute Information	Written	Within two business days from the time the dispute occurs	As required	COTR
	C.1.9	QUALITY ASSURANCE AND QUALITY CONTROL				
C.1.9-1	C.1.9.2.1	Quality Control Plan	Electronic	Within 20 business days of Task Order award	As required	COTR
C.1.9-2	C.1.9.2.2	Customer Evaluation Plan	Electronic	No later than 20 business days after Task Order award	Within 20 business days of the requested change	COTR
	C.1.11	OPERATING ENVIRONMENT				
C.1.11-1	C.1.11.2.4	Essential Personnel Contact List	Electronic	10 business days after Task Order start	Update as necessary	COTR
C.1.11-2	C.1.11.3.2	Travel Requests	Written or Electronic	Prior to travel	As required	COTR
	C.1.12	CONTRACT TRANSITION				
C.1.12-1	C.1.12.1.1	Contract Transition Plan	Electronic	Within 20 business days of Task Order award	Update as necessary	COTR
	C.3.1.2	GOVERNMENT FURNISHED SERVICES				
C.3.1-1	C.3.1.2.4	Government Furnished Service Discrepancy	Electronic	N/A	As required	COTR

CDRL Number	Task Order Section	Title	Format	Required Date	Frequency	Distribution
		Report				
	C.3.1.4	GOVERNMENT FURNISHED EQUIPMENT				
C.3.1-2	C.3.1.4.2.3	Government Property Report – Annual	Electronic	As directed	Annually	COTR
C.3.1-3	C.3.1.4.4.2	Government Property Inventory – Initial	Electronic	Within ten business days prior to Task Order start date	Task Order award	COTR
	C.4.1.1	CONTRACTOR FURNISHED FACILITIES				
C.4.1-1	C.4.1.1.1	Contractor Owned, Contractor Operated Facilities List (used in Task Order performance)	Electronic	Within ten business days prior to Task Order start date	Update as necessary	COTR
	C.5.1	APPLICATIONS MANAGEMENT AND SUPPORT SERVICES				
C.5.1-1	C.5.1.1.4	Applications Consolidation and Rationalization Plan	Electronic	Within twenty business days after Task Order start date	Annually and as required	COTR
C.5.1-2	C.5.1.2.1	Up/Down Status Report	Electronic		As required	COTR
C.5.1-3	C.5.1.3.1	Application Maintenance and Operation Reports – Weekly	Electronic	First business day of week	Weekly	COTR
C.5.1-4	C.5.1.3.1.1	Root Cause Analysis Report	Electronic	Within 48 hours of incident	As required	COTR
C.5.1-5	C.5.1.5.1	Performance Trend of Major Applications on the Network Report	Electronic	As directed	As required	COTR
	C.5.2	DEPLOYMENT SUPPORT				
C.5.2-1	C.5.2.1.3	Deployment Project Plan	Electronic	Prepared for each project	As required	COTR
C.5.2-2	C.5.2.1.6	Proposed Workspace Report	Electronic	Within five business days of conducting site survey	Report as required	COTR
C.5.2-3	C.5.2.1.7	Trip Report	Electronic	Within five business days of	As required	COTR

CDRL Number	Task Order Section	Title	Format	Required Date	Frequency	Distribution
				trip conclusion		
C.5.2-4	C.5.2.1.8	Site report	Electronic	Within five business days of site survey	As required	COTR
C.5.2-5	C.5.2.2	Deployment Plan Template	Electronic	Within 20 business days of Task Order start	Initial and updated as required	COTR
C.5.2-6	C.5.2.3	Site Acceptance Process	Electronic	Within 20 business days of Task Order start	Initial and updated as required	COTR
C.5.2-7	C.5.2.3	Test Plans and Test Results Report	Electronic	Within 20 business days of Task Order start	Initial and updated as required	COTR
C.5.2-8	C.5.2.5.3	Deployment Project Plan/Status Report	Electronic	As required for each project	As required	COTR
	C.5.3	INFRASTRUCTURE ENGINEERING SERVICES				
C.5.3-1	C.5.3.4.2.5	Gold Copy Images	Electronic	Within five business days of any approved change	As required	COTR
	C.5.4	TESTING				
C.5.4-1	C.5.4.1	Individual Test Plans	Electronic	60 days prior to Task Order start	Update as changes Occur	COTR
C.5.4-2	C.5.4.2.5	Test Lab Issues and Risks Report	Electronic	Within three business days of identification of problem or risk	Report as required	COTR
C.5.4-3	C.5.4.2.10	Testing Lab Findings Report	Electronic	Within ten business days of findings	Report as required	COTR
	C.5.5	OPERATIONS AND MAINTENANCE FOR END USER SUPPORT				
C.5.5-1	C.5.5.1	End User and Desk Side Support Concept of Operations Plan	Electronic	Within five business days prior to Task Order start	Initial and Annual Review	COTR
C.5.5-2	C.5.5.2.1	Preventative Maintenance Plan, Policies and Procedures	Electronic	Within 40 business days after Task Order start	Initial and update within five business days of changes	COTR

CDRL Number	Task Order Section	Title	Format	Required Date	Frequency	Distribution
	C.5.8	PHONE AND PBX OPERATIONS				
C.5.8-1	C.5.8.1.7	Phone and PBX Service Report	Electronic	Within 60 days of Task Order start	Update within five business days of changes	COTR
C.5.8-2	C.5.8.2.2.1	Switchboard Knowledgebase Reference	Electronic	Within 20 business days of Task Order start	Update the reference within five business days of DHS announcement of functional re-alignment or organization moves	COTR
C.5.8-3	C.5.8.2.2.2	Automatic Call Directory	Electronic	Within 40 business days of Task Order start	As directed	COTR
C.5.8-4	C.5.8.2.6	Call Pattern Statistics Reports-Monthly	Electronic	Within 30 days of Task Order start	Monthly	COTR
C.5.8-5	C.5.8.2.7	Switchboard COOP Plan	Electronic	60 days prior to Task Order start	Update as required upon changes	COTR
C.5.8-6	C.5.8.2.8.2	Switchboard Training Lesson Plan	Electronic	Initial within 40 days of Task Order start	Updates as required	COTR
	C.5.9	NETWORK MANAGEMENT CENTER				
C.5.9-1	C.5.9.1.4	NMC Standard Operating Procedures	Electronic	Within 60 days of Task Order start	Update within five business days of changes	COTR
C.5.9-2	C.5.9.1.12	Network and Systems Infrastructure Report	Electronic	Within 60 days of Task Order start	Update within five business days of changes	COTR
C.5.9-3	C.5.9.1.19	Network Metrics Reports	Electronic	No later than 7:30AM each business day	Daily	COTR

CDRL Number	Task Order Section	Title	Format	Required Date	Frequency	Distribution
	C.5.10	SECURITY MANAGEMENT CENTER				
C.5.10-1	C.5.10.1.2	Information Technology Services Office Security Management Approach and SOPs, Checklists and a DHS Information Technology Services Office Security Plan	Electronic	Within 60 days of Task Order start	Update within one business day of changes	COTR
C.5.10-2	C.5.10.2.1	Vulnerability Assessment Report	Electronic	PII Incidents: Within 30 minutes of identification of vulnerability Non PII Incidents: Within two hours for critical, four hours for high, one day for medium, two days for low of identification of vulnerability	As vulnerabilities are identified	COTR
C.5.10-3	C.5.10.2.6	Application Vulnerability Cost Benefit Analysis	Electronic	Within five business days of direction	As required	COTR
C.5.10-4	C.5.10.5.4	Patch/Service Pack Deployment Reports	Electronic	Within one business day of Deployment	As Deployments are performed	COTR
C.5.10-5	C.5.10.6.4	System Log Security Review Reports	Electronic	The first business day following the end of the previous month	Monthly	COTR
C.5.10-6	C.5.10.9.2	Forensics Investigations SOPs	Electronic	Within 60 days of Task Order start	Update within one business day of changes	COTR
C.5.10-7	C.5.10.9.4	Event and Incident Reports	Electronic	PII Incidents: Within 30	As incidents are	COTR

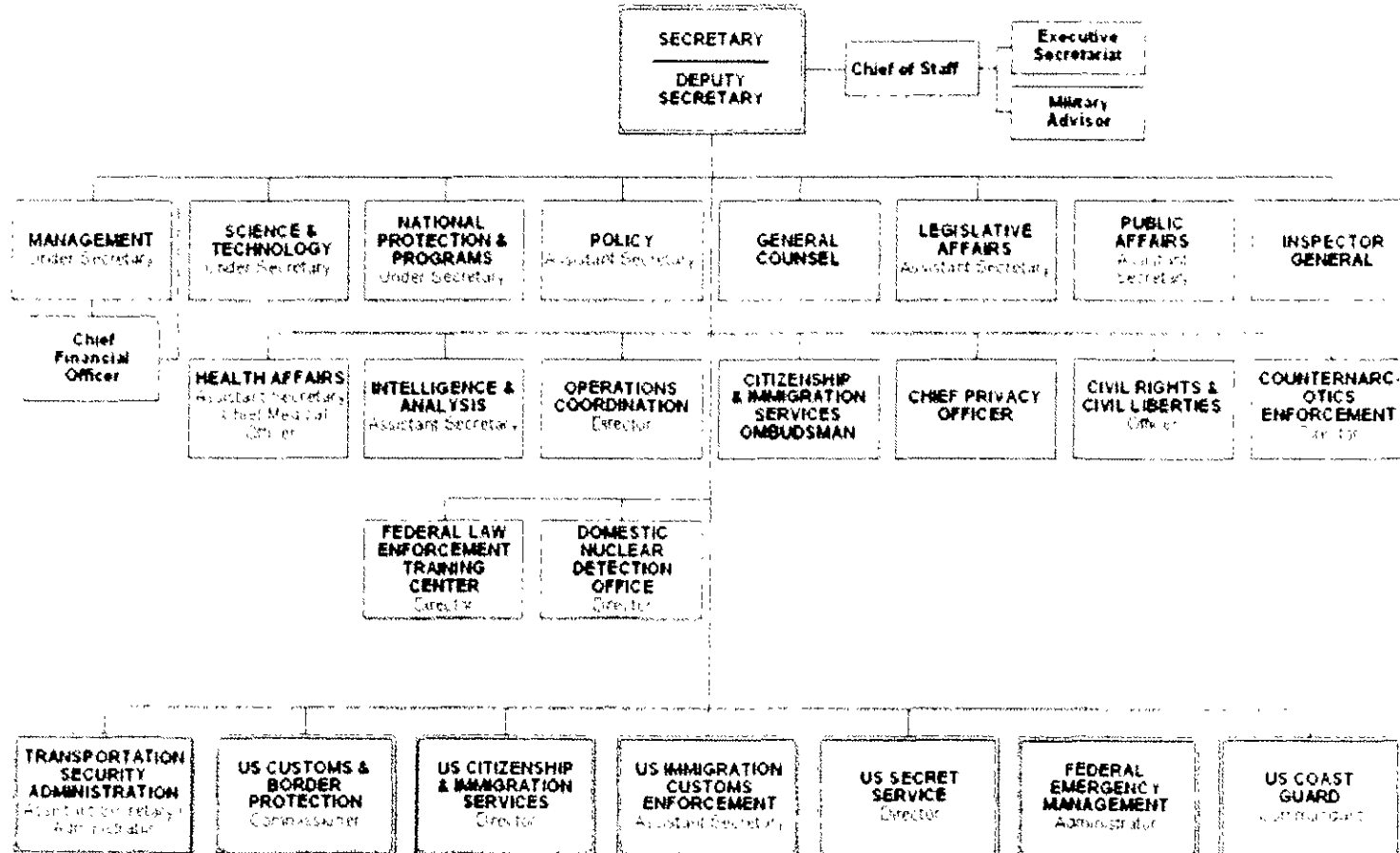
CDRL Number	Task Order Section	Title	Format	Required Date	Frequency	Distribution
				minutes of identification of event or incident Non PII Incidents: Within two hours for critical, four hours for high, one day for medium, two days for low of identification of event or incident	identified	
C.5.10-8	C.5.10.10.3	INFOCON Level SOPs and Checklists	Electronic	Within 60 days of Task Order start	Update within one business day of changes	COTR
	C.5.11	COMMUNICATIONS SECURITY (COMSEC) MANAGEMENT				
C.5.11-1	C.5.11.1.6	COMSEC Plan	Electronic	Within 60 days of Task Order start	Update within one business day of changes	COTR
	C.5.13	TRAINING				
C.5.13-1	C.5.13	Training Plan	Electronic	Within 60 days of Task Order start	Update within one business day of changes	COTR
	C.5.14	WIRELESS MANAGEMENT				
C.5.14-1	C.5.14.2.5	Wireless Systems Engineering Framework	Electronic	Within 60 business days of Task Order start	Initial with Updates	COTR
C.5.14-2	C.5.14.2.8	Wireless SEMP & CONOPS, Baseline, System & System Development Specifications	Electronic	Within 60 business days of Task Order start and update as changes occur	Initial with Updates	COTR
	C.5.15	IT CONTINUITY MANAGEMENT				
C.5.15-1	C.5.15.1.1	Business Continuity Initial Assessment	Electronic	Within 40 business days of Task Order start	Once	COTR
C.5.15-2	C.5.15.1.2	Business	Electronic	Within 60	Once	COTR

CDRL Number	Task Order Section	Title	Format	Required Date	Frequency	Distribution
		Continuity Framework Gap Analysis		business days of Business Contintuity Initial Assessment approval by COTR		
C.5.15-3	C.5.15.2.1	Multi-Year Strategic Program Management Plan	Electronic	Annual suspense date or within 60 business days of direction	Annually and as directed	COTR
C.5.15-4	C.5.15.2.2	CIO COOP Implementation Plan	Electronic	Annual suspense date or within 60 business days of direction	Annually and as directed	COTR
C.5.15-5	C.5.15.2.3	Incident Response and Management Plan	Electronic	Annual suspense date or within 60 business days of direction	Annually and as directed	COTR
C.5.15-6	C.5.15.2.4	CIO Operational Recovery Plan and IT Disaster Recovery/ Business Continuity Plan	Electronic	Annual suspense date or within 60 business days of direction	Annually and as directed	COTR
C.5.15-7	C.5.15.3.2	Plans and Exercises Coordination Meeting Minutes	Electronic	Within 3 business days of meeting	Bi-weekly	COTR
C.5.15-8	C.5.15.4.1	Continuity Policy, Guidance, Methodologies and Tools	Electronic	Annual suspense date or within 60 business days of direction	Annually and as directed	COTR
C.5.15-9	C.5.15.4.2	Essential Functions, Critical IT/Telecommunications Networks, Systems, Facilities, and Critical Positions List	Electronic	Annual suspense date or within 3 business days of change	Annually and as directed	COTR
C.5.15-10	C.5.15.4.3	Continuity Management Review	Electronic	Annual suspense date or within 20 business days of	Annually and as required	COTR

CDRL Number	Task Order Section	Title	Format	Required Date	Frequency	Distribution
				change		
C.5.15-11	C.5.15.4.5	Business Continuity Executive Briefings	Electronic	As directed	As required	COTR
C.5.15-12	C.5.15.5.1	Test/Exercise Plans	Electronic	Within 60 days of Task Order start	Update within one business day of changes	COTR
C.5.15-13	C.5.15.5.2	Test/Exercise After Action Report	Electronic	Within 20 business day of direction	Annually and as directed	COTR
C.5.15-14	C.5.15.6.1	Electronic Vital Records Program Test Report	Electronic	Within five business days of completing the test	Quarterly	COTR

PROCUREMENT SENSITIVE

TE C.1.2-001 Department of Homeland Security Organization Chart



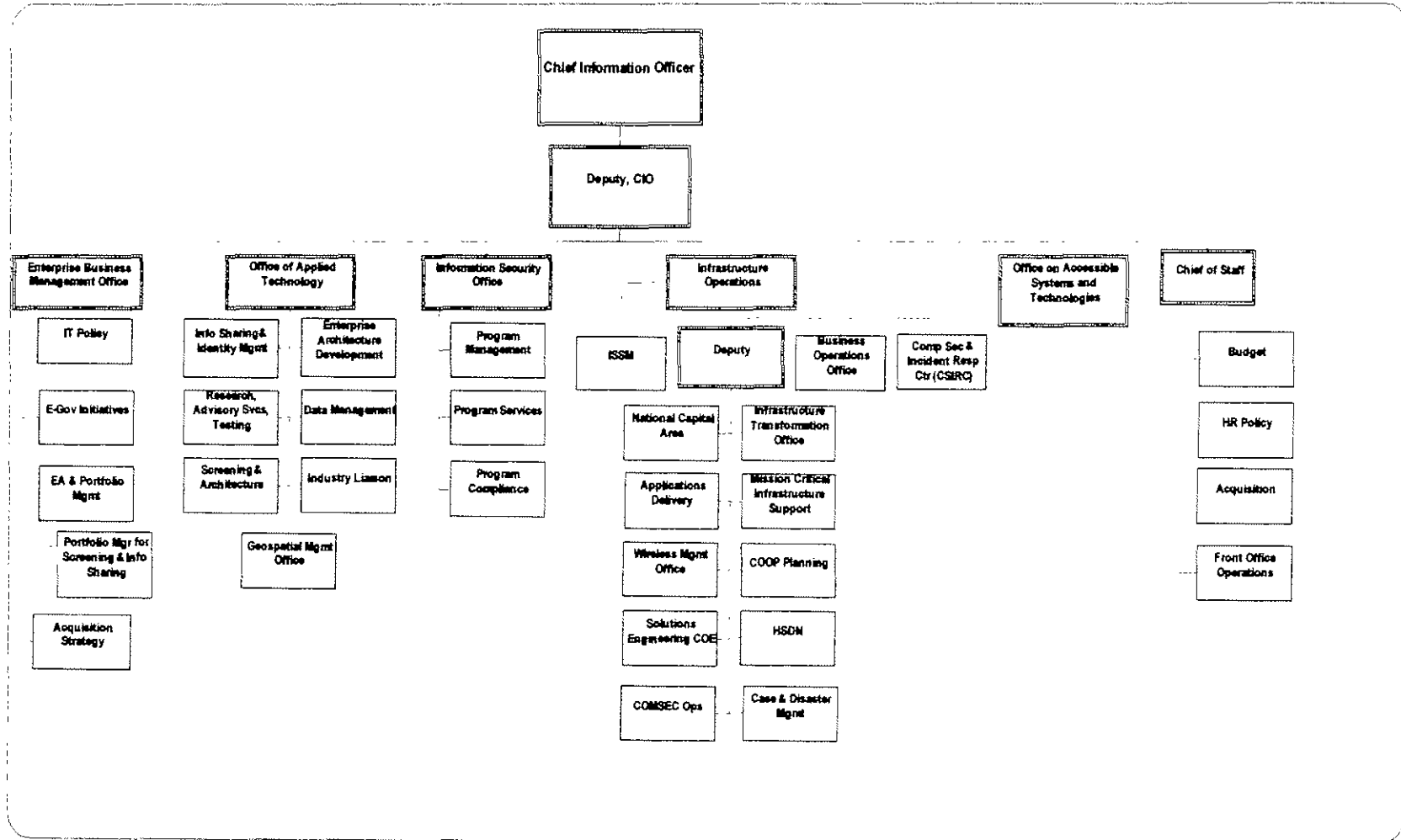
PROCUREMENT SENSITIVE

TE C.1.2-002 Locations Supported Summary

**See DHS Interactive Website for Locations Supported Summary
(Information is Sensitive But Unclassified)**

PROCUREMENT SENSITIVE

TE C.1.2-003 DHS IT Organization Chart



PROCUREMENT SENSITIVE

TE C.1.3-003 Seats by Network

Table 1: Projected Seat Count for LAN – Sensitive But Unclassified (LAN-A)

Projected LAN Seat Count (By Customer View)								
Fiscal Year	Total	Intelligence & Analysis	PD	Operations	Science & Technology	Grants & Training	Undersecretary of Management	Domestic Nuclear Detection Office
FY06	3527	331	700	115	691	290	1319	81
FY07	4371	300	840	241	693	375	1702	220
FY08	5202	640	980	280	693	450	1919	240
FY09	5626	640	1120	300	693	525	2068	280
FY10	5969	640	1260	300	693	600	2176	300
FY11	6028	640	1260	300	693	600	2215	320
FY12	6050	640	1260	300	693	600	2217	340
FY13	6070	640	1260	300	693	600	2217	360

PROCUREMENT SENSITIVE

TE C.1.3-003 Seats by Network

Table 2: Projected Seat Count for LAN – HSDN
 Seats are at 79 locations

Projected Seat Count (By Customer View)	
Fiscal Year	Total
FY06	1550
FY07	1630
FY08	1710
FY09	1800
FY10	1880
FY11	1960
FY12	2040
FY13	2120

PROCUREMENT SENSITIVE

TE C.1.3-003 Seats by Network

Table 3: Projected Seat Count for LAN – Top Secret (LAN – C)

Projected LAN Seat Count (By Customer View)								
Fiscal Year	Total	Intelligence & Analysis	PD	Operations	Science & Technology	Grants & Training	Undersecretary of Management	Domestic Nuclear Detection Office
FY06	516	348	40	76	33	0	19	0
FY07	519	300	44	90	33	0	42	10
FY08	912	640	48	138	33	0	43	10
FY09	933	640	53	150	33	0	47	10
FY10	933	640	53	150	33	0	47	10
FY11	933	640	53	150	33	0	47	10
FY12	933	640	53	150	33	0	47	10
FY13	933	640	53	150	33	0	47	10

PROCUREMENT SENSITIVE

TE C.1.6-001 Performance Requirements Summary (PRS)

TASK ORDER SECTION NUMBER	SECTION TITLE/TOPIC	ESTIMATED WORKLOAD	STANDARD	STANDARD DESCRIPTION	MAXIMUM ALLOWABLE DEVIATION	SURVEILLANCE METHOD
C.5.1.1.4 C.5.1.2.1 C.5.1.3.1 C.5.1.3.1.1 C.5.1.5.1 C.5.2.1.3 C.5.2.1.6 C.5.2.1.7 C.5.2.1.8 C.5.2.2 C.5.2.3 C.5.2.5.3 C.5.3.4.2.1 C.5.3.4.2.2 C.5.3.4.2.3 C.5.4.1 C.5.4.2.3 C.5.4.2.5 C.5.4.2.10 C.5.5.1 C.5.6.1.5 C.5.7.1 C.5.7.1.4 C.5.7.1.6 C.5.8.1.7 C.5.8.1.7.1 C.5.8.2.2 C.5.8.2.3 C.5.8.2.6 C.5.8.2.7 C.5.9.1.4 C.5.9.1.12 C.5.9.1.20 C.5.9.1.22.3	Plans, reports, documentation and other deliverables		Quality	The item is accurate, grammatically correct and adheres to the deliverable requirements	10% for initial 0% for final	Random sampling
			Timeliness	The item is provided to the designated government representative no latter than five business days after DHS approval and adoption unless otherwise specified.	5%	

PROCUREMENT SENSITIVE

TE C.1.6-001 Performance Requirements Summary (PRS)

TASK ORDER SECTION NUMBER	SECTION TITLE/TOPIC	ESTIMATED WORKLOAD	STANDARD	STANDARD DESCRIPTION	MAXIMUM ALLOWABLE DEVIATION	SURVEILLANCE METHOD
C.5.1, C.5.1.1, C.5.1.1.1 C.5.1.1.2 C.5.1.7 C.5.2.1.9 C.5.2.5.2 C.5.2.5.3 C.5.3.2 C.5.3.3 and subsections C.5.5.1 C.5.5.1.1 C.5.5.1.2 C.5.5.1.3 C.5.5.1.4 C.5.5.2.3 C.5.6.1.1 C.5.6.1.2 C.5.6.1.3 C.5.6.1.6 C.5.7 C.5.7.1.2 C.5.8 C.5.8.1.2 C.5.9.1 C.5.9.1.21 C.5.9.1.23 C.5.11.1.1	Applications and Systems availability, reliability and support		Accessibility	The contractor provided availability rates based on mission criticality as specified in the Task Order Section C.1 Table 1 for all applications and systems at all times 7X24X365 (366 for leap years). The availability rate for each application or system is determined by dividing the total time the application or system functioned properly by the total time of the measurement period. The composite availability rate shall be determined using an average based upon the weighted use of each application or system. Application acceptance is a function of identified user acceptance testing in accordance with DHS requirements.	0.10%	Random sampling
			Timeliness	Mission Applications – The contractor corrects problem within two hours of discovery or notification	3%	Random sampling
C.5.5.1.1 C.5.5.1.2 C.5.5.1.3 C.5.5.1.4	Customer Support	See Help Desk Ticket Volume TE C.5.5.001 at DHS Interactive Website	Timeliness	Category I - VIP User: The contractor corrects problem within two hours of discovery or notification	1%	Random Sampling
				Category II - DHS End-User at Primary Location: The contractor corrects problem within eight hours of discovery or notification	5%	
				Category III - DHS End-User at Non-Primary Location: The contractor corrects problem within ten hours of discovery or notification	5%	

PROCUREMENT SENSITIVE

TE C.1.6-001 Performance Requirements Summary (PRS)

TASK ORDER SECTION NUMBER	SECTION TITLE/TOPIC	ESTIMATED WORKLOAD	STANDARD	STANDARD DESCRIPTION	MAXIMUM ALLOWABLE DEVIATION	SURVEILLANCE METHOD
C.5.1 C.5.2.5.2 C.5.2.7.1 C.5.3.1 C.5.3.2 C.5.4.2.1 C.5.4.2.7 C.5.4.2.9 C.5.4.2.10 C.5.4.2.11 C.5.6.1.6 C.5.6.1.7 C.5.7.1.4 C.5.8.1.4 C.5.8.1.6 C.5.8.2.3 C.5.8.2.4 C.5.9.1.1 C.5.9.1.2 C.5.9.1.3 C.5.9.1.5 C.5.9.1.9 C.5.9.1.11 C.5.9.1.15 C.5.9.1.22 C.5.10.1.1 C.5.10.2.2 C.5.10.3.2 C.5.10.4.1 C.5.10.4.2 C.5.10.4.4 C.5.10.9 C.5.10.10.2 C.5.11.1.1 C.5.11.1.2 C.5.12.2 C.5.14.5.1	Applications and Infrastructure Support	See Help Desk Ticket Volume TE C.5.5.001 at DHS Interactive Website for information on volume of work for each section	Availability	The contractor provided uninterrupted O&M support during the timeframes specified for the particular section	As specified in applicable sections	Random sampling
C.5.3.3.3 and subsections	Engineering Projects	See Projects List, TE C.1.12.002 at DHS Interactive Website	Timeliness	The contractor completed all projects and work assignments and the application or service was useable by the specified DHS community by assigned due dates.	5%	Random sampling

PROCUREMENT SENSITIVE

TE C.1.6-001 Performance Requirements Summary (PRS)

TASK ORDER SECTION NUMBER	SECTION TITLE/TOPIC	ESTIMATED WORKLOAD	STANDARD	STANDARD DESCRIPTION	MAXIMUM ALLOWABLE DEVIATION	SURVEILLANCE METHOD
C.5.1.1.2 C.5.2.1.2 C.5.3.1.1	Requirements Analysis		Quality	The contractor collected, documented, obtained customer requirements certification and performed analysis and management service in compliance with DHS Policy and Guidelines	5%	Random sampling
			Timeliness	The contractor provided analysis to the COTR within the timeframe	5%	Random sampling
C.5.1.1.2	Application and Web Service Enhancements		Quality	The contractor provided accurate support for application development services that allowed each application to operate without interrupting business activities or causing performance degradation	5% of requirements per Application	Random sampling
			Timeliness	The contractor provided application support to the COTR within timeframes specified.	5%	Random sampling
C.5.1.1.4.1 C.5.4.2.2 C.5.4.2.3 C.5.5.2.2 C.5.5.2.3.3 C.5.9.1.16 C.5.10.1.6 C.5.10.5 C.5.10.10.3	Configuration and Change Management compliance		Quality	The contractor accurately configured the IT systems or managed documentation in accordance with established DHS configuration and change management requirements, policy, guidelines, and processes.	1%	Random sampling
			Timeliness	The element was completed and submitted within establish CM timeframes.	1%	Random sampling
C.5.1.2.1 C.5.1.2.2 C.5.6.1.3 C.5.8.1.10 C.5.9.1.2 C.5.9.1.9 C.5.9.1.14 C.5.9.1.17 C.5.9.1.18 C.5.9.1.22 C.5.9.1.22.1 C.5.9.10.1.3 C.5.10.1.7 C.5.10.1.8 C.5.10.2.3 C.5.10.3.1 C.5.10.4.1	Monitoring		Quality	The contractor provided current status monitoring for all DHS major system applications.	0.50%	Random sampling
			Timeliness	The contractor submitted the reports within the specified timeframes for review and complied with all timeframes for submission.	0.50%	Random sampling
C.5.1.4.1 C.5.1.5.3 C.5.4.2.6 C.5.5.2.2 C.5.5.2.3.1	Operations, Maintenance & Upgrades	The contractor shall identify the requirements for and install	Quality	The contractor successfully identified requirements for and installed all upgrades, updates, service packs, and patches without interrupting the business activities of DHS or causing degradation in the performance of the network or applications	5%	Random Sampling

PROCUREMENT SENSITIVE

TE C.1.6-001 Performance Requirements Summary (PRS)

TASK ORDER SECTION NUMBER	SECTION TITLE/TOPIC	ESTIMATED WORKLOAD	STANDARD	STANDARD DESCRIPTION	MAXIMUM ALLOWABLE DEVIATION	SURVEILLANCE METHOD
C.5.5.2.3.1 C.5.5.2.3.2 C.5.7.1.3 C.5.7.1.4 C.5.7.1.7 C.5.8.1.1 C.5.8.1.8 C.5.8.2.9 C.5.9.1.3 C.5.9.1.6 C.5.9.1.8 C.5.9.1.13 C.5.9.1.19 C.5.9.1.22.2 C.5.10.1.4 C.5.10.1.6 C.5.10.4.4 C.5.10.5.1 C.5.10.5.3 C.5.11.1.5 C.5.11.1.8 C.5.12.1.4		Weekly & Monthly	Quality	The contractor accomplished complete and accurate upgrades, updates, service pack installations and patches in accordance configuration requirements negotiated with the requestor for installations performed	5%	Random Sampling
			Timeliness	The contractor completed timely upgrades, updates, service pack installations and patches	5%	Random Sampling
C.5.1.4.2	Security Remediation		Quality	The contractor allowed no security violations that permitted access to the databases by unauthorized individuals, allowed the unauthorized release of data, caused loss of data integrity, or caused data degradation due to circumstances such as external intrusion or improper use by authorized users.	0.01%	100% Inspection
			Timeliness	The contractor corrected security violations and performed maintenance on operating systems within 30 minutes of discovery or notification.	0%	100% Inspection
C.5.1.4.3 C.5.4.2.5 C.5.9.1.1 C.5.9.1.13	Notification & Escalation		Quality	The contractor successfully identified incompatible requirements and notified the COTR installed all upgrades, updates, service packs, and patches without interrupting the business activities of DHS or causing degradation in the performance of the network or applications	5%	100% Inspection
			Timeliness	The contractor identified and notified the COTR no later than the end of the business day following the identification of incompatibility	5%	100% Inspection
C.5.1.4.4 C.5.1.6.1	Analysis, Review, and Management Recommendations		Quality	The contractor performed review, analysis and provided a recommendation to DHS	5%	Random sampling
			Timeliness	The contractor's recommendations shall be provided within one hour of discovery or notification	5%	Random sampling

PROCUREMENT SENSITIVE

TE C.1.6-001 Performance Requirements Summary (PRS)

TASK ORDER SECTION NUMBER	SECTION TITLE/TOPIC	ESTIMATED WORKLOAD	STANDARD	STANDARD DESCRIPTION	MAXIMUM ALLOWABLE DEVIATION	SURVEILLANCE METHOD
C.5.1.5.2	Knowledge system		Quality	The contractor provided a system for maintaining the required data based on DHS requirements, provided required system access and produced required deliverables from the system	25% initial submittal and 0% for final	100% Inspection
			Timeliness	The contractor completed the specifications of the plan within the established milestones.	10% for initial 0% for final	Random sampling
			Timeliness	The contractor performed all updates within the designated timelines	5%	Random Sample
C.5.1.6.2	Asset Tracking		Quality	The contractor maintained accurate asset records regardless of administrative assignment of the asset	5%	Random Sample
			Timeliness	The contractor entered asset data into the asset management system within two business days of receipt of asset.	5%	Random Sample
C.5.2.1.1 C.5.3.1.1 C.5.3.2 C.5.3.3 and subsections C.5.3.4.1	Project Management		Quality	The contractor acceptably applied DHS Information Technology (DHS IT) Project Management policies and procedures to all projects. Acceptable performance of a project means that it has been completed in accordance with the milestones, objectives and timelines established by the Project Management Policies.	Revisions accomplished within 5% of milestone dates	Random Sample
			Timeliness	Acceptable performance of Deployment Projects requires that all projects are deployed and rendered completed and useable by the entire DHS community (or otherwise specified) no later than identified project timelines.	5%	100% Inspection
C.5.2.5.1 C.5.9.1.25 C.5.10.9.3 C.5.11.1.7	Compliance		Quality	The contractor successfully completed installations and check-out work in compliance with established DHS MDs, policies, guidelines, processes, procedures or other requirements without interrupting the business activities of DHS or causing degradation in network performance	5%	Random Sampling
			Timeliness	The contractor completed each installation and checkout within timeframes specified by the Deployment Project Plan/COTR.	1%	Random Sampling
5.3.4.1	Project Template	Once with updates as required	Quality	The contractor acceptably developed and applied an engineering development lifecycle methodology template including procedures, to support each project. Acceptable performance consisted of a methodology containing factors that allowed each project to be completed in accordance with the technical requirements, geography, milestones, objectives and timelines while minimizing disruptions to users, systems, applications and DHS operations.	5% of projects unless approved by COTR	Random Sampling

PROCUREMENT SENSITIVE

TE C.1.6-001 Performance Requirements Summary (PRS)

TASK ORDER SECTION NUMBER	SECTION TITLE/TOPIC	ESTIMATED WORKLOAD	STANDARD	STANDARD DESCRIPTION	MAXIMUM ALLOWABLE DEVIATION	SURVEILLANCE METHOD
			Timeliness	The contractor provided the proposed template within 20 business days of Task Order start, and met all COTR specified timeframes for rewrites or changes.	25%	100% inspection
C.5.3.4.2.4	Configuration Management Data Base (CMDB)		Quality	The contractor maintained & updated the CMDB accurately	5%	Random Sampling
			Timeliness	The contractor performed all updates within the designated timelines	5%	Random Sampling
C.5.3.4.2.5 C.5.4.2.8	Image Library		Quality	The contractor created, updated and maintained an electronic library of all images in accordance with COTR Direction and DHS policy	5%	Random Sampling
			Timeliness	The contractor shall maintain configuration management of all images and provided Gold Copy images to the Government as a deliverable to this task within five business days of any approved changes	5%	
5.5.1	End User and Desk Side Support		Quality	The contractor developed, updated and maintained an accurate and comprehensive plan, policies, and procedures. Acceptable performance resulted in a comprehensive plan that provided a detailed description of policies, procedures, work breakdown structure (WBS), process flow charts, detailed performance metrics, evaluation/inspection methodology and criteria for the entire Help Desk operations including Tier 1, 2 and 3., and field site support	10% for initial and 0% for final	100% inspection
			Timeliness	The contractor provided the initial document within 40 business days of Task Order start.	5%	100% inspection
C.5.9.1.23	Web page content		Quality	The contractor provided Web page content that was Section 508 compliant	0%	100% Inspection
C.5.10.2.1 C.5.10.2.2 C.5.10.2.6 C.5.10.4.3 C.5.10.5.2	Vulnerability Assessment	Quarterly	Quality	The contractor accurately and correctly conducted all required assessments	5%	Random Sampling
			Timeliness	The contractor will devise an audit review process that collects and reviews all critical IT systems no less than once every 90 days or as directed by the appropriate COTR.	0%	Random Sampling
C.5.10.8	Data Spills and Response		Quality	The contractor's guards and gateways did not allow any unauthorized releases of Secret or TS/SCI data	0%	100% inspection
C.5.11.1.4	COMSEC equipment		Quality	The contractor maintained accurate records of the receipt and distribution of COMSEC equipment and accurate records of COMSEC accounts	0%	100% Inspection

PROCUREMENT SENSITIVE

TE C.1.6-001 Performance Requirements Summary (PRS)

TASK ORDER SECTION NUMBER	SECTION TITLE/TOPIC	ESTIMATED WORKLOAD	STANDARD	STANDARD DESCRIPTION	MAXIMUM ALLOWABLE DEVIATION	SURVEILLANCE METHOD
C.5.12.1.1 C.5.14.1 and subsections C.5.14.2.1	Training		Quality	The contractor provided all required user training. Acceptable performance allowed users to correctly operate the system after training.	1%	Random Sampling
			Timeliness	The contractor provided all training within the timelines specified by the COTR.	5%	Random Sampling
C.5.12.1.2 C.5.12.14	Coordination		Quality	The contractor performed all interface and coordination efforts for demand maintenance and software upgrades. Acceptable performance allows the system to be operational at all times.	1%	Random Sampling
			Timeliness	The contractor performed all interface and coordination efforts within the timeframes specified by the COTR.	5%	Random Sampling
C.5.14	Training		Quality	The contractor maintained an accurate record of system user, security, and end-user training	5%	Random Sampling
			Timeliness	The contractor provided training records on time each year two months prior to the end of the fiscal year or when requested.	5%	Random Sampling
C.5.15.1.1	Continuity Assessment	Once	Timeliness	The contractor successfully performed the baseline infrastructure analysis within 40 business days of Task Order start. Acceptable performance allowed the contractor to document content of existing plans.	0%	100% Inspection
C.5.15.1.2	Continuity Assessment	Once	Timeliness	The contractor successfully evaluated the baseline infrastructure analysis against the Business Continuity Framework and identified the gaps between existing and required capability. Acceptable performance allowed the contractor to accurately document the gap analysis findings which were submitted to the COTR within 60 business days of the Task Order start date.	5%	100% Inspection
C.5.15.2.1	Continuity Planning	Once	Timeliness	The contractor successfully developed and finalized strategic plans for required programs and offices. An initial strategic plan was submitted within 40 business days of Task Order start and a finalized strategic plan was approved within 20 business day of the DHS review of the initial plan.	Initial 10%, Final 0%	100% Inspection
C.5.15.2.1	Continuity Planning	Annually	Timeliness	The contractor facilitated strategic planning with the program offices and developed the Multi-Year Strategic Program Management Plan containing planning goals, objectives and performance measures		
C.5.15.2.2	Continuity Planning	Annually	Quality	The contractor successfully updated and maintained the CIO COOP Implementation Plan according to specified DHS requirements.	0%	100% Inspection
			Timeliness	The contractor updated and maintained the CIO COOP Implementation Plan within specified timeframes	0%	100% Inspection

PROCUREMENT SENSITIVE

TE C.1.6-001 Performance Requirements Summary (PRS)

TASK ORDER SECTION NUMBER	SECTION TITLE/TOPIC	ESTIMATED WORKLOAD	STANDARD	STANDARD DESCRIPTION	MAXIMUM ALLOWABLE DEVIATION	SURVEILLANCE METHOD
C.5.15.2.3	Continuity Planning		Quality	The contractor successfully updated and maintained the IT Incident Response and Management Plan according to specified DHS requirements.	0%	100% Inspection
			Timeliness	The contractor updated and maintained the IT Incident Response and Management Plan within specified timeframes.	0%	100% Inspection
C.5.15.2.4	Continuity Planning		Quality	The contractor successfully updated and maintained the CIO Operational Recovery Plan according to specified DHS requirements.	0%	100% Inspection
			Timeliness	The contractor updated and maintained the CIO Operational Recovery Plan within specified timeframes.	5%	100% Inspection
C.5.15.3.1	Continuity Planning		Quality	The contractor successfully performed Enterprise Architecture Center of Excellence (EACOE) reviews, Enterprise Change Control Board (ECCB) reviews, and compliance activities for IT continuity planning impact according to specified DHS requirements.	0%	Random Sampling
			Timeliness	The contractor completed all reviews and submitted findings within specified timeframes.	0%	Random Sampling
C.5.15.3.2	Continuity Reviews and Coordination	26 two-hour meetings per year	Timeliness	The contractor planned, scheduled and conducted bi-weekly meetings for the coordination, development, and maintenance of Disaster Recovery, IT contingency planning, and COOP exercise scenarios. The contractor provided minutes within three business days of the meeting.	0%	100% Inspection
C.5.15.4.1	Continuity Program Administration	Annually and as required	Quality	The contractor developed, maintained, updated and implemented IT continuity policy, guidance, methodologies and tools that accurately and completely included each requirement.	Initial 10% Final 0%	100% Inspection
C.5.15.4.2	Continuity Program Administration	Annually	Quality	The contractor accurately updated and maintained CIO functions according to specific requirements and COTR direction. Acceptable performance allowed the contractor to support DHS without interrupting the deployment or business activities of DHS or causing degradation in the performance of the supported services.	0%	100% Inspection
C.5.15.4.3	Continuity Program Administration	Annually or when significant IT infrastructure changes occur	Quality	The contractor performed a continuity management review, Risk Assessment, Interdependency Analysis, and Business Impact Analysis that identify threat and vulnerability exposure. The contractor prepared reports and executive briefings for the CIO that identify the risks.	0%	100% Inspection
			Timeliness	The contractor performed the continuity management review, Risk Assessment, Interdependency Analysis, and Business Impact Analysis within the required timeframe.	0%	100% Inspection

PROCUREMENT SENSITIVE

TE C.1.6-001 Performance Requirements Summary (PRS)

TASK ORDER SECTION NUMBER	SECTION TITLE/TOPIC	ESTIMATED WORKLOAD	STANDARD	STANDARD DESCRIPTION	MAXIMUM ALLOWABLE DEVIATION	SURVEILLANCE METHOD
C.5.15.4.4	Continuity Program Administration	Quarterly update 15 offices/46 functions	Timeliness	The contractor successfully completed a review of the CIO COOP Implementation program, Operational Recovery/ IT Contingency Plans, within specified timeframes. Acceptable performance resulted from the contractor providing feedback on program compliance in accordance with DHS guidelines and reporting the results to the COTR within specified timeframes.	0%	100% Inspection
C.5.15.5.1	Testing and Exercises	Semi-annually	Quality	The contractor successfully developed test plans and training factors and administered them according to COTR direction. Acceptable performance resulted from the contractor participating in all after test exercise reviews and documenting all related issues in accordance with DHS guidelines for FIPS 199 availability and within specified timeframes.	0%	100% Inspection
			Timeliness	Comply with FISMA and FPC-65 requirements.	0%	100% Inspection
C.5.15.5.2	Testing and Exercises	Component COOP Exercises average two per year	Quality	The contractor successfully participated in designated exercises according to COTR direction. Acceptable performance resulted from the contractor participating in all tests/exercises and exercise reviews	Initial 10%, Final 0%	100% Inspection
			Timeliness	The contractor documented all related issues in accordance with DHS guidelines and submitted an initial After Action Report within 10 business days of the test/exercise conclusion and a finalized report within 3 business day of the DHS report review.	Initial 10%, Final 0%	100% Inspection
C.5.15.6.1	Electronic Records	Quarterly or as directed by COTR	Quality	The contractor successfully tested, updated and maintained the electronic vital records programs for all LANs according to specified DHS requirements. Acceptable performance allowed the system to operate according to specified requirements without interrupting the business activities of DHS or causing degradation in the performance of associated business units (offices and programs) networks, systems, applications or provided services.	0%	100% Inspection
			Timeliness	The contractor tested, updated and maintained the electronic vital records program within specified timeframes and submitted all test artifacts to the COTR. The initial test report provided within 5 days and the final report within 10 business days.	0%	100% Inspection

TE C.1.6-002 IT NOVA Plan Development, Maintenance and Updates

Task Order Paragraph	Plan Name/Description	Contractor Provided Plan
C.1.4.2.5	Enterprise Architecture Compliance Plan	Yes
C.1.6.4.2	Architectural Compliance Plan	Yes
C.1.7.1.1	PM Succession Plan	Yes
C.1.7.1.2	Key Personnel Succession Plan	Yes
C.1.7.3.2	Employee Training Plan	Yes
C.1.9.2.1	Quality Control Plan	Yes
C.1.9.2.2	Customer Evaluation Plan	Yes
C.1.11.1.4	Building Occupant Emergency Plan	No
C.1.12.1.1	Transition Plan	Yes
C.1.5.1.1.3	Applications Consolidation and Rationalization Plan	Yes
C.5.2.1.3	Deployment Project Plan	Yes
C.5.2.4	Facility Modification Plan	Yes
C.5.5.1	Desk Side Support Concept of Operations Plan	Yes
C.5.5.2.1	Preventative Maintenance Plan	Yes
C.5.8.1.7	DHS Dial Plan	Yes
C.5.8.2.7	Switchboard Operations COOP Plan	Yes
C.5.8.2.8.2	Switchboard Training Lesson Plan	Yes
C.5.10.1.2	DHS Information Technology Services Office	Yes
C.5.10.9.4	DHS Initial National Response Plan	No
C.5.10.10.4	DHS Computer Network Defense Continuity of	No
C.5.11.1.6	COMSEC Plan	Yes
C.5.13.1.2	Project Management Plan	Yes
C.5.13	Training Plans	Yes
C.5.13.2	Security Training Plan	Yes
C.5.15.2.1	Multi-Year Strategic Program Management Plan	Yes
C.5.15.2.2	CIO COOP Implementation Plan	Yes
C.5.15.2.3	Incident Response Management Plan	Yes
C.5.15.2.4	CIO Operational Recovery Plan	Yes
C.5.15.2.4	Disaster Recovery /Business Continuity Plan	Yes
C.5.15.1	Test/Exercise Plans	Yes

TE C.1.7-001 Key Personnel Positions and Descriptions**Project Manager Level IV**

The Project Managers shall act as point of contact for all task-wide interaction, issues, and will represent the contractor at all post-award status meetings. The Project Managers shall be responsible for all issue resolution, program management, and other Task Order and management support that include providing comprehensive accountability for all requirements of the EAGLE task order. The Project Managers are responsible for overseeing Task Order performance.

Functional Area:

- All

Duties:

- Overall management responsibilities, including, all project oversight, resource management, risk management, service delivery and incident management
- The PM will be responsible for the day-to-day management and leadership to the contractors' functional teams.
- Overseeing & managing contractor responsibility to Government contractual agreements
- Developing & managing client relationships at all levels of the organization

Skills Required:

- Experience as a manager for in IT organization or program, including experience managing both business & technical resources
- Client interface experience; proven experience managing client expectations & relationships
- Experience in performing detailed analysis and evaluation of information and to make informed to the Government.
- Proven knowledge of IT infrastructure operations management, finance and governmental procurement.
- Ability to represent management across all levels of the organization: peers, cross-functional and senior management.
- Proven track record to identify potential project and process risks and formulate/implement effective mitigation plans.
- Excellent written and oral communication and meeting facilitation skills required
- Prior experience managing large, integrated teams including client and third-party vendors
- Ability to manage in a dynamic work environment and ability to coordinate and perform multiple assignments
- Experience delivering full lifecycle development initiatives with cross-functional development teams

Project Control Specialist Level III Minimum

The Project Control Specialists shall serve as the first level managers for a particular functional area and manage other Contractor personnel, mentor, manage, and resolve issues within their particular area. The team leads are responsible for requirements and deliverables under their purview.

TE C.1.7-001 Key Personnel Positions and Descriptions

Functional Areas:

- C.5.3 Infrastructure Engineering Services and C.5.5 Operations and Maintenance for End User Support

Duties:

- Oversight of particular discipline(s) the individual is assigned to manage (e.g., PMO, Technical)
- Serve as a liaison between Government and Task Order line-of business; Establish and maintain strong working relationship Serve as a liaison between Government and Task Order line-of business
- Ensure that Task Order requirements, deliverables and performance levels are maintained to ensure Task Order success
- Coordinate resources, oversee work and projects delivered to the Government
- Manage and report on infrastructure variances
- Provide continuous improvement to process and procedures

Skills:

- Experience in coordinating and managing particular area to be lead (e.g., program, security, IT infrastructure area)
- Ability to manage resources, quickly prioritize, and be proactive
- Interpersonal skills to maintain and develop relationships within the Government, peers, subordinates, and customers
- Detail oriented with focus on producing high quality work
- Experience taking initiative and working proactively to complete tasks, solve problems and making decisions
- Ability to absorb a lot of information at one time, work independently and manage workload
- Excellent oral and written communication skills
- Exceptional organizational skills with the ability to meet deadlines and prioritize
- An understanding of the ITIL process / disciplines

Disaster Recovery Specialist Level II Minimum

Functional Area:

- C.5.15 IT Continuity Management
- Duties and skills as specified in the EAGLE contract

Systems Architect Level III Minimum

Functional Area:

- C.5.3 Infrastructure Engineering Services

Duties:

TE C.1.7-001 Key Personnel Positions and Descriptions

- Participate in planning and design sessions with engineering management, architects, operations, deployment and customers
- Drive decision-making efforts to consensus and ensure that steps are taken to actual implementation of key engineering decisions
- Lead the effort to evolve a long term, scalable IT infrastructure architecture
- Articulate the engineering architecture and promote DHS technology vision and strategy to both technical and non-technical audiences
- Oversee technology decisions as they are introduced into the development, testing, and operational environments
- Communicate across the senior management team on technology and technology decisions

Skills:

- Experience in IT system engineering as a lead architect
- Experience building highly scalable websites and web-based applications
- Experience scaling IT infrastructures, including networks, telecommunications, active directory, mail systems and application integration
- Ability to articulate engineering design strategies related to scalability, performance, security, usability and development platforms
- Exceptionally strong written and verbal communication skills, as well as good interpersonal skills and organizational skills
- Ability and interest to closely collaborate with a wide-range of individuals to understand business needs and requirements and to understand how these can be met using a variety of different technologies

Deployment Manager Level III Minimum**Functional Area:**

- C.5.2 Deployment Support

Duties:

- Oversee a small project or phases of a larger project
- Responsible for coordinating activities of project team, identifying appropriate resources needed, and developing schedules to ensure timely completion of project.
- Communicates with Senior Project Manager regarding status of specific projects

Skills:

- Must be familiar with system's scope and project's objectives, as well as the role and function of each team member, in order to effectively coordinate the activities of the team.
- Demonstrate the ability to make sound decisions, recognition of when issues to need be escalated to senior staff, provide guidance as related to project execution.
- IT experience, with the ability to demonstrate a working knowledge of existing IT technologies (data and voice) and services,

TE C.1.7-001 Key Personnel Positions and Descriptions

- Project management experience, with the ability to execute activities derived from a project plan
- Basic computer skills, word-processing, email, spreadsheets, etc.
- Oral and written communication skills

Systems Engineer (Senior) Level III Minimum

Functional Areas:

- C.5.3 Infrastructure Engineering Services, C.5.5 Operations and Maintenance for End User Support, and C.5.9 Network Management Center
- Duties and skills as specified in the EAGLE contract
- Related technical certifications in networking, and hardware architecture, storage systems, or database for particular area, required

IT Security Specialist (Senior) Level III Minimum

Functional Area:

- C.5.10 Security Management Center
- Duties and skills as specified in the EAGLE contract

SME Level III Minimum

Functional Area:

- C.5.5 Operations and Maintenance for End User Support
- Duties and skills as specified in the EAGLE contract

Communication & Network Engineer Level IV

The Engineer/Designer shall support the development of data center, network and communications systems, structured cabling, data center layout and LAN/WAN design. Design tasks include creation of plans, schematics, equipment selection, systems narratives and specifications. The ability to effectively and personably, communicate with, and organize staff and client activities is critical.

Functional Areas:

- C.5.3 Infrastructure Engineering Services, C.5.5 Operations and Maintenance for End User Support, and C.5.8 Phone and PBX Operations

Duties:

- Design and engineer data center projects, prepare reports and specifications, and provide a very high level of technical leadership.
- Perform calculations, equipment selection, equipment specification, system design, system layout, facility management, due diligence, gap analysis, and feasibility reports.
- Perform all work with minimal supervision and coordinate with all applicable parties, while maintaining customer satisfaction.

TE C.1.7-001 Key Personnel Positions and Descriptions

- Responsible for producing drawings consistent with DHS's drawing organization format & drawing standards.

Skills:

- Relevant experience in the, data center, network & communications design field
- Ability to complete a variety of architectural and technical documents including drawing sections, single line diagrams, technical reports, engineering proposals for projects, engineering design sketches and renderings, observation reports, and Rough Order of Magnitude /Bill of Material documents
- Demonstrated ability to handle multiple projects at one time with little oversight/direction and see projects through to completion
- Possess detailed knowledge of equipment from various manufacturers and able to make proper selections independently.
- Ability to perform calculations for his/her trade to support design and conduct field visits
- AutoCAD and MS Visio proficiency is required; proficient in design and calculation software; MS Excel; MS Word
- RCDD certification is beneficial

Communications Network Manager Level III Minimum

The Network Management Center (NMC) Lead will be responsible for ensuring the health and operation of the networks across the DHS enterprise. The position will require an experienced telecommunications professional capable of utilizing a variety of administrative, managerial and technical skills to develop process and procedures that ensure the network is monitored and managed to meet and exceed the Organization's SLA's. This individual is responsible for evaluating current NMC tools and determining enhancements.

Functional Area:

- C.5.9 Network Management Center

Duties:

- Lead a team whose primary role is to keep the network up and running to meet and exceed published service level agreements
- Document process and procedures so that standard methods are used for isolating, troubleshooting and resolving network problems
- Create and utilize reports that tracking of performance and when hardware/software related problems are impacting our network
- Perform advanced outage troubleshooting when critical components are not operational
- Provide monthly statistics on the performance of the network; maintenance dispatches

Skills:

- Experience working and leading a Network Management Center using HP OpenView and other management systems
- Working knowledge of TCP/IP and Internet routing concepts, system administration experience with Windows 2000/2003 and XP

TE C.1.7-001 Key Personnel Positions and Descriptions

- Advanced understanding of networking equipment including Cisco
- Strong communication skills and problem solving analytics
- Comfortable working in cross-functional team environment, and possess excellent oral and written communication skills
- Network Management certification

COMSEC SME Level III Minimum

The COMSEC SME is responsible for the proper management and security of all COMSEC materials and accounts as well as the daily operations of the Communications Center.

Functional Area:

- C.5.11 Communications security (COMSEC) Management

Duties:

- Maintains proper storage and adequate physical security of COMSEC material held by the account to include the destruction of classified material when authorized while maintaining Two-Person Integrity (TPI).
- Provides authorized personnel with guidance and appropriate extracts on handling accountability and the disposition of COMSEC material.
- Oversees the implementation of and compliance with all OTAR/OTAT procedures.
- Ensures proper handling, accountability and disposition of all COMSEC material
- Communicates with other DHS functional areas via Crisis Management Network

Skills:

- Experience leading a Communications Center
- Proficient in DMS (Defense Messaging system) and AMHS (Automated Message Handling system)
- Knowledge of INFOSEC security procedures and instructions required to check user authorization; reports INFOSEC security violations
- Ability to set up COMSEC equipment with the understanding of OTAR/OTAT procedures
- Ability to set up, configure and maintain encryption devices such as TACLANES, FASTLANES, KIV-7s, Red Eagles, etc.
- Ability to troubleshoot, repair, reprogram or replace Secure Voice (STE, STU-III) equipment as required
- Comfortable working in cross-functional team environment

Systems Operations Manager Level III Minimum

This position manages the Tier 1 support technicians. This position is responsible for managing, planning, developing, and supporting computer systems within the DHS and field sites. Additionally, this position is responsible for ensuring adherence to SLA, and operational policies and procedures.

Functional Area:

TE C.1.7-001 Key Personnel Positions and Descriptions

- C.5.5 Operations and Maintenance for End User Support

Duties:

- Oversees desktop systems operations, which includes hardware and software technology deployment and retirement of desktop and other distributed hardware
- Ensures that identification, evaluation and resolution of system and software problems and malfunctions are performed in accordance with SLA and operational policies and procedures
- Manage user support requests to evaluate and prioritize incoming requests for assistance

Skills:

- Experience leading an enterprise support organization
- Excellent working knowledge of Internet, MS Office suite
- Strong working knowledge of Windows Operating System environment and related tools such as Group Policies, and desktop/laptop imaging (Symantec Ghost)
- Excellent problem solving, decision-making skills

Systems Engineer (Senior) Level III Minimum

This position manages the Tier 2 support technicians. This position is responsible for managing, planning, and support of computer systems at within the DHS HQ and field site. Additionally, this position is responsible for ensuring adherence to SLA, and operational policies and procedures.

Functional Area:

- C.5.5 Operations and Maintenance for End User Support

Duties:

- The Operational Engineering Lead will manage the implementation, administration, maintenance and operation of DHS Local and Wide Networks
- This position is responsible for planning and recommending network hardware, systems management software and architecture, ensuring compliance, as well as configuring and maintaining routers, switches, and appliances for the network systems, monitoring performance and ensuring capacity planning is performed and is proactive in assessing and making recommendations for improvement
- Manage and monitor recurring operational run and maintenance activities involving Wintel Network technologies and platforms
- Manage and monitor technical system administration staff assigned to the technologies and platforms
- Coordinate, communicate and develop processes for leveraging and using resources to meet customer needs

Skills:

- IT or computer operations experience recommended

TE C.1.7-001 Key Personnel Positions and Descriptions**Help Desk Manager Level III**

Ensure the team utilizes the appropriate tools and processes in order to provide an exceptional level of customer service. Call avoidance and Root-cause Analysis strategies will be implemented to reduce or eliminate preventive service request occurrences. Best Practices such as these will allow customers to be more productive, and efficient, and allow the client's Customer Support Organization to handle more complex issues by reducing the number of occurrences and escalations.

Functional Area:

- C.5.5 Operations and Maintenance for End User Support

Duties:

- Supervising the day-to-day activities of the Help Desk Team to ensure client's standards for customer service are maintained
- Implementing and overseeing all Best Practices for the Help Desk.
- Conducting team meetings, communicating recommendations for improvement as necessary, and providing metric reports
- Managing and monitoring service levels to ensure the Help Desk Team meets all service level agreements and continuously provides high-quality support services
- Monitoring adherence to Help Desk procedures with regards to customer service and Quality Assurance
- Assessing changes in workload and evaluating impact to service levels to make necessary adjustments
- Reviewing and analyzing service requests, and call volume reports and implementing solutions to improve service delivery
- Developing and improving upon support policies and proactive solutions

Skills:

- Experience as a Team Lead or Supervisor in an Enterprise Help Desk
- Demonstrated analytical and problem solving skills
- Outstanding customer service skills
- Extensive understanding of Help Desk metrics and Best Practices; ability to utilize metrics to identify opportunities for training and process improvement
- Extensive experience supporting customers in multiple remote locations, utilizing all appropriate methods including the use of remote support tools in a LAN/WAN environment
- ITIL Knowledge desired

Help Desk Manager Level II

This position will resolve end user desktop computer issues such as, printer troubleshooting and configuration, installing software and/or hardware peripherals, rollout of new software packages, upgrades and new desktop hardware. Troubleshoot subsequent problems; apply established techniques and, procedures.

TE C.1.7-001 Key Personnel Positions and Descriptions

Functional Area:

- C.5.5 Operations and Maintenance for End User Support

Duties:

- Ensure that Service Operations policies and procedures are followed, e.g. support request ticket documentation, documentation management, and technical standards.
- Create and maintain a climate of continuous improvement, pro-actively identifying opportunities for service improvements and internal efficiencies
- Motivating and leading the department to deliver a world-class service
- Ensuring that the end-user demand for support is appropriately delivered, building relationships with 'customers' to gain feedback as to their level of satisfaction with the support service
- Form and build relationships with other teams to ensure optimum performance across teams and therefore to enable the business to meet its control and growth agenda

Skills:

- Experience as a Team Lead or Supervisor in an Enterprise Helpdesk
- Strong teamwork and leadership
- Excellent organizational and follow-up skills with strong attention to detail
- Outstanding customer service skills
- Experience supporting customers in multiple remote locations, utilizing all appropriate methods including the use of remote support tools in a LAN/WAN environment

Communications/Network Engineer Level IV

This position is responsible for the day-to-day maintenance and facilitation of enterprise VTC services. The Lead must have a full working knowledge of video conferencing and visual information systems related devices. The Lead installs, operates and troubleshoots integrated multimedia systems.

Functional Area:

C.5.6 Video Teleconferencing

Duties:

- Assist help desk personnel with the schedule, setup, and management of VTC sessions.
- Responsible for Tier I & II troubleshooting of all VTC A/V hardware, software, room equipment, and network connectivity issues
- Respond to action items, impact requests for changes and conduct briefings and demonstrations of systems and/or technology as required
- Provide weekly tracking and reporting on all projects and VTC/bridge activity
- Provide technical oversight to the customer, identifying required spare parts; perform field service and/or technical assistance as required

TE C.1.7-001 Key Personnel Positions and Descriptions**Skills:**

- Experience as a Team Lead in VTC/Multi-media environment
- Outstanding customer service skills
- Technical background includes an understanding of all major video equipment, both ISDN and IP based VTC systems
- Experience with video bridges and video endpoints
- Possess knowledge in video bridges such as: Polycom MGC-50 and 100 and Gateways, video and audio protocols
- Configuring, utilizing, troubleshooting, and correcting problems and failures with the video bridges, gateways, and bridges
- Full understanding, ability to configure and utilize the following peripherals: Codecs, document cameras, and laptop interfaces
- Possess knowledge and configuration skills in network components such as: CSU/DSU, IMUX, Gateways, Crypto equipment, Multiplexes, Fiber Transceivers, Cisco Routers, Switches
- Must be familiar with how T1, PRI, BRI Circuits function
- Experience with MCU's and endpoints. A/V and video troubleshooting
- Possess a knowledge of COMSEC devices such as: TACLANES, Kiv-7s and Kiv-19s, DTD's
- VTC certification desired

Voice Communications Manager Level III

Lead the following functions within the realm of voice networking technologies: planning, engineering, testing, evaluation and integration services; large-scale project management. Provide senior level skills required in projects, upgrades, ACD, capacity planning and IP voice technologies. Facilitate and manage the implementation of voice and telecommunications infrastructure components

Functional Area:

- C.5.8 Phone and PBX Operations

Duties:

- Technical leadership and mentoring of Support Technicians, systems design validation, technical solution development and delivery, project management, deployment and advanced troubleshooting of Voice systems
- Installation and Maintenance of a PBX platform
- Installs, repairs and troubleshoots customer service orders
- Performs moves, adds and changes
- Provides high level of customer service when responding to a customer request or fulfilling project requirements
- Able to program and perform upgrades to PBX independently
- Able to take a lead role in large system maintenance and upgrade projects

TE C.1.7-001 Key Personnel Positions and Descriptions

- Performs configuration, scripting, testing and implementation of all telephony applications
- Performs maintenance and support for all telecommunications equipment
- Provides work direction and assists less senior team members to ensure proper configuration for telecommunications

Skills:

- Experience as a PBX engineer
- Experience with multi-site configurations, in a consulting or large system maintenance and administration role
- In depth knowledge of and experience supporting telephony applications and components, including switches, peripherals circuitry and routing
- In depth understanding of telecommunications protocols such as ISDN and VOIP
- Outstanding customer service skills
- PBX certification desired

Communications/Network Engineer Level IV

Provide technical expertise in engineering, configuration, integration, and acceptance testing of various deployed equipment items found in the CATV, Satellite Broadcasting and Telecommunications systems.

Functional Area:**C.5.3 Infrastructure Engineering Services****Duties:**

- Work jointly with internal and client engineering personnel to develop tactical and strategic engineering solutions for large scale CATV/Satellite video transport networks
- Technical leadership and mentoring of Support Technicians, systems design validation, technical solution development and delivery, deployment and advanced troubleshooting of CATV/Satellite systems
- Installation and Maintenance of a CATV/Satellite platform
- Installs, repairs and troubleshoots customer support requests
- Performs moves, adds and changes
- Provides high level of customer service when responding to a customer request or fulfilling support requirements
- Able to program and perform upgrades to CATV/Satellite systems independently
- Performs maintenance and support for all CATV/Satellite equipment
- Provides work direction and assists less senior team members to ensure proper configuration for telecommunications

TE C.1.7-001 Key Personnel Positions and Descriptions**Skills:**

- Experience as a CATV/Satellite engineer
- Experience with multi-site configurations, in a consulting or large system maintenance and administration role
- In depth knowledge of and experience supporting CATV/Satellite systems to include head end
- Outstanding customer service skills
- CATV/Satellite certification desired

Business Case Analyst Level III Minimum

Evaluate and recommend the implementation of various LAN/WAN hardware and software based on user requirements or improved technologies.

Functional Area:

- C.5.9 Network Management Center

Duties:

- Work collaboratively with various groups, components, and technical partners to identify solutions and long-term solutions using innovative technology
- Evaluate, monitor, and perform analyses of forthcoming LAN/WAN hardware, software, and technologies
- Work with architects, analysts, and developers to identify relevant technologies as they become available
- Work with vendors to identify upgrade paths
- Evaluate various equipment (e.g., PDA, workstation/laptop/printer, etc) to perform comparative analysis against existing equipment

Skills:

- Demonstrated knowledge of networking concepts and technologies
- Must possess the communication and interpersonal skills necessary to interact with the group's internal and external customers
- Working knowledge of market research methodologies (qualitative and quantitative) and skills (e.g. statistical analysis, interpretation of results, data visualization)
- Experience managing client driven research projects
- Outstanding customer service skills

TE C.1.12-001 Current Contracts Periods of Performance (POP)

Contractor	Description	Contract Term	Current Period of Performance
A	LAN – SBU (Sensitive but Unclassified) Provide IT support services and products for DHS HQ		1/1/2007 to 12/31/2007
B	LAN – HSDN support	04/12/2004 to 04/11/2011	01/01/2006 to 06/30/2006 followed by 07/01/07 to 12/31/2007
C	LAN – HSDN (partial) & LAN – C Operations & Maintenance	10/01/2005 to 09/30/2008	10/01/2006 to 09/30/2007
C	Secure and non secure telephone, VTC, multimedia, and TV Operations & Maintenance	06/16/2004 to 15/06/2009	07/09/2004 to 06/15/2007
C	Communications Center Operations & Maintenance at NAC	05/01/2006 to 04/30/2008	05/01/2007 to 04/30/2008
D	Mission Critical Infrastructure Operations (MCIO) Secure/Non-secure Video Conferencing (VTC) Operations and Data Communications."	09/06/2006 to 09/28/2007	09/06/2006 to 09/28/2007
D	Mission Critical Infrastructure Operations (MCIO) Secure Video Operations	04/01/2006 to 03/31/2008	04/01/2007 to 03/31/2008
E	Mission Critical Infrastructure Operations (MCIO) ITAC IT Support Services	09/30/2006 to 09/29/2008	09/30/2006 to 09/29/2008
F	COOP Planning, Program Directorate Compliance and Governance	03/30/2006 to 08/31/2008	01/01/2007 to 12/31/2007
G	Executive Telecommunications Travel Services	03/06/2006 to 06/05/2007	03/05/2007 to 06/05/2007
H	Wireless Communications Architecture, Systems Engineering Technical Support and Architecture Program Management to the DHS Wireless Management Office (WMO)	06/05/2006 to 06/04/2007	11/17/2006 to 06/04/2007

TE C.1.12-002 Projects

**See DHS Interactive Website for Projects List
(Information is applicable to Task Orders PMO and O&M)**

TE C.3.1-001 Government Furnished Equipment (GFE)

The Product Guide provided at this TE identifies the most frequently requested IT products for the LAN – SBU (LAN – A) environment available through DHS IT-NOVA.

Product Guide

Version 1.1

October 1, 2006

TE C.3.1-001 Government Furnished Equipment (GFE)

Contents

Introduction

Introduction 3

Hardware/Software Exceptions

Standard A-LAN Computer Images 3

Standard Seat Components 4

IT Products

Workstations 4

Printers 5

Scanners and Fax Machines 6

Photocopiers 8

Accessories and Miscellaneous Equipment 9

Network and Power Supplies 10

Wireless Devices and Services 11

Software 13

Reference Data

Directorate Approving Authorities 16

Glossary 16

TE C.3.1-001 Government Furnished Equipment (GFE)**Introduction**

This Catalog serves as a cost estimate guide for the most frequently requested IT products for the A-LAN environment available through DHS IT-NOVA. . Version 2.0 of this Catalog will include additional services, regulatory data and process information to assist in accessing the services and products that are available to you.

Standard Seat Components

The Standard Image Software Bundle included on your workstation is reflected separately from the billing for equipment. The software pricing includes one year Software Assurance (maintenance), which provides you with free upgrades to any future versions of the product throughout the year of purchase.

Software purchased for a single user that has both a desktop and a laptop may be duplicated on both machines without additional license.

21.00	Symantec Anti-Virus
8.00	WinZip
11.00	Ghost
602.04	Desktop Pro (<i>includes operating system, plus the Microsoft Office Suite: Word, Outlook, Excel, Access, PowerPoint, Publisher, Office Tools</i>)

The standard workstation consists of either a Dell OptiPlex GX620 (SFF) desktop system or a Dell Latitude D620 laptop with docking station, keyboard and mouse. The system specifications and estimated hardware costs are listed in the IT Products.

IT PRODUCTS

Commodity items include a three-year warranty. The items listed in this section are the most frequently requested commodities and are approved for use by DHS. Pricing is based on market trends at the time of inventory procurement and are subject to change.

Workstations

TE C.3.1-001 Government Furnished Equipment (GFE)**Desktop: Dell OptiPlex GX620 (SFF)**

Dell™ OptiPlex GX620 (SFF) – Full Desktop Workstation

Intel Pentium D 800MHz FSB socket T w/Dual Core technology XD, EM64T 2x1MB L2 cache and EIST; Four DIMM slots; Integrated Intel Graphics Media Accelerator 950 VGC, DVI Adapter card; 80 GB RPM; Broadcom 5751 GB Ethernet LAN; 8 7 USB 2.0, 1 Ethernet (RJ45), 1 9-pin serial, 1 parallel, VGA out, stereo line-in, mic-in (front), speakers/line-out and headphone (front); Small form factor, 17" TFT Flat Panel monitor; Keyboard, Mouse, Speakers

Estimated Hardware Cost: 1,300

Laptop: Dell Latitude D620 (with docking station, keyboard, mouse)

Dell™ Latitude D620

Pentium M 750 (1.86GHz) 14.1 XGA, Intel Extreme; 1GB, Double Data Rate 2-533 SDRAM, 2 Dimms; 60GB Hard Drive 9.5MM, 5400RPM; Windows XP Professional, SP2 with media, Dell USB 2 Button Optical Mouse with Scroll for Latitude Notebooks, USB, Enhanced Multimedia Keyboard, Internal 56K Modem; 65W AC Adapter; 24X CDRW/DVD; Dell Wireless 1370 WLAN (802.11b/g,54Mbps) mini PCI Card, US, D/Port, Port Replicator; 6-Cell/53 WHr Primary Battery, Nylon Carrying Case; D/View Notebook Stand; MicroSaver Security Cable; 6-Cell/53WHr Primary Battery; 128MB USB 2.0

Graphics Desktop Workstation: OptiPlex GX620 Mini Tower

OptiPlex GX620 Mini Tower (Graphics Workstation)

(Item not maintained in inventory; can be ordered)

Intel Pentium D Processor 960 (3.60 GHz, 2x2M, 800 MHz FSB), Windows XP Professional, SP2, without media, NTFS File System for all operating systems, 4 GB DDR2 Non-ECC SDRAM, 533 MHz (4DIMM), (2) 24" UltraSharp 2407FP Widescreen, Adjustable stand, VGA/DVI, PCIe 256MB ATI Radeon X600, Dual Monitor DVI or VGA full height, (2) 250GB SATA 3.0 GB/s and 8 MB DataBurst Cache, Dell USB Keyboard, no hot keys, Dell USB 2-button Optical mouse with scroll, black, Integrated AC97 Audio, Dell A525 30 watt 2.1 3-piece stereo speakers w/subwoofers (black), 16X DVD+/-RW and 16X DVD with Roxio Creator, Dell edition, no media, PS2 serial port adapter, full height, RoHS Compliant Lead-free chassis and motherboard, Diagnostics/Drivers CD enabled, Federal KYHD service; Gold Technical Support, OptiPlex, 3-year ltd warranty & NBD on-site service

The following items represent some of the preferred products that have been priced based on previous market research and are maintained or may be procured based on these estimates. If pricing for bulk inventory or build-out, market research may be requested in order to receive additional discounts or favorable pricing.

Representative Photo

Product Description & Specifications

TE C.3.1-001 Government Furnished Equipment (GFE)

STANDARD MONITOR: Dell™ UltraSharp 1707 Flat Panel Monitor

Manufacturer Part# : CC280
Dell Part# : 320-4567

Black Flat Panel monitor LCD with Height Adjustable Stand, 1280x1024 resolution, Digital DVI-D and analog inputs, Four USB 2.0 high speed ports for connecting peripheral devices



Dell™ UltraSharp 20.1" Flat Panel Monitor

Manufacturer Part @2007FP

1600 x 1200 resolution, DVI Connector, S-Video; 4 USB 2.0 high speed ports; height adjustability (130mm up/down), swivel (45° left/right), tilt (4° forward/21° backwards)



Dell™ UltraSharp 24.1" Flat Panel Monitor

Manufacturer Part #2407WFP (Item not maintained in inventory; can be ordered)

1600 x 1200 resolution, DVI Connector, S-Video; 4 USB 2.0 high speed ports; height adjustability (130mm up/down), swivel (45° left/right), tilt (4° forward/21° backwards)

Printers

Representative Photo**Product Description & Specifications**

HP DeskJet 460cb color printer (MOBILE ONLY)

Up to 17 ppm black& white; 16 ppm color. Monthly volume up to 500 pages. Manual duplex printing; Input capacity – 50 sheets. Media sizes supported: Legal, letter, executive, statement, index (5 x 8-in, 4 x 6-in, 3 x 5-in), photo (5 x 7-in, 4 x 6-in), envelope (# 10, Monarch)



HP Color LJ 2600n desktop color printer

Manufacturer Part #Q6455A

Dimensions: 16.02 x 17.83 x 14.6 in; Weight 40.5 lbs

Up to 8 ppm, monthly volume up to 35,000 pages. Manual duplex printing, 1 standard paper tray; accepted media: letter, legal, executive and envelope. 16 MB memory

TE C.3.1-001 Government Furnished Equipment (GFE)**Representative Photo****Product Description & Specifications**

HP Color LJ 4700n network color printer

Manufacturer Part #Q7492A

Dimensions: 20.5 x 37.4 x 22.9 in (w/paper tray extended); Weight 105.1 lbs

100-sheet multipurpose tray and 500-sheet input tray 2 for a 600-sheet capacity • 500-sheet output bin • 128 MB RAM • One empty DIMM slot and two empty flash memory slots • HP Jetdirect Fast Ethernet embedded print server • Two open EIO slots

HP Color LJ 5550dn duplexing color printer

Manufacturer Part #Q3715A (Item not maintained in inventory; can be ordered)

Dimensions: 22.7 x 27.7 x 25.2 in; Weight 114 lbs

100-sheet multipurpose tray, 500-sheet input tray, 160 MB of printer memory, 533 MHz RISC processor, two open EIO slots and HP Jetdirect 620n Fast Ethernet print server in one EIO slot; automatic two-sided printing

Scanners & Fax Machines**Representative Photo****Product Description & Specifications**

Visioneer Strobe XP 100 Sheet-fed Scanner

Manufacturer Part #SXP1001-DB

Color portable sheet-fed scanner; 600 x 600 dpi; max scan size 8.5" x 14"; Weight 10.6 oz. Scan speed: 10 seconds per page

HP ScanJet 5590 Digital Flatbed Scanner

Manufacturer Part #L1910A#201

Dimensions - 19.21 x 13.39 x 6.38 inch

Scan resolution, hardware - 2400 x 2400 dpi, Hi-Speed USB 2.0 port, Operating systems - Microsoft® Windows® 98, 98 SE, Me, 2000, XP Professional and Home Edition, Mac OS

9.1 or higher, or Mac OS X 10.1.5 or 10.2 or higher, ADF capacity & speed - Standard, 50 sheets, 8 ppm, 4 ipm, Scan speed, preview - Up to 7 seconds, Scan task speed (4 x 6-in) - 4 x 6-in color photo to Word: less than 24 sec 4 x 6-in color photo to e-mail: less than 18 sec

Scan task speed (OCR) - OCR letter-size black and white text to MS Word: less than 36 sec

three slides or four 35 mm negative frames. Scan resolution, enhanced - 2400



TE C.3.1-001 Government Furnished Equipment (GFE)

HP ScanJet 7650 Flatbed Scanner

Manufacturer Part #L1940A#201

Dimensions - 19.21 x 13.39 x 6.38 inch



Scan resolution, enhanced - 12 dpi to 999,999 enhanced dpi, 2400 x 2400 dpi, OCR letter-size black and white text to MS Word: less than 47 sec, Transparent materials adapter - Satellite; three slides or four 35 mm negative frames, Connectivity, standard - Hi-Speed USB 2.0 port, Scan speed, preview - 6 sec., Scan size, max - 8.5 x 14 in. through the ADF, Operating systems - Microsoft® Windows® 98, 98 SE, Me, 2000, XP; MacOS X v 10.2 and later ADF capacity & speed - Standard, 50 sheets, 12 ppm, 6 ipm (duplex); 3-year warranty

Brother Intellifax Unclassified Facsimile Machine

Manufacturer Part #FAX 2820



Laser printer, copier and fax with 8 MB memory which can store up to 500 pages for out-of-paper reception. Transmission Speed: 3.5 sec/page (up to 14 ppm); Paper Capacity: 250 pgs; Document Feeder: 20 sheets; 20 location one-touch dialing; 200 speed dial locations; reduction/ enlargement; copy speed of 14 cpm.

Ilex 795SF Secure Fax (Item not maintained in inventory; can be ordered)



MIL-STD-181-161D & STANAG 5000 compliant, Laser printing, plain paper facsimile, Interface circuits are IAW MIL-STD-188-114. High resolution, 16, 32 and 64 kbps operation in handshake and broadcast compressed modes with and without FEC. Multi-page operation. EOT Signal

Business Card Scanner



May be ordered in Executive (single-use) model or CRM (multi-user) models. Compatible with MS Outlook/Exchange, Palm handhelds, smart phones. USB powered, 5 3/4 x 3 1/4" x 1 1/2"; weight 8 oz.

TE C.3.1-001 Government Furnished Equipment (GFE)**Photocopiers****Description**

Work Centre 245H with Offset Catch Tray and Hi-Capacity Feeder. Includes: two 550-sheet user-adjustable front loading paper trays, 100-sheet Bypass Tray, Office Finisher (50-sheet multi-position and stapling, 2,000 + 250-sheet trays), Scan/Email capabilities; 3,600-Sheet High Capacity Paper Tray (1,600- and 2,000-sheet drawers); total paper capacity of 4,800 sheets and 300 sheet Offset Catch Tray

Flat Rate Maintenance for 10,000-25,000 b&w copies (Band B)

Work Centre 265H with Offset Catch Tray and Hi-Capacity Feeder. Includes two 550-sheet user-adjustable front loading paper trays, 100-sheet Bypass Tray, Office Finisher (50-sheet multi-position and stapling, 2,000 + 250-sheet trays), Scan/Email capabilities; 3,600-Sheet High Capacity Paper Tray (1,600- and 2,000-sheet drawers); total paper capacity of 4,800 sheets and 300 sheet Offset Catch Tray

Flat Rate Maintenance for 10,000-25,000 b&w copies (Band B)

Work Centre Pro 2128 Color Copier/Copier. Includes two 520-sheet Paper Trays, Office Finisher (1,000 sheet stacker and 50-sheet multi-position stapling), High Capacity Feeder (two Trays with total 2,000-sheet capacity); total paper capacity of 3,140 sheets and Print/Copy/Scan Controller

Flat Rate Maintenance for 10,000-25,000 b&w copies (Band B)

TE C.3.1-001 Government Furnished Equipment (GFE)**Accessories & Miscellaneous Equipment****Representative Photo****Product Description & Specifications**

Polycom Soundstation2 Conference Phone with display

Manufacturer Part # 2200-16200-001

For small/medium-size rooms with three microphones and digitally tuned speaker. Optional accessories include: wireless mic, two external microphones (part # 2200-00696-001)



InFocus 4805 Multi-media projector

Manufacturer Part #653428

Width 9.8"xDepth 12.5"xHeight 4.2"xWeight 6.8 lb., Projection Method - Front, Rear, Ceiling; On Screen Menu, Keystone Correction, Screen Distance 5'- 20'. Image Aspect Ratio 16:9 (Wide Screen), Image Size (diagonal) 32.3-256.7", 750 ANSI lumens (Optional equipment: ceiling mount, carrying case, screen, cables)



USB Flash Drives - 1 gb/2gb

Supports USB Specification 1.1/2.0, USB 2.0 data transfer rate up to 480Mbps at "High Speed" (USB 2.0 is 40X faster than USB 1.1)

Speed: Read 8M bit/sec, Write 6.4M bit/sec (Max), Size: 0.63" x 1.02" x 3.42";



Multi-card USB Card reader

Manufacturer Part #655629

Transfers files from multi-media devices to computer. Compatible with: CompactFlash, SmartMedia, Memory Stick, Memory Stick Duo, Memory Stick PRO Duo, Memory Stick Pro, MMC, SD and xD-Picture Card.



Secure Shredder (medium volume) - DestroyIt 2401

Cross cut 3/32 x 5/8 shred size; Security level 3, Shreds staples, paperclips, credit cards. Strip cut 3/15 shred size; Security level 2, Shreds CDs, staples, paperclips, credit cards. Bin capacity 8 gallons, dimensions 10¾ l x 14½ w x 24¾ h. Auto start/stop; single, multifunction switch, wooden cabinet mounted on casters.



DEFCON KL Notebook Key Lock

Manufacturer Part #A0001666

Six foot steel cable locking device with a pass through loop on one end and lock on the other end; uses security slot already built into notebook computer. Two keys provided. Size: 0.95" x 0.88"; diameter-0.84"; cable diameter - 0.16"; cable length - 6'; wt - 5.5 oz

TE C.3.1-001 Government Furnished Equipment (GFE)



Dell Travel Plug Adapter

Manufacturer Part# : 33117/Dell Part# : A0436661

Pocket-sized adapter provides power outlets for laptops, cell phones, chargers and similar electronic devices.



Dell Latitude Laptop Charger

Manufacturer Part #: PA-1900-02D/ Dell Part Number 9T215

TE C.3.1-001 Government Furnished Equipment (GFE)

Network & Power Supplies

A limited inventory of cables, power supply units and Fiber NIC cards are available upon approved request for new items. Listed below is a small list of items for individual order. Network cables and supplies that are part of a build-out project will be managed separately.

Warranty and maintenance supplies are available through O&M.

Multi-mode SC/SC Fiber Patch Cables

Fiber Patch Cables (multi-mode) 6'

Ethernet Cables (8'), Category 6; booted

USB Printer Cables (8')

KVM Switchview PC 4-port KVM Switch

Power supply for OTPN-800/400 (12 v)

MITRJ Fiber NIC Card

TE C.3.1-001 Government Furnished Equipment (GFE)

Wireless Devices and Services

Wireless devices include: cell phones, BlackBerries, pagers and PDAs. The pricing and services for each wireless device are included in this section. To receive these services/devices, the RFE/S worksheet must be completed and POCs approval.

Banded Service for Cell Phones & Blackberries

Monthly usage charges are determined by taking the total monthly minutes used for all wireless devices (secure and non-secure) and computing a single total charge based upon pre-negotiated banded usage rates. Charges will be billed back to Component Organizations based upon their share of the total minutes used.

Cell Phones

There are four cell phone packages available that are detailed below:

Basic Cell Phone		
The devices and carriers available under this package are:	<u>Standard Device(s)</u>	<u>Vendor</u>
	LG3300	Verizon
	Motorola I205	Nextel
	Nokia 6010	Cingular
	Nokia 6010	T-Mobile
Mid-Level Cell Phone		
The devices and carriers available under this package are:	<u>Standard Device(s)</u>	<u>Vendor</u>
	LG 4650	Verizon
	Motorola I530	Nextel
	Samsung X497	Cingular
	Samsung X495	T-Mobile
Secure Cell Phone		
Secure Cell Phone devices are available from your component's COMSEC Manager.	<u>Standard Device</u>	<u>Vendor</u>
	QSEC-2700	COMSEC

TE C.3.1-001 Government Furnished Equipment (GFE)**Blackberry (Voice & Data)**

Product(s)
<ul style="list-style-type: none">▪ Verizon Model 7250 or 7130e▪ Nextel Model 7520▪ Cingular Model 7290, 8700, 7100 series▪ T-Mobile Model 7230

The features are comparable on the various models with slight differences between the models and carriers. The primary difference is aesthetics and some key functionality.

Accessories

- Accessory Kit (spare battery, travel charger, wall charger, case, earpiece)
- Travel Charger or Car charger
- Bluetooth

TE C.3.1-001 Government Furnished Equipment (GFE)**Software**

Software includes one year Software Assurance (maintenance), which provides free upgrades to any future versions of the product throughout the year of purchase.

DHS has Enterprise Agreements established with organizations such as Microsoft and Oracle that solidifies competitive prices for their products. The EA agreements allow immediate deployment of the products with an approved Purchase Order that can be installed by the Desk side Support Technicians and licenses trued-up at specific intervals. The Products Catalog will be updated as new Enterprise Agreements are established.

Pricing of the available software products are listed below. Please note that these prices do not include the cost of media which can be purchased separately:

Product Description	Part #
Adobe Acrobat Professional 7.0	AGC-54016725RT
Adobe Acrobat Standard 7.0	AGC-54016535RT
Adobe Illustrator	AGC-54017198RT
Adobe Photoshop CS2	AGC-54018226RT
Adobe Studio8 (includes Macromedia Flash)	38000960DG
Adobe Elements 4	AGC-54018958RT
Symantec Anti Virus Client 10.0.2000 License	SGL-10522833
Ghost Client 10.0	SGL-10485751
WinZip	NIC-N67-0616
(MEL) Press eLearning - Desktop Win 32 Listed Languages Lic/SA Pack VML	M70-00098
BizTalk Server Ent Listed Languages Lic/SA Pack MVL 1 Processor License	F52-00434
Content Mgmt Svr Ent Ed Listed Languages Lic/SA Pack MVL 1 Proc Lic	V04-00057
Data Analyzer Win32 Listed Languages Lic/SA Pack MVL	HO2-00031
Exchange Svr Ent Listed Languages Lic/SA Pack MVL	395-02611

TE C.3.1-001 Government Furnished Equipment (GFE)

Product Description	Part #
Exchange Svr Listed Languages Lic/SA Pack MVL	312-02356
FrontPage Win32 Listed Languages Lic/SA Pack MVL	392-02065
ISA Server Listed Languages Lic/SA Pack MVL 1 Processor License	E84-00372
MapPoint Win32 Listed Languages Lic/SA Pack MVL	B21-00381
MOM Application Mgmt Pack Listed Languages Lic/SA Pack MVL 1 Procsr Lic	M02-00072
MSDN Ent Win32 Listed Languages Lic/SA Pack MVL	389-00153
MSDN Unvrsl Win32 Listed Languages Lic/SA Pack MVL	534-02123
Project Pro Win32 Listed Languages Lic/SA Pack MVL w/1 ProjectSvr CAL	H30-00235
Project Server Win32 Listed Languages Lic/SA Pack MVL	H22-00478
Publisher Win32 Listed Languages Lic/SA Pack MVL	164-02595
SharePoint Portal Svr Listed Languages Lic/SA Pack MVL	H04-00321
SQL CAL Listed Languages Lic/SA Pack MVL Device CAL	359-00851
SQL Svr Enterprise Edtn Listed Languages Lic/SA Pack MVL	810-01714
SQL Svr Standard Edtn Listed Languages Lic/SA Pack MVL	228-01720
SQL Svr Standard Edtn Listed Languages Lic/SA Pack MVL 1 Proc Lic	228-01721
Sys Mgmt Svr Ent Ed Listed Languages Lic/SA Pack MVL	271-01147
Visio Pro Win32 Listed Languages Lic/SA Pack MVL	D87-01251
Windows Svr Enterprise Listed Languages Lic/SA Pack MVL	P72-00164
Windows Svr Listed Languages Lic/SA Pack MVL	P73-00202
Windows Trmnl Svcs CAL Listed Languages Lic/SA Pack MVL Device CAL	R19-00094
Digital Image Suite Win32 Listed Languages Lic/SA Pack MVL	S83-00062
OneNote Win32 Listed Languages Lic/SA Pack MVL	S26-00116
OneNote Win32 Listed Languages Lic/SA Pack MVL for Office SA	S26-00384
Press eLearning - Develop Win 32 Listed Languages Lic/SA Pack MVL	M70-00097
Press eLearning - IT Pro Win32 Listed Languages Lic/SA Pack MVL	M70-00099
Project Std Win32 Listed Languages Lic/SA Pack MVL	076-02036
Virtual PC Win32 Listed Languages Lic/SA Pack MVL	T31-00057
Visio Std Win32 Listed Languages Lic/SA Pack MVL	D86-01345
Application Center Ent Listed Languages Lic/SA Pack MVL 1 Proc Lic	D93-00215
BizTalk Server Dev Listed Languages Lic/SA Pack MVL	R04-00064
BizTalk Server Std Listed Languages Lic/SA Pack MVL 1 Proc Lic	D75-00287
BizTalk Supplier Accel Listed Languages Lic/SA Pack MVL 1 Proc Lic	G21-00034

TE C.3.1-001 Government Furnished Equipment (GFE)

Product Description	Part #
Commerce Svr Dev Listed Languages Lic/SA Pack MVL Dev/Test	532-00725
Commerce Svr Ent Listed Languages Lic/SA Pack MVL 1 Proc Lic	G20-00144
Commerce Svr Std Listed Languages Lic/SA Pack MVL 1 Proc Lic	532-00726
Content Mgmt Svr Std Ed Listed Languages Lic/SA Pack MVL 1 Proc Lic	R92-00028
Exchange Svr ExtnConn Listed Languages Lic/SA Pack MVL	394-00478
Host Integration Svr Std Listed Languages Lic/SA Pack MVL 1 Proc Lic	660-00196
Identity Intgrtn Svr Ent WinNT Listed Languages Lic/SA Pack MVL 1 Proc Lic	R15-00007
ISA Server Ent Edtn Listed Languages Lic/SA Pack MVL 1 Processor License	F89-00452
MBN Pro WinNT Listed Languages Lic/SA Pack MVL	V43-00042
MBN Std WinNT Listed Languages Lic/SA Pack MVL	V42-00039
MOM Ops Mgr Base Ent Ed Listed Languages Lic/SA Pack MVL w/SQL2000Tech	L09-00391
MOM Ops Mgr Base Ent Ed Listed Languages Lic/SA Pack MVL 1 Proc Lic	L09-00079
Off Live Comm Svr ExtConn Listed Languages Lic/SA Pack MVL	U63-00005
Off Live Comm Svr Listed Languages Lic/SA Pack MVL	U65-00044
Off Live Comm Svr-CAL Listed Languages Lic/SA Pack MVL Core CAL Promo Dev	U64-00461
Off Live Comm Svr-CAL Listed Languages Lic/SA Pack MVL Core CAL Promo User	U64-00462
Off Live Comm Svr-CAL Listed Languages Lic/SA Pack MVL Device CAL	U64-00386
Off Live Comm Svr-CAL Listed Languages Lic/SA Pack MVL User CAL	U64-00416
Project External Conn Win32 Listed Languages Lic/SA Pack MVL	T76-00046
Project Server CAL Win32 Listed Languages Lic/SA Pack MVL Device CAL	H21-00415
Project Server CAL Win32 Listed Languages Lic/SA Pack MVL User CAL	H21-00594
SPS Extnl Conn Non Empl Listed Languages Lic/SA Pack MVL	H32-00018
SQL CAL Listed Languages Lic/SA Pack MVL User CAL	359-01177
SQL Svr Ent Edtn Listed Languages Lic/SA Pack MVL 1 Proc Lic	810-01713
SQL Svr Std Edtn Listed Languages Lic/SA Pack MVL 1 Proc Lic	228-01721
Sys Mgmt Svr Ent Ed Listed Languages Lic/SA Pack MVL w/SQL2000Tech	271-01527
Technet Plus Single Svr Win32 Listed Languages Lic/SA Pack MVL	R10-00017
Technet Plus Single User Win32 Listed Languages Lic/SA Pack MVL	Q99-00017

TE C.3.1-001 Government Furnished Equipment (GFE)

Product Description	Part #
Win Rghts Mgt Svc CAL WinNT Listed Languages Lic/SA Pack MVL Device CAL	T98-00826
Win Rghts Mgt Svc CAL WinNT Listed Languages Lic/SA Pack MVL User CAL	T98-00827
Win Rghts Mgt Svc ExtnConn WinNT Listed Languages Lic/SA Pack MVL	T99-00395
Win Rghts Mgt SvcCAL WinNT Listed Langs Lic/SA Pck MVL CoreCAL Promo Dev	T98-00923
Win Rghts Mgt SvcCAL WinNT Listed Langs Lic/SA Pck MVL CoreCAL Promo User	T98-00924
Windows Svr ExtrmConn Listed Languages Lic/SA Pack MVL	R39-00387
Windows Svr Web Listed Languages Lic/SA Pack MVL	P70-00013
Windows Term Svr ExtrmConn Listed Languages Lic/SA Pack MVL	R59-00354
Windows Terminal Svr CAL Listed Languages Lic/SA Pack MVL User CAL	R19-00093

Directorate Approving Authorities _____

Authorized Federal approvers of requests for IT commodities or services are maintained by the Customer Liaison within the PMO. Contact hilary.jackson@dhs.gov for the most updated list or to have an alternate approver added for your Component. The approver authorizes procurement or assignment of IT assets to the requestor and authorizes billing of these services and products to their Draw-Down account, as appropriate.

Glossary _____

Acronyms and abbreviations used within this document are documented below.

A-LAN	Non-secure Local Area Network
CPO	
DHS ISSM	Information System Security Management
EOT	
IO	Infrastructure Operations
IT	Information Technology
PMO	Project Management Office
O&M	IT Operations & Maintenance

TE C.3.1-001 Government Furnished Equipment (GFE)

OGC	Office of the General Counsel
POC	Point of Contact
PR	Purchase Requisition
RFE/S	Request for Equipment and/or Services worksheet
ROM	Rough Order of Magnitude
WCF	Working Capital Fund

TE C.3.1-002 Government Furnished Equipment (GFE)

OEM Software

See DHS Interactive Website for Software List

TE C.3.1-003 Government Furnished Equipment (GFE)

Inventory

**See DHS Interactive Website for Inventory List
(Data is provided with detailed Location information)**

TE C.3.1-004 Government Furnished Facilities

See DHS Interactive Website for Facility Information

TE C.5.1-001 DHS Custom Applications**Future Years Homeland Security Program (FYHSP):**

This system provides a data warehouse of future year budget requests that are used to develop budgets for all of DHS

CRCL Matters Tracking System:

This system allows users to track external (non-employee) civil rights and civil liberty complaints

TSA Matters Tracking System:

This system is a customized version of the CRCL Matters. Its files and tomcat context are separate because of its customization

MD 715 Tables:

The system is a data warehouse of EEO data that is pulled from DHS Personnel tracking system which allows CRCL office to generate the MD 715 tables report for OMB.

EEO Eagle:

This system allows members of each component of DHS (Headquarter, CBP, CIS, FEMA, FLETC, ICE, TSA, USSS and USCG) to enter complaint case related data into the Equal Employment Opportunity (EEO) System.

MBIT:

The purpose of this tool is help DHS oversee, define, and measure all postal/mail operations in the organization.

DHSOnline:

DHSOnline is the corporate intranet for DHS and the single source of information within DHS for news and announcements. DHSOnline has an easy to use content management interface that allows content managers from all of the DHS Components and mission areas to update content on their DHSOnline page(s). DHSOnline is currently used as the primary Intranet platform for DHS Headquarters, ICE and the United States Customs and Immigration Service (USCIS)

DHSInteractive:

DHSInteractive is the administrative collaboration tool for DHS. DHSInteractive provides tools for sharing information across functional, geographical and departmental boundaries. All DHS employees and contractors can create work spaces on DHSInteractive that allows them to facilitate the development and exchange of information using web based collaboration. DHS employees and contractors are able to sponsor people who do not have DHS accounts for access to DHSInteractive. Workgroups can use DHSInteractive to share information with other government agencies, research facilities, etc. The DHSInteractive platform will support up to Sensitive but Unclassified (SBU) content.

TE C.5.5-001 Help Desk Ticket Volume

See DHS Interactive Website for Help Desk Ticket Volume

(Data is too extensive to include with Task Order)

PROCUREMENT SENSITIVE

TE C.5.8-001 Switchboard Call Volume

See DHS Interactive Website for Switchboard Call Volume Information

MATERIAL INSPECTION AND RECEIVING REPORT

1. CONTRACT NO.

2. ORDER NO.

3. REPORT NO.

4. MATERIAL AND/OR SERVICES INSPECTED

5. CONTRACTOR

6. MANUFACTURER

7. PLACE OF INSPECTION

8. CONTRACT LINE ITEM NO(S) (If applicable)	INSPECTION DATES				QUANTITY	
	10. RECEIVED	10. READY	11. STARTED	12. COMPLETED	13. REJECTED	14. ACCEPTED
	PREVIOUS REPORTS	THIS REPORT	TOTAL TO DATE	18. QUANTITY ON ORDER		
15. SUBMITTED				19. ACCEPTED TO DATE		
16. REJECTED						
17. ACCEPTED				20. BALANCE REMAINING		

21. REMARKS (Use Continuation Sheet for Additional Entries)

22. INSPECTED BY

23. TITLE

The materials and/or services listed herein have been inspected or certified test data has been examined, by me or under my supervision. The materials and/or services listed above as accepted conform to contract requirements. Those listed as rejected do not conform and may not be delivered, except as authorized under "Remarks."

24. SIGNATURE OR NAME

25. TITLE

26. DATE

DEPARTMENT OF HOMELAND SECURITY
MATERIAL INSPECTION AND RECEIVING REPORT (Cont'd)

3. REPORT NO.

8. CONTRACT LINE ITEM NO(S) <i>(If applicable)</i>	INSPECTION DATES				QUANTITY	
	10. RECEIVED	10. READY	11. STARTED	12. COMPLETED	13. REJECTED	14. ACCEPTED

Implementing Instructions for Compliance with HSAR clause 3052.204-71, “Contractor Employee Access”

1. GENERAL

Department of Homeland Security Acquisition Regulation (HSAR) clause 3052.204-71 requires that contractor personnel requiring unescorted access to government facilities, access to sensitive information, or access to government information technology (IT) resources are required to have a favorably adjudicated background investigation prior to commencing work on this contract.

Department of Homeland Security (DHS) policy requires a favorably adjudicated background investigation prior to commencing work on this contract for all contractor personnel who require recurring access to government facilities or access to sensitive information, or access to government IT resources.

Contractor employees will be given a suitability determination unless this requirement is waived under Departmental procedures. Requirements for suitability determination are defined in paragraph 3.0.

1.1 ADDITIONAL INFORMATION FOR CLASSIFIED CONTRACTS:

Performance of this contract requires the Contractor to gain access to classified National Security Information (includes documents and material). Classified information is Government information which requires protection in accordance with Executive Order 12958, National Security Information (NSI) as amended and supplemental directives.

The Contractor shall abide by the requirements set forth in the DD Form 254, Contract Security Classification Specification, an attachment to the contract, and the National Industrial Security Program Operating Manual (NISPOM) for protection of classified information at its cleared facility, if applicable, as directed by the Defense Security Service. If the Contractor is required to have access to classified information at a DHS or other Government Facility, it shall abide by the requirements set forth by the agency.

1.2 GENERAL REQUIREMENT:

The Contractor shall ensure these instructions are expressly incorporated into any and all subcontracts or subordinate agreements issued in support of this contract.

2. CONTRACTOR PERSONNEL

2.1 EMPLOYMENT ELIGIBILITY

To comply with the requirements HSAR Clause 3052.204-71, and Department policy, the contractor must complete the following forms for applicable personnel who will be performing work under this contract as indicated:

- Standard Form (SF) 85P, "Questionnaire for Public Trust Positions"
- FD-258 fingerprint cards
- DHS Form 11000-6, "Conditional Access to Sensitive But Unclassified Information Non-Disclosure Agreement". Required of all applicable contractor personnel.
- DHS Form 11000-9, "Disclosure and Authorization Pertaining to Consumer Reports Pursuant to the Fair Credit Reporting Act (FCRA)"

2.2 CONTINUED ELIGIBILITY

The Contracting Officer may require the contractor to prohibit individuals from working on contracts if the government deems their initial or continued employment contrary to the public interest for any reason, including, but not limited to, carelessness, insubordination, incompetence, or security concerns.

2.3 TERMINATION

The DHS Security Office shall be notified of all terminations/resignations within five (5) days of occurrence. The Contractor shall return to the Contracting Officer Technical Representative (COTR) all DHS issued identification cards and building passes that have either expired or have been collected from terminated employees. If an identification card or building pass is not available to be returned, a report shall be submitted to the COTR, referencing the pass or card number, name of individual to who it was issued and the last known location and disposition of the pass or card.

3.0 SUITABILITY DETERMINATION

DHS may, as it deems appropriate, authorize and grant a favorable entry on duty (EOD) decision based on preliminary suitability checks. The favorable EOD decision would allow the employees to commence work temporarily prior to the completion of the full investigation. The granting of a favorable EOD decision shall not be considered as assurance that a full employment suitability authorization will follow. A favorable EOD decision or a full employment suitability determination shall in no way prevent, preclude, or bar DHS from withdrawing or terminating access government facilities or information, at any time during the term of the contract. No employee of the Contractor shall be allowed unescorted access to a Government facility without a favorable EOD decision or suitability determination by the Security Office.

Contract employees waiting for an EOD decision may begin work on the contract provided they do not access sensitive Government information. Limited access to Government buildings is allowable prior to the EOD decision if the Contractor is escorted by a Government employee. This limited access is to allow Contractors to attend briefings, non-recurring meetings and begin transition work.

4.0 BACKGROUND INVESTIGATIONS

Contract employees (to include applicants, temporaries, part-time and replacement employees) under the contract, requiring access to sensitive information, shall undergo a position sensitivity analysis based on

... duties each individual will perform on the contract. The results of the position sensitivity analysis will identify the appropriate background investigation to be conducted. All background investigations will be processed through the DHS Security Office. Prospective Contractor employees shall submit the following completed forms to the DHS Security Office. The Standard Form 85P will be completed electronically, through the Office of Personnel Management's e-QIP SYSTEM. The completed forms must be given to the DHS Security Office no less than thirty (30) days before the start date of the contract or thirty (30) days prior to entry on duty of any employees, whether a replacement, addition, subcontractor employee, or vendor:

- a. Standard Form 85P, "Questionnaire for Public Trust Positions"
- b. FD Form 258, "Fingerprint Card" (**2 copies**)
- c. DHS Form 11000-6 "Conditional Access To Sensitive But Unclassified Information Non-Disclosure Agreement"
- d. DHS Form 11000-9, "Disclosure and Authorization Pertaining to Consumer Reports Pursuant to the Fair Credit Reporting Act"

Only complete packages will be accepted by the DHS Security Office. Specific instructions on submission of packages will be provided upon award of the contract.

... advised that unless an applicant requiring access to sensitive information has resided in the US for three the past five years, the Government may not be able to complete a satisfactory background investigation.

Non-U.S. citizens shall not be authorized to access or assist in the development, operation, management or maintenance of Department IT systems under the contract, unless a waiver has been granted by the Head of the Component or designee, with the concurrence of both the Department's Chief Security Officer (CSO) and the Chief Information Officer (CIO) or their designees. Within DHS Headquarters, the waiver may be granted only with the approval of both the CSO and the CIO or their designees. In order for a waiver to be granted:

- (1) The individual must be a legal permanent resident of the U. S. or a citizen of Ireland, Israel, the Republic of the Philippines, or any nation on the Allied Nations List maintained by the Department of State;
- (2) There must be a compelling reason for using this individual as opposed to a U. S. citizen; and
- (3) The waiver must be in the best interest of the Government.

4.1 ALTERNATIVE CITIZENSHIP REQUIREMENTS FOR NON-IT CONTRACTS

For non-Classified or non-IT contracts the above citizenship provision shall be replaced with the citizenship provision below:

Each individual employed under the contract shall be a citizen of the United States of America, or an alien who has been lawfully admitted for permanent residence as evidenced by a Permanent Resident Card (USCIS I-551). Any exceptions must be approved by the Department's Chief Security Officer or designee.

5.0 INFORMATION TECHNOLOGY SECURITY CLEARANCE

When sensitive government information is processed on Department telecommunications and automated information systems, the Contractor shall provide for the administrative control of sensitive data being processed. Contractor personnel must have favorably adjudicated background investigations commensurate with the defined sensitivity level.

Contractors who fail to comply with Department security policy are subject to having their access to Department IT systems and facilities terminated, whether or not the failure results in criminal prosecution. Any person who improperly discloses sensitive information is subject to criminal and civil penalties and sanctions under a variety of laws (e.g., Privacy Act).

Contractor access will be terminated for unauthorized use. The contractor agrees to hold and save DHS harmless from any unauthorized use and agrees not to request additional time or money under the contract for any delays resulting from unauthorized use or access.

INFORMATION TECHNOLOGY SECURITY TRAINING AND OVERSIGHT

Before receiving access to IT resources under this contract the individual must receive a security briefing, which the Contracting Officer's Technical Representative (COTR) will arrange, and complete any nondisclosure agreement furnished by DHS.

7.0 REFERENCES

7.1 DHS Office of Security

DHS, Office of Security
Personnel Security Staff
Attn: Ora Smith
Washington DC 20528
Telephone: (202) 447-5372

NON-DISCLOSURE AGREEMENT

I, _____, an individual official, employee, consultant, or subcontractor of or to _____ (the Authorized Entity), intending to be legally bound, hereby consent to the terms in this Agreement in consideration of my being granted conditional access to certain information, specified below, that is owned by, produced by, or in the possession of the United States Government.

(Signer will acknowledge the category or categories of information that he or she may have access to, and the signer's willingness to comply with the standards for protection by placing his or her initials in front of the applicable category or categories.)

Initials:	Protected Critical Infrastructure Information (PCII)
-----------	---

I attest that I am familiar with, and I will comply with all requirements of the PCII program set out in the Critical Infrastructure Information Act of 2002 (CII Act) (Title II, Subtitle B, of the Homeland Security Act of 2002, Public Law 107-296, 196 Stat. 2135, 6 USC 101 et seq.), as amended, the implementing regulations thereto (6 CFR Part 29), as amended, and the applicable PCII Procedures Manual, as amended, and with any such requirements that may be officially communicated to me by the PCII Program Manager or the PCII Program Manager's designee.

Initials:	Sensitive Security Information (SSI)
-----------	---

I attest that I am familiar with, and I will comply with the standards for access, dissemination, handling, and safeguarding of SSI information as cited in this Agreement and in accordance with 49 CFR Part 1520, "Protection of Sensitive Security Information," "Policies and Procedures for Safeguarding and Control of SSI," as amended, and any supplementary guidance issued by an authorized official of the Department of Homeland Security.

Initials:	Other Sensitive but Unclassified (SBU)
-----------	---

As used in this Agreement, sensitive but unclassified information is an over-arching term that covers any information, not otherwise indicated above, which the loss of, misuse of, or unauthorized access to or modification of could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under Section 552a of Title 5, as amended, but which has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense or foreign policy. This includes information categorized by DHS or other government agencies as: For Official Use Only (FOUO); Official Use Only (OUO); Sensitive Homeland Security Information (SHSI); Limited Official Use (LOU); Law Enforcement Sensitive (LES); Safeguarding Information (SGI); Unclassified Controlled Nuclear Information (UCNI); and any other identifier used by other government agencies to categorize information as sensitive but unclassified.

I attest that I am familiar with, and I will comply with the standards for access, dissemination, handling, and safeguarding of the information to which I am granted access as cited in this Agreement and in accordance with the guidance provided to me relative to the specific category of information.

I understand and agree to the following terms and conditions of my access to the information indicated above:

1. I hereby acknowledge that I have received a security indoctrination concerning the nature and protection of information to which I have been provided conditional access, including the procedures to be followed in ascertaining whether other persons to whom I contemplate disclosing this information have been approved for access to it, and that I understand these procedures.
2. By being granted conditional access to the information indicated above, the United States Government has placed special confidence and trust in me and I am obligated to protect this information from unauthorized disclosure, in accordance with the terms of this Agreement and the laws, regulations, and directives applicable to the specific categories of information to which I am granted access.
3. I attest that I understand my responsibilities and that I am familiar with and will comply with the standards for protecting such information that I may have access to in accordance with the terms of this Agreement and the laws, regulations, and/or directives applicable to the specific categories of information to which I am granted access. I understand that the United States Government may conduct inspections, at any time or place, for the purpose of ensuring compliance with the conditions for access, dissemination, handling and safeguarding information under this Agreement.

4. I will not disclose or release any information provided to me pursuant to this Agreement without proper authority or authorization. Should situations arise that warrant the disclosure or release of such information I will do so only under approved circumstances and in accordance with the laws, regulations, or directives applicable to the specific categories of information. I will honor and comply with any and all dissemination restrictions cited or verbally relayed to me by the proper authority.

5. (a) For PCII - (1) Upon the completion of my engagement as an employee, consultant, or subcontractor under the contract, or the completion of my work on the PCII Program, whichever occurs first, I will surrender promptly to the PCII Program Manager or his designee, or to the appropriate PCII officer, PCII of any type whatsoever that is in my possession.

(2) If the Authorized Entity is a United States Government contractor performing services in support of the PCII Program, I will not request, obtain, maintain, or use PCII unless the PCII Program Manager or Program Manager's designee has first made in writing, with respect to the contractor, the certification as provided for in Section 29.8(c) of the implementing regulations to the CII Act, as amended.

(b) For SSI and SBU - I hereby agree that material which I have in my possession and containing information covered by this Agreement, will be handled and safeguarded in a manner that affords sufficient protection to prevent the unauthorized disclosure of or inadvertent access to such information, consistent with the laws, regulations, or directives applicable to the specific categories of information. I agree that I shall return all information to which I have had access or which is in my possession 1) upon demand by an authorized individual; and/or 2) upon the conclusion of my duties, association, or support to DHS; and/or 3) upon the determination that my official duties do not require further access to such information.

6. I hereby agree that I will not alter or remove markings, which indicate a category of information or require specific handling instructions, from any material I may come in contact with, in the case of SSI or SBU, unless such alteration or removal is consistent with the requirements set forth in the laws, regulations, or directives applicable to the specific category of information or, in the case of PCII, unless such alteration or removal is authorized by the PCII Program Manager or the PCII Program Manager's designee. I agree that if I use information from a sensitive document or other medium, I will carry forward any markings or other required restrictions to derivative products, and will protect them in the same manner as the original.

7. I hereby agree that I shall promptly report to the appropriate official, in accordance with the guidance issued for the applicable category of information, any loss, theft, misuse, misplacement, unauthorized disclosure, or other security violation, I have knowledge of and whether or not I am personally involved. I also understand that my anonymity will be kept to the extent possible when reporting security violations.

8. If I violate the terms and conditions of this Agreement, such violation may result in the cancellation of my conditional access to the information covered by this Agreement. This may serve as a basis for denying me conditional access to other types of information, to include classified national security information.

9. (a) With respect to SSI and SBU, I hereby assign to the United States Government all royalties, remunerations, and emoluments that have resulted, will result, or may result from any disclosure, publication, or revelation of the information not consistent with the terms of this Agreement.

(b) With respect to PCII I hereby assign to the entity owning the PCII and the United States Government, all royalties, remunerations, and emoluments that have resulted, will result, or may result from any disclosure, publication, or revelation of PCII not consistent with the terms of this Agreement.

10. This Agreement is made and intended for the benefit of the United States Government and may be enforced by the United States Government or the Authorized Entity. By granting me conditional access to information in this context, the United States Government and, with respect to PCII, the Authorized Entity, may seek any remedy available to it to enforce this Agreement including, but not limited to, application for a court order prohibiting disclosure of information in breach of this Agreement. I understand that if I violate the terms and conditions of this Agreement, I could be subjected to administrative, disciplinary, civil, or criminal action, as appropriate, under the laws, regulations, or directives applicable to the category of information involved and neither the United States Government nor the Authorized Entity have waived any statutory or common law evidentiary privileges or protections that they may assert in any administrative or court proceeding to protect any sensitive information to which I have been given conditional access under the terms of this Agreement.

11. Unless and until I am released in writing by an authorized representative of the Department of Homeland Security (if permissible for the particular category of information), I understand that all conditions and obligations imposed upon me by this Agreement apply during the time that I am granted conditional access, and at all times thereafter.

12. Each provision of this Agreement is severable. If a court should find any provision of this Agreement to be unenforceable, all other provisions shall remain in full force and effect.

13. My execution of this Agreement shall not nullify or affect in any manner any other secrecy or non-disclosure Agreement which I have executed or may execute with the United States Government or any of its departments or agencies.

14. These restrictions are consistent with and do not supersede, conflict with, or otherwise alter the employee obligations, rights, or liabilities created by Executive Order No. 12958, as amended; Section 7211 of Title 5, United States Code (governing disclosures to Congress); Section 1034 of Title 10, United States Code, as amended by the Military Whistleblower Protection Act (governing disclosure to Congress by members of the military); Section 2302(b)(8) of Title 5, United States Code, as amended by the Whistleblower Protection Act (governing disclosures of illegality, waste, fraud, abuse or public health or safety threats); the Intelligence Identities Protection Act of 1982 (50 USC 421 et seq.) (governing disclosures that could expose confidential Government agents); and the statutes which protect against disclosure that may compromise the national security, including Sections 641, 793, 794, 798, and 952 of Title 18, United States Code, and Section 4(b) of the Subversive Activities Act of 1950 (50 USC 783(b)). The definitions, requirements, obligations, rights, sanctions, and liabilities created by said Executive Order and listed statutes are incorporated into this agreement and are controlling.

15. Signing this Agreement does not bar disclosures to Congress or to an authorized official of an executive agency or the Department of Justice that are essential to reporting a substantial violation of law.

16. I represent and warrant that I have the authority to enter into this Agreement.

17. I have read this Agreement carefully and my questions, if any, have been answered. I acknowledge that the briefing officer has made available to me any laws, regulations, or directives referenced in this document so that I may read them at this time, if I so choose.

DEPARTMENT OF HOMELAND SECURITY
NON-DISCLOSURE AGREEMENT
Acknowledgement

Typed/Printed Name:	Government/Department/Agency/Business Address	Telephone Number:

I make this Agreement in good faith, without mental reservation or purpose of evasion.

Signature:

WITNESS:

Typed/Printed Name:	Government/Department/Agency/Business Address	Telephone Number:

Signature:

This form is not subject to the requirements of P.L. 104-13, "Paperwork Reduction Act of 1995" 44 USC, Chapter 35.

<u>Instructions</u>	
<p>Each offeror should pay special attention to completing the attached price sheets to facilitate DHS' evaluation of their price proposal. Sections L and M of the RFP provide additional instructions on the Price Proposal requirements and evaluation criteria. It is the responsibility of the offeror to provide complete, accurate, and comprehensive information and supporting detail for the basis of estimate for your price quote. This information must be realistic and reasonable. All assumptions must be clearly identified and support the basis of estimate. It is the Government's intent to evaluate this information, and where necessary, make a most probable cost determination based on the reasonableness and realism of each offeror's prices in order to reach recommendations and a decision on the best value to the Government.</p>	
<u>General Information</u>	<p>The price proposal must provide prices for each of the Performance Work Statement (PWS) sections in Section C of the Request for Proposals (RFP) for the task order period of performance. The task order period of performance includes a transition period and a base period plus four option periods. For each period the offeror must provide Government site hourly labor rates for the labor categories being proposed for the specific PWS requirement. The general format and concept for rolling up prices in this spreadsheet should be followed.</p> <p>It is anticipated that PWS Requirement C.5.5 Will be conducted at the Contractor's facilities. Each offeror is required to provide prices using the Contractor Site (CS) worksheets for this PWS requirement for the performance periods.</p> <p>The price proposal must reflect the labor categories proposed for each PWS requirement. Each proposed labor category must be mapped to the EAGLE labor categories and hourly labor rates in your EAGLE contract.</p>
SPECIFIC INSTRUCTIONS	
<u>Labor Category Worksheets</u>	<p>The labor category spreadsheets must indicate the proposed labor categories for all PWS requirements. These spreadsheets should show the full time equivalencies (FTE) and price summaries for all periods. Government Site (GS) hourly labor rates are to be proposed for all PWS requirements except C.5.5. Contractor Site (CS) hourly labor rates are to be proposed for PWS C.5.5 only.</p>
<u>Government Site (GS) Labor Rates</u>	<p>The GS Labor Category worksheets must provide the proposed hourly labor rates for PWS work to be performed at DHS facilities. The GS tabs identified by Transition, Base, Option 1,2,3,4 must include the proposed FTEs and discounted hourly labor rates. The Extended Price column is derived by multiplying the proposed FTE times the discounted hourly rate.</p>
<u>Contractor Site (CS) Labor Rates</u>	<p>The CS Labor Category worksheets must provide the proposed hourly labor rates for PWS work to be performed at contractor facilities. The CS tabs identified by Transition, Base, Option 1,2,3,4 must include the proposed FTEs and discounted hourly labor rates. The Extended Price column is derived by multiplying the proposed FTE times the discounted hourly rate.</p>
<u>Overtime Government Site (GS) Labor Rates</u>	<p>The Labor Category worksheets must provide the proposed hourly labor overtime rates for PWS work to be performed at DHS facilities. It is anticipated that overtime rates will be consistent with exempt employee standards of straight time versus time and a half. Overtime hourly rates that exceed the "straight time" standard for exempt employees must be included on each Labor Category Worksheet, as applicable.</p>
<u>Optional Other Direct Costs</u>	<p>The estimated amount to be allocated for Optional Other Direct Costs is \$74,000,000 for each period (except Transition). Optional Other Direct Costs include travel, materials and subcontracts (other than labor). The percentage markup for ODCs must be indicated, along with anticipated increases for each period.</p> <p>Each ODC Contract Line Item Number (CLIN) and dollar amount is optional and will be funded quarterly (amount not to exceed \$18.5 million) subject to the availability of funds (FAR 52.232-18-Availability of Funds).</p>
<u>Price Schedule (Rollup Worksheet)</u>	<p>This spreadsheet summarizes the proposed prices by year for each PWS requirement. It must be an automatic roll-up of the information from each of the Labor Category PWS spreadsheets.</p>

**OPERATIONS AND MAINTENANCE
EAGLE FC2 LABOR CATEGORY TABLE
Transition Period
(Government Site Rates)**

EAGLE FC2 Labor Categories	Offeror's Labor Categories	EAGLE Gov. Site Hourly Labor Rate	Transition Period (6 months from date of award)			
			Proposed FTE *	Discounted Gov. Site Hourly Rate	Extended Price **	Overtime Gov. Site Hourly Rate
Administrative Specialist						
Sr. Administrative Specialist						
Computer Systems Analyst						
Associate Configuration Management Specialist						
Intermediate Configuration Management Specialist						
Lead Configuration Management Specialist						
Database Analyst/Programmer						
Information Resource Management Analyst						
Information Technology						
Junior IT Security Specialist						
Senior IT Security Specialist						
Project Control Specialist						
Project Manager						
Quality Assurance Analyst						
Quality Assurance Manager						
Quality Assurance Specialist						
Subject Matter Expert						
Technical Writer/Editor						
Training Specialist						
Web Content Administrator						
Disaster Recovery Specialist						

* 1 FTE equals 1920 hours

** Extended Price equals Proposed FTE times Discounted Hourly Rate

**OPERATIONS AND MAINTENANCE
EAGLE FC2 LABOR CATEGORY TABLE
Transition Period
(Government Site Rates)**

EAGLE FC2 Labor Categories	Offeror's Labor Categories	EAGLE Gov. Site Hourly Labor Rate	Transition Period (6 months from date of award)			
			Proposed FTE *	Discounted Gov. Site Hourly Rate	Extended Price **	Overtime Gov. Site Hourly Rate
Systems Engineer						
Junior Information Technology Training Specialist						
Systems Administrator						
Voice Communications Database Management Management Specialist						
System Developer						
Business Case Analyst						
Communications Network Communications Specialist						
Communications/Network						
Deployment Manager						
Deployment Technician						
Senior Deployment Technician						
Hardware Specialist						
Hardware Technician						
Senior Hardware Technician						
LAN/Deskside Support						
Help Desk Manager						
Help Desk Specialist						
System Operations Manager						
System Operator						
Junior Systems Administrator						
PWS Section	TOTAL					

* 1 FTE equals 1920 hours

** Extended Price equals Proposed FTE times Discounted Hourly Rate

Source Selection Information - see FAR 3.104

**OPERATIONS AND MAINTENANCE
EAGLE FC2 LABOR CATEGORY TABLE
Transition Period
(Contractor Site Rates)**

EAGLE FC2 Labor Categories	Offeror's Labor Categories	EAGLE Contractor Site Hourly Labor Rate	Transition Period (6 months from date of award)			
			Proposed FTE *	Discounted Contractor Site Hourly Rate	Extended Price **	Overtime Contractor Site Hourly Rate
Administrative Specialist						
Sr. Administrative Specialist						
Computer Systems Analyst						
Associate Configuration Management Specialist						
Intermediate Configuration Management Specialist						
Lead Configuration Management Specialist						
Database Analyst/Programmer						
Information Resource Management Analyst						
Information Technology						
Junior IT Security Specialist						
Senior IT Security Specialist						
Project Control Specialist						
Project Manager						
Quality Assurance Analyst						
Quality Assurance Manager						
Quality Assurance Specialist						
Subject Matter Expert						
Technical Writer/Editor						
Training Specialist						
Web Content Administrator						
Disaster Recovery Specialist						
Systems Engineer						

* 1 FTE equals 1920 hours

** Extended Price equals Proposed FTE times Discounted Hourly Rate

Source Selection Information - see FAR 3.104

**OPERATIONS AND MAINTENANCE
EAGLE FC2 LABOR CATEGORY TABLE
Transition Period
(Contractor Site Rates)**

EAGLE FC2 Labor Categories	Offeror's Labor Categories	EAGLE Contractor Site Hourly Labor Rate	Transition Period (6 months from date of award)			
			Proposed FTE *	Discounted Contractor Site Hourly Rate	Extended Price **	Overtime Contractor Site Hourly Rate
Junior Information Technology Training Specialist						
Systems Administrator						
Voice Communications Database Management Management Specialist						
System Developer						
Business Case Analyst						
Communications Network Communications Specialist						
Communications/Network Deployment Manager						
Deployment Technician Senior Deployment Technician						
Hardware Specialist Hardware Technician						
Senior Hardware Technician LAN/Deskside Support						
Help Desk Manager Help Desk Specialist						
System Operations Manager System Operator						
Junior Systems Administrator						
PWS Section	TOTAL					

* 1 FTE equals 1920 hours

** Extended Price equals Proposed FTE times Discounted Hourly Rate

Source Selection Information - see FAR 3.104

**OPERATIONS AND MAINTENANCE
EAGLE FC2 LABOR CATEGORY TABLE
Base Period
(Government Site Rates)**

EAGLE FC2 Labor Categories	Offeror's Labor Categories	EAGLE Gov. Site Hourly Labor Rate	Base Period (12 months from date of award)			
			Proposed FTE *	Discounted Gov. Site Hourly Rate	Extended Price **	Overtime Gov. Site Hourly Rate
Administrative Specialist						
Sr. Administrative Specialist						
Computer Systems Analyst						
Associate Configuration Management Specialist						
Intermediate Configuration Management Specialist						
Lead Configuration Management Specialist						
Database Analyst/Programmer						
Information Resource Management Analyst						
Information Technology						
Junior IT Security Specialist						
Senior IT Security Specialist						
Project Control Specialist						
Project Manager						
Quality Assurance Analyst						
Quality Assurance Manager						
Quality Assurance Specialist						
Subject Matter Expert						
Technical Writer/Editor						
Training Specialist						
Web Content Administrator						
Disaster Recovery Specialist						
Systems Engineer						

* 1 FTE equals 1920 hours

** Extended Price equals Proposed FTE times Discounted Hourly Rate

**OPERATIONS AND MAINTENANCE
EAGLE FC2 LABOR CATEGORY TABLE
Base Period
(Government Site Rates)**

EAGLE FC2 Labor Categories	Offeror's Labor Categories	EAGLE Gov. Site Hourly Labor Rate	Base Period (12 months from date of award)			Overtime Gov. Site Hourly Rate
			Proposed FTE *	Discounted Gov. Site Hourly Rate	Extended Price **	
Junior Information Technology Training Specialist						
Systems Administrator						
Voice Communications Database Management Management Specialist						
System Developer						
Business Case Analyst						
Communications Network Communications Specialist						
Communications/Network						
Deployment Manager						
Deployment Technician						
Senior Deployment Technician						
Hardware Specialist						
Hardware Technician						
Senior Hardware Technician						
LAN/Deskside Support						
Help Desk Manager						
Help Desk Specialist						
System Operations Manager						
System Operator						
Junior Systems Administrator						
PWS Section						
	TOTAL					

* 1 FTE equals 1920 hours

** Extended Price equals Proposed FTE times Discounted Hourly Rate

**OPERATIONS AND MAINTENANCE
EAGLE FC2 LABOR CATEGORY TABLE
Base Period
(Contractor Site Rates)**

EAGLE FC2 Labor Categories	Offeror's Labor Categories	EAGLE Contractor Site Hourly Labor Rate	Base Period (12 months from date of award)			
			Proposed FTE *	Discounted Contractor Site Hourly Rate	Extended Price **	Overtime Contractor Site Hourly Rate
Administrative Specialist						
Sr. Administrative Specialist						
Computer Systems Analyst						
Associate Configuration Management Specialist						
Intermediate Configuration Management Specialist						
Lead Configuration Management Specialist						
Database Analyst/Programmer						
Information Resource Management Analyst						
Information Technology						
Junior IT Security Specialist						
Senior IT Security Specialist						
Project Control Specialist						
Project Manager						
Quality Assurance Analyst						
Quality Assurance Manager						
Quality Assurance Specialist						
Subject Matter Expert						
Technical Writer/Editor						
Training Specialist						
Web Content Administrator						
Disaster Recovery Specialist						
Systems Engineer						

* 1 FTE equals 1920 hours

** Extended Price equals Proposed FTE times Discounted Hourly Rate

Source Selection Information - see FAR 3.104

**OPERATIONS AND MAINTENANCE
EAGLE FC2 LABOR CATEGORY TABLE
Base Period
(Contractor Site Rates)**

EAGLE FC2 Labor Categories	Offeror's Labor Categories	EAGLE Contractor Site Hourly Labor Rate	Base Period (12 months from date of award)			
			Proposed FTE *	Discounted Contractor Site Hourly Rate	Extended Price **	Overtime Contractor Site Hourly Rate
Junior Information Technology Training Specialist						
Systems Administrator						
Voice Communications						
Database Management						
Management Specialist						
System Developer						
Business Case Analyst						
Communications Network						
Communications Specialist						
Communications/Network						
Deployment Manager						
Deployment Technician						
Senior Deployment Technician						
Hardware Specialist						
Hardware Technician						
Senior Hardware Technician						
LAN/Deskside Support						
Help Desk Manager						
Help Desk Specialist						
System Operations Manager						
System Operator						
Junior Systems Administrator						
PWS Section	TOTAL					

* 1 FTE equals 1920 hours

** Extended Price equals Proposed FTE times Discounted Hourly Rate

Source Selection Information - see FAR 3.104

**OPERATIONS AND MAINTENANCE
EAGLE FC2 LABOR CATEGORY TABLE
Option 1 Period
(Government Site Rates)**

EAGLE FC2 Labor Categories	Offeror's Labor Categories	EAGLE Gov. Site Hourly Labor Rate	Option Period One (12 months)			
			Proposed FTE *	Discounted Gov. Site Hourly Rate	Extended Price **	Overtime Gov. Site Hourly Rate
Administrative Specialist						
Sr. Administrative Specialist						
Computer Systems Analyst						
Associate Configuration Management Specialist						
Intermediate Configuration Management Specialist						
Lead Configuration Management Specialist						
Database Analyst/Programmer						
Information Resource Management Analyst						
Information Technology						
Junior IT Security Specialist						
Senior IT Security Specialist						
Project Control Specialist						
Project Manager						
Quality Assurance Analyst						
Quality Assurance Manager						
Quality Assurance Specialist						
Subject Matter Expert						
Technical Writer/Editor						
Training Specialist						
Web Content Administrator						
Disaster Recovery Specialist						
Systems Engineer						
Junior Information Technology						
Training Specialist						

* 1 FTE equals 1920 hours

** Extended Price equals Proposed FTE times Discounted Hourly Rate

Source Selection Information - see FAR 3.104

**OPERATIONS AND MAINTENANCE
EAGLE FC2 LABOR CATEGORY TABLE
Option 1 Period
(Government Site Rates)**

EAGLE FC2 Labor Categories	Offeror's Labor Categories	EAGLE Gov. Site Hourly Labor Rate	Option Period One (12 months)			
			Proposed FTE *	Discounted Gov. Site Hourly Rate	Extended Price **	Overtime Gov. Site Hourly Rate
Systems Administrator						
Voice Communications						
Database Management						
Management Specialist						
System Developer						
Business Case Analyst						
Communications Network						
Communications Specialist						
Communications/Network						
Deployment Manager						
Deployment Technician						
Senior Deployment Technician						
Hardware Specialist						
Hardware Technician						
Senior Hardware Technician						
LAN/Deskside Support						
Help Desk Manager						
Help Desk Specialist						
System Operations Manager						
System Operator						
Junior Systems Administrator						
PWS Section	TOTAL					

* 1 FTE equals 1920 hours

** Extended Price equals Proposed FTE times Discounted Hourly Rate

Source Selection Information - see FAR 3.104

**OPERATIONS AND MAINTENANCE
EAGLE FC2 LABOR CATEGORY TABLE
Option 1 Period
(Contractor Site Rates)**

EAGLE FC2 Labor Categories	Offeror's Labor Categories	EAGLE Contractor Site Hourly Labor Rate	Option Period One (12 months)		
			Proposed FTE *	Discounted Contractor Site Hourly Rate	Overtime Contractor Site Hourly Rate
			Extended Price **		
Administrative Specialist					
Sr. Administrative Specialist					
Computer Systems Analyst					
Associate Configuration Management Specialist					
Intermediate Configuration Management Specialist					
Lead Configuration Management Specialist					
Database Analyst/Programmer					
Information Resource Management Analyst					
Information Technology Junior IT Security Specialist					
Senior IT Security Specialist					
Project Control Specialist					
Project Manager					
Quality Assurance Analyst					
Quality Assurance Manager					
Quality Assurance Specialist					
Subject Matter Expert					
Technical Writer/Editor					
Training Specialist					
Web Content Administrator					
Disaster Recovery Specialist					
Systems Engineer					

* 1 FTE equals 1920 hours

** Extended Price equals Proposed FTE times Discounted Hourly Rate

Offeror. _____

IT-N

PWS Section: _____

**OPERATIONS AND MAINTENANCE
EAGLE FC2 LABOR CATEGORY TABLE
Option 1 Period
(Contractor Site Rates)**

EAGLE FC2 Labor Categories	Offeror's Labor Categories	EAGLE Contractor Site Hourly Labor Rate	Option Period One (12 months)			
			Proposed FTE *	Discounted Contractor Site Hourly Rate	Extended Price **	Overtime Contractor Site Hourly Rate
Junior Information Technology						
Training Specialist						
Systems Administrator						
Voice Communications						
Database Management						
Management Specialist						
System Developer						
Business Case Analyst						
Communications Network						
Communications Specialist						
Communications/Network						
Deployment Manager						
Deployment Technician						
Senior Deployment Technician						
Hardware Specialist						
Hardware Technician						
Senior Hardware Technician						
LAN/Deskside Support						
Help Desk Manager						
Help Desk Specialist						
System Operations Manager						
System Operator						
Junior Systems Administrator						
PWS Section	TOTAL					

* 1 FTE equals 1920 hours

** Extended Price equals Proposed FTE times Discounted Hourly Rate

**OPERATIONS AND MAINTENANCE
EAGLE FC2 LABOR CATEGORY TABLE
Option 2 Period
(Government Site Rates)**

EAGLE FC2 Labor Categories	Offeror's Labor Categories	EAGLE Gov. Site Hourly Labor Rate	Option Period Two (12 months)			
			Proposed FTE *	Discounted Gov. Site Hourly Rate	Extended Price **	Overtime Gov. Site Hourly Rate
Administrative Specialist						
Sr. Administrative Specialist						
Computer Systems Analyst						
Associate Configuration Management Specialist						
Intermediate Configuration Management Specialist						
Lead Configuration Management Specialist						
Database Analyst/Programmer						
Information Resource Management Analyst						
Information Technology Junior IT Security Specialist						
Senior IT Security Specialist						
Project Control Specialist						
Project Manager						
Quality Assurance Analyst						
Quality Assurance Manager						
Quality Assurance Specialist						
Subject Matter Expert						
Technical Writer/Editor						
Training Specialist						
Web Content Administrator						
Disaster Recovery Specialist						
Systems Engineer						

* 1 FTE equals 1920 hours

** Extended Price equals Proposed FTE times Discounted Hourly Rate

Offeror: _____

IT-NC . A

PWS Section: _____

**OPERATIONS AND MAINTENANCE
EAGLE FC2 LABOR CATEGORY TABLE
Option 2 Period
(Government Site Rates)**

EAGLE FC2 Labor Categories	Offeror's Labor Categories	EAGLE Gov. Site Hourly Labor Rate	Option Period Two (12 months)			
			Proposed FTE *	Discounted Gov. Site Hourly Rate	Extended Price **	Overtime Gov. Site Hourly Rate
Junior Information Technology Training Specialist						
Systems Administrator						
Voice Communications Database Management Management Specialist						
System Developer						
Business Case Analyst						
Communications Network Communications Specialist						
Communications/Network Deployment Manager						
Deployment Technician Senior Deployment Technician						
Hardware Specialist Hardware Technician						
Senior Hardware Technician LAN/Deskside Support						
Help Desk Manager Help Desk Specialist						
System Operations Manager System Operator						
Junior Systems Administrator						
PWS Section	TOTAL					

* 1 FTE equals 1920 hours

** Extended Price equals Proposed FTE times Discounted Hourly Rate

Offeror: _____

IT-NOVA

PWS Section: _____

**OPERATIONS AND MAINTENANCE
EAGLE FC2 LABOR CATEGORY TABLE
Option 2 Period
(Contractor Site Rates)**

EAGLE FC2 Labor Categories	Offeror's Labor Categories	EAGLE Contractor Site Hourly Labor Rate	Option Period Three (12 months)			
			Proposed FTE *	Discounted Contractor Site Hourly Rate	Extended Price **	Overtime Contractor Site Hourly Rate
Administrative Specialist						
Sr. Administrative Specialist						
Computer Systems Analyst						
Associate Configuration Management Specialist						
Intermediate Configuration Management Specialist						
Lead Configuration Management Specialist						
Database Analyst/Programmer						
Information Resource Management Analyst						
Information Technology						
Junior IT Security Specialist						
Senior IT Security Specialist						
Project Control Specialist						
Project Manager						
Quality Assurance Analyst						
Quality Assurance Manager						
Quality Assurance Specialist						
Subject Matter Expert						
Technical Writer/Editor						
Training Specialist						
Web Content Administrator						
Disaster Recovery Specialist						
Systems Engineer						

* 1 FTE equals 1920 hours

** Extended Price equals Proposed FTE times Discounted Hourly Rate

Offeror: _____

IT-NOVA

PWS Section: _____

**OPERATIONS AND MAINTENANCE
EAGLE FC2 LABOR CATEGORY TABLE
Option 2 Period
(Contractor Site Rates)**

EAGLE FC2 Labor Categories	Offeror's Labor Categories	EAGLE Contractor Site Hourly Labor Rate	Option Period Three (12 months)			
			Proposed FTE *	Discounted Contractor Site Hourly Rate	Extended Price **	Overtime Contractor Site Hourly Rate
Junior Information Technology Training Specialist						
Systems Administrator						
Voice Communications						
Database Management						
Management Specialist						
System Developer						
Business Case Analyst						
Communications Network						
Communications Specialist						
Communications/Network						
Deployment Manager						
Deployment Technician						
Senior Deployment Technician						
Hardware Specialist						
Hardware Technician						
Senior Hardware Technician						
LAN/Deskside Support						
Help Desk Manager						
Help Desk Specialist						
System Operations Manager						
System Operator						
Junior Systems Administrator						
PWS Section		TOTAL				

* 1 FTE equals 1920 hours

** Extended Price equals Proposed FTE times Discounted Hourly Rate

**OPERATIONS AND MAINTENANCE
EAGLE FC2 LABOR CATEGORY TABLE
Option 3 Period
(Government Site Rates)**

EAGLE FC2 Labor Categories	Offeror's Labor Categories	EAGLE Gov. Site Hourly Labor Rate	Option Period Three (12 months)			Overtime Gov. Site Hourly Rate
			Proposed FTE *	Discounted Gov. Site Hourly Rate	Extended Price **	
Administrative Specialist						
Sr. Administrative Specialist						
Computer Systems Analyst						
Associate Configuration Management Specialist						
Intermediate Configuration Management Specialist						
Lead Configuration Management Specialist						
Database Analyst/Programmer						
Information Resource Management Analyst						
Information Technology						
Junior IT Security Specialist						
Senior IT Security Specialist						
Project Control Specialist						
Project Manager						
Quality Assurance Analyst						
Quality Assurance Manager						
Quality Assurance Specialist						
Subject Matter Expert						
Technical Writer/Editor						
Training Specialist						
Web Content Administrator						
Disaster Recovery Specialist						
Systems Engineer						

* 1 FTE equals 1920 hours

** Extended Price equals Proposed FTE times Discounted Hourly Rate

**OPERATIONS AND MAINTENANCE
EAGLE FC2 LABOR CATEGORY TABLE
Option 3 Period
(Government Site Rates)**

EAGLE FC2 Labor Categories	Offeror's Labor Categories	EAGLE Gov. Site Hourly Labor Rate	Option Period Three (12 months)			
			Proposed FTE *	Discounted Gov. Site Hourly Rate	Extended Price **	Overtime Gov. Site Hourly Rate
Junior Information Technology Training Specialist						
Systems Administrator						
Voice Communications						
Database Management						
Management Specialist						
System Developer						
Business Case Analyst						
Communications Network						
Communications Specialist						
Communications/Network						
Deployment Manager						
Deployment Technician						
Senior Deployment Technician						
Hardware Specialist						
Hardware Technician						
Senior Hardware Technician						
LAN/Deskside Support						
Help Desk Manager						
Help Desk Specialist						
System Operations Manager						
System Operator						
Junior Systems Administrator						
PWS Section	TOTAL					

* 1 FTE equals 1920 hours

** Extended Price equals Proposed FTE times Discounted Hourly Rate

**OPERATIONS AND MAINTENANCE
EAGLE FC2 LABOR CATEGORY TABLE
Option 3 Period
(Contractor Site Rates)**

EAGLE FC2 Labor Categories	Offeror's Labor Categories	EAGLE Contractor Site Hourly Labor Rate	Option Period Three (12 months)			
			Proposed FTE *	Discounted Contractor Site Hourly Rate	Extended Price **	Overtime Contractor Site Hourly Rate
Administrative Specialist						
Sr. Administrative Specialist						
Computer Systems Analyst						
Associate Configuration Management Specialist						
Intermediate Configuration Management Specialist						
Lead Configuration Management Specialist						
Database Analyst/Programmer						
Information Resource Management Analyst						
Information Technology						
Junior IT Security Specialist						
Senior IT Security Specialist						
Project Control Specialist						
Project Manager						
Quality Assurance Analyst						
Quality Assurance Manager						
Quality Assurance Specialist						
Subject Matter Expert						
Technical Writer/Editor						
Training Specialist						
Web Content Administrator						
Disaster Recovery Specialist						
Systems Engineer						

* 1 FTE equals 1920 hours

** Extended Price equals Proposed FTE times Discounted Hourly Rate

Source Selection Information - see FAR 3.104

**OPERATIONS AND MAINTENANCE
EAGLE FC2 LABOR CATEGORY TABLE
Option 3 Period
(Contractor Site Rates)**

EAGLE FC2 Labor Categories	Offeror's Labor Categories	EAGLE Contractor Site Hourly Labor Rate	Option Period Three (12 months)		
			Proposed FTE *	Discounted Contractor Site Hourly Rate	Overtime Contractor Site Hourly Rate
			Extended Price **		
Junior Information Technology Training Specialist					
Systems Administrator					
Voice Communications Database Management Management Specialist					
System Developer					
Business Case Analyst					
Communications Network Communications Specialist					
Communications/Network					
Deployment Manager					
Deployment Technician					
Senior Deployment Technician					
Hardware Specialist					
Hardware Technician					
Senior Hardware Technician					
LAN/Deskside Support					
Help Desk Manager					
Help Desk Specialist					
System Operations Manager					
System Operator					
Junior Systems Administrator					
PWS Section		TOTAL			

* 1 FTE equals 1920 hours

** Extended Price equals Proposed FTE times Discounted Hourly Rate

Source Selection Information - see FAR 3.104

**OPERATIONS AND MAINTENANCE
EAGLE FC2 LABOR CATEGORY TABLE
Option 4 Period
(Government Site Rates)**

EAGLE FC2 Labor Categories	Offeror's Labor Categories	EAGLE Gov. Site Hourly Labor Rate	Option Period Four (12 months)			Overtime Gov. Site Hourly Rate
			Proposed FTE *	Discounted Gov. Site Hourly Rate	Extended Price **	
Administrative Specialist						
Sr. Administrative Specialist						
Computer Systems Analyst						
Associate Configuration Management Specialist						
Intermediate Configuration Management Specialist						
Lead Configuration Management Specialist						
Database Analyst/Programmer						
Information Resource Management Analyst						
Information Technology						
Junior IT Security Specialist						
Senior IT Security Specialist						
Project Control Specialist						
Project Manager						
Quality Assurance Analyst						
Quality Assurance Manager						
Quality Assurance Specialist						
Subject Matter Expert						
Technical Writer/Editor						
Training Specialist						
Web Content Administrator						
Disaster Recovery Specialist						
Systems Engineer						

* 1 FTE equals 1920 hours

** Extended Price equals Proposed FTE times Discounted Hourly Rate

Offer: _____

IT- A

PWS Section: _____

**OPERATIONS AND MAINTENANCE
EAGLE FC2 LABOR CATEGORY TABLE
Option 4 Period
(Government Site Rates)**

EAGLE FC2 Labor Categories	Offeror's Labor Categories	EAGLE Gov. Site Hourly Labor Rate	Option Period Four (12 months)			Overtime Gov. Site Hourly Rate
			Proposed FTE *	Discounted Gov. Site Hourly Rate	Extended Price **	
Junior Information Technology Training Specialist						
Systems Administrator						
Voice Communications Database Management						
Management Specialist						
System Developer						
Business Case Analyst						
Communications Network						
Communications Specialist						
Communications/Network						
Deployment Manager						
Deployment Technician						
Senior Deployment Technician						
Hardware Specialist						
Hardware Technician						
Senior Hardware Technician						
LAN/Deskside Support						
Help Desk Manager						
Help Desk Specialist						
System Operations Manager						
System Operator						
Junior Systems Administrator						
PWS Section	TOTAL					

* 1 FTE equals 1920 hours

** Extended Price equals Proposed FTE times Discounted Hourly Rate

**OPERATIONS AND MAINTENANCE
EAGLE FC2 LABOR CATEGORY TABLE
Option 4 Period
(Contractor Site Rates)**

EAGLE FC2 Labor Categories	Offeror's Labor Categories	EAGLE Contractor Site Hourly Labor Rate	Option Period Four (12 months)			
			Proposed FTE *	Discounted Contractor Site Hourly Rate	Extended Price **	Overtime Contractor Site Hourly Rate
Administrative Specialist						
Sr. Administrative Specialist						
Computer Systems Analyst						
Associate Configuration Management Specialist						
Intermediate Configuration Management Specialist						
Lead Configuration Management Specialist						
Database Analyst/Programmer						
Information Resource Management Analyst						
Information Technology Consultant						
Junior IT Security Specialist						
Senior IT Security Specialist						
Project Control Specialist						
Project Manager						
Quality Assurance Analyst						
Quality Assurance Manager						
Quality Assurance Specialist						
Subject Matter Expert						
Technical Writer/Editor						
Training Specialist						
Web Content Administrator						
Disaster Recovery Specialist						
Systems Engineer						

* 1 FTE equals 1920 hours

** Extended Price equals Proposed FTE times Discounted Hourly Rate

**OPERATIONS AND MAINTENANCE
EAGLE FC2 LABOR CATEGORY TABLE
Option 4 Period
(Contractor Site Rates)**

EAGLE FC2 Labor Categories	Offeror's Labor Categories	EAGLE Contractor Site Hourly Labor Rate	Option Period Four (12 months)			
			Proposed FTE *	Discounted Contractor Site Hourly Rate	Extended Price **	Overtime Contractor Site Hourly Rate
Junior Information Technology Training Specialist						
Systems Administrator						
Voice Communications Manager						
Database Management Management Specialist						
System Developer						
Business Case Analyst						
Communications Network Manager						
Communications Specialist						
Communications/Network Engineer						
Deployment Manager						
Deployment Technician						
Senior Deployment Technician						
Hardware Specialist						
Hardware Technician						
Senior Hardware Technician						
LAN/Deskside Support						
Help Desk Manager						
Help Desk Specialist						
System Operations Manager						
System Operator						
Junior Systems Administrator						
PWS Section						
	TOTAL					

* 1 FTE equals 1920 hours

** Extended Price equals Proposed FTE times Discounted Hourly Rate

SC
1
OPERATIONS AND MAINTENANCE

This table represents DHS' current estimate of FTEs performing the PWS requirements. Offerors shall propose FTEs based on their professional knowledge, experience, and consistent with their proposed technical and staffing approach to meet the requirements in the PWS. Proposed FTEs should be based on the offeror's professional knowledge, experience, and consistent with their proposed technical and staffing approach to meet the requirements in the PWS.

PWS SECTION	Base Year			Option Year One			Option Year Two			Option Year Three			Option Year Four			ALL PERIODS (Base plus options)	
	FTE		Price	FTE		Price	FTE		Price	FTE		Price	FTE		Price	TOTAL PROPOSED FTE	TOTAL PRICE
	Range	Proposed		Range	Proposed		Range	Proposed		Range	Proposed		Range	Proposed			
C.1,3,4 Management	11 to 21	\$															
C.5.1 Application Management and Support Services	1 to 4	\$															
C.5.1.1 Application Management Services																	
C.5.1.2 Up/Down Status and Availability of Major Applications on the Network																	
C.5.1.3 Application Maintenance and Operation Documentation																	
C.5.1.4 Application Database and Systems Maintenance																	
C.5.1.5 Performance Trends of Major Applications on the Network																	
C.5.1.6 Enterprise Desk Application Licensing																	
C.5.1.7 Collaborative Applications																	
C.5.2 Deployment Support	13 to 21	\$															
C.5.2.1 Provide Deployment Support																	
C.5.2.2 Provide Deployment Planning																	
C.5.2.3 Site Activation																	
C.5.2.4 Facilities Modifications																	
C.5.2.5 Installation and Checkout																	
C.5.2.6 Transition to O&M																	
C.5.2.7 Engineering and Project Management																	
C.5.3 Infrastructure Engineering Services	17 to 27	\$															
C.5.3.1 On-site Engineering Team																	
C.5.3.2 Systems Engineering Support																	
C.5.3.3 Engineering Projects																	
C.5.3.4 Engineering Process and Methodology																	
C.5.4 Testing	3 to 9	\$															
C.5.4.1 Test Support and Documentation																	
C.5.4.2 Test and Development Lab																	
C.5.5 Operations and Maintenance for End User Support ¹	219 to 259	\$		264 to 304	\$												
C.5.5.1 End User and Desk Side Support																	
C.5.5.2 DHS Approved Maintenance Downtime																	
C.5.6 Video Teleconferencing	3 to 12	\$															
C.5.6.1 Video Teleconferencing (VTC)																	
C.5.7 Satellite/Cable TV Operations	1 to 8	\$															
C.5.7.1 Operations																	
C.5.8 Phone and PBX Operations	6 to 14	\$															
C.5.8.1 Private Branch Exchange (PBX) Infrastructure																	
C.5.8.2 Telephone Switchboard Operations Center																	
C.5.9 Network Management Center	12 to 20	\$															
C.5.9.1 Network Management Center (NMC) Operations																	
C.5.10 Security Management Center	9 to 17	\$															
C.5.10.1 SMC Operations																	
C.5.10.2 Vulnerability Assessment																	
C.5.10.3 Security Information Management (SIM) & Security Management Capability																	
C.5.10.4 Security Systems Administration																	

¹ Range is based on actual FTEs, new requirements, and help desk and deskside support estimates

² Range of FTEs based on DHS projection. This is a new requirement

SC
1
OPERATIONS AND MAINTENANCE

PWS SECTION	Base Year			Option Year One			Option Year Two			Option Year Three			Option Year Four			ALL PERIODS (Base plus options)	
	FTE		Price	FTE		Price	FTE		Price	FTE		Price	FTE		Price	TOTAL PROPOSED FTE	TOTAL PRICE
	Range	Proposed		Range	Proposed		Range	Proposed		Range	Proposed		Range	Proposed			
C.5.10 Security Change Management Security Log Access, Retention and C.5.10 Review																	
C.5.10 Provide System Security Administrators C.5.10 Data Spills and Response C.5.10 Incident Response Information Condition (INFOCON) C.5.10 Management																	
C.5.11 Communications Security Management	1 to 6		\$			\$			\$			\$			\$		\$
C.5.11 COMSEC Security																	
C.5.12 Other Communications Operations	4 to 16		\$			\$			\$			\$			\$		\$
C.5.12 Emergency Notification System C.5.12 Executive Telecommunications Support																	
C.5.13 Training²	2 to 10		\$			\$			\$			\$			\$		\$
C.5.13 System User Training C.5.13 Provide Security Training																	
C.5.14 Wireless Management	29 to 43		\$			\$			\$			\$			\$		\$
C.5.14 Wireless Communication Architecture C.5.14 Development C.5.14 Systems Engineering Support C.5.14 Working Group Support C.5.14 Enterprise Architecture Governance C.5.14 Support C.5.14 Frequency Management Support C.5.14 Spectrum Planning																	
C.5.15 Continuity Management	2 to 8		\$			\$			\$			\$			\$		\$
C.5.15 Continuity Assessment C.5.15 Continuity Planning C.5.15 Continuity Reviews and Coordination C.5.15 Continuity Program Administration C.5.15 Testing and Exercise C.5.15 Electronic Records																	
SUBTOTAL - TOTAL FTEs AND LABOR PRICE (C.1.7.4, C.5.1 to C.5.15)			\$			\$			\$			\$			\$		\$
OPTIONAL OTHER DIRECT COSTS (ODCs) (not to exceed \$18,500,000 per quarter/Maximum \$370,000,000 per 12 month period)			\$74,000,000			\$74,000,000			\$74,000,000			\$74,000,000			\$74,000,000		\$370,000,000
Travel Markup Percentage		27%															
Material Markup Percentage		27%															
Subcontract Markup Percentage		27%															
GRAND TOTAL (TOTAL FTEs, LABOR PRICE AND ODCs)			\$			\$											
Cost Impact of Total Discount/Savings (for statistical purposes, not evaluated)			\$			\$											

¹ Range is based on actual FTEs, new requirements, and help desk and desk-side support estimates

² Range of FTEs based on DHS projection. This is a new requirement

<p>DEPARTMENT OF DEFENSE</p> <p>CONTRACT SECURITY CLASSIFICATION SPECIFICATION</p> <p><i>(The requirements of the DoD Industrial Security Manual apply to all security aspects of this effort.)</i></p>	<p>1. CLEARANCE AND SAFEGUARDING</p> <p>a. FACILITY CLEARANCE REQUIRED Top Secret</p> <p>b. LEVEL OF SAFEGUARDING REQUIRED Top Secret</p>
---	--

<p>2. THIS SPECIFICATION IS FOR: (X and complete as applicable)</p> <p><input checked="" type="checkbox"/> a. PRIME CONTRACT NUMBER</p> <p><input type="checkbox"/> b. SUBCONTRACT NUMBER</p> <p><input type="checkbox"/> c. SOLICITATION OR OTHER NUMBER</p> <p>Due Date (YYYYMMDD)</p> <p>NA RUIO-04-00249</p>	<p>3. THIS SPECIFICATION IS: (X and complete as applicable)</p> <p><input checked="" type="checkbox"/> a. ORIGINAL (Complete date in all cases) Date (YYYYMMDD)</p> <p><input type="checkbox"/> b. REVISED (Supersedes all previous specs) Revision No. Date (YYYYMMDD)</p> <p><input type="checkbox"/> c. FINAL (Complete item 5 in all cases) Date (YYYYMMDD)</p>
---	--

4. IS THIS A FOLLOW-ON CONTRACT? YES NO. If Yes, complete the following:
 Classified material received or generated under Contract # _____ (Preceding Contract Number) is transferred to this follow-on contract.

5. IS THIS A FINAL DD FORM 254? YES NO. If Yes, complete the following:
 In Response to the contractor's request dated _____, retention of the identified classified material is authorized for the period of _____

6. CONTRACTOR (Include Commercial and Government Entity (CAGE) Code)

a. NAME, ADDRESS, AND ZIP CODE	B. CAGE CODE	C. COGNIZANT SECURITY OFFICE (Name, Address, and Zip Code)

7. SUBCONTRACTOR

a. NAME, ADDRESS, AND ZIP CODE	B. CAGE CODE	C. COGNIZANT SECURITY OFFICE (Name, Address, and Zip Code)
NA		

8. QUAL PERFORMANCE

a. NAME, ADDRESS, AND ZIP CODE	B. CAGE CODE	C. COGNIZANT SECURITY OFFICE (Name, Address, and Zip Code)
VARIOUS GOVERNMENT, AND (DHS) FACILITIES AND AT OTHER CONTRACTOR LOCATIONS		

9. GENERAL IDENTIFICATION OF THE PROCUREMENT

Provide IT Operations & Maintenance support to all LAN environments (SBU, Secret & Top Secret), COMSEC support and COOP for the DHS Headquarters and Components directly supported by the DHS CIO.

10. THIS CONTRACT WILL REQUIRE ACCESS TO:	YES	NO	11. IN PERFORMING THIS CONTRACT, THE CONTRACTOR WILL:	YES	NO
a. COMMUNICATIONS SECURITY (COMSEC) INFORMATION	<input checked="" type="checkbox"/>	<input type="checkbox"/>	a. HAVE ACCESS TO CLASSIFIED INFORMATION ONLY AT ANOTHER CONTRACTOR'S FACILITY OR A GOVERNMENT ACTIVITY	<input type="checkbox"/>	<input checked="" type="checkbox"/>
b. RESTRICTED DATA	<input checked="" type="checkbox"/>	<input type="checkbox"/>	b. RECEIVE CLASSIFIED DOCUMENTS ONLY	<input type="checkbox"/>	<input checked="" type="checkbox"/>
c. CRITICAL NUCLEAR WEAPON DESIGN INFORMATION	<input type="checkbox"/>	<input checked="" type="checkbox"/>	c. RECEIVE AND GENERATE CLASSIFIED MATERIAL	<input checked="" type="checkbox"/>	<input type="checkbox"/>
d. FORMERLY RESTRICTED DATA	<input type="checkbox"/>	<input checked="" type="checkbox"/>	d. FABRICATE, MODIFY, OR STORE CLASSIFIED HARDWARE	<input checked="" type="checkbox"/>	<input type="checkbox"/>
e. INTELLIGENCE INFORMATION:			e. PERFORM SERVICES ONLY	<input type="checkbox"/>	<input checked="" type="checkbox"/>
(1) Sensitive Compartmented Information (SCI)	<input checked="" type="checkbox"/>	<input type="checkbox"/>	f. HAVE ACCESS TO U.S. CLASSIFIED INFORMATION OUTSIDE THE U.S., PUERTO RICO, U.S. POSSESSIONS AND TRUST TERRITORIES	<input type="checkbox"/>	<input checked="" type="checkbox"/>
(2) Non-SCI	<input checked="" type="checkbox"/>	<input type="checkbox"/>	g. BE AUTHORIZED TO USE THE SERVICES OF DEFENSE TECHNICAL INFORMATION CENTER (DTIC) OR OTHER SECONDARY DISTRIBUTION CENTER	<input type="checkbox"/>	<input checked="" type="checkbox"/>
f. SPECIAL ACCESS INFORMATION	<input type="checkbox"/>	<input checked="" type="checkbox"/>	h. REQUIRE A COMSEC ACCOUNT	<input checked="" type="checkbox"/>	<input type="checkbox"/>
g. NATO INFORMATION	<input type="checkbox"/>	<input checked="" type="checkbox"/>	i. HAVE TEMPEST REQUIREMENTS	<input type="checkbox"/>	<input checked="" type="checkbox"/>
h. FOREIGN GOVERNMENT INFORMATION	<input type="checkbox"/>	<input checked="" type="checkbox"/>	j. HAVE OPERATIONS SECURITY (OPSEC) REQUIREMENTS	<input checked="" type="checkbox"/>	<input type="checkbox"/>
i. LIMITED DISSEMINATION INFORMATION	<input type="checkbox"/>	<input checked="" type="checkbox"/>	k. BE AUTHORIZED TO USE THE DEFENSE COURIER SERVICE	<input type="checkbox"/>	<input checked="" type="checkbox"/>
j. TOP OFFICIAL USE ONLY INFORMATION	<input checked="" type="checkbox"/>	<input type="checkbox"/>	l. OTHER (Specify)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Business sensitive information	<input checked="" type="checkbox"/>	<input type="checkbox"/>			

12. PUBLIC RELEASE. Any information (classified or unclassified) pertaining to this contract shall not be released for public dissemination except as provided by the Industrial Security Manual or unless it has been approved for public release by appropriate U.S. Government authority. Proposed public releases shall be submitted for approval prior to release

Direct Through (Specify) **TOP SECRET - SCI WILL NOT BE RELEASED TO PUBLIC**

Contractors for Freedom of Information and Security Review, Office of the Assistant Secretary of Defense (Public Affairs)* for review. Requests for disclosure shall be submitted to that agency.

13. SECURITY GUIDANCE. The security classification guidance needed for this classified effort is identified below. If any difficulty is encountered in applying this guidance or if any other contributing factor indicates a need for changes in this guidance, the contractor is authorized and encouraged to provide recommended changes to challenge the guidance or the classification assigned to any information or material developed or generated under this contract, and to submit any questions for interpretation of this guidance to the official identified below. Pending final decision, the information involved shall be handled and protected at the highest classification assigned or recommended. (Fill in as appropriate for the classified effort. Attach, or forward under separate correspondence, any documents guides extracts referenced herein. Add additional pages as needed to provide complete guidance.)

Per Executive Order 12829 "National Industrial Security Program" (NISP) and Executive Order 12958 "Classified Information Security Information" as amended, all "offerors" are hereby informed that this contract will require access to classified information, a requirement for security safeguards in addition to those provided in the security clause (52.204-2, Security Requirements) as indicated in the Scope of Work will be assigned upon award. Awardees must be covered by NISP to perform in this contract award and will be required to use the Contract Security Classification Specification, DD Form 254.

Ref. Item 10a, 11 j. COMSEC and COMSEC Account: COMSEC Access will involve the installation, maintenance, or use of crypto-equipment, systems, or keying material. Access to COMSEC requires a final US Government Clearance. Disclosure to Subcontractor requires prior approval of DHS. The contractor upon award shall contact the DHS COMSEC Control Office of Record (COR) at commercial (540) 542-3848, to receive current COMSEC guidance.

Ref. Item 10b. RD: RD requires "Q" clearance issued by DOE, which equates to a final US government clearance. The contractor upon award will be required to contact the Office of Security, Administrative Security Division at (202) 447-5337 for briefing requirements. Subcontracting will require prior approval of DHS Contracting Officer and DHS Office of Security.

Ref. Item 10e. 1) SCI and 2) Non-SCI - All contractor personnel are subject to suitability review and acceptance prior to beginning work on this contract IAW DHS MD 11055, regardless of security clearance status. All contractor personnel assigned to this contract shall possess security clearances issued by the Defense Security Service (DSS) commensurate with the level of required access to classified information that is directly in support of this contract. Immigrant aliens, personnel cleared on an interim basis, or personnel holding contractor-generated Confidential clearances are not eligible for access to classified information released or generated under this contract. Contractor personnel who are specifically designated as requiring access to Sensitive Compartmented Information (SCI) must be eligible under the provisions of DCID 6/4 without exception. Personnel will be submitted for access by their DHS manager and verified by their Cognizant Technical Representative. If approved for access, they will receive an indoctrination briefing by DHS security staff prior to being granted access to SCI. All personnel security reporting requirements of DCID 6/4 will be made directly to the DHS SSO. Prior to leaving this contract, personnel will be scheduled for debriefing with the DHS SSO or by calling (202) 447-0509.

Ref. Item 10j. FOUO: The contractor is responsible for handling and marking FOUO, information in accordance with DHS Directive (MD 11042.1) "Safeguarding Sensitive but Unclassified (For Official Use Only) Information," dated January 6, 2005. Furthermore, DHS contractors must sign a special Non-Disclosure Agreement before receiving access to unclassified FOUO information. Contractors with questions on handling DHS FOUO shall contact DHS OS ASD at (202) 772-5012.

14. ADDITIONAL SECURITY REQUIREMENTS. Requirements in addition to ISM requirements, are established for this contract. (If Yes, identify the pertinent contractual clauses in the contract document itself, or provide an appropriate statement which identifies the additional requirements. Provide a copy of the requirements to the cognizant security office. Use Item 13 if additional space is needed.)

	Yes	No
	<input checked="" type="checkbox"/>	<input type="checkbox"/>

15. INSPECTIONS. Elements of this contract are outside the inspection responsibility of the cognizant security office. (If Yes, explain and identify specific areas or elements carved out and the activity responsible for inspections. Use item 13 if additional space is needed.)

	Yes	No
	<input checked="" type="checkbox"/>	<input type="checkbox"/>

16. CERTIFICATION AND SIGNATURE. Security requirements stated herein are complete and adequate for safeguarding the classified information to be released or generated under this classified effort. All questions shall be referred to the official named below.

a. TYPED NAME OF AUTHORIZING OFFICIAL _____ b. TITLE _____ c. TELEPHONE (Include Area Code) _____

d. ADDRESS (Include Zip Code) _____

e. SIGNATURE _____	17. REQUIRED DISTRIBUTION <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 20px; text-align: center;"><input checked="" type="checkbox"/></td> <td>a. CONTRACTOR</td> </tr> <tr> <td style="text-align: center;"><input type="checkbox"/></td> <td>b. SUBCONTRACTOR</td> </tr> <tr> <td style="text-align: center;"><input checked="" type="checkbox"/></td> <td>c. COGNIZANT SECURITY OFFICE FOR PRIME AND SUBCONTRACTOR</td> </tr> <tr> <td style="text-align: center;"><input type="checkbox"/></td> <td>d. U.S. ACTIVITY RESPONSIBLE FOR OVERSEAS SECURITY ADMINISTRATION</td> </tr> <tr> <td style="text-align: center;"><input checked="" type="checkbox"/></td> <td>e. ADMINISTRATIVE CONTRACTING OFFICER</td> </tr> <tr> <td style="text-align: center;"><input checked="" type="checkbox"/></td> <td>f. OTHERS AS NECESSARY</td> </tr> </table>	<input checked="" type="checkbox"/>	a. CONTRACTOR	<input type="checkbox"/>	b. SUBCONTRACTOR	<input checked="" type="checkbox"/>	c. COGNIZANT SECURITY OFFICE FOR PRIME AND SUBCONTRACTOR	<input type="checkbox"/>	d. U.S. ACTIVITY RESPONSIBLE FOR OVERSEAS SECURITY ADMINISTRATION	<input checked="" type="checkbox"/>	e. ADMINISTRATIVE CONTRACTING OFFICER	<input checked="" type="checkbox"/>	f. OTHERS AS NECESSARY
<input checked="" type="checkbox"/>	a. CONTRACTOR												
<input type="checkbox"/>	b. SUBCONTRACTOR												
<input checked="" type="checkbox"/>	c. COGNIZANT SECURITY OFFICE FOR PRIME AND SUBCONTRACTOR												
<input type="checkbox"/>	d. U.S. ACTIVITY RESPONSIBLE FOR OVERSEAS SECURITY ADMINISTRATION												
<input checked="" type="checkbox"/>	e. ADMINISTRATIVE CONTRACTING OFFICER												
<input checked="" type="checkbox"/>	f. OTHERS AS NECESSARY												

Continuation to Block 13 of DD Form 254 contract Security Classification Specification to Solicitation for ITNOVA (O&M)

Ref. Item 11a. Contract performance for all SCI work is restricted to DHS Government buildings located in and at the metropolitan area of Washington, D.C., and at other locations in the metropolitan area of Wash DC. Contractor is authorized safeguarding and will be required to generate and receive classified up to Top Secret at the address indicated in Item 6 a., b, under the cognizance of DSS. All contractor personnel must be U.S. citizens, have been granted a final security clearance by the U.S. Government, have been approved as meeting suitability criteria by DHS CSO, and have been indoctrinated by a Non Disclosure Agreement, Standard Form 312 for this specific program prior to being given any access to such information released or generated under this contract. Immigrant aliens, personnel cleared on an interim basis, or personnel holding contractor granted CONFIDENTIAL clearances, are not eligible for access to classified information released or generated under this contract without the express permission of the CSO through the DHS Personnel Division (DHS/PSD). The contractor and the Contracting Officer Technical Representative or other delegated representative will revalidate all SCI staffing requirements under the contract with the CSO annually or when a revised DD Form 254 is issued, whichever is sooner.

Ref. Item 11 c/d: The contractor upon award will be required to use Department of Homeland Security Homeland Security Data Network Security Classification Guide (DHS SCG OS-001 (IT)), dated February 2004 and Department of Homeland Security National Security IT Systems Certification and Accreditation, Security Classification Guide (DHS SCG OS-002 (IT)), dated March 2004 for classification of information associated with this effort. All classified information shall be marked in accordance with the NISPOM. The ISOO Pamphlet on "Marking Classified National Security Information, dated March 25, 2003, may be used as a guide on the proper marking of classified information. Question relating to Marking Classified National Security Information can be addressed to DHS Office of Security Administrative Security Division, at telephone (202) 447-5840.

Ref. Item 11 j: OPSEC – The contractor upon award will be required to address and develop how the contractor plans to identify those activities likely to produce intelligence for an adversary through an OPSEC Plan. Contractor will be required to contact the DHS OPSEC Branch at (202) 205-2484 for further OPSEC guidance.

FOR SOLICITATION ONLY

FOR OFFICIAL USE ONLY

DEPARTMENT OF HOMELAND SECURITY
HOMELAND SECURITY DATA NETWORK
SECURITY CLASSIFICATION GUIDE
(DHS SCG OS-001 (IT))

February 2004



Issued and Approved By:

A handwritten signature in black ink, appearing to read "Jack L. Johnson, Jr.", is written over a horizontal line.

Jack L. Johnson, Jr.
Chief Security Officer
Department of Homeland Security

A handwritten date "2/29/04" is written over a horizontal line.

Date

FOR OFFICIAL USE ONLY

DHS SCG OS-001 (IT)

Homeland Security Data Network

February 2004

Department of Homeland Security

Office of Security

Washington D.C. 20528

Change Number	Date of Change Notice

**HOEMALD SECURITY DATA NETWORK (HSDN)
SECURITY CLASSIFICATION GUIDE
TABLE OF CONTENTS**

1	GENERAL	PAGE
1.1	PURPOSE	4
1.2	AUTHORITY	4
1.3	SCOPE AND APPLICABILITY	4
1.4	OFFICE OF PRIMARY RESPONSIBILITY	4
2	POLICY	
2.1	GENERAL	5
2.2	REASON FOR CLASSIFICATION	5
2.3	CLASSIFICATION BY COMPILATION	5
2.4	EXCEPTIONAL CIRCUMSTANCES	6
2.5	CHALLENGES TO CLASSIFICATION	6
2.6	USE OF THIS GUIDE	6
2.7	CLASSIFIED PROCESSING	7
2.8	MARKING	7
2.9	REPRODUCTION AND DISSEMINATION	7
3	RELEASE OF INFORMATION	
3.1	PUBLIC RELEASE	7
3.2	SENSITIVE UNCLASSIFIED INFORMATION	8
4	EFFECTIVE DATE AND IMPLEMENTATION	8
	CLASSIFICATION GUIDANCE	9-14
	DEFINITIONS	15-17

1 GENERAL

1.1 PURPOSE

This classification guide is issued for the purpose of identifying specific topics of information associated with the DHS Homeland Security Data Network (HSDN) requiring classification and protection in accordance with Executive Order 12958, "Classified National Security Information," as amended, and its implementing directives. The guide also provides topics of information that do not meet the standards and criteria for classification under E.O. 12958, as amended, but are nonetheless sensitive and require protection against unauthorized disclosure. Such sensitive but unclassified information shall be categorized as "FOR OFFICIAL USE ONLY" (FOUO) and marked as applicable to reflect that status.

1.2 AUTHORITY

This guide is approved by Jack L. Johnson, Jr., Chief Security Officer, Department of Homeland Security, a delegated TOP SECRET Original Classification Authority. It is issued in accordance with Executive Order 12958, as amended, and Information Security Oversight Office (ISOO), Directive No. 1 (32 CFR, Part 2001/2004), "Classified National Security Information; Final Rule."

1.3 SCOPE AND APPLICABILITY

This document provides security classification guidance for information associated with HSDN. This guide shall be cited as the basis for classification, reclassification, and declassification of information and materials under DHS cognizance and control related to the HSDN. Changes in classification guidance required for operational necessity will be made immediately upon notification and concurrence of the approving authority and will be disseminated to original recipients of this guide. The provisions of this guide are applicable to all organizational entities and contractors associated with the Department of Homeland Security.

1.4 OFFICE OF PRIMARY RESPONSIBILITY

The Office of Primary Responsibility (OPR) for this guide is:

Department of Homeland Security
Office of Security
Administrative Security Division
Washington D.C. 20528

Telephone: (202) 772-5012
Fax: (202) 772-9990

2 POLICY

2.1 GENERAL

The HSDN system has been initiated to address the Department of Homeland Security (DHS) requirements for secure classified, computer-to-computer (C2C) connectivity. This access to classified data is an essential element in supporting intelligence, operational, and investigative components, field activities, interdiction, investigation, inspection, arrest efforts, scientific research, and emergency preparedness and response efforts of the Border and Transportation Security (BTS), Information Analysis and Infrastructure Protection (IAIP), Science and Technology (S&T), and the Emergency Preparedness and Response (EPR) directorates, United States Secret Service (USSS), United States Coast Guard (USCG), and DHS Headquarters (HQ) organizations. The HSDN is a classified network environment for DHS and its components, with specific and controlled interconnections to Department of Defense, Intelligence Community and Federal Law Enforcement resources. It will be run internally within DHS and serve as a gateway to external partners.

2.2 REASON FOR CLASSIFICATION

Classification is reserved for specific categories of information or the compilation of related information meeting the standards and criteria for classification as defined in E.O. 12958, as amended, and falling within one or more of the categories of information eligible for classification per Section 1.4 of the Order. The topics of information cited in this guide are classified pursuant to:

Section 1.4(e): scientific, technological, or economic matters relating to the national security, which includes defense against transnational terrorism;

Section 1.4(g): vulnerabilities or capabilities of systems, installations, infrastructures, projects, plans, or protection services relating to the national security, which includes defense against transnational terrorism

2.3 CLASSIFICATION BY COMPILATION

A compilation of unclassified information is normally not classified. However, in certain circumstances, information that would otherwise be marked unclassified may become classified when combined or associated with other unclassified information, if the compiled information reveals an additional association or relationship that meets the standards and criteria for classification. Under such circumstances, it is the additional association or relationship revealed by the combination or compilation of information that is classified, not the individual items of information. Users of this SCG should be aware of such a possibility when compiling unclassified information. (See 2.4 Below)

Likewise, the compilation of classified information will be classified, at a minimum, at the highest classification within the aggregated data, but may become a higher classification if the compiled information reveals an additional association or relationship that warrants a higher level of classification. (See 2.4 Below)

2.4 EXCEPTIONAL CIRCUMSTANCES

Should a situation arise where a holder of information believes the information should be classified but it is not covered by this classification guide, or, a compilation of unclassified information should be classified or, if already classified, classified at a higher level, the information will be handled and safeguarded in accordance with the level of classification the holder believes it to be.

In such instances, the information will be marked with the tentative level of classification and the notation "*Pending Classification Review.*"

The information will be transmitted, by a means approved for the level of classification, to the OPR identified in Section 1.4 of this guide, for a classification determination.

2.5 CHALLENGES TO CLASSIFICATION

If at any time security classification guidance contained herein is challenged, the items of information involved shall continue to be protected at the level prescribed by this guide until such time as a formal decision by an appropriate authority is made. Classification challenges should be addressed to the OPR identified in Section 1.4 of this guide. Appeal procedures to classification determinations are found in 32 CFR Part 2001/2004, "Classified National Security Information," Directive No. 1, Final Rule.

2.6 USE OF THIS GUIDE

This guide is for the use of DHS employees and contractors performing derivative classification actions when addressing the elements of information covered by this guide.

For the purpose of marking documents containing classified information covered by this guide, derivative classifiers will cite "DHS SCG OS-001 (IT), Dated February 2004," on the "Derived From" line, followed by the declassification instruction as specified in the guide. For Example:

Derived From: DHS SCG OS-001 (IT), February 2004
Declassify On: (Insert declassification instruction as cited for the particular Topic in the SCG)

If classified information covered by this guide, as well as classified information from other classified sources, is included in the same document, the document will be marked as follows:

Derived From: Multiple Sources
Declassify On: (Carry forward the single most restrictive declassification instruction from all source documents)

NOTE: If "Multiple Sources" are used for a derivatively classified document, a record of the sources used will be maintained with the file copy of the document.

FOR OFFICIAL USE ONLY

Where the declassification instruction of a source(s) is marked "OADR" or "Originating Agency Determination Required," or, the declassification instruction from a source(s) cites X-1 thru X-8, the declassification instructions for the newly created document will state: "Source Marked OADR," followed by the date of the most recent source; or, "Source Marked X-(applicable exemption number)" followed by the date of the most recent source. For example:

Derived From: Multiple Sources
Declass On: Source Marked OADR, Date of Source Sep 21, 1995

Derived From: Multiple Sources
Declass On: Source Marked X-1, Date of Source Sep 21, 2003

2.7 CLASSIFIED PROCESSING

Classified information will not be processed on any automated IT equipment unless the equipment has been specifically accredited and approved for classified processing. Consult office/organizational element security officials for instructions on what equipment may be used.

2.8 MARKING

Detailed instructions for marking classified materials can be found in the DHS Security Manual and the ISOO pamphlet titled "Marking." Training on marking classified materials can be obtained by contacting the DHS Office of Security at (202) 358-1438. The ISOO Marking Pamphlet is available for download at <http://www.archives.gov/isoo/index.html>. You can also download it from the DHS internal intra-net, DHSONline, by going to the Security portal, Information Security, "ISOO Marking Booklet 2003."

2.9 REPRODUCTION AND DISSEMINATION

This guide may be reproduced and disseminated within DHS as needed. However, to ensure receipt of updates, revisions, and classification changes, whenever the guide is disseminated beyond an initial addressee, notify the OPR.

Coordinate dissemination to government agencies outside of DHS through the OPR.

RELEASE OF INFORMATION

3.1 PUBLIC RELEASE

The fact that this guide indicates that some information may be unclassified does not imply that the information is automatically releasable to the public. Request for public release of information will be processed in accordance with the DHS MD Number 0460.1, "Freedom of Information Act Compliance."

FOR OFFICIAL USE ONLY

This guide is designated "FOR OFFICIAL USE ONLY" and will not be released to the public. Requests for copies of this guide by non-governmental officials will be processed under the Freedom of Information Act.

3.2 SENSITIVE UNCLASSIFIED INFORMATION

The classification guide applies to information that requires protection to prevent damage to the national security and thus requires classification in accordance with E.O. 12958, as amended. In addition to classified information, there are certain types of sensitive but unclassified information for which Executive Branch agencies require application of controls and protective measures for a variety of reasons. FOR OFFICIAL USE ONLY (FOUO) is the designation that is applied by DHS to sensitive but unclassified information that may be exempt from mandatory release to the public under Section 552 of Title 5, U.S.C., "Freedom of Information Act (FOIA)."

4 EFFECTIVE DATE AND IMPLEMENTATION

This classification guide is effective immediately upon release.

**Homeland Security Data Network
Security Classification Guidance
(DHS SCG OS-001 (IT))**

1. GENERAL			
TOPIC	CLASSIFICATION	DURATION	REMARKS
a. Existence of HSDN.	UNCLASSIFIED	N/A	
b. Functions and mission of HSDN.	FOUO	N/A	
c. HSDN accounting or appropriation data, budget estimates, and/or funding levels.	FOUO	N/A	
d. HSDN program/project milestone schedule.	FOUO (See Remarks)	(See Remarks)	Milestone schedules of HSDN and HSDN associated programs, shown by themselves, are not classified unless the information is associated with other information classified in accordance with this guide. In this case, the information will be classified at the same level and declassified in accordance with the instructions provided herein.
e. HSDN Login ID.	FOUO	N/A	
f. Passwords to HSDN.	Secret	Declassify when the password is changed and no longer affords access to HSDN.	
g. List revealing the locations of HSDN sites/remote terminals.	FOUO	N/A	
2. SYSTEMS INFORMATION			
a. Location of servers, routers, switches, or other systems management equipment or devices.	FOUO	N/A	
b. Types of servers, routers, switches, etc., being used in HSDN.	FOUO	N/A	

FOR OFFICIAL USE ONLY

TOPIC	CLASSIFICATION	DURATION	REMARKS
c. Remote dial-up telephone numbers.	FOUO	N/A	
d. IP addresses associated with HSDN.	FOUO	N/A	
e. Identification of software used on HSDN.	FOUO	N/A	
f. Type of Intrusion Detection software and/or hardware used in HSDN.	FOUO	N/A	
g. Identification of cryptographic and encryption equipment/infrastructure.	FOUO	N/A	
h. Network Diagrams, drawings, flow charts that depict non-specific HSDN connectivity.	FOUO	N/A	
i. Network Diagrams, drawings, flow charts that depict the complete HSDN connectivity, node information, port information, and geographic locations.	SECRET	December 31, 2018	
j. Planned outages or upgrades to HSDN that do not otherwise contain information classified pursuant to this guide.	FOUO	N/A	
k. HSDN Certification and Accreditation (C&A) documentation containing information classified pursuant to this guide.	(See Remarks)	(See Remarks)	Classify and declassify in accordance with the applicable instructions provided in this guide. C&A documentation containing no information classified pursuant to this guide will, at a minimum, be categorized as FOUO. (See Section 3)

FOR OFFICIAL USE ONLY

TOPIC	CLASSIFICATION	DURATION	REMARKS
<p>I. System Test and Evaluation (ST&E) results containing information classified pursuant to this guide.</p>	(See Remarks)	(See Remarks)	<p>Classify and declassify in accordance with the applicable instructions provided in this guide.</p> <p>ST&E documentation containing no information classified pursuant to this guide will, at a minimum, be categorized as FOUO.</p> <p>(See Section 3)</p>
3. VULNERABILITIES			
<p>a. Identification of specific architecture or application vulnerabilities which, if exploited, could result in the compromise of the confidentiality, integrity or availability of HSDN.</p>	SECRET	<p>10 years from date of discovery, or, upon confirmed elimination of the vulnerability, whichever occurs sooner. (See Remarks)</p>	<p>If the vulnerability exists at multiple locations, declassification will not occur until the vulnerability has been eliminated at all locations.</p>
<p>b. Details of an exploitable security system vulnerability that, if disclosed, could lead to the compromise of classified information.</p>	SECRET	<p>10 years from date of discovery, or, upon confirmed elimination of the vulnerability, whichever occurs sooner. (See Remarks)</p>	<p>If the vulnerability exists at multiple locations, declassification will not occur until the vulnerability has been eliminated at all locations.</p>
<p>c. Details of an exploitable physical security vulnerability that, if disclosed, could lead to the compromise of classified information.</p>	<p>SECRET Or FOUO (See Remarks)</p>	<p>10 years from date of discovery, or, upon confirmed elimination of the vulnerability, whichever occurs sooner.</p>	<p>Classify as Secret if the exploitable vulnerability offers direct and unimpeded access to classified information with a negligible chance of detection.</p> <p>Classify as Confidential if the exploitable vulnerability offers potential access to classified information with minimal effort.</p> <p>Categorize as FOUO if the exploitable vulnerability is one of multiple layers of a defense in depth with minimal chance of an unauthorized person gaining access to classified information.</p>

FOR OFFICIAL USE ONLY

TOPIC	CLASSIFICATION	DURATION	REMARKS
d. Status of corrective action to address vulnerabilities of applications or operating systems (COTS or GOTS) that are used by and associated by name with HSDN.	SECRET	10 years from date of discovery, or, upon confirmed elimination of the vulnerability, whichever occurs sooner. (See Remarks)	If the vulnerability exists at multiple locations, declassification will not occur until the vulnerability has been eliminated at all locations.
e. Status of corrective action to address vulnerabilities of applications or operating systems (COTS or GOTS) that are used by but not associated by name with HSDN.	FOUO	N/A	
f. Vulnerabilities of data links that are used by and associated by name with HSDN.	SECRET	10 years from date of discovery, or, upon confirmed elimination of the vulnerability, whichever occurs sooner. (See Remarks)	If the vulnerability exists at multiple locations, declassification will not occur until the vulnerability has been eliminated at all locations.
g. Vulnerabilities of data links that are used by but not associated by name with HSDN.	UNCLASSIFIED	N/A	
h. HSDN system vulnerabilities not listed in this guide which, if exploited, could result in the compromise of classified information or the confidentiality, integrity or availability of HSDN.	SECRET	10 years from date of discovery, or, upon confirmed elimination of the vulnerability, whichever occurs sooner. (See Remarks)	If the vulnerability exists at multiple locations, declassification will not occur until the vulnerability has been eliminated at all locations.
4. INCIDENTS			
a. Existence of a penetration to HSDN without further elaboration.	FOUO	N/A	

FOR OFFICIAL USE ONLY

TOPIC	CLASSIFICATION	DURATION	REMARKS
<p>b. Details of a penetration or attempted penetration of HSDN that if disclosed, could lead to the compromise of classified information.</p>	<p>SECRET</p>	<p>10 years from date of discovery, or, upon confirmed and successful deployment or installation of countermeasures that prevent similar events from occurring, whichever occurs sooner. (See Remarks)</p>	<p>If the vulnerability exists at multiple locations, declassification will not occur until the vulnerability has been eliminated at all locations.</p>
<p>b. Information concerning the loss or mishandling of classified information:</p> <ul style="list-style-type: none"> • Report of the compromise of classified information without elaboration. • Report of the compromise of classified information that is specific and details the classified information compromised. 	<p>FOUO (See Remarks)</p>	<p>N/A (See Remarks)</p>	<p>Classify and declassify in accordance with the classification/declassification instructions cited on the compromised material.</p>
<ul style="list-style-type: none"> • Report confirming that classified information was sent to an unauthorized recipient or over an unclassified network. • Report that identifies by name the individual who obtained unauthorized access to classified information and/or the HSDN. 	<p>CONFIDENTIAL CONFIDENTIAL</p>	<p>5 years from date of incident, or, upon execution of a non-disclosure agreement by the unauthorized recipient or upon successful sanitization of the classified material from the system. 5 years from date of incident, or, upon execution of a non-disclosure agreement by the unauthorized recipient or upon successful sanitization of the classified material from the system.</p>	

5. CONTINUITY OF OPERATIONS			
a. Disaster recovery and continuity of operations plans (COOP) that associate HSDN with specific alternative sites.	SECRET	January 15, 2020	
b. Disaster recovery and continuity of operations plans (COOP) that do not associate HSDN with specific alternative sites.	FOUO	N/A	

DEFINITIONS

Access. The ability and opportunity to obtain knowledge of classified information.

Applicable Associated Markings. Markings, other than those which designate classification level, that are required to be placed on classified documents. These include the "Derived From" line, downgrading and declassification instructions, special control notices, Special Access Program caveats, etc.

Automatic Declassification. The declassification of information based upon: (1) the occurrence of a specific date or event as determined by the original classification authority; or (2) the expiration of a maximum time frame for duration of classification established under Executive Order 12958, as amended.

Classification. The act or process by which information is determined to be classified information.

Classification Guidance. Any instruction or source that prescribes the classification of specific information.

Classification Guide. A documentary form of classification guidance issued by an original classification authority that identifies the elements of information regarding a specific subject that must be classified and establishes the level and duration of classification for each such element.

Classified National Security Information. Information that has been determined pursuant to E.O. 12958, as amended, or any predecessor order to require protection against unauthorized disclosure and is marked to indicate its classified status when in documentary form. Also known as classified information.

Classifier. An individual who makes a classification determination and applies a security classification to information or material. A classifier may be an original classification authority (OCA) or a person who derivatively assigns a security classification based on a properly classified source or a classification guide.

Communications Security (COMSEC). The protection resulting from all measures designed to deny unauthorized persons information of value that might be derived from the possession and study of telecommunications and to ensure the authenticity of such communications. COMSEC includes cryptosecurity, emission security, transmission security, and physical security of COMSEC materials and information.

Compilation. An aggregation of pre-existing unclassified items of information. Compilations of information that are individually unclassified may be classified if the compiled information reveals an additional association or relationship that qualifies for classification pursuant to E.O. 12958, as amended, and is not otherwise revealed by the

FOR OFFICIAL USE ONLY

individual information. Classification by compilation must meet the same standards and criteria as other original classification actions.

Confidential Information. Information, the unauthorized disclosure of which reasonably could be expected to cause damage to the national security that the original classification authority is able to identify or describe.

Configuration Management. The process involving identifying, controlling, accounting for, and auditing all changes made to the baseline system architecture. Included are hardware, firmware, and software.

Cryptology. The branch of knowledge which treats the principles of cryptography and cryptanalytics; and the activities involved in producing signals intelligence (SIGINT) and maintaining communications security (COMSEC).

Damage to the National Security. Harm to the national defense or foreign relations of the United States from the unauthorized disclosure of information.

Declassification. The authorized change in the status of information from classified information to unclassified information.

Declassification Authority. a. The official who authorized the original classification, if that official is still serving in the same position; b. the originator's current successor in function; c. a supervisory official of either; or d. officials delegated declassification authority in writing by the agency head or the senior agency official.

Derivative Classification. Incorporating, paraphrasing, restating, or generating in new form information that is already classified, and marking the newly developed material consistent with the classification markings that apply to the source information. Derivative classification includes the classification of information based on classification guidance provided in a security classification guide. The duplication or reproduction of existing classified information is not derivative classification.

Document. Any physical medium in or on which information is recorded or stored, to include written or printed matter, audio-visual materials, and electromagnetic storage media.

Event. An occurrence or happening that is reasonably certain to occur and that can be set as the signal for automatic declassification of information.

For Official Use Only. The term used within DHS to identify sensitive but unclassified information, in any form, the release of which could cause harm to a persons privacy or welfare, adversely impact economic or industrial institutions or infrastructure, compromise programs or operations essential to the safeguarding of our national interests, or violate a statute, treaty, or other agreement enforceable by law. Information impacting the National Security of the United States and classified

FOR OFFICIAL USE ONLY

Confidential, Secret, or Top Secret under Executive Order 12958, "Classified National Security Information," as amended, or its predecessor or successor orders, is not to be considered FOUO. FOUO is not to be considered classified information.

HSDN. Homeland Security Data Network (HSDN) is the Secret Classified Network for the Department of Homeland Security.

Information. Any knowledge that can be communicated or documentary material, regardless of its physical form or characteristics, that is owned by, produced by or for, or is under the control of the United States Government. "Control" means the authority of the agency that originates information, or its successor in function, to regulate access to the information.

Information Security. The system of policies, procedures, and requirements established under the authority of E.O. 12958, as amended, to protect information that, if subjected to unauthorized disclosure, could reasonably be expected to cause damage to the national security.

Material. Any product or substance on or in which information is embodied.

National security. The national defense or foreign relations of the United States.

Need-to-know. A determination made by an authorized holder of classified information that a prospective recipient requires access to specific classified information in order to perform or assist in a lawful and authorized governmental function.

Original Classification. An initial determination that information requires, in the interest of national security, protection against unauthorized disclosure.

Original Classification Authority. An individual authorized in writing, either by the President, or by agency heads or other officials designated by the President, to originally classify information.

Regrade. To raise or lower the classification assigned to an item of information.

Secret Information. Information, the unauthorized disclosure of which reasonably could be expected to cause serious damage to the national security that the original classification authority is able to identify or describe.

Telecommunications. The preparation, transmission, or communication of information by electronic means.

Top Secret. Information, the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to the national security that the original classification authority is able to identify or describe.

FOR OFFICIAL USE ONLY

**DEPARTMENT OF HOMELAND SECURITY
NATIONAL SECURITY IT SYSTEMS CERTIFICATION AND
ACCREDITATION
SECURITY CLASSIFICATION GUIDE
(DHS SCG OS-002 (IT))**

March 2004



Issued and Approved By:

Signed 3/29/2004 Original Signed Copy Maintained at DHS Office of Security

Jack L. Johnson, Jr.
Chief Security Officer
Department of Homeland Security
March 29, 2004

Date

FOR OFFICIAL USE ONLY

DHS SCG OS-002 (IT)

National Security IT Systems Certification & Accreditation

March 2004

Department of Homeland Security

Office of Security

Washington D.C. 20528

Change Number	Date of Change Notice

**NATIONAL SECURITY IT SYSTEMS CERTIFICATION & ACCREDITATION
SECURITY CLASSIFICATION GUIDE
TABLE OF CONTENTS**

1	GENERAL	PAGE
1.1	PURPOSE	4
1.2	AUTHORITY	4
1.3	SCOPE AND APPLICABILITY	4
1.4	OFFICE OF PRIMARY RESPONSIBILITY	4
1.5	RELATED GUIDANCE	5
2	POLICY	
2.1	GENERAL	5
2.2	REASON FOR CLASSIFICATION	5
2.3	CLASSIFICATION BY COMPILATION	6
2.4	EXCEPTIONAL CIRCUMSTANCES	6
2.5	CHALLENGES TO CLASSIFICATION	6
2.6	USE OF THIS GUIDE	6
2.7	CLASSIFIED PROCESSING	7
2.8	MARKING	7
2.9	REPRODUCTION AND DISSEMINATION	7
3	RELEASE OF INFORMATION	
3.1	PUBLIC RELEASE	8
3.2	SENSITIVE UNCLASSIFIED INFORMATION	8
4	EFFECTIVE DATE AND IMPLEMENTATION	8
	CLASSIFICATION GUIDANCE	9-13
	DEFINITIONS	14-17

1 GENERAL

1.1 PURPOSE

This classification guide is issued for the purpose of identifying specific topics of information associated with the certification and accreditation (C&A) of information technology (IT) systems used for storing, transmitting, and processing classified national security information (classified information) and requiring classification and protection in accordance with Executive Order 12958, "Classified National Security Information," as amended, and its implementing directives. The guide also provides topics of information that do not meet the standards and criteria for classification under E.O. 12958, as amended, but are nonetheless sensitive and require protection against unauthorized disclosure. Such sensitive but unclassified information shall be categorized as "FOR OFFICIAL USE ONLY" (FOUO) and marked as applicable to reflect that status.

1.2 AUTHORITY

This guide is approved by Jack L. Johnson, Jr., Chief Security Officer, Department of Homeland Security, a delegated TOP SECRET Original Classification Authority. It is issued in accordance with Executive Order 12958, as amended, and Information Security Oversight Office (ISOO), Directive No. 1 (32 CFR, Part 2001/2004), "Classified National Security Information; Final Rule."

1.3 SCOPE AND APPLICABILITY

This document provides security classification guidance for information associated with the C&A of IT systems used for storing, transmitting, and processing classified information. This guide shall be cited as the basis for classification, reclassification, and declassification of information and materials under DHS cognizance and control related to the C&A process. Changes in classification guidance required for operational necessity will be made immediately upon notification and concurrence of the approving authority and will be disseminated to original recipients of this guide. The provisions of this guide are applicable to all organizational entities and contractors associated with the Department of Homeland Security.

1.4 OFFICE OF PRIMARY RESPONSIBILITY

The Office of Primary Responsibility (OPR) for this guide is:

Department of Homeland Security
Office of Security
Administrative Security Division
Washington D.C. 20528

Telephone: (202) 772-5012
Fax: (202) 772-9990

1.5 RELATED GUIDANCE

Classification guidance related too or associated with the topical guidance provided in this SCG can be found in DHS SCG OS-001(IT), Homeland Security Data Network. A copy of the related guidance can be requested from the Office of Primary Responsibility identified in Section 1.4 above.

2 POLICY

2.1 GENERAL

The Certification and Accreditation of DHS National Security IT Systems will be in accordance with MD-4300B, DHS Policy Guide for National Security Systems. Certification of National Security IT Systems establishes the extent to which a particular IT design and implementation meets a specified set of security requirements. Certification primarily addresses software and hardware security safeguards, but also considers procedural, physical, and personnel security measures employed to enforce IT security policy.

Accreditation is the official management authorization to operate an IT system based on a particular mode of operation; a prescribed set of security safeguards; a defined threat with stated vulnerabilities and safeguards; a given operational environment; a stated operational concept; a stated interconnection to other IT; an operational necessity; and an acceptable level of risk for which a Designated Approval Authority (DAA) has formally assumed responsibility.

2.2 REASON FOR CLASSIFICATION

Classification is reserved for specific categories of information or the compilation of related information meeting the standards and criteria for classification as defined in E.O. 12958, as amended, and falling within one or more of the categories of information eligible for classification per Section 1.4 of the Order. The topics of information cited in this guide are classified pursuant to:

Section 1.4(e): scientific, technological, or economic matters relating to the national security, which includes defense against transnational terrorism;

Section 1.4(g): vulnerabilities or capabilities of systems, installations, infrastructures, projects, plans, or protection services relating to the national security, which includes defense against transnational terrorism

2.3 CLASSIFICATION BY COMPILATION

A compilation of unclassified information is normally not classified. However, in certain circumstances, information that would otherwise be marked unclassified may become classified when combined or associated with other unclassified information, if the

compiled information reveals an additional association or relationship that meets the standards and criteria for classification. Under such circumstances, it is the additional association or relationship revealed by the combination or compilation of information that is classified, not the individual items of information. Users of this SCG should be aware of such a possibility when compiling unclassified information. (See 2.4 Below)

Likewise, the compilation of classified information will be classified, at a minimum, at the highest classification within the aggregated data, but may become a higher classification if the compiled information reveals an additional association or relationship that warrants a higher level of classification. (See 2.4 Below)

2.4 EXCEPTIONAL CIRCUMSTANCES

Should a situation arise where a holder of information believes the information should be classified but it is not covered by this classification guide, or, a compilation of unclassified information should be classified or, if already classified, classified at a higher level, the information will be handled and safeguarded in accordance with the level of classification the holder believes it to be.

In such instances, the information will be marked with the tentative level of classification and the notation "*Pending Classification Review.*"

The information will be transmitted, by a means approved for the level of classification, to the OPR identified in Section 1.4 of this guide, for a classification determination.

2.5 CHALLENGES TO CLASSIFICATION

If at any time security classification guidance contained herein is challenged, the items of information involved shall continue to be protected at the level prescribed by this guide until such time as a formal decision by an appropriate authority is made. Classification challenges should be addressed to the OPR identified in Section 1.4 of this guide. Appeal procedures to classification determinations are found in 32 CFR Part 2001/2004, "Classified National Security Information," Directive No. 1, Final Rule.

2.6 USE OF THIS GUIDE

This guide is for the use of DHS employees and contractors performing derivative classification actions when addressing the elements of information covered by this guide. For the purpose of marking documents containing classified information covered by this guide, derivative classifiers will cite "DHS SCG OS-002 (IT), Dated March 2004," on the "Derived From" line, followed by the declassification instruction as specified in the guide. For Example:

Derived From: DHS SCG OS-002 (IT), March 2004

Declassify On: (Insert declassification instruction as cited for the particular Topic in the SCG)

If classified information covered by this guide, as well as classified information from other classified sources, is included in the same document, the document will be marked as follows:

Derived From: Multiple Sources

Declassify On: (Carry forward the single most restrictive declassification instruction from all source documents)

NOTE: If "Multiple Sources" are used for a derivatively classified document, a record of the sources used will be maintained with the file copy of the document.

Where the declassification instruction of a source(s) is marked "OADR" or "Originating Agency Determination Required," or, the declassification instruction from a source(s) cites X-1 thru X-8, the declassification instructions for the newly created document will state: "Source Marked OADR," followed by the date of the most recent source; or, "Source Marked X-(applicable exemption number)" followed by the date of the most recent source. For example:

Derived From: Multiple Sources

Declass On: Source Marked OADR, Date of Source Sep 21, 1995

Derived From: Multiple Sources

Declass On: Source Marked X-1, Date of Source Sep 21, 2003

2.7 CLASSIFIED PROCESSING

Classified information will not be processed on any automated IT equipment unless the equipment has been specifically accredited and approved for classified processing. Consult office/organizational element security officials for instructions on what equipment may be used.

2.8 MARKING

Detailed instructions for marking classified materials can be found in the DHS Security Manual and the ISOO pamphlet titled "Marking." Training on marking classified materials can be obtained by contacting the DHS Office of Security at (202) 358-1438. The ISOO Marking Pamphlet is available for download at <http://www.archives.gov/isoo/index.html>. You can also download it from the DHS internal intra-net, DHSOnline, by going to the Security portal, Information Security, "ISOO Marking Booklet 2003."

2.9 REPRODUCTION AND DISSEMINATION

This guide may be reproduced and disseminated within DHS as needed. However, to ensure receipt of updates, revisions, and classification changes, whenever the guide is disseminated beyond an initial addressee, notify the OPR.

Coordinate dissemination to government agencies outside of DHS through the OPR.

RELEASE OF INFORMATION

3.1 PUBLIC RELEASE

The fact that this guide indicates that some information may be unclassified does not imply that the information is automatically releasable to the public. Request for public release of information will be processed in accordance with the DHS MD Number 0460.1, "Freedom of Information Act Compliance."

This guide is designated "FOR OFFICIAL USE ONLY" and will not be released to the public. Requests for copies of this guide by non-governmental officials will be processed under the Freedom of Information Act.

3.2 SENSITIVE UNCLASSIFIED INFORMATION

The classification guide applies to information that requires protection to prevent damage to the national security and thus requires classification in accordance with E.O. 12958, as amended. In addition to classified information, there are certain types of sensitive but unclassified information for which Executive Branch agencies require application of controls and protective measures for a variety of reasons. FOR OFFICIAL USE ONLY (FOUO) is the designation that is applied by DHS to sensitive but unclassified information that may be exempt from mandatory release to the public under Section 552 of Title 5, U.S.C., "Freedom of Information Act (FOIA)."

4 EFFECTIVE DATE AND IMPLEMENTATION

This classification guide is effective immediately upon release.

National Security IT Systems Certification & Accreditation
Security Classification Guidance
(DHS SCG OS-002 (IT))

1. GENERAL			
TOPIC	CLASSIFICATION	DURATION	REMARKS
a. Information revealing the location of a Special Compartmented Information Facility (SCIF) <u>in association with</u> the categories of SCI information processed on classified IT system(s) in those locations.	CONFIDENTIAL	15 Years From Date of Origin	
b. Information revealing the location of a collateral classified IT systems, sites, remote terminals, etc.	FOUO (See Remarks)	(See Remarks)	Information will be designated as FOUO unless it is otherwise classified under authorities associated with a classified program or process that is itself classified. In this instance, classification and declassification will be applied in accordance with the program guidance.
c. Classified IT systems accounting or appropriation data, budget estimates, and/or funding levels.	FOUO (See Remarks)	(See Remarks)	Information will be designated as FOUO unless it is otherwise classified under authorities associated with a classified program or process that is itself classified. In this instance, classification and declassification will be applied in accordance with the program guidance.
d. Classified IT systems program/project milestone schedule.	FOUO (See Remarks)	(See Remarks)	Information will be designated as FOUO unless it is otherwise classified under authorities associated with a classified program or process that is itself classified. In this instance, classification and declassification will be applied in accordance with the program guidance.
2. SYSTEMS INFORMATION			
a. Location of servers, routers, switches, or other systems management equipment or devices.	FOUO (See Remarks)	(See Remarks)	Information will be designated as FOUO unless it is otherwise classified under authorities associated with a classified program or process that is itself classified. In this instance, classification and declassification will be applied in accordance with the program guidance.

TOPIC	CLASSIFICATION	DURATION	REMARKS
b. Types of servers, routers, switches, etc., in use.	FOUO (See Remarks)	(See Remarks)	Information will be designated as FOUO unless it is otherwise classified under authorities associated with a classified program or process that is itself classified. In this instance, classification and declassification will be applied in accordance with the program guidance.
c. Identification of software used on the system.	FOUO (See Remarks)	(See Remarks)	Information will be designated as FOUO unless it is otherwise classified under authorities associated with a classified program or process that is itself classified. In this instance, classification and declassification will be applied in accordance with the program guidance.
d. Type of Intrusion Detection software and/or hardware used on the system.	FOUO (See Remarks)	(See Remarks)	Information will be designated as FOUO unless it is otherwise classified under authorities associated with a classified program or process that is itself classified. In this instance, classification and declassification will be applied in accordance with the program guidance.
e. Identification of cryptographic and encryption equipment/infrastructure.	FOUO (See Remarks)	(See Remarks)	Information will be designated as FOUO unless it is otherwise classified under authorities associated with a classified program or process that is itself classified. In this instance, classification and declassification will be applied in accordance with the program guidance.
f. Network Diagrams, drawings, flow charts that depict non-specific classified IT connectivity.	FOUO (See Remarks)	(See Remarks)	Information will be designated as FOUO unless it is otherwise classified under authorities associated with a classified program or process that is itself classified. In this instance, classification and declassification will be applied in accordance with the program guidance.
g. Network Diagrams, drawings, flow charts that depict the complete classified system IT connectivity, node information, port information, and geographic locations.	SECRET	15 Years from date of origin	

TOPIC	CLASSIFICATION	DURATION	REMARKS
<p>h. System Test and Evaluation (ST&E) results containing information classified pursuant to this guide.</p>	(See Remarks)	(See Remarks)	<p>Classify and declassify in accordance with the applicable instructions provided in this guide.</p> <p>ST&E documentation containing no information classified pursuant to this guide will, at a minimum, be categorized as FOUO.</p> <p>(See Section 3)</p>
3. VULNERABILITIES			
<p>a. Identification of specific architecture or application vulnerabilities which, if exploited, could result in the compromise of the confidentiality, integrity or availability of the classified IT system.</p>	SECRET	<p>10 years from date of discovery, or, upon confirmed elimination of the vulnerability, whichever occurs sooner. (See Remarks)</p>	<p>If the vulnerability exists at multiple locations, declassification will not occur until the vulnerability has been eliminated at all locations.</p>
<p>b. Details of an exploitable security system vulnerability that, if disclosed, could lead to the compromise of classified information.</p>	SECRET	<p>10 years from date of discovery, or, upon confirmed elimination of the vulnerability, whichever occurs sooner. (See Remarks)</p>	<p>If the vulnerability exists at multiple locations, declassification will not occur until the vulnerability has been eliminated at all locations.</p>
<p>c. Details of an exploitable physical security vulnerability that, if disclosed, could lead to the compromise of classified information.</p>	<p>SECRET CONFIDENTIAL Or FOUO (See Remarks)</p>	<p>10 years from date of discovery, or, upon confirmed elimination of the vulnerability, whichever occurs sooner.</p>	<p>Classify as Secret if the exploitable vulnerability offers direct and unimpeded access to classified information with a negligible chance of detection.</p> <p>Classify as Confidential if the exploitable vulnerability offers potential access to classified information with minimal effort.</p> <p>Categorize as FOUO if the exploitable vulnerability is one of multiple layers of a defense in depth with minimal chance of an unauthorized person gaining access to classified information.</p>

TOPIC	CLASSIFICATION	DURATION	REMARKS
d. Status of corrective action to address vulnerabilities of applications or operating systems (COTS or GOTS) that are used by and associated by name with the classified IT system.	SECRET	10 years from date of discovery, or, upon confirmed elimination of the vulnerability, whichever occurs sooner. (See Remarks)	If the vulnerability exists at multiple locations, declassification will not occur until the vulnerability has been eliminated at all locations.
e. Status of corrective action to address vulnerabilities of applications or operating systems (COTS or GOTS) that are used by but not associated by name with the classified IT system.	FOUO	N/A	
f. Vulnerabilities of data links that are used by and associated by name with the classified IT system.	SECRET	10 years from date of discovery, or, upon confirmed elimination of the vulnerability, whichever occurs sooner. (See Remarks)	If the vulnerability exists at multiple locations, declassification will not occur until the vulnerability has been eliminated at all locations.
g. Vulnerabilities of data links that are used by but not associated by name with the classified IT system.	UNCLASSIFIED	N/A	
h. Classified IT system vulnerabilities not listed in this guide which, if exploited, could result in the compromise of classified information or the confidentiality, integrity or availability of HSDN.	SECRET	10 years from date of discovery, or, upon confirmed elimination of the vulnerability, whichever occurs sooner. (See Remarks)	If the vulnerability exists at multiple locations, declassification will not occur until the vulnerability has been eliminated at all locations.
4. INCIDENTS			
a. Existence of a penetration to the classified IT system without further elaboration.	FOUO	N/A	

TOPIC	CLASSIFICATION	DURATION	REMARKS
<p>b. Details of a penetration or attempted penetration of a classified IT system that if disclosed, could lead to the compromise of classified information.</p>	<p>SECRET</p>	<p>10 years from date of discovery, or, upon confirmed and successful deployment or installation of countermeasures that prevent similar events from occurring, whichever occurs sooner. (See Remarks)</p>	<p>If the vulnerability exists at multiple locations, declassification will not occur until the vulnerability has been eliminated at all locations.</p>
<p>c. Information concerning the loss or mishandling of classified information:</p> <ul style="list-style-type: none"> • Report of the compromise of classified information without elaboration. • Report of the compromise of classified information that is specific and details the classified information compromised. 	<p>FOUO (See Remarks)</p>	<p>N/A (See Remarks)</p>	<p>Classify and declassify in accordance with the classification/declassification instructions cited on the compromised material.</p>
<ul style="list-style-type: none"> • Report confirming that classified information was sent to an unauthorized recipient or over an unclassified network. • Report that identifies by name the individual who obtained unauthorized access to classified information and/or the classified IT system. 	<p>CONFIDENTIAL CONFIDENTIAL</p>	<p>5 years from date of incident, or, upon execution of a non-disclosure agreement by the unauthorized recipient or upon successful sanitization of the classified material from the system. 5 years from date of incident, or, upon execution of a non-disclosure agreement by the unauthorized recipient or upon successful sanitization of the classified material from the system.</p>	

DEFINITIONS

Access. The ability and opportunity to obtain knowledge of classified information.

Accreditation. The official management authorization to operate an IT system based on a particular mode of operation; a prescribed set of security safeguards; a defined threat, with stated vulnerabilities and safeguards; a given operational environment; a stated operational concept; a stated interconnection to other IT; an operational necessity; and an acceptable level of risk for which the DAA has formerly assumed responsibility.

Applicable Associated Markings. Markings, other than those which designate classification level, that are required to be placed on classified documents. These include the "Derived From" line, downgrading and declassification instructions, special control notices, Special Access Program caveats, etc.

Automatic Declassification. The declassification of information based upon: (1) the occurrence of a specific date or event as determined by the original classification authority; or (2) the expiration of a maximum time frame for duration of classification established under Executive Order 12958, as amended.

Certification. The comprehensive testing and evaluation of the technical and non-technical IT security features, and other safeguards used in support of the accreditation process.

Classification. The act or process by which information is determined to be classified information.

Classification Guidance. Any instruction or source that prescribes the classification of specific information.

Classification Guide. A documentary form of classification guidance issued by an original classification authority that identifies the elements of information regarding a specific subject that must be classified and establishes the level and duration of classification for each such element.

Classified National Security Information. Information that has been determined pursuant to E.O. 12958, as amended, or any predecessor order to require protection against unauthorized disclosure and is marked to indicate its classified status when in documentary form. Also known as classified information.

Classifier. An individual who makes a classification determination and applies a security classification to information or material. A classifier may be an original classification authority (OCA) or a person who derivatively assigns a security classification based on a properly classified source or a classification guide.

Document. Any physical medium in or on which information is recorded or stored, to include written or printed matter, audio-visual materials, and electromagnetic storage media.

Event. An occurrence or happening that is reasonably certain to occur and that can be set as the signal for automatic declassification of information.

For Official Use Only. The term used within DHS to identify sensitive but unclassified information, in any form, the release of which could cause harm to a persons privacy or welfare, adversely impact economic or industrial institutions or infrastructure, compromise programs or operations essential to the safeguarding of our national interests, or violate a statute, treaty, or other agreement enforceable by law. Information impacting the National Security of the United States and classified Confidential, Secret, or Top Secret under Executive Order 12958, "Classified National Security Information," as amended, or its predecessor or successor orders, is not to be considered FOUO. FOUO is not to be considered classified information.

Information. Any knowledge that can be communicated or documentary material, regardless of its physical form or characteristics, that is owned by, produced by or for, or is under the control of the United States Government. "Control" means the authority of the agency that originates information, or its successor in function, to regulate access to the information.

Information Security. The system of policies, procedures, and requirements established under the authority of E.O. 12958, as amended, to protect information that, if subjected to unauthorized disclosure, could reasonably be expected to cause damage to the national security.

Material. Any product or substance on or in which information is embodied.

National security. The national defense or foreign relations of the United States.

Need-to-know. A determination made by an authorized holder of classified information that a prospective recipient requires access to specific classified information in order to perform or assist in a lawful and authorized governmental function.

Original Classification. An initial determination that information requires, in the interest of national security, protection against unauthorized disclosure.

Original Classification Authority. An individual authorized in writing, either by the President, or by agency heads or other officials designated by the President, to originally classify information.

Regrade. To raise or lower the classification assigned to an item of information.

Secret Information. Information, the unauthorized disclosure of which reasonably could be expected to cause serious damage to the national security that the original classification authority is able to identify or describe.

Telecommunications. The preparation, transmission, or communication of information by electronic means.

Top Secret. Information, the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to the national security that the original classification authority is able to identify or describe.

AWARD/CONTRACT		1. THIS CONTRACT IS A RATED ORDER UNDER DPAS (15 CFR 350)		RATING	PAGE OF PAGES 1 9
2. CONTRACT (Proc Inst Ident) NO. HQDC-06-D-00017/HSHQDC-08-J-00138			3. EFFECTIVE DATE 06/02/2008	4. REQUISITION/PURCHASE REQUEST/PROJECT NO. RUIO-08-00273	
5. ADMINISTERED BY (if other than Item 5) DHS/OPO/ITAC		6. ADMINISTERED BY (if other than Item 5) DHS/OPO/ITAC			
U.S. Dept. of Homeland Security Office of Procurement Operations Information Tech. Acquisition Div. 245 Murray Lane, SW Building 410 Washington DC 20528			Department of Homeland Security Office of Procurement Ops. (ITAC) 245 Murray Drive Bldg. 410 Washington DC 20528		

7. NAME AND ADDRESS OF CONTRACTOR (No., Street, City, Country, State and ZIP Code) LOCKHEED MARTIN SERVICES INC 2339 ROUTE 70 WEST FLOOR 3W CHERRY HILL NJ 080023315		8. DELIVERY <input type="checkbox"/> FOB ORIGIN <input checked="" type="checkbox"/> OTHER (See below)	
		9. DISCOUNT FOR PROMPT PAYMENT Net 30	
10. SUBMIT INVOICES (4 copies unless otherwise specified) TO THE ADDRESS SHOWN IN		ITEM	
CODE 8052583730000	FACILITY CODE		

11. SHIP TO/MARK FOR Department of Homeland Security 245 Murray Lane Bldg. 410 Washington DC 20528		12. PAYMENT WILL BE MADE BY Department of Homeland Security Departmental Operations Branch Room 3621 245 Murray Lane, SW Building 410 Washington DC 20528	
CODE DHS	CODE DHS-MANAGEMENT (D)		

13. AUTHORITY FOR USING OTHER THAN FULL AND OPEN COMPETITION: <input type="checkbox"/> 10 U.S.C. 2304 (c) () <input type="checkbox"/> 41 U.S.C. 253 (c) ()		14. ACCOUNTING AND APPROPRIATION DATA See Schedule			
ITEM NO	15B. SUPPLIES/SERVICES	15C. QUANTITY	15D. UNIT	15E. UNIT PRICE	15F. AMOUNT
Continued					
15G. TOTAL AMOUNT OF CONTRACT					\$40,168,230.00

16. TABLE OF CONTENTS							
(X)	SEC.	DESCRIPTION	PAGE(S)	(X)	SEC.	DESCRIPTION	PAGE(S)
PART I - THE SCHEDULE				PART II - CONTRACT CLAUSES			
	A	SOLICITATION/CONTRACT FORM			I	CONTRACT CLAUSES	
	B	SUPPLIES OR SERVICES AND PRICES/COSTS		PART III - LIST OF DOCUMENTS, EXHIBITS AND OTHER ATTACH.			
	C	DESCRIPTION/SPECS./WORK STATEMENT			J	LIST OF ATTACHMENTS	
	D	PACKAGING AND MARKING		PART IV - REPRESENTATIONS AND INSTRUCTIONS			
	E	INSPECTION AND ACCEPTANCE			K	REPRESENTATIONS, CERTIFICATIONS AND OTHER STATEMENTS OF OFFERORS	
	F	DELIVERIES OR PERFORMANCE			L	INSTRS., CONDS., AND NOTICES TO OFFERORS	
	G	CONTRACT ADMINISTRATION DATA			M	EVALUATION FACTORS FOR AWARD	
	H	SPECIAL CONTRACT REQUIREMENTS					

CONTRACTING OFFICER WILL COMPLETE ITEM 17 OR 18 AS APPLICABLE

17. <input checked="" type="checkbox"/> CONTRACTOR'S NEGOTIATED AGREEMENT (Contractor is required to sign this document and return 1 copies to Issuing office.) Contractor agrees to furnish and deliver all items or perform all the services set forth or otherwise identified above and on any continuation sheets for the consideration stated herein. The rights and obligations of the parties to this contract shall be subject to and governed by the following documents: (a) this award/contract, (b) the solicitation, if any, and (c) such provisions, representations, certifications, and specifications, as are attached or incorporated by reference herein. (Attachments are listed herein.)		18. <input type="checkbox"/> AWARD (Contractor is not required to sign this document) Your offer on Solicitation Number _____ including the additions or changes made by you which additions or changes are set forth in full above, is hereby accepted as to the items listed above and on any condition sheets. This award consummates the contract which consists of the following documents: (a) the Government's solicitation and your offer, and (b) this award/contract. No further contractual document is necessary.	
19A. NAME AND TITLE OF SIGNER (Type or print) <i>Barbara L. Donigan, Contracts Manager</i>		20A. NAME OF CONTRACTING OFFICER Charles Conrad	
19B. NAME OF CONTRACTOR		20B. UNITED STATES OF AMERICA	
19C. DATE SIGNED 5 June 2008		20C. DATE SIGNED 6/5/08	
Signature of person authorized to sign		Signature of the Contracting Officer	

Contract Base Award

CONTINUATION SHEET

REFERENCE NO. OF DOCUMENT BEING CONTINUED
HSHQDC-06-D-00017/HSHQDC-08-J-00138

PAGE OF
2 9

NAME OF OFFEROR OR CONTRACTOR

CKHEED MARTIN SERVICES INC

ITEM NO. (A)	SUPPLIES/SERVICES (B)	QUANTITY (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)
0001	<p>DUNS Number: 805258373+0000 Request for Proposals dated June 19, 2007 with Amendments 1 through 13, Section 2.0, Technical Capability of the contractor's proposal dated August 31, 2007 and September 19, 2007 and contractor's labor rate schedule dated May 30, 2008 are hereby incorporated into this task order to form an integral part of this contract.</p> <p>The ceiling for this task order is \$288,499,204. FOB: Destination Period of Performance: 06/01/2008 to 01/31/2013</p> <p>Base Year Operations and Maintenance Support Services (HSD) NTE \$29,789,173.00</p> <p>Accounting Info: RWC8049 RWC WF-99-01-00-000-02-05-0000-00-00-00-00 GE OE 25 84 FY2008 Funded: \$12,625,516.00</p> <p>Accounting Info: SCAC008-000-IX-22-11-02-000-02-05-0000-00-00-00-00 -GE-OE-25-41-EM0122 Funded: \$130,000.00</p> <p>Accounting Info: SCAC008-000-IX-22-11-02-000-02-05-0000-00-00-00-00 -GE-OE-25-44-S00024 Funded: \$400,000.00</p> <p>Accounting Info: RWC8049 RWC WF-99-01-00-000-02-05-0000-00-00-00-00 GE OE 25 44 FY2008 Funded: \$6,707,462.00</p> <p>Accounting Info: RWC8049 RWC WF-99-01-00-000-02-05-0000-00-00-00-00 GE OE 31 18 FY2008 Funded: \$7,173,043.00</p> <p>Accounting Info: RWC8049 RWC WF-99-01-00-000-02-05-0000-00-00-00-00 GE OE 25 76 FY2008 Funded: \$2,331,776.00</p> <p>Accounting Info: RWC8049 RWC WF-99-01-00-000-02-05-0000-00-00-00-00 GE OE 25 Continued ...</p>				29,789,173.00

CONTINUATION SHEET

REFERENCE NO OF DOCUMENT BEING CONTINUED
 HSHQDC-06-D-00017/HSHQDC-08-J-00138

PAGE OF
 3 9

NAME OF OFFEROR OR CONTRACTOR

CKHEED MARTIN SERVICES INC

ITEM NO. (A)	SUPPLIES/SERVICES (B)	QUANTITY (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)
	74 FY2008 Funded: \$421,376.00 Period of Performance: 06/05/2008 to 01/31/2009				
0002	Base Year Operations and Maintenance Support Services ODC's HSD NTE \$6,000,000 Award Type: Time-and-materials Accounting Info: RWC8049 RWC WF-99-01-00-000-02-05-0000-00-00-00-00 GE OE 25 84 FY2008 Funded: \$6,000,000.00 Period of Performance: 06/01/2008 to 01/31/2009				6,000,000.00
0003	Base Year Spectrum Support Services ESD NTE \$1,080,000 Award Type: Time-and-materials Accounting Info: WLP007-000-IX-22-12-00-000-02-05-0000-00-00-00-00 GE OE 25 44 WL0032 Funded: \$1,080,000.00 Period of Performance: 06/01/2008 to 01/31/2009				1,080,000.00
0004	Base Year Spectrum ODCs ESD NTE \$20,000 Award Type: Time-and-materials Accounting Info: WLP007-000-IX-22-12-00-000-02-05-0000-00-00-00-00 GE OE 25 44 WL0032 Funded: \$20,000.00 Period of Performance: 06/01/2008 to 01/31/2009				20,000.00
0005	Base Year Infrastructure Transformation Program (ITP) ESD NTE \$830,916.80 Award Type: Time-and-materials Accounting Info: SCAC007-000-IX-22-11-02-000-02-05-0000-00-00-00-00 -GE-OE-25-44-EP0012 Continued ...				830,916.80

CONTINUATION SHEET

REFERENCE NO. OF DOCUMENT BEING CONTINUED
 HSHQDC-06-D-00017/HSHQDC-08-J-00138

PAGE OF
 4 9

NAME OF OFFEROR OR CONTRACTOR

CKHEED MARTIN SERVICES INC

ITEM NO. (A)	SUPPLIES/SERVICES (B)	QUANTITY (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)
0006	Funded: \$830,916.80 Period of Performance: 06/01/2008 to 01/31/2009 Base Year Infrastructure Transformation Program ODC's ESD NTE \$40,000 Award Type: Time-and-materials Accounting Info: SCAC007-000-IX-22-11-02-000-02-05-0000-00-00-00-00 (GE) OE 25 44 EP0012 Funded: \$40,000.00 Period of Performance: 06/01/2008 to 01/31/2009				40,000.00
0007	Base Year Security Support Services ESD NTE \$690,977.20 Award Type: Time-and-materials Amount: \$452,987.00 Accounting Info: IFSR008-000-IX-22-10-05-000-02-05-0000-00-00-00-00 -GE OE 25 44 SC0032 Funded: \$452,987.00 Amount: \$237,990.20 Accounting Info: OINF008-000-IT-21-14-10-000-02-05-0500-00-00-00-00 -GE OE 25 44 SC0021 Funded: \$237,990.20 Period of Performance: 06/01/2008 to 01/31/2009				690,977.20
0008	Base Year Security Support Services ODC's ESD NTE \$40,000 Award Type: Time-and-materials Accounting Info: OINF008-000-IT-21-14-10-000-02-05-0500-00-00-00-00 -GE OE 25 44 SC0021 Funded: \$40,000.00 Period of Performance: 06/01/2008 to 01/31/2009				40,000.00
0009	Base Year DHS Headquarters Coop Support and Exercises NTE \$1,677,163 Award Type: Time-and-materials Continued ...				1,677,163.00

CONTINUATION SHEET

REFERENCE NO. OF DOCUMENT BEING CONTINUED
 HSHQDC-06-D-00017/HSHQDC-08-J-00138

PAGE OF
 5 9

NAME OF OFFEROR OR CONTRACTOR

CKHEED MARTIN SERVICES INC

ITEM NO. (A)	SUPPLIES/SERVICES (B)	QUANTITY (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)
	Accounting Info: NONE008-000-MA-20-01-00-000-02-07-0800-00-00-00-00 -GE-OE-25-44-000000 Funded: \$1,677,163.00 Period of Performance: 06/01/2008 to 01/31/2009				
0010	Option Year 1 Operations and Maintenance Support Services HSD NTE \$50,244,421.00 Award Type: Time-and-materials Amount: \$50,244,421.00 (Option Line Item) Product/Service Code: D399 Product/Service Description: OTHER ADP & TELECOMMUNICATIONS SERVICES Period of Performance: 02/01/2009 to 01/31/2010				0.00
0011	Option Year 1 Operations and Maintenance Support Services ODCs HSD NTE \$6,000,000.00 Award Type: Time-and-materials Amount: \$6,000,000.00 (Option Line Item) Product/Service Code: D399 Product/Service Description: OTHER ADP & TELECOMMUNICATIONS SERVICES Period of Performance: 02/01/2009 to 01/31/2010				0.00
0012	Option Year 1 Wireless Management Office ESD NTE \$3,996,518.00 Award Type: Time-and-materials Amount: \$3,996,518.00 (Option Line Item) Product/Service Code: D399 Product/Service Description: OTHER ADP & TELECOMMUNICATIONS SERVICES Period of Performance: 02/01/2009 to 01/31/2010				0.00
0013	Option Year 1 Wireless Management Office ODCs ESD NTE \$120,000.00 Award Type: Time-and-materials Amount: \$120,000.00 (Option Line Item) Product/Service Code: D399 Product/Service Description: OTHER ADP & TELECOMMUNICATIONS SERVICES Period of Performance: 02/01/2009 to 01/31/2010 Continued ...				0.00

CONTINUATION SHEET

REFERENCE NO. OF DOCUMENT BEING CONTINUED
 HSHQDC-06-D-00017/HSHQDC-08-J-00138

PAGE OF
 6 9

NAME OF OFFEROR OR CONTRACTOR

CKHEED MARTIN SERVICES INC

ITEM NO. (A)	SUPPLIES/SERVICES (B)	QUANTITY (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)
0014	Option Year 2 Operations and Maintenance Support Services (HSD) NTE \$51,371,156.00 Award Type: Time-and-materials Amount: \$51,371,156.00 (Option Line Item) Accounting Info: RWC8049 RWC WF-99-01-00-000-02-05-0000-00-00-00-00 GE OE 25 84 FY2008 Funded: \$0.00 Accounting Info: SCAC008-000-IX-22-11-02-000-02-05-0000-00-00-00-00 -GE-OE-25-41-EM0122 Funded: \$0.00 Accounting Info: SCAC008-000-IX-22-11-02-000-02-05-0000-00-00-00-00 -GE-OE-25-44-S00024 Funded: \$0.00 Accounting Info: RWC8049 RWC WF-99-01-00-000-02-05-0000-00-00-00-00 GE OE 25 44 FY2008 Funded: \$0.00 Accounting Info: RWC8049 RWC WF-99-01-00-000-02-05-0000-00-00-00-00 GE OE 31 18 FY2008 Funded: \$0.00 Accounting Info: RWC8049 RWC WF-99-01-00-000-02-05-0000-00-00-00-00 GE OE 25 76 FY2008 Funded: \$0.00 Accounting Info: RWC8049 RWC WF-99-01-00-000-02-05-0000-00-00-00-00 GE OE 25 74 FY2008 Funded: \$0.00 Period of Performance: 02/01/2010 to 01/31/2011				0.00
0015	Option Year 2 Operations and Maintenance Support Services ODCs HSD NTE \$6,000,000.00 Award Type: Time-and-materials Amount: \$6,000,000.00 (Option Line Item) Product/Service Code: D399 Continued ...				0.00

CONTINUATION SHEET

REFERENCE NO OF DOCUMENT BEING CONTINUED
 HSHQDC-06-D-00017/HSHQDC-08-J-00138

PAGE OF
 7 9

NAME OF OFFEROR OR CONTRACTOR

CKHEED MARTIN SERVICES INC

ITEM NO. (A)	SUPPLIES/SERVICES (B)	QUANTITY (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)
0016	Product/Service Description: OTHER ADP & TELECOMMUNICATIONS SERVICES Period of Performance: 02/01/2010 to 01/31/2011 Option Year 2 Wireless Management Office ESD NTE \$4,115,942.00 Award Type: Time-and-materials Amount: \$4,115,942.00 (Option Line Item) Product/Service Code: D399 Product/Service Description: OTHER ADP & TELECOMMUNICATIONS SERVICES Period of Performance: 02/01/2010 to 01/31/2011				0.00
0017	Option Year 2 Wireless Management Office ODCs ESD NTE \$120,000.00 Award Type: Time-and-materials Amount: \$120,000.00 (Option Line Item) Product/Service Code: D399 Product/Service Description: OTHER ADP & TELECOMMUNICATIONS SERVICES Period of Performance: 02/01/2010 to 01/31/2011				0.00
0018	Option Year 3 Operations and Maintenance Support Services HSD NTE \$52,442,323.00 Award Type: Time-and-materials Amount: \$52,442,323.00 (Option Line Item) Product/Service Code: D399 Product/Service Description: OTHER ADP & TELECOMMUNICATIONS SERVICES Period of Performance: 02/01/2011 to 01/31/2012				0.00
0019	Option Year 3 Operations and Maintenance Support Services ODCs HSD NTE \$6,000,000.00 Award Type: Time-and-materials Amount: \$6,000,000.00 (Option Line Item) Product/Service Code: D399 Product/Service Description: OTHER ADP & TELECOMMUNICATIONS SERVICES Period of Performance: 02/01/2011 to 01/31/2012				0.00
0020	Option Year 3 Wireless Management Office Continued ...				0.00

CONTINUATION SHEET

REFERENCE NO. OF DOCUMENT BEING CONTINUED
 HSHQDC-06-D-00017/HSHQDC-08-J-00138

PAGE OF
 8 9

NAME OF OFFEROR OR CONTRACTOR

OCKHEED MARTIN SERVICES INC

ITEM NO. (A)	SUPPLIES/SERVICES (B)	QUANTITY (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)
	ESD NTE \$4,238,554.00 Award Type: Time-and-materials Amount: \$4,238,554.00 (Option Line Item) Product/Service Code: D399 Product/Service Description: OTHER ADP & TELECOMMUNICATIONS SERVICES Period of Performance: 02/01/2011 to 01/31/2012				
0021	Option Year 3 Wireless Management Office ODCs ESD NTE \$120,000.00 Award Type: Time-and-materials Amount: \$120,000.00 (Option Line Item) Product/Service Code: D399 Product/Service Description: OTHER ADP & TELECOMMUNICATIONS SERVICES Period of Performance: 02/01/2011 to 01/31/2012				0.00
0022	Option Year 4 Operations and Maintenance Support Services HSD NTE \$53,075,751.00 Award Type: Time-and-materials Amount: \$53,075,751.00 (Option Line Item) Product/Service Code: D399 Product/Service Description: OTHER ADP & TELECOMMUNICATIONS SERVICES Period of Performance: 02/01/2012 to 01/31/2013				0.00
0023	Option Year 4 Operations and Maintenance Support Services ODCs HSD NTE \$6,000,000.00 Award Type: Time-and-materials Amount: \$6,000,000.00 (Option Line Item) Product/Service Code: D399 Product/Service Description: OTHER ADP & TELECOMMUNICATIONS SERVICES Period of Performance: 02/01/2012 to 01/31/2013				0.00
0024	Option Year 4 Wireless Management Office ESD NTE \$4,366,310.00 Award Type: Time-and-materials Amount: \$4,366,310.00 (Option Line Item) Product/Service Code: D399 Product/Service Description: OTHER ADP & Continued ...				0.00

CONTINUATION SHEET

REFERENCE NO. OF DOCUMENT BEING CONTINUED
 HSHQDC-06-D-00017/HSHQDC-08-J-00138

PAGE OF
 9 9

NAME OF OFFEROR OR CONTRACTOR

CKHEED MARTIN SERVICES INC

ITEM NO. (A)	SUPPLIES/SERVICES (B)	QUANTITY (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)
0025	TELECOMMUNICATIONS SERVICES Period of Performance: 02/01/2012 to 01/31/2013 Option Year 4 Wireless Management Office ODCs ESD NTE \$120,000.00 Award Type: Time-and-materials Amount: \$120,000.00 (Option Line Item) Product/Service Code: D399 Product/Service Description: OTHER ADP & TELECOMMUNICATIONS SERVICES Period of Performance: 02/01/2012 to 01/31/2013 The total amount of award: \$288,499,205.00. The obligation for this award is shown in box 15G.				0.00

Mod #1

AMENDMENT OF SOLICITATION/MODIFICATION OF CONTRACT		1. CONTRACT ID CODE	PAGE OF PAGES 1 8
2 AMENDMENT/MODIFICATION NO. P0C001	3 EFFECTIVE DATE See Block 16C	4. REQUISITION/PURCHASE REQ NO	5 PROJECT NO (If applicable)
ISSUED BY .S. Dept. of Homeland Security Office of Procurement Operations Information Tech. Acquisition Div. 245 Murray Lane, SW Building 410 Washington DC 20528	CODE DHS/OPO/ITAC	7 ADMINISTERED BY (If other than Item 6) Department of Homeland Security Office of Procurement Ops. (ITAC) 245 Murray Drive Bldg. 410 Washington DC 20528	CODE DHS/OPO/ITAC
8 NAME AND ADDRESS OF CONTRACTOR (No. street, county, State and ZIP Code) LOCKHEED MARTIN SERVICES INC 2339 ROUTE 70 WEST FLOOR 3W CHERRY HILL NJ 080023315		(x) 9A. AMENDMENT OF SOLICITATION NO	9B. DATED (SEE ITEM 11)
CODE 8052583730000	FACILITY CODE	X 10A. MODIFICATION OF CONTRACT/ORDER NO. HSHQDC-06-D-00017 HSHQDC-08-J-00138	10B. DATED (SEE ITEM 11) 06/02/2008

11. THIS ITEM ONLY APPLIES TO AMENDMENTS OF SOLICITATIONS

The above numbered solicitation is amended as set forth in Item 14. The hour and date specified for receipt of Offers is extended. is not extended.
Offers must acknowledge receipt of this amendment prior to the hour and date specified in the solicitation or as amended, by one of the following methods: (a) By completing Items 8 and 15, and returning _____ copies of the amendment; (b) By acknowledging receipt of this amendment on each copy of the offer submitted; or (c) By separate letter or telegram which includes a reference to the solicitation and amendment numbers. FAILURE OF YOUR ACKNOWLEDGEMENT TO BE RECEIVED AT THE PLACE DESIGNATED FOR THE RECEIPT OF OFFERS PRIOR TO THE HOUR AND DATE SPECIFIED MAY RESULT IN REJECTION OF YOUR OFFER. If by virtue of this amendment you desire to change an offer already submitted, such change may be made by telegram or letter, provided each telegram or letter makes reference to the solicitation and this amendment, and is received prior to the opening hour and date specified.

12. ACCOUNTING AND APPROPRIATION DATA (If required)
See Schedule

13. THIS ITEM ONLY APPLIES TO MODIFICATION OF CONTRACTS/ORDERS. IT MODIFIES THE CONTRACT/ORDER NO. AS DESCRIBED IN ITEM 14.

CHECK ONE	A. THIS CHANGE ORDER IS ISSUED PURSUANT TO: (Specify authority) THE CHANGES SET FORTH IN ITEM 14 ARE MADE IN THE CONTRACT ORDER NO. IN ITEM 10A.
	B. THE ABOVE NUMBERED CONTRACT/ORDER IS MODIFIED TO REFLECT THE ADMINISTRATIVE CHANGES (such as changes in paying office, appropriation date, etc.) SET FORTH IN ITEM 14, PURSUANT TO THE AUTHORITY OF FAR 43 103(b).
X	C. THIS SUPPLEMENTAL AGREEMENT IS ENTERED INTO PURSUANT TO AUTHORITY OF FAR 43.103 (a) (3) Mutual Agreement of Both Parties
	D. OTHER (Specify type of modification and authority)

E. IMPORTANT: Contractor is not. (X) is required to sign this document and return 1 copies to the issuing office.

14. DESCRIPTION OF AMENDMENT/MODIFICATION (Organized by UCF section headings, including solicitation/contract subject matter where feasible.)

DUNS Number: 805258373+0000
The purpose of this modification is to appoint the task order Contracting Officer's Technical Representative (COTR) and Sub-COTRs, change Section 5.14 of the Performance Work Statement and and establish the ceiling price for the purchase of Citrix licenses. Please see page 2 for modification details.
Period of Performance: 06/01/2008 to 01/31/2013

Except as provided herein, all terms and conditions of the document referenced in Item 9A or 10A, as heretofore changed, remains unchanged and in full force and effect.

15A NAME AND TITLE OF SIGNER (Type or print) Barbara L. Denigan BA CONTRACTS MGR	16A NAME AND TITLE OF CONTRACTING OFFICER (Type or print) Constance Fortune
15B CONTRACTOR/OFFEROR <i>(Signature)</i>	15C DATE SIGNED 10 Sept 08
16B UNITED STATES OF AMERICA	16C DATE SIGNED 9/10/2008
<i>(Signature of person authorized to sign)</i>	<i>(Signature of Contracting Officer)</i>

The purpose of this modification is to appoint the task order Contracting Officer's Technical Representative (COTR) and Sub-COTRs, replace Section 5.14 of the Performance Work Statement and establish the ceiling for the purchase of the CITRIX licenses.

Modification

1. Section G.3.2 COTR Designation of the task order is hereby changed to appoint Fawn Pettigrew as the COTR for task order HSHQDC-06-D-00017/ HSHQDC-08-J-00138. Tyrone Hamilton, Terrence Dixon, Robert Ellison, Dave Campbell, Rhonda Orndorff, Paul Beckman and Chris Lane are hereby appointed as Sub-COTRs for the task order.
2. Section C. 5.14 Wireless Services Management of the task order Performance Work Statement is hereby modified as follows:

C.5.14 Wireless Services Management

The Contractor shall provide support to ESD Wireless Services (WS) to include wireless coordination support, frequency management support, and frequency spectrum planning.

C.5.14.1 Wireless Coordination Support

The Contractor shall support ESD Wireless Services in facilitating the coordination of DHS wireless investments through the DHS Wireless Working Group (WWG). The Contractor shall perform the following tasks:

C.5.14.1.1 the Contractor shall provide support to include the development and tracking of program metrics, development and execution of program strategy, development of program governance documentation (e.g., MD4100 updates), and reporting.

C.5.14.1.2 The Contractor shall support the WWG through process development, development of Governance documentation and templates, facilitation of meetings, and managing communications.

C.5.14.1.3 The Contractor shall provide technical and operational subject matter expertise to support IT acquisition reviews and WWG investment/resource coordination efforts.

C.5.14.2 Frequency Management Support

The contractor shall perform frequency management functions as follows:

C.5.14.2.1 Provide proficient technical expertise for Spectrum Software tools and products such as Spectrum XXI and ATDI Hertz Warfare.

C.5.14.2.2 Assist with the daily selection, coordination, and processing of all radio frequency authorizations in support of DHS components. The selected/approved frequencies shall be registered by the contractor in the Government Master File, GMF.

C.5.14.2.3 Assist in the development of frequency plans that meet new communications requirements and improve methodologies for interoperability among the DHS components and key federal, state, and local partners.

C.5.14.2.4 Ensure that systems will neither cause nor receive harmful interference to or from other authorized users when placed in their intended operational environments.

C.5.14.2.5 Ensure accuracy of all frequency assignments by conducting “five-year-reviews” or “ten-year reviews” as required by NTIA regulations of all DHS GMF records.

C.5.14.3 Frequency Spectrum Planning

The contractor shall support Spectrum Planning as follows:

C.5.14.3.1 Develop and recommend frequency changes to eliminate technical incompatibilities, improve interoperability, and reduce and/or eliminate interference.

C.5.14.3.2 Refine the nationwide channel plan with the support of the WWG to include identifying frequencies and developing a logical structure for nationwide channels (e.g., component specific channels, DHS common channels, interoperability channels).

C.5.14.3.3 Develop a nationwide strategy to define optimal geographic spacing for frequency reuse zones; identify the number of frequencies needed for a successful regional/zone system design, use temporary transition frequencies (if required), and use permanent narrowband frequencies of the new wireless systems.

C.5.14.3.4 Prepare equipment and system certification documentation as required by NTIA regulations.

C.5.14.3.5 Coordinate new, proposed frequencies within DHS and with other federal departments and government agencies.

C.5.14.3.6 Prepare spectrum Planning analyses and documentation as directed, including documentation for spectrum management support of the National Response Framework (NRF) Emergency Support Function #2 – Communications (ESF #2).

C.5.14.4 Security Support

C.5.14.4.1 The contractor shall prepare a DHS Information Technology Services Office (ITSO), Enterprise Services Division (ESD) Security Management Approach and SOPs, Checklists and a DHS Information Technology Services Office Security Plan, for ESD operations, and submit to the COTR for approval. (CDRL C.5.10-1, Information

Technology Services Office Security Management Approach and SOPs, Checklists and
DHS Information Technology Services Office Security Plan)

C.5.14.4.2 The contractor shall identify and notify the COTR and the ESD Security Manager of any upgrades, updates, service packs, and patches determined to be incompatible with system or application specifications and proceed as directed by the COTR.

C.5.14.4.3 The contractor shall identify specific security weaknesses on target systems, and provide recommended techniques and/or improvements to strengthen the security of the target system.

C.5.14.4.4 The contractor shall manage and monitor all DHS security components including intrusion detection systems (IDSs) and PEPs. Security systems shall use an automated delivery function to the maximum extent possible to push anti-virus software signature updates to the desktops and provide the results to Information Technology Services Office NMC/SMC management for analysis. Security systems administration shall include the following:

C.5.14.4.5 The contractor shall monitor DHS systems for intrusion activity, and be prepared to take appropriate steps to mitigate any suspected intrusion while maintaining the availability of the system for all authorized users.

C.5.14.4.6 The contractor shall conduct computer forensics, law enforcement evidence collection and preservation efforts in support of the system.

C.5.14.4.7 The contractor shall conduct assessments quarterly (or as directed) at all major nodes, such as gateways and regional centers where data is stored and report the results of such findings to the COTR and the ESD Security Manager.

C.5.14.4.8 The contractor shall perform anti-virus scans of the entire DHS networks in accordance with the proscribed procedures in DHS Approved Maintenance Downtime as described in Section C.5.6.4.

C.5.14.4.9 For all new installations, system upgrades or routine maintenance, the contractor shall ensure all requested administrative requirements, compliance with DHS Security Architecture and hardening guidance. The contractor shall test to ensure that installation will be able to sustain and /or improve the operational and security posture of the systems prior to submission to CCB for approval.

C.5.14.4.10 The contractor, in coordination with DHS, shall determine the schedule for deploying Information Assurance and Vulnerability Alerts (IAVAs), patches, and service packs and document completion to the COTR and the ESD Security Manager.

C.5.14.4.11 The contractor shall provide monthly reports to the appropriate COTR and the ESD Security Manager on the success of the patch/service pack deployment, and any issues preventing completion. (CDRL C.5.10-4, Patch/Service Pack Deployment Report)

C.5.14.4.12 The contractor shall provide Weekly quad reports, in accordance with ITSO Standards, to the ESD Security Manager and other appropriate Technical Point of Contacts as directed by the COTR.

C.5.14.4.13 In response to potential threats to the DHS (and U.S. infrastructure assets in general), the Secretary of the DHS (SECDHS) may direct the elevation of the protection levels of the network and IT assets through the implementation of INFOCON levels. The INFOCON level is determined based upon an assessment of risk to the DHS networks. When directed by DHS, the Designated Accrediting Authority (DAA) will approve specific measures of protection for the networks.

C.5.14.4.14 The contractor shall implement INFOCON conditions within the DHS, and will track the attainment of the directed INFOCON level across the networks.

C.5.14.4.15 The contractor shall assist in the coordination of DHS INFOCON levels and that of external entities such as DOD as directed by the ESD Security Manager and the COTR.

C.5.14.4.16 The contractor shall develop, submit to the COTR for approval and follow SOPs and checklists to track the changes in INFOCON level and the attainment of the directed INFOCON. (CDRL C.5.10-8, INFOCON Level SOPs and Checklists)

C.5.14.4.17 The Information Technology Services Office SMC shall create SOPs based upon DHS policies to support the DHS Computer Network Defense Continuity of Operations Plan.

C.5.14.5 Data Center Infrastructure

C.5.14.5.1 The contractor will perform as the single point of contact for the Component, Managed Service Provider(s) (MSP) and DHS Data and Application Services Program Management Office. In this capacity the Contractor will “manage” the day-to-day interaction with the MSP to ensure the business needs of the Component are being satisfied.

C.5.14.5.2 Component Point of Contact for data center Operations and Maintenance

- Define/monitor Service Level Agreement’s (SLA) required by the Component.
- Escalate the systemic problems experienced by components to the DHS Data and Application Services Program Management Office
- Collaborate with IT Service Delivery on application deployment
- Educate IT Infrastructure on Component business

- Define and support business continuity requirements at the Data Centers

C.5.14.5.3 Component IT Strategic Planning

- Develop standards for migration planning

- Develop and collaborate in the development of IT Infrastructure Strategies with IT planning and architecture
- Provide input into IT planning and architecture on potential uses of emerging technologies on the conduct of Component Business
- Define new requirements to IT planning and architecture

C.5.14.5.4 Interact with the Managed Service Provider's Relationship Manager for:

- Transition and migration planning
- Day-to-day service delivery activities

C.5.14.5.5 Interact with the Component's Infrastructure Leader for:

- Physical consolidation planning and implementation
- Day-to-day service delivery activities
- Monitor component migration plan

C.5.14.6 Office Management

C.5.14.6.1 The contractor shall take initiative to identify, respond to problems, and propose solutions for issues that have a potential negative impact to the mission environment. The contractor shall analyze the operational environment, identify and propose solutions to improve the efficiency and effectiveness of the Information Technology Services Office.

C.5.14.6.2 Administrative Services: The contractor shall perform all related administrative services required to perform services such as, material requisitioning, documentation Quality Control (QC), status and tracking of ESD reports, develop and review correspondence for executive formatting/appropriateness; develop travel requests, develop and execute travel reimbursements, time and attendance monitoring, meeting coordination/scheduling and reception. The contractor shall maintain accurate and complete records, files, and libraries of or access to documents to such as Federal, state, and local regulations, codes, laws, technical manuals, manufacturer's instructions, Standard Operating Procedures (SOPs), and recommendations, which are necessary and related to the functions being performed. The contractor shall support DHS during audits and inspections, and provide support and responses to audit and inspection items (internal and external).

C.5.14.6.3 Submittal of Reports and Information: The contractor shall compile data, prepare required reports, and submit information as directed by the COTR. The reports include daily, weekly, monthly and annual reports the contractor shall submit at the specified time.

C.5.14.6.4 Ad hoc Requirements: Upon notification from the Government, the contractor shall provide management and technical information to the Government such as: (CDRL C.1.4-1, Ad hoc Requirements)

- Technical evaluation of suggestions
- Input for staff studies
- Fact sheets
- Audits
- Congressional inquiries
- One-time reports
- Recommendations for amending, revising, or originating Government regulations or policies within the scope of this Task Order
- Information requested by the CO/COTR on other interfacing Task Orders that support this effort

C.5.14.6.5 Paper File Archiving: The contractor shall prepare all correspondence in and maintain all files using DHS specific, and generally accepted commercial industry standards. All files, records, and documents maintained in the performance of this Task Order are Government property and the contractor shall return them upon completion or termination of the work.

C.5.14.6.6 Electronic File Archiving: The contractor shall provide daily, weekly, and monthly electronic file and system backups with copies provided at both an on site and off site storage location, per Government established processes and procedures.

C.5.14.6.7 Document Management: For all deliverables within this Task Order, the contractor shall implement document management to include version control and comment resolution such that each release has clear inventory of comments accepted/rejected as part of the version.

CDRL Deliverables:

CDRL Number	Task Order Section	Title	Format	Required Date	Frequency	Distribution
	C.5.14	SECURITY SUPPORT				
C.1.4-1	C.5.14.6.4	Ad hoc Requirements	Electronic / Paper	As directed by the COTR	As directed by the COTR	As directed by the COTR
C.5.10-1	C.5.14.4.1	Information Technology Services Office Security Management Approach and SOPs, Checklists and a DHS Information Technology Services	Electronic / Paper	Within 60 days of Task Order start	Update within one business day of changes	COTR ESD Sub-COTR Security Manager

CDRL Number	Task Order Section	Title	Format	Required Date	Frequency	Distribution
		Office Security Plan				
C.5.10-4	C.5.14.4.11	Patch Service Pack Deployment Reports	Electronic / Paper	Within one business day of Deployment	As Deployments are performed	COTR ESD Sub-COTR Security Manager
C.5.10-8	C.5.14.4.16	INFOCON Level SOPs and Checklists	Electronic / Paper	Within 60 days of Task Order start	Update within one business day of changes	COTR ESD Sub-COTR Security Manager

3. In accordance with the Purchase Agent Authority provided on June 30, 2008, Lockheed Martin is authorized to purchase CITRIX licenses on behalf of DHS. The Contractor shall use the prices provided in the Lockheed Martin quotation dated July 17, 2008 to purchase the CITRIX licenses. Purchases made under this authorization shall be billed against the HSD ODC Clin 2 and shall not exceed the quotation price of \$204,366.50.

4. All other terms and conditions unless modified herein remain in full force and effect.

AMENDMENT OF SOLICITATION/MODIFICATION OF CONTRACT		1. CONTRACT ID CODE	PAGE OF PAGES 1 2
2 AMENDMENT/MODIFICATION NO. P00002	3. EFFECTIVE DATE 09/11/2008	4. REQUISITION/PURCHASE REQ. NO. Sec Schedule	5 PROJECT NO. (if applicable)
6 ISSUED BY U.S. Dept. of Homeland Security Office of Procurement Operations Information Tech. Acquisition Div. 245 Murray Lane, SW Building 410 Washington DC 20528	CODE DHS/OPO/ITAC	7 ADMINISTERED BY (if other than item 6)	CODE DHS/OPO/ITAC
8 NAME AND ADDRESS OF CONTRACTOR (pub. or priv., county, state and ZIP Code) LOCKHEED MARTIN SERVICES INC 2339 ROUTE 70 WEST FLOOR 3W CHERRY HILL NJ 080023315		(X) 9A. AMENDMENT OF SOLICITATION NO. 9B. DATED (SEE ITEM 11)	X 10A. MODIFICATION OF CONTRACT/ORDER NO. HSHQDC-06-0-00017 HSHQDC-08-1-00138 10B. DATED (SEE ITEM 11) 06/02/2008
CODE 8052583730000	FACILITY CODE	11. THIS ITEM ONLY APPLIES TO AMENDMENTS OF SOLICITATIONS	

The above numbered solicitation is amended as set forth in item 14. The hour and date specified for receipt of offers is extended. is not extended. Offers must acknowledge receipt of this amendment prior to the hour and date specified in the solicitation or as amended by one of the following methods: (a) By completing items 8 and 15, and returning _____ copies of the amendment; (b) By acknowledging receipt of this amendment on each copy of the offer submitted; or (c) By separate letter or telegram which includes a reference to the solicitation and amendment numbers. FAILURE OF YOUR ACKNOWLEDGEMENT TO BE RECEIVED AT THE PLACE DESIGNATED FOR THE RECEIPT OF OFFERS PRIOR TO THE HOUR AND DATE SPECIFIED MAY RESULT IN REJECTION OF YOUR OFFER. If by virtue of this amendment you desire to change an offer already submitted, such change may be made by telegram or letter, provided each telegram or letter makes reference to the solicitation and this amendment, and is received prior to the opening hour and date specified.

12 ACCOUNTING AND APPROPRIATION DATA (if required)
 Not Decrease: -\$4,300,000.00
 RWC9049 PWC WF-99-01-00-000-02-05-0000-00-00-00-00 GE OF 25 F4 FY2008

13. THIS ITEM ONLY APPLIES TO MODIFICATION OF CONTRACTS/ORDERS. IT MODIFIES THE CONTRACT/ORDER NO. AS DESCRIBED IN ITEM 14.

CHECK ONE	A THIS CHANGE ORDER IS ISSUED PURSUANT TO: (Specify authority) THE CHANGES SET FORTH IN ITEM 14 ARE MADE IN THE CONTRACT ORDER NO. IN ITEM 10A.
	B THE ABOVE NUMBERED CONTRACT/ORDER IS MODIFIED TO REFLECT THE ADMINISTRATIVE CHANGES (such as changes in buying office, appropriation date, etc.) SET FORTH IN ITEM 14, PURSUANT TO THE AUTHORITY OF FAR 43.103(L).
X	C THIS SUPPLEMENTAL AGREEMENT IS ENTERED INTO PURSUANT TO AUTHORITY OF FAR 43.103 (a) (3) Mutual Agreement of Both Parties
	D OTHER (Specify type of modification and authority)

E. IMPORTANT: Contractor is not, is required to sign this document and return _____ 1 _____ copies to the issuing office.

14 DESCRIPTION OF AMENDMENT/MODIFICATION (Organized by UCF section headings, including solicitation/contract subject matter where feasible.)

DDNS Number: 305258373+0000

The purpose of this modification is to de-obligate funding from Clin 2 HSD OIG's at the task order.

Modification

1. The total amount of obligated funding for Clin 2 is hereby reduced from \$6,000,000.00 by \$4,300,000.00 to \$1,700,000.00. The total amount of obligated funding for Clin 2 is \$1,700,000.00.

2. The total amount of obligated funding of the task order is reduced from \$40,168,231.00
Continued ...

Except as provided herein, all terms and conditions of the document referenced in item 5A or 10A, as hereinafter changed, remains unchanged and in full force and effect.

15A NAME AND TITLE OF SIGNER (Type or print) Barbara L. Donigan, Contracts Mgr	16A NAME AND TITLE OF CONTRACTING OFFICER (Type or print) Constance Fortune
15B CONTRACTOR OFFEROR <i>(Signature)</i>	15C DATE SIGNED 16 Sep 08
16B UNITED STATES OF AMERICA <i>(Signature)</i>	16C DATE SIGNED 9/17/2008

CONTINUATION SHEET	REFERENCE NO. OF DOCUMENT BEING CONTINUED	PAGE OF
	HSHQDC-06-D-00017/HSHQDC-08-J-00138/P00002	2

NAME OF OFFEROR OR CONTRACTOR
 LOCKHEED MARTIN SERVICES INC

ITEM NO (A)	SUPPLIES/SERVICES (B)	QUANTITY (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)
	by \$4,300,000.00 to \$35,868,230.00. The total amount of obligated task order funding is \$35,868,230.00. 3. All other terms and conditions unless modified herein remain in full force and effect. Discount Terms: Net 30 Delivery Location Code: DHS Department of Homeland Security 245 Murray Lane Bldg. 410 Washington DC 20528 FOB: Destination Period of Performance: 06/01/2008 to 01/31/2013 Change Item 0002 to read as follows (amount shown is the obligated amount): 0002 Base Year Operations and Maintenance Support Services CDC's RSD NTR \$1,700,000.00 Award Type: Time-and-materials Requisition No: RUIO-08-00273, RUIO-08-00648 Period of Performance: 06/01/2008 to 01/31/2009				4,300,000.00

Mod. # 3

AMENDMENT OF SOLICITATION/MODIFICATION OF CONTRACT		1. CONTRACT NUMBER	PAGE OF PAGES
2. AMENDMENT/MODIFICATION NO.	3. EFFECTIVE DATE	4. REQUISITION/PURCHASE REQ. NO.	5. PROJECT NO. (if applicable)
P00003	10/30/2008		
6. ISSUED BY	7. ADMINISTERED BY (if other than item 6)	CODE	
DHS/OPO/ITAC	DHS/OPO/ITAC		
U.S. Dept. of Homeland Security Office of Procurement Operations Information Tech. Acquisition Div. 245 Murray Lane, SW Building 410 Washington DC 20528		U.S. Dept. of Homeland Security Office of Procurement Operations Information Tech. Acquisition Div. 245 Murray Lane, SW Building 410 Washington DC 20528	
8. NAME AND ADDRESS OF CONTRACTOR (Name, street, county, State and Zip Code)		9A. AMENDMENT OF SOLICITATION NUMBER	
LOCKHEED MARTIN SERVICES INC 2339 ROUTE 70 WEST FLOOR 3 W CHERRY HILL NJ 080023315			
9B. DATED (SEE ITEM 11)		10A. MODIFICATION OF CONTRACT NUMBER NO.	
		HSHQDC-06-D-00017 HSHQDC-06-J-00138	
10B. DATED (SEE ITEM 11)		10C. DATED (SEE ITEM 11)	
06/02/2008		06/02/2008	
CODE 8092583730000	FACILITY CODE		

11. THIS ITEM ONLY APPLIES TO AMENDMENTS OF SOLICITATIONS

The above numbered solicitation is amended as set forth in item 14. The hour and date specified for receipt of Offers must acknowledge receipt of this amendment prior to the hour and date specified in the solicitation or as amended, by one of the following methods: (a) By completing and returning copies of the amendment on each copy of the solicitation and amendment number. FAILURE OF YOUR ACKNOWLEDGMENT TO BE RECEIVED AT THE HOUR AND DATE SPECIFIED MAY RESULT IN REJECTION OF YOUR OFFER. If by separate letter or telegram which includes a reference to the solicitation and this amendment, and is received prior to the opening date and date specified.

is extended. is not extended.

12. ACCOUNTING AND APPROPRIATION DATA (required)
See Schedule

13. THIS ITEM ONLY APPLIES TO MODIFICATION OF CONTRACTS/ORDERS: IT MODIFIES THE CONTRACT/ORDER NO. DESCRIBED IN ITEM 14.

CHECK ONE	A. THIS CHANGE ORDER IS ISSUED PURSUANT TO: (Specify authority)	THE CHANGES SET FORTH IN ITEM 14 ARE MADE IN THE CONTRACT
	B. THE ABOVE NUMBERED CONTRACT/ORDER IS NOT INTENDED TO REPLICATE THE ADMINISTRATIVE CHANGES (such as changes in paying office, etc.) SET FORTH IN ITEM 14. PURSUANT TO THE AUTHORITY OF FAR 43.103(b).	
X	C. THIS SUPPLEMENTAL AGREEMENT IS ENTERED INTO PURSUANT TO FAR 43.103 (a) (3) Mutual Agreement of Both Parties	
	D. OTHER (Specify type of modification and authority)	

14. IMPORTANT: Contractor is required to sign this document and return 1 copies to the issuing office.

14. DESCRIPTION OF AMENDMENT/MODIFICATION (Organized by UCF section headings, including solicitation/contract subject matter where feasible)

DUNS Number: 805258373+000

The purpose of this modification is to incorporate the updated Key Personnel Listing and change the task order COVER.

MODIFICATION

1. In accordance with Section I.11, "Key Personnel or Facilities" of the task order, Technical Exhibit 1.7-00 Key Personnel Listing, effective as of October 23, 2008, is hereby incorporated into this task order. (See Attachment 1)

2. Changes made to the Key Personnel Listing are in bold type.

Continued ...

Except as provided herein, all terms and conditions of the document referenced in item 9A or 14A, as heretofore changed, remain unchanged and in full force and effect.

16A. NAME AND TITLE OF SIGNER (Type or print)	16B. NAME AND TITLE OF CONTRACTING OFFICER (Type or print)
Andrea Hansen Sr. Mgr Contracts	Constance Fortune
17A. DATE SIGNED	17B. DATE SIGNED
11/5/08	10/30/2008
(Signature of person authorized to sign)	(Signature of Contracting Officer)

CONTINUATION SHEET

REFERENCE NO. OF DOCUMENT BEING CONTINUED
 HSHQDC-06-D-00017/HSHQDC-08-J-00138/P00003

PAGE OF
 2 2

NAME OF OFFEROR OR CONTRACTOR
 LOCKHEED MARTIN SERVICES INC

ITEM NO. (A)	SUPPLIES/SERVICES (B)	QUANTITY (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)
	<p>3. Section G.3.2 COTR Designation of the task order is hereby changed to remove Fawn Pettigrew as the COTR and appoint Lattia Baker as the COTR.</p> <p>4. Fawn Pettigrew is hereby appointed as a Sub-COTR for the task order.</p> <p>Lattia Baker may be contacted at: Phone: 202-447-0091 Email: Lattia.Baker@dhs.gov</p> <p>All other terms and conditions unless modified herein remain unchanged and in full force and effect.</p> <p>Period of Performance: 06/01/2008 to 01/31/2013</p>				



**Key Personnel for IT-NOVA
23 October 2008**

Number	Labor Category	Originally Proposed Key Personnel	Interim Proposed Key Personnel (proposed substitutions bolded)	Proposed Key Personnel for Base Period (proposed substitutions bolded)
1	Program Manager	(b) (4)		
2	Deputy Program Manager			
3	Project Control Specialist			
4	Disaster Recovery Specialist			
5	Deployment Manager			
6	Systems Architect			
7	Systems Engineer			
8	SME Level III			
9	IT Security Specialist Level III			
10	Comm & Network Engineer Level IV			
11	Comm NW Mgr Level III			
12	COMSEC SME Level III			
13	Systems Ops Mgr Level III			
14	Systems Engineer Level III			
15	Help Desk Mgr (RC) Level III			
16	Help Desk Mgr (End User) Level III			
17	Comm Network Engineer Level IV			
18	Voice Comm Mgr Level III			
19	Comm Network Engineer (CATV) Level IV			
20	Bus Cas Analyst Level III			
21	Wireless Communications			
22	Executive Comms Manager			

AMENDMENT OF SOLICITATION/ MODIFICATION OF CONTRACT

1. CONTRACT NUMBER PAGE OF PAGE 5

2. AMENDMENT/MODIFICATION NO. P00004	3. EFFECTIVE DATE See Block 16C	4. REQUISITION/PURCHASE REQ. NO.	5. PROJECT NO. (If applicable)
6. ISSUED BY U.S. Dept. of Homeland Security Office of Procurement Operations Information Tech. Acquisition Div. 245 Murray Lane, SW Building 410 Washington DC 20528	CODE DHS/OPD, ITAC	7. ADMINISTERED BY (If other than Item 6) U.S. Dept. of Homeland Security Office of Procurement Operations Information Tech. Acquisition Div. 245 Murray Lane, SW Building 410 Washington DC 20528	CODE DHS/OPD/ ITAC
8. NAME AND ADDRESS OF CONTRACTOR (City, street, county, State and ZIP Code) LOCKHEED MARTIN SERVICES INC 2339 ROUTE 70 WEST FLOOR 3W CHERRY HILL NJ 080023315		9A. AMENDMENT OF SOLICITATION NO. (X)	
CODE 8052583730000		9B. DATED (SEE ITEM 11)	
FACILITY CODE		9C. MODIFICATION OF CONTRACT/ORDER NO. HSHQDC-06-D-00017 HSHQDC-08-J-00138 10B. DATED (SEE ITEM 11) 06/02/2008	

11. THIS ITEM ONLY APPLIES TO AMENDMENTS OF SOLICITATIONS

The above numbered solicitation is amended as set forth in Item 14. The hour and date specified for receipt of Offers must acknowledge receipt of this amendment prior to the hour and date specified for receipt of Offers. is extended. is not extended. Offers must acknowledge receipt of this amendment prior to the hour and date specified for receipt of Offers. The solicitation or as amended by one of the following methods: (a) By completing copies of the amendment; (b) By acknowledging receipt of this amendment on each copy of the offer submitted; or (c) By separate letter or telegram which includes a reference to the solicitation and amendment numbers. FAILURE OF YOUR ACKNOWLEDGEMENT TO BE RECEIVED AT THE PLACE DESIGNATED FOR THE RECEIPT OF OFFERS PRIOR TO THE HOUR AND DATE SPECIFIED MAY RESULT IN REJECTION OF YOUR OFFER. If by virtue of this amendment you desire to change an offer already submitted, such change must be made by telegram or letter, provided each telegram or letter makes reference to the solicitation and this amendment, and is received prior to the open hour and date specified.

12. ACCOUNTING AND APPROPRIATION DATA (If required)

See Schedule

13. THIS ITEM ONLY APPLIES TO MODIFICATION OF CONTRACTS/ORDERS. IF IT MODIFIES THE CONTRACT/ORDER NO. AS DESCRIBED IN ITEM 14.

CHECK ONE	A. THIS CHANGE ORDER (S IS ORDER NO. IN ITEM 10A.)	ED PURSUANT TO: (Specify authority)	THE CHANGES SET FORTH IN ITEM 14 ARE MADE IN THE CONTRACT
	B. THE ABOVE NUMBERED CONTRACT/ORDER IS MODIFIED TO REFLECT THE ADMINISTRATIVE CHANGES (such as changes in paying office, appropriation date, etc.) SET FORTH IN ITEM 14, PURSUANT TO THE AUTHORITY OF FAR 43.103(b)		
	C. THE SUPPLEMENTAL AGREEMENT IS ENTERED INTO PURSUANT TO AUTHORITY OF:		
X	FAR 43.103 (a) (3)	Mutual Agreement of Both Parties	
	D. OTHER (Specify type of modification and authority)		

E. IMPORTANT: Contractor is not is required to sign this document and return 1 copies to the issuing office.

14. DESCRIPTION OF AMENDMENT/MODIFICATION (Organized by UIC's when headings including solicitation/contract subject matter where feasible.)

DUNS Number: 805258373+000

The purpose of this modification is as follows:

1. Delete Section C Statement of Work (8/17/07)
2. Incorporate Section C Statement of Work (11/26/08)
3. Delete references of the Transition phase in period
4. Modify Section C.B Contract Data Requirement Listing
5. Revise Section F.2 Option to Extend the Term of the Contract

Modification

Period of Performance: 06 01/2008 to (1/31/2013

Except as provided herein, all terms and conditions of the document referred to in Item 8A or 14, as heretofore changed, remain unchanged and in full force and effect.

15A. NAME AND TITLE OF BUYER (Type or print) Zanetta Williams, Contracts Mgr.	15B. DATE SIGNED 12/23/08	15A. NAME AND TITLE OF CONTRACTING OFFICER (Type or print) Constance Portune	15B. DATE SIGNED 12/23/2008
16. CONTRACTING OFFICER'S SIGNATURE <i>[Signature]</i>	17. UNITED STATES OF AMERICA	16. CONTRACTING OFFICER'S SIGNATURE <i>[Signature]</i>	17. UNITED STATES OF AMERICA

HSHQDC-08-J-00133

P00001

Modification

1. Section C Statement of Work dated August 17, 2007 and Section C.5.14 Wireless Service: Management of modification P00001 dated September 10, 2008 are deleted in their entirety.
2. Section C Statement of Work dated November 26, 2008 is hereby incorporated in its entirety (See Attachment 1) Changes have been made to specific sections of the task order where bold and underlined text appears.
3. All references to the "Transition In" period are hereby deleted in their entirety. (See Attachment 1)

The following sections are hereby deleted in their entirety:

- a. C.1.12.1 Transition and Phase In
 - b. C.1.12.1.1 Transition Plan
 - c. C.1.12.1.2 Transition Tasks
 - d. C.1.12.1.3 Transition Ramp-Up
4. Section C.8 Contract Data Requirements Listing (CDRL) is hereby modified. Please see Attachment 2 for a summary of the Statement of Work revisions and CDRL deletions. Changes have been made to specific sections of the task order where bold text appears.
 5. Section F.2-Option to Extend the Term of the Contract (FAR 52.217-9)(Mar 2007)(a) is hereby changed as follows:

From:

(a) The Government may extend the term of this task order by written notice to the Contractor at any time within the term of the EAGLE contract, provided that the Government gives the Contractor a preliminary written notice of its intent to extend at least thirty (60) days before the contract expires. The preliminary notice does not commit the Government to an extension.

To:

(a) The Government may extend the term of this task order by written notice to the Contractor at any time within the term of the EAGLE contract, provided that the Government gives the Contractor a preliminary written notice of its intent to extend at least thirty (30) days before the contract expires. The preliminary notice does not commit the Government to an extension.

All other terms and conditions unless modified herein remain unchanged and in full force and effect.

U.S. DEPARTMENT OF HOMELAND SECURITY

TASK ORDER

For

**Information Technology Network Operations Virtual Alliance
(IT-NOVA)**

Operations and Maintenance (O&M)



November 26, 2008

TABLE OF CONTENTS

C.1	GENERAL INFORMATION	1
C.1.1	Introduction	1
C.1.2	Background	1
C.1.3	Span of Support	2
C.1.3.1	Service Model.....	2
C.1.3.2	Information Technology Services.....	2
C.1.3.3	Network Services.....	3
C.1.3.4	Network Interfaces.....	4
C.1.4	General Requirements	4
C.1.4.1	Contractor Responsibilities	4
C.1.4.2	Function-Specific Contractor Requirements.....	6
C.1.5	Layout of Section C	8
C.1.5.1	Section C Contents.....	8
C.1.5.2	Document Information	9
C.1.6	Required Reports and Meetings	9
C.1.6.1	Task Order Administration	9
C.1.6.2	Required Reports	10
C.1.6.3	Required Meetings	11
C.1.6.4	Function Specific Reports and Documents	12
C.1.7	Contractor Personnel.....	13
C.1.7.1	Key Personnel	13
C.1.7.2	Personnel Staffing	14
C.1.7.3	Personnel Training	15
C.1.7.4	Personnel Security Requirements	15
C.1.8	Contractor Interfaces	16
C.1.8.1	Personnel Performing Security/Continuity/Quality.....	16
C.1.9	Quality Assurance and Quality Control	17
C.1.9.1	Quality Assurance	17
C.1.9.2	Quality Control.....	17
C.1.10	Property Control	18
C.1.11	Operating Environment.....	18
C.1.11.1	Operating Hours	18

C.1.11.2	Operations Under Adverse Conditions.....	20
C.1.11.3	Travel	21
C.1.12	Contract Transition	22
C.1.12.1	Transition and Phase In.....	22
C.1.12.2	Phase Out	22
C.2	DEFINITIONS AND ACRONYMS	23
C.2.1	Definitions	23
C.2.2	Acronyms	35
C.3	GOVERNMENT – FURNISHED PROPERTY (GFP) AND SERVICES.....	45
C.3.1	Scope	45
C.3.1.1	Government-Furnished Property	45
C.3.1.2	Government-Furnished Services	45
C.3.1.3	Supplies and Materials	46
C.3.1.4	Government-Furnished Equipment (GFE)	46
C.4	CONTRACTOR – FURNISHED PROPERTY AND SERVICES	48
C.4.1	Scope	48
C.4.1.1	Contractor-Furnished Facilities (CFF).....	48
C.5	SCOPE OF WORK	49
C.5.1	Applications Management, Support, and Development	49
C.5.1.1	Application Management Services.....	49
C.5.1.2	Status and Availability of Major Applications on the Network	50
C.5.1.3	Application Maintenance and Operation Documentation.....	50
C.5.1.4	Application Database and Systems Maintenance	50
C.5.1.5	Performance Trends of Major Applications on the Network	51
C.5.1.6	Enterprise Desk Application Licensing.....	51
C.5.1.7	Collaborative Applications	51
C.5.1.8	Application Development	51
C.5.1.9	Ensure New Acquisitions Include Common Security Configurations	51
C.5.2	Deployment Support.....	52
C.5.2.1	Provide Deployment Support.....	52
C.5.2.2	Develop Deployment Plan Template.....	53
C.5.2.3	Site Activation.....	53
C.5.2.4	Facilities Modifications.....	53
C.5.2.5	Installation and Checkout	53

C.5.2.6	Transition to O&M.....	54
C.5.2.7	Engineering and Project Management.....	54
C.5.3	Infrastructure Engineering Services.....	54
C.5.3.1	On-site Engineering Team.....	54
C.5.3.2	Systems Engineering Support.....	54
C.5.3.3	Engineering Projects.....	55
C.5.3.4	Engineering Process and Methodology.....	56
C.5.4	Testing.....	57
C.5.4.1	Test Support and Documentation.....	57
C.5.4.2	Test and Development Lab.....	58
C.5.5	Operations and Maintenance For End User Support.....	59
C.5.5.1	End User and Desk Side Support.....	59
C.5.5.2	Maintenance.....	61
C.5.6	Video Teleconferencing.....	62
C.5.6.1	Video Teleconferencing (VTC).....	62
C.5.7	Satellite/Cable Television Operations.....	62
C.5.7.1	Operations.....	62
C.5.8	Voice Communications and Messaging.....	63
C.5.8.1	Private Branch Exchange (PBX) Infrastructure.....	63
C.5.8.2	Telephone Switchboard Operations Center.....	64
C.5.8.3	Voice Over Internet Protocol (VOIP).....	65
C.5.8.4	Unified Messaging.....	65
C.5.9	Network Management Center (NMC).....	65
C.5.9.1	NMC Operations.....	65
C.5.10	Security Management Center (SMC).....	68
C.5.10.1	SMC Operations.....	68
C.5.10.2	Vulnerability Assessment.....	69
C.5.10.3	Security Information Management (SIM) & Security Management Capability ...	69
C.5.10.4	Security Systems Administration.....	70
C.5.10.5	Security Change Management.....	70
C.5.10.6	Security Log Access, Retention and Review.....	71
C.5.10.7	System Security Administrators.....	71
C.5.10.8	Data Spills and Response.....	71
C.5.10.9	Incident Response.....	71

PROCUREMENT SENSITIVE

- C.5.10.10 Information Condition (INFOCON) Management 72
- C.5.11 Communications Security (COMSEC) Management..... 72
 - C.5.11.1 COMSEC Security 72
- C.5.12 Other Communications Operations..... 73
 - C.5.12.1 Emergency Notification System 73
 - C.5.12.2 Executive Telecommunications Support..... 73
- C.5.13 Training 74
 - C.5.13.1 System Administrator Training..... 74
 - C.5.13.2 Security Training..... 74
 - C.5.13.3 End-User Training 75
- C.5.14 Wireless Services Management (p00001) 75
 - C.5.14.1 Wireless Coordination Support 75
 - C.5.14.2 Frequency Management Support 75
 - C.5.14.3 Frequency Spectrum Planning..... 76
 - C.5.14.4 Security Support..... 76
 - C.5.14.5 Data Center Infrastructure 77
 - C.5.14.6 Office Management 78
 - C.5.14.6.5 Paper File Archiving. The contractor shall prepare all correspondence in and maintain all files using DHS specific, and generally accepted commercial industry standards. All files, records, and documents maintained in the performance of this Task Order are Government property and the contractor shall return them upon completion or termination of the work. 79
 - C.5.14.6.6 79
 - C.5.14.6.7 Document Management: For all deliverables within this Task Order, the contractor shall implement document management to include version control and comment resolution such that each release has clear inventory of comments accepted/rejected as part of the version. 79
- C.5.15 IT Continuity Management..... 79
 - C.5.15.1 Continuity Assessment 79
 - C.5.15.2 Continuity Planning..... 80
 - C.5.15.3 Continuity Reviews and Coordination 80
 - C.5.15.4 Continuity Program Administration 80
 - C.5.15.5 Testing and Exercises 81
 - C.5.15.6 Electronic Records 81
- C.6 APPLICABLE LAWS, PUBLICATIONS, AND FORMS 83**
 - C.6.1 General Information..... 83

PROCUREMENT SENSITIVE

C.6.1.1	Applicable Publications and Forms	83
C.6.1.2	Publication Conflict Resolution	83
C.6.2	Federal Publications	83
C.6.2.1	Federal Regulation and Guidelines	83
C.6.3	Other Publications	84
C.6.3.1	U.S. Congress-Public Law (PL) and United States Code (U.S.C.)	84
C.6.3.2	Executive Orders—Office of Management and Budget (OMB), Homeland Security Presidential Directive (HSPD) and Presidential Decision Directive	84
C.6.3.3	DHS Management Directive (MD)	85
C.6.3.4	DHS Regulations	87
C.6.3.5	DHS Guides	88
C.6.3.6	National Institute of Standards and Technology (NIST), Special Publications...	88
C.6.3.7	Federal Information Processing Standards Publications (FIPS PUBS)	89
C.6.4	Forms	89
C.7	TECHNICAL EXHIBITS	90
C.8	CONTRACT DATA REQUIREMENTS LISTING (CDRL)	93

C.1 GENERAL INFORMATION

C.1.1 INTRODUCTION

The contractor shall provide Information Technology (IT) support services to the Department of Homeland Security (DHS) headquarters, the department's Associate Components, select field offices of the department's Major Components and to other federal, state, and local level government organizations through this Information Technology Networking Operations Virtual Alliance (IT-NOVA) Operations & Maintenance (O&M) Task Order under the Enterprise Acquisition Gateway for Leading Edge Solutions (EAGLE) information Technology Support Services Contract. The support services include all network components, services, and monitoring; network and internet access; infrastructure transformation and support; applications management, delivery, and development; wireless communications systems management; communications and messaging; communications security (COMSEC); Continuity of Operations (COOP) planning; and IT operations disaster management. The contractor shall provide all labor to complete the services herein in accordance with the terms, conditions, and specifications of this Task Order. The contractor shall assume total responsibility for all requirements performed by incumbent contractors whose period of performance expires on or by the commencement date of this Task Order. In those instances where incumbent contractor periods of performance expire after the commencement date of this task order, the contractor shall assume responsibility of those requirements based upon the Government approved transition plan.

C.1.2 BACKGROUND

In March 2003, Congress passed the Homeland Security Act of 2003 (Public Law 107-296) creating a single department from 22 components that had previously resided in other agencies. One primary reason for the establishment of the Department of Homeland Security (DHS) was to provide the unifying core for the vast national network of organizations and institutions involved in efforts to secure our nation.

To comply with the new legislative requirement, the President directed the DHS Secretary to integrate the 22 legacy components into one organization and the DHS Secretary stated the objective to centrally manage services, including Information Technology (IT).

The DHS components are as follows:

- Associate Components
 - Office of the Secretary
 - Citizenship and Immigration Services, Ombudsman (CISOMB)
 - Civil Rights and Civil Liberties (CRCL)
 - Counternarcotics Enforcement (CNE)
 - Domestic Nuclear Detection Office (DNDO)
 - Executive Secretariat (ESEC)
 - Federal Emergency Management Agency (FEMA)
 - Office of the General Counsel (OGC)
 - Gulf Coast Region (GCR)
 - Office of Health Affairs (OHA)
 - Office of Intelligence and Analysis (I&A)

- Military Advisor's Office (MIL)
- National Protection and Programs Directorate (NPPD)
- Office of Inspector General (OIG)
- Office of Legislative Affairs (OLA)
- Office of Operations Coordination (OPS)
- Office of Policy (PLCY)
- Chief Privacy Officer (PRIV)
- Office of Public Affairs (OPA)
- Science and Technology (S&T)
- Major Components
 - Federal Law Enforcement Training Center (FLETC)
 - Transportation Security Administration (TSA)
 - United States Citizenship and Immigration Services (USCIS)
 - United States Coast Guard (USCG)
 - United States Customs and Border Protection (CBP)
 - United States Immigration and Customs Enforcement (ICE)
 - United States Secret Service (USSS)

TE C.1.2-001 is a chart of the DHS organizational structure. TE C.1.2-002 is a Sensitive But Unclassified listing of the locations supported by this Task Order.

The DHS Management Directorate is responsible for budgets and appropriations, expenditure of funds, accounting and finance, procurement, human resources, information technology systems, facilities and equipment, and the identification and tracking of performance measurements. Their mission is to ensure the DHS's more than 170,000 employees have well-defined responsibilities and those managers and their employees have effective means of communicating with one another, with other governmental and nongovernmental bodies, and with the public, they serve.

The DHS Office of the Chief Information Officer (OCIO) falls under the Management Directorate. Within the OCIO is the Information Technology Services Office whose mission is to provide IT services to the department. The contractor shall provide IT Support Services to the Information Technology Services Office throughout the duration of this Task Order. TE C.1.2-003 is a chart of the OCIO organizational structure.

C.1.3 SPAN OF SUPPORT

C.1.3.1 Service Model

The DHS uses the Information Technology Service Library (ITIL) version 2 framework as the basis for its service model. The contractor shall adopt the ITIL version 3 service model framework (Service Strategies, Service Design, Service Transition, Service Operation, and Continual Service Improvement) for the execution of the DHS IT System Development Life Cycle (SDLC).

C.1.3.2 Information Technology Services

C.1.3.2.1 The Contactor shall provide the DHS a full line of Information Technology (IT), telecommunications, and related services to manage the baseline requirements defined in this Task Order. The contractor shall provide IT

PROCUREMENT SENSITIVE

infrastructure services that conform to specified standards for reliability, readiness, sustainability, supportability, availability, stability, security, flexibility, responsiveness and cost effectiveness. DHS Headquarters and DHS Associate Components shall receive the entire range of support and monitoring as described in this Task Order. DHS Major Components and other Federal/State/Local/Tribal Government organizations that have connectivity to at least one of the three DHS networks shall receive the entire range of support and monitoring as described in this Task Order with the exception of Desk Side Support. However, these entities may require Desk Side Support in emergency situations facilitated through logical follow-on Task Orders. TE C.1.3-002 identifies the number of supported users by network for the FY06 to FY13 time frame.

- C.1.3.2.2 The contractor shall demonstrate a proactive and technologically aggressive methodology to identify and pursue new IT advancements, forecast IT trends and provide a comprehensive system of support. The support shall include conducting frequent and thorough market research of new or updated IT technologies, equipment, and data acquisition and availability including software based reporting and performing subjective and comparative analysis to existing DHS technology. If authorized by the COTR, the contractor shall perform and conduct operational and theoretical performance evaluations of current IT capabilities and propose recommended IT advancements.
- C.1.3.2.3 To effectively meet their mission objectives, DHS requires a robust, reliable, scalable, integrated, secure, and flexible IT Infrastructure support Task Order that employs methodologies to achieve mission and business-critical systems and applications in accordance with the DHS business critical system reliability levels identified in Table 1 below. An integrated IT infrastructure Task Order will provide for a more cohesive IT support structure for DHS. Improved information sharing via a consolidated, enterprise wide IT infrastructure support will achieve DHS' strategic goals and business objectives that consist of: awareness, prevention, protection, response, recovery, service, and organizational excellence.
- C.1.3.2.3.1 IT Support Services shall be governed by the DHS reliability levels for critical and non-critical systems identified in Table 1.

Table 1 – Reliability for Critical and Non-Critical Systems

Minimum Reliability Level	Hours of Unscheduled Downtime	Minutes of Unscheduled Downtime	Seconds of Unscheduled Downtime
99%	Up to 87.6	Up to 5,256	Up to 315,360
99.9%	Up to 8.76	Up to 525.6	Up to 31,536
99.99%	Up to .876	Up to 52.559	Up to 3,153.6
99.999%	Up to .0876	Up to 5.256	Up to 315.36

C.1.3.3 Network Services

The contractor shall provide IT Support Services for Unclassified, Classified, and Top Secret Networks. The extent of the support services for each of the networks is as follows:

PROCUREMENT SENSITIVE

- Unclassified and Top Secret Networks: The Headquarters and Associate Component locations identified in TE C.1.2-002 receive all the services described in this Task Order
- Classified Network – referred to as Homeland Security Data Network (HSDN): Certain Major Component field office locations, certain other Federal government organizations and select State and Local government organizations identified in TE C.1.2-002 receive all the services described in this Task Order with the exception of Desk-Side Support; however, Desk-Side Support may be required on an exception basis or in emergency cases only. For security the field office locations are not named and their information is provided in an aggregated manner by state.

C.1.3.4 Network Interfaces

The contractor shall provide, and maintain operability, of interfaces to multiple networks such as the following:

- DHS National Capital Region Metropolitan Area Network (MAN)
- DHS National Capital Region Wide Area Network (WAN)
- Homeland Security Information Network (HSIN)
- Homeland Security Information Network – Secret (HSIN-S)
- Director of National Intelligence – Secret (DNI-S)
- Secret Internet Protocol Router Network (SIPRnet)
- Joint Worldwide Intelligence Communications System (JWICS)

C.1.4 GENERAL REQUIREMENTS**C.1.4.1 Contractor Responsibilities**

The Government requires that the contractor adhere to and follow all applicable executive orders, presidential directives, other federal and DHS laws, federal orders management policies, handbooks, guidelines, processes, and procedures provided in section C-6. The contractor shall take initiative to identify, respond to problems, and propose solutions for issues that have a potential negative impact to the mission environment. The contractor shall analyze the operational environment, identify and propose solutions to improve the efficiency and effectiveness of the Information Technology Services Office.

C.1.4.1.1 Administrative Services: The contractor shall perform all related administrative services required to perform services such as, material requisitioning, Quality Control (QC), financial control (cost control and savings), status and tracking reports, and correspondence. The contractor shall also maintain accurate and complete records, files, and libraries of or access to documents to such as Federal, state, and local regulations, codes, laws, technical manuals, manufacturer's instructions, Standard Operating Procedures (SOPs), and recommendations, which are necessary and related to the functions being performed. The contractor shall support DHS during audits and inspections, and provide support and responses to audit and inspection items (internal and external).

C.1.4.1.2 Submittal of Reports and Information: The contractor shall compile data, prepare required reports, and submit information as specified by the Contract Data Requirements Lists (CDRLs), Section C.8, and as presented in this Task

PROCUREMENT SENSITIVE

Order. The reports include daily, weekly, monthly and annual reports the contractor shall submit at the specified time. The COTR will forward the approved reports to the proper Government element.

- C.1.4.1.3 Ad hoc Requirements: Upon notification from the Government, the contractor shall provide management and technical information to the Government such as: (CDRL C.1.4-1, Ad hoc Requirements)
- Technical evaluation of suggestions
 - Input for staff studies
 - Fact sheets
 - Audits
 - Congressional inquiries
 - One-time reports
 - Material, equipment, facilities, and other property listings or inventories
 - Equipment maintenance records
 - Recommendations for amending, revising, or originating Government regulations or policies within the scope of this Task Order
 - Information requested by the CO/COTR on other interfacing Task Orders that support this effort
- C.1.4.1.4 Paper File Archiving. The contractor shall prepare all correspondence in and maintain all files using DHS specific, and generally accepted commercial industry standards in accordance with the appropriate current National Archives and Record Administration (NARA), and General Records Schedule (36 Code of Federal Regulations (CFR) 122014 and 44 U.S.C. 3301). The website at <http://www.archives.gov/records-mgmt/ardor/records-schedules.html> contains the index of NARA schedules. All contractor files, records, and documents maintained in the performance of this Task Order are Government property and the contractor shall return them upon completion or termination of the work. However, internal proprietary contractor business files are not Government property.
- C.1.4.1.5 Electronic File Archiving: The contractor shall provide daily, weekly, and monthly electronic file and system backups with copies provided at both an on site and off site storage location, per Government established processes and procedures.
- C.1.4.1.6 Document Management: For all deliverables within this Task Order, the contractor shall implement document management to include version control and comment resolution such that each release has clear inventory of comments accepted/rejected as part of the version.
- C.1.4.1.7 Enterprise Architecture Compliance: All solutions and services shall meet DHS Enterprise Architecture policies, standards, and procedures as it relates to this Task Order. Specifically, the contractor shall comply with the following Homeland Security Enterprise Architecture (HLSEA) requirements:
- All developed solutions and requirements shall comply with the HLSEA
 - All IT hardware or software shall comply with the HLSEA Technical Reference Model (TRM) Standards and Products Profile

- The contractor shall submit all data assets, information exchanges and data standards, whether adopted or developed to the DHS Enterprise Data Management Office (EDMO) for review and insertion into the DHS Data Reference Model.

C.1.4.2 Function-Specific Contractor Requirements

C.1.4.2.1 Project Support: The purpose of this task is to provide project management support, monitoring, and lifecycle systems development methodologies for all DHS IT projects.

C.1.4.2.1.1 The contractor shall provide project management support to include executive level Information Assurance (IA), planning, implementation, reporting and other services as required or directed.

C.1.4.2.1.2 The contractor shall support projects by providing services such as: Development, coordination, scheduling, design validation, documentation, migration planning, writing service delivery guidance and other references, and weekly status reporting.

C.1.4.2.1.3 The contractor shall attend the Weekly Project Team Meeting and provide a summary of the Weekly Status Report. The contractor shall prepare support documentation for the Weekly Project Team Meeting (e.g. project issue updates, action issue updates, and project plan/status updates) to support the summary presentation.

C.1.4.2.2 Systems Security: The contractor shall ensure systems security for network environments, applications, databases, Internet, Portal and Intranet that allows access only by authorized users, prevention of unauthorized release of information, prevention of degradation due to circumstances such as unauthorized internal use and external intrusion, maintenance of data integrity, and authorized utilization by the user community.

C.1.4.2.3 Change Management Requirements: The contractor shall manage the Change Management process in accordance with the DHS Change Management Policy Process and Procedures and will maintain the Change Management Database. The Government will provide detailed Configuration Management Database information after Task Order award. The contractor shall comply with the DHS Change Management requirements for all equipment, hardware, system software, applications software (both source and executable), data files, and control-language.

C.1.4.2.4 Deliverables

C.1.4.2.4.1 Any change to the Task Order list of deliverables or the scheduled delivery date shall be coordinated with the COTR with a written copy to the CO for Task Order modification if required.

C.1.4.2.4.2 The contractor shall notify the appropriate project and DHS personnel when a deliverable is ready for review and provide the document online.

C.1.4.2.4.3 The contractor shall post, store and maintain all deliverables and all documentation produced pursuant to this Task Order on the DHS SharePoint Portal. The Project Management Office (PMO) shall be provided access to the Portal.

PROCUREMENT SENSITIVE

- C.1.4.2.4.4 The contractor shall review deliverables at appropriate points in the development process to verify accuracy, completeness, and timeliness of each deliverable product.
- C.1.4.2.5 Enterprise Architecture (EA) Compliance: The contractor shall perform work in compliance with the EA Plan. The contractor shall support and comply with the standards and technologies of the DHS target architecture as described in the DHS EA Blueprint. The source website for the DHS EA Blueprint is provided in Section C-6.
- C.1.4.2.6 Maintenance and Outages: The contractor shall perform maintenance and other related activities that degrade or may degrade the performance of network environments, operating systems, databases and applications during outage periods that occur on weekends, federal holidays, or between the hours of 10:00 pm ET and 6:00 am ET on weekdays. The contractor shall avoid performing these maintenance and other activities during periods of the year that require continuous availability 24 hours each day. The COTR will notify the contractor a minimum of five business days prior to periods requiring continuous availability.
- C.1.4.2.7 Program Development: The contractor shall establish and maintain a program for the enhancement and improvement of information technology services. (CDRL C.1.4-2, Information Technology Improvement Program) The contractor shall baseline the existing systems and infrastructure for items such as configuration and performance metrics. As part of the baseline the contractor shall submit an initial plan September 10, 2008 (has already occurred) defining timelines and operations, improvements based upon findings and supported by and compared to industry standards and metrics. The final IT Improvement Plan for the base year is due March 1, 2009. The Plan shall be re-baselined every year. The contractor shall conduct an analysis every six months or as required of future programmatic and cost requirements for information technology services for the DHS. A written analysis and recommendations shall be provided to the COTR within five business days of completing the analysis. An initial analysis will be performed and the report provided March 5, 2009 and subsequent analysis will be directed by the COTR. (CDRL C.1.4-3, Future Programmatic and Cost Requirements for IT Services) The contractor must base the analysis upon an assessment of the current information technology capabilities, evaluations of the operations efficiency of information technology, considerations regarding the adequacy of information technology, market surveys of new and emerging technologies, and technological developments that could improve the cost effectiveness of the delivery of information technology services. The contractor shall also consider the following factors in the analysis:
- Known future requirements and program requirements established or stated by the DHS authorization language contained in Congressional Committee bills.
 - Appropriation language
 - Programs and directives received from the Department of Labor and Office of Management and Budget
 - Budgetary information

PROCUREMENT SENSITIVE

- Information and requests received from other sources that utilize information technology services
- C.1.4.2.7.1 The contractor shall conduct an analysis that results in the identification of projects and initiatives necessary to support the needs of the DHS. The analysis shall also identify projects and initiatives that represent “State-of-the-Art” advancements in the capability supporting the DHS.
- C.1.4.2.8 Standard Operating Procedures: The contractor shall, prepare and submit separate Standard Operating Procedures (SOPs) for each of the Functional Areas listed in paragraph C.1.5.1.2. . (CDRL C.1.4-4, Standard Operating Procedures for Each Functional Area) The SOPs shall describe, at a minimum, the organization, methodology, approach, procedures, monitoring, auditing, problem escalation, documentation and reporting used by the contractor to accomplish the work required for the Functional Area. The COTR will review the Standard Operating Procedures and provide written comments to the contractor within ten business days following plan delivery to the COTR. The contractor shall address Government comments and deliver the final Standard Operating Procedures within five business days.
- C.1.4.2.9 Plans and Standard Operating Procedures: The contractor shall maintain and update all Plans and Standard Operating Procedures throughout the life of the Contract as changes occur or as directed by the COTR. The contractor shall submit in writing to the COTR changes in Plans and Standard Operating Procedures not less than 45 days prior to the desired date of implementation. The contractor shall not implement any changes until authorized in writing by the COTR. The contractor shall notify the Contracting Officer (CO) in writing of any changes that affect Task Order cost, Task Order requirements or terms and conditions and not implement these changes until receiving written approval from the CO.
- C.1.5 LAYOUT OF SECTION C**
- C.1.5.1 Section C Contents**
- C.1.5.1.1 Section C Structure: The following bullets identify the structure of Section C in this Task Order:
- C-1 General Information
 - C-2 Definitions and Acronyms
 - C-3 Government-Furnished Property (GFP) and Services
 - C-4 Contractor-Furnished Property and Services
 - C-5 Scope of Work
 - C-6 Applicable Laws, Publications, and Forms
 - C-7 Technical Exhibits
 - C-8 Contract Data Requirements List (CDRL)
- Paragraphs in Section C-1 all begin with the number “1,” paragraphs in Section C-2 all begin with the number “2,” and the pattern continues for the other sections.
- C.1.5.1.2 Functional Areas: Section C-5, Scope of Work, contains the Functional Areas which are organized into the following broad work categories:
- 5.1 Applications Management and Support Services

- 5.2 Deployment Support
- 5.3 Infrastructure Engineering Services
- 5.4 Testing
- 5.5 Operations and Maintenance for End User Support
- 5.6 Video Teleconferencing
- 5.7 Satellite/Cable TV Operations
- 5.8 Phone and PBX Operations
- 5.9 Network Management Center (NMC)
- 5.10 Security Management Center (SMC)
- 5.11 Communications Security Management
- 5.12 Other Communications Operations
- 5.13 Wireless Management
- 5.14 Training
- 5.15 IT Continuity Management

C.1.5.2 Document Information

C.1.5.2.1 **Pagination:** Pagination for all parts of the document is sequential with the prefix of “C” designating this as the Task Order Section of a Request for Proposal (RFP). Technical Exhibits have page numbers in relation to their TE title. For example, page three of TE C.5.2.-001 is shown as page number TE C.5.2.-001-03 to indicate that it is the third page of TE C.5.2.-001.

C.1.5.2.2 **Technical Exhibits:** Technical Exhibits provide supplementary information in forms of text, tables, graphs, or maps. Any part of the Task Order may reference Technical Exhibits. Technical Exhibits for Section C have a 5-digit number that links them to a designated Task Order Section. For example, Technical Exhibit 5.3-002 is the second Technical Exhibit referenced from Sub-Functional Area 5.3. Section C-7 contains all Technical Exhibits except those maintained on the DHS Interactive website.

C.1.5.2.3 **Contract Data Requirements List (CDRL):** The contractor shall compile historical data, prepare required reports, and submit information as specified by CDRLs in this Task Order. CDRLs may be referenced from any part of the Task Order. CDRLs for Section C have a two-digit number, which links them to a designated Task Order Section, e.g., CDRL C.5.3-1, is the first CDRL referenced in Section C.5.3. A listing of all CDRLs is located in Section C-8 of this Task Order.

C.1.5.2.4 **Other Document Information:** As a rule, the term “contractor” refers to the contractor who is contracted to provide service on this Task Order. The term “third party contractor” refers to all other contractors with whom the contractor may interact with in the performance of their duties on this Task Order.

C.1.6 REQUIRED REPORTS AND MEETINGS

C.1.6.1 Task Order Administration

Workload Data Collection and Analysis: The contractor shall collect, analyze, maintain and provide to the COTR on a monthly basis and upon request workload data for all of the specific requirements identified in the Task Order.. The contractor shall provide to

PROCUREMENT SENSITIVE

the COTR for approval a proposed format and shall track all workload data by functional service area from Task Order start date, throughout the life of the Task Order, and provide a monthly report of the data to the COTR. The contractor shall analyze monthly data and determine the level and frequency of data necessary to capture, and provide recommended initiation or adjustments of systems and methods to accurately capture the necessary detail of workload data. In addition, the contractor shall provide the COTR an annual workload data report that summarizes the monthly workload data, identifies trends and statistical variations, and provides a logistical forecast for future years, by the last business day of each fiscal year. (CDRL C.1.6-1, Monthly and C.1.6-1a Annual Workload Data Reports)

C.1.6.1.1 Performance Requirements: The contractor shall attain the performance requirements depicted in the task order. The contractor can provide suggestions to the COTR for refinement and adjustment of the performance requirements during the transition period. The COTR will evaluate the suggestions and notify the contractor in writing of any changes to the performance requirements, at least 20 business days prior to implementing the adjusted performance requirements.

C.1.6.2 Required Reports

C.1.6.2.1 Weekly Status Report: The contractor shall submit a Weekly Status Report to the COTR no later than 9:00 am each Tuesday, including one hard copy and an electronic file of the report. The Weekly Status Report shall include the following:

- Activities and accomplishments in each functional area during the previous week
- Task Order status (e.g., completed activities, current activities, activities planned for the following two weeks, issues or problems anticipated or encountered and proposed or implemented resolution) review of any associated project plan
- Project related issues/problems by functional area and actions taken/planned to resolve those issues/problems, and cost impact, if any
- Summary of any actual, planned or anticipated staffing changes
- Summary of any actual, planned or anticipated changes to procedures
- Summary of any actual or potential problems with procurement, asset management, and IT Infrastructure Library activities
- Summary of any issues regarding the achievement of performance standards
- Projected date when funds will be exhausted, if applicable
- Activities planned for the next week
- Actions required of DHS

C.1.6.2.2 Monthly Performance Summary Report: The contractor shall provide the COTR with a Monthly Performance Summary Report evaluating their performance in terms of the Performance Standards. The contractor shall submit the report no later than the fifth business day of each month and must include the quantitative data and calculations. The report must provide sufficient detail to allow auditing to the databases and other performance records maintained by the contractor. The report must provide the results of

PROCUREMENT SENSITIVE

monitoring and simulations including the number of occurrences, the number of successful occurrences and the calculated percentage of successful occurrences. The report must list the date, time and duration of outages interruptions or periods of degradation for applications, network environments, and databases.

C.1.6.2.3 Monthly Quality Control Report: The contractor shall submit a Quality Control Report to the COTR no later than the 10th business day after the end of the quarter beginning with Year 2009: Quarter 1: February 1 through April 30 is due is May 14; Quarter 2: May 1 through July 31 is due August 14, 2009; Quarter 3: August 1 through October 31 is due November 16; Quarter 4: November 1 through January 31 2010 is due February 13, 2010, etc.). The report shall summarize the results obtained from quality assurance monitoring in accordance with the Contractors Quality Control Plan and include a list of the tasks inspected, the number of completed tasks sampled, and the number of tasks determined by the Government as acceptably performed. The contractor shall provide a copy of the metrics data along with analysis to the COTR as part of the report. The contractor shall also include a summary of customer evaluations including the number received, a description of any evaluations with negative comments or complaints and the corrective actions taken. The contractor shall identify any tasks that fail to meet the performance standards specified in the Contract and shall describe the actions taken to correct performance. (CDRL C.1.6-4, Monthly Quality Control Report)

C.1.6.2.4 List of Plans: TE C.1.6-002 contains a comprehensive list of plans that the contractor shall develop, maintain, and update.

C.1.6.3 Required Meetings

The contractor's key staff shall attend meetings and provide status reports as outlined below. Status reports are due even in the event of the cancellation of meetings. Due to the parties' geographical locations, status meetings may be accomplished via telephone conferencing with the agreement of the Government.

C.1.6.3.1 Contract Administration Review (Monthly): The objective of the Contract Administration Review (CAR) is for DHS and the contractor to provide management consultation and assistance when resolving task order performance issues that will enhance efficiency and effectiveness and mission performance component-wide. Furthermore, the CAR will also ensure that O&M Task Order standards conform to DHS expectations.

C.1.6.3.1.1 The contractor's key staff (e.g., Program Manager and Project Managers) shall attend a monthly Contract Administration Review Status Meeting with representatives from the OCIO and Office of Procurement Operations – Information Technology Acquisition Center (OPO-ITAC). The contractor shall brief attendees on contractual issues that may impact Task Order performance or schedule. Action items from previous meetings (e.g., open action items, long-term action items, and action items closed during period) shall be addressed at meetings.

C.1.6.3.1.2 Section Intentionally Left Blank

PROCUREMENT SENSITIVE

C.1.6.3.2 Program Management Review and Report (Quarterly): The objective of the Program Management Review (PMR) is to determine the state of the O&M program in a systematic on-going manner to manage risks.

C.1.6.3.2.1 The contractor shall attend a quarterly Program Management Review (PMR) with representatives from the Office of the Chief Information Officer (OCIO) and the OPO-ITAC. The contractor shall prepare and deliver a meeting agenda. The contractor shall brief attendees on issues that may impact on-time completion of project milestones and deliverables.

C.1.6.3.2.2 The contractor shall provide a status report for each meeting. The report will provide highlights of the accomplishments for the reporting period, activities anticipated for the next reporting period, outstanding issues and recommendations for resolution, and resolved issues since the previous reporting period. (CDRL C.1.6-8, Quarterly Program Management Review Status Report)

C.1.6.3.2.3 The contractor shall prepare and distribute a PMR status report with accompanying agenda documenting the status of issues, decisions, assignments, and pending matters from the PMR. The contractor shall prepare and deliver the quarterly status report and agenda by close of business at least two business days prior to the scheduled PMR

C.1.6.3.2.4 To assist DHS in compiling useful data on work performed under this contract, each status report shall contain the following support items:

- A brief, factual summary description of system operations activities
- A brief, factual summary of technical progress made for each task during the reporting period
- Customer support metrics (general user queries, FOIA requests received, completed, and in progress)
- Number of help-desk tickets opened, closed, and in progress
- Level of Effort Metrics (for each task/activity performed include Level of Effort, Available Range of Hours, Actual Hours Used, Contract Occurrences, and Occurrences Remaining) Any significant problems and their impacts, causes, proposed corrective actions, and the effect that such corrective actions will have on the accomplishments of the contract/task order objectives
- A status of overall project schedule and/or degree of completion of tasks/activities by time intervals
- Status of user support activities
- Significant concerns/risks/mitigation options and recommendations
- Summary of Change Requests, Problem Reports, responses, and solutions

C.1.6.3.2.5 The contractor shall prepare and distribute meeting minutes within 3 business days after the meeting that document issues, decisions, assignments, and pending matters from the PMR.

C.1.6.4 Function Specific Reports and Documents

C.1.6.4.1 Security Violation Report: The contractor shall prepare and submit a Security Violation Report to CIO Management and the Information Systems

PROCUREMENT SENSITIVE

Security Manager (ISSM) within one hour of determining the occurrence of a security violation. The report must include a description of the security violation, the name and telephone number of the point-of-contact, the time of the security violation, the extent of the security violation, the potential threat that could arise from the violation. It must also include any potential or real data compromise or system degradation resulting from the security violation, and recommendations regarding resolution or resolution actions undertaken to address the impact of the security violation.

C.1.6.4.2 Architectural Compliance Plan: The contractor shall prepare and submit to the COTR no later than 30 business days after Task Order award an Architectural Compliance Plan that demonstrates that the technologies utilized by the contractor conform to the target architecture. The contractor shall update and submit the Architectural Compliance Plan no later than the first business day of May and November in subsequent performance periods. (CDRL C.1.6-11, Architectural Compliance Plan)

C.1.6.4.3 Program Development Report: The contractor shall submit a Program Development Report to the COTR on the last business day of April and October of each year. The contractor shall base the report upon the program for the enhancement and improvement of information technology services. The report shall identify projects and initiatives recommended to support the needs of the DHS. The report shall also identify projects and initiatives that represent "State-of-the-Art" advancements in the capability to support the DHS. (CDRL C.1.6-12, Program Development Report)

C.1.6.4.4 Network and Application Diagrams: The contractor shall maintain the Network and Application Diagrams. The contractor shall submit updated diagrams to the COTR semi-annually no later than the first business day in June and December. The submission shall consist of a separate electronic file for each network, entity relationship and application. The name of the network or application shall appear in the filename and the tab of the worksheet. (CDRL C.1.6-13, Network and Application Diagrams)

C.1.7 CONTRACTOR PERSONNEL

C.1.7.1 Key Personnel

C.1.7.1.1 Project Manager/Alternate(s): The contractor shall provide an on-site Project Manager (PM) who shall be responsible for the performance of the work and provide overall direction to the personnel working under this EAGLE Task Order. The name and resume of this person and of an alternate(s), who shall act for the manager when the on-site manager is absent, shall be designated in writing to the CO for approval prior to Task Order start date. The contractor shall provide a PM succession plan and keep it updated throughout the life of the Task Order. (CDRL C.1.7-1, Project Manager Succession Plan)

C.1.7.1.1.1 The PM shall be the contractor's authorized representative for the technical and administrative performance of all services required under this Task Order. The PM shall be the first Point of Contact (POC) for Task Order or administrative questions or difficulties that arise related to this Task Order. The PM shall be the primary point through which communications, work assignments, and technical direction flow between the Government and the contractor.

PROCUREMENT SENSITIVE

- C.1.7.1.1.2 The PM, or designated alternate, shall be available during normal work hours to meet with the DHS, in person or as otherwise agreed upon by the DHS, to discuss problem areas within 30 minutes. After normal duty hours, the manager or alternate shall be available in accordance with DHS approved escalation protocol procedures and in the event of disaster recovery or Continuity of Operations event.
- C.1.7.1.1.3 The PM shall be available during normal hours of operation, and during periods of no-notice emergencies, including localized acts of nature, accidents, and military or terrorist attacks, to plan, direct, and control the overall management and operational functions specified herein. The PM shall provide the necessary level of Task Order management and administrative oversight to achieve the quantitative and qualitative requirements of this Task Order.
- C.1.7.1.1.4 The PM or alternate shall have full authority to act for the contractor on all matters relating to daily operation of this Task Order.
- C.1.7.1.2 Other Key Personnel: The contractor shall provide key personnel as defined in TE C.1.7-001. In the event of key personnel departures, the contractor shall ensure support for all DHS requirements until permanent replacements are available. These replacements, on an acting or permanent basis, are required within 20 business days after the departure of a key individual. Final approval of key personnel is the responsibility of the DHS. The contractor shall provide a current succession plan for the key personnel positions. (CDRL C.1.7-2, Key Personnel Succession Plan)

C.1.7.2 Personnel Staffing

- C.1.7.2.1 Employees: The contractor shall ensure that employees (other than managers) are competent in Operation and Maintenance of Information Technology systems to include project management, engineering, end user services, application services, infrastructure services, IT Continuity Management and security services.
- C.1.7.2.2 Staffing Roster: The contractor shall submit a staffing roster to the COTR monthly, no later than the 15th business day of each month. The staffing roster shall list the names of each employee working on the Task Order. The roster shall include as a minimum, the Contract Number, contractor Name, Employee Primary User ID, Employee Last Name, Employee First Name, Current DHS Security Classification, Work Location, Office Number, Phone Number, Emergency Point of Contact, Emergency Point of Contact Phone Number, Primary Project Number, and Secondary Project Number for each employee. The contractor shall notify the COTR of any additions, deletions, or changes within one business day after the change(s). (CDRL C.1.7-3, Staffing Roster)
- C.1.7.2.2.1 If the Contracting Office identifies an employee to the contractor as a potential threat to the health, safety, security, general well being, or operational mission of the DHS, the contractor shall not employ persons for work on this Task Order. The Government reserves the right to remove such persons. Where reading, understanding, and discussing safety and environmental warnings are an integral part of a contract employee's duties; that employee must be able to understand, read, write, and speak English.

PROCUREMENT SENSITIVE

C.1.7.2.2.2 The contractor shall not employ any person who is an employee of the United States (U.S.) Government if employing that person would create a conflict of interest. Contractor personnel shall meet relevant DHS security requirements as identified in DHS regulations and orders. The contractor shall provide a sufficient number of personnel possessing the skills, knowledge, training, and security clearance to perform the services required by this Task Order for each specific functional area.

C.1.7.2.2.3 The contractor shall maintain agreed upon staffing levels at or above 95% for the life of the Task Order.

C.1.7.2.3 Subcontractor Personnel: Subcontractors must comply with all employee provisions identified in the Task Order.

C.1.7.3 Personnel Training

C.1.7.3.1 Personnel Proficiency: All contractor Personnel shall be trained, competent, and skilled in the performance of their assigned work. The contractor shall ensure they provide any necessary refresher training to their employees in order to maintain required certification levels and proficiency to perform assigned duties.

C.1.7.3.2 Employee Training: The contractor shall be responsible for all new and recurring training of contractor personnel in such a manner as to ensure performance of all tasks required by this Task Order.

C.1.7.3.2.1 The contractor shall conduct or provide to their employees detailed instruction on Government statutes, regulations, policies, and guidelines in areas such as employee conduct ethics, safety, security, health, fire prevention, and the environment as they pertain to the operations specified in this Task Order. This contractor shall conduct or provide this training upon initial employee hire, annually, and as directed by the Government. The contractor shall ensure all new employees attend DHS Security Education, Training, and Awareness training as described in DHS Management Directive (MD) 11053.

C.1.7.3.2.2 The contractor shall develop, implement, and maintain written guidelines or standard procedures necessary for effective accomplishment of Task Order requirements. The contractor shall comply with all Privacy Act and other regulations governing personal and private information.

C.1.7.3.2.3 The contractor shall conduct any remediation training necessary to ensure competency of contractor employees. The contractor shall conduct remediation training in a manner to minimize adverse impact on contract performance and interruption of normal business processes.

C.1.7.3.3 Knowledge Management: The contractor shall develop, maintain, update, and implement a knowledge management system for retention and referencing of processes, procedures, best practices, lessons learned, and any other information that can be used to enhance IT operations. The knowledge management system shall reside on the DHS intranet and be accessible to DHS IT management and the contractor's personnel.

C.1.7.4 Personnel Security Requirements

C.1.7.4.1 Access Requirements: The Government has the right to restrict and control access to its facilities, property, and data, including those identified in this Task

PROCUREMENT SENSITIVE

Order. The contractor shall ensure all contractor employees pass DHS suitability screening requirements, and receive an Entry on Duty (EOD) date from the DHS Office of Security, prior to beginning performance. Personnel requiring clearances under the task order will not be eligible for billing to the Government prior to EOD determination. Contractor administrative/support staff personnel not requiring EOD determinations are available for billing to the government upon task order award. The Government will be the final authority in determining access privileges. The Government's exercise of its right to grant and revoke the access of particular individual(s) to its facilities, or parts thereof, shall not constitute a breach or change to the Task Order. Regardless of whether the contractor employs said individual(s), and regardless of whether it precludes said individual(s) from performing work under the resulting Task Order.

C.1.7.4.2 Personnel Security Clearances: Much of the scope of work required within the Task Order requires access to classified data and/or classified areas. Personnel requiring access to classified data and/or classified areas are required to have a current Secret, Top Secret, or Top Secret/Sensitive Compartmentalized Information (TS/SCI) access authorization clearance prior to the commencement of the work. All access authorization clearances must be active and in place prior to the start of any work on any tasking within this Task Order which requires a clearance. DHS has final authority on determining an individual's security clearance eligibility. The contractor shall submit requests for security clearances for staff. All personnel assigned to functions described in this document must be U.S. Citizens. Contractor administrative or technical personnel who will not require access to classified areas or information will not require access authorizations. The contractor shall identify, on the contractor Employee Roster, those employees who require access to restricted areas or classified information, and shall obtain and maintain the appropriate security clearances as identified in this solicitation.

C.1.7.4.3 Personnel Access Badges: The contractor shall ensure all contractor personnel requiring access authorization have valid badges and shall collect and return badges for employees: 1) who are no longer working on the Task Order; 2) who no longer require access; 3) upon expiration of badges; or 4) when the Task Order expires or terminates. The contractor shall return badges to the appropriate DHS security office. The contractor shall notify the COTR by e-mail within one hour of any of these occurrences and return the badges to the appropriate DHS security office.

C.1.7.4.4 Personnel Separation: The contractor shall ensure all contractor personnel who are no longer working on the Task Order, or when the Task Order expires or terminates, shall comply with DHS established contract employee separation procedures.

C.1.8 CONTRACTOR INTERFACES

C.1.8.1 Personnel Performing Security/Continuity/Quality

C.1.8.1.1 Coordination with Other Performing Activities: The contractor shall coordinate with Government and third party contractor personnel performing required services in areas associated with the requirements of this Task Order. Some examples of the required services are personnel performing security and

PROCUREMENT SENSITIVE

continuity functions, audits, inspections, delivery services, construction, and telecommunication services.

C.1.8.1.1.1 The DHS COTR will facilitate initial contact between the contractor and other third party contractors performing work for DHS, as necessary. The contractor shall provide support services to other third party contractors within the scope of this Task Order as required by the Government.

C.1.8.1.1.2 The contractor shall notify the COTR in writing of unresolved disputes in receiving support from or providing support to customers or other third party contractors within two business days from the time the dispute occurs, unless otherwise specified in SLAs.

C.1.8.1.2 Inspection by Government Agencies: Per FAR 52.246-6 the contractor shall provide access to and cooperate with Government personnel conducting official inspections and surveys. Government personnel other than CO or Quality Assurance Personnel may periodically observe contractor operations. However, the CO is the only person that may obligate the Government or direct contractor operations. The following list identifies agencies performing inspections:

- Quality Assurance Evaluators
- Property Inspectors
- The Inspector General (IG)
- Other offices in the DHS such as the Facilities and Services Department
- Other federal agencies such as the Occupational Safety and Health Administration (OSHA)
- Environmental Protection Agency (EPA)
- Government Accountability Office (GAO)
- General Services Administration (GSA)
- Defense Contracting Audit Agency (DCAA)
- DHS Office of Security

C.1.9 QUALITY ASSURANCE AND QUALITY CONTROL

C.1.9.1 Quality Assurance

C.1.9.1.1 Quality Assurance: The Government will evaluate the contractor's performance under this Task Order. The Government will conduct surveillance according to standard inspection procedures or other Task Order provisions. Any action taken by the CO because of surveillance will be according to the terms and conditions of this Task Order.

C.1.9.1.1.1 The COTR will record the results of surveillance. The COTR will provide copies of surveillance reports to the contractor. The contractor shall sign the surveillance reports and return them to the COTR within two business days. The contractor shall annotate on the signed copy any exceptions or disagreement with the surveillance report.

C.1.9.2 Quality Control

C.1.9.2.1 Quality Control: The contractor shall provide a revision to the Quality Control Plan submitted as part of the Contractor's proposal, to the COTR for approval within 20 business days of Task Order award. The plan shall include

PROCUREMENT SENSITIVE

a detailed description of the processes used during performance to ensure the services meet or exceed the requirements of the Task Order and contract. The plan shall address each mission essential objective of the PRS, and all others considered necessary to meet the Task Order requirements. The plan shall systematically provide for early identification of nonconforming services, develop, maintain, update and implement metrics to track performance trends, detail corrective action plans including milestones. (CDRL C.1.9-1, Quality Control Plan)

C.1.9.2.1.1 Revisions to the Quality Control Plan may be required at any time. The contractor shall make appropriate revisions and obtain acceptance of the revised plan from the COTR. The contractor shall provide revised copies of the Quality Control Plan to the COTR and Quality Assurance Personnel (QAP) upon approval from the COTR.

C.1.9.2.1.2 The contractor shall maintain records of the work sampled and the results of the inspection for each discrete sample. The records shall allow the COTR to review each discrete sample and validate the determinations made during the performance of Quality Control.

C.1.9.2.2 Customer Evaluation: The contractor shall create, maintain, and update a customer evaluation plan to include identifying and implementing customer satisfaction improvements, as part of the Quality Control Plan. The contractor's plan shall adhere to the ITIL framework for Service Delivery and Service Support. The contractor shall submit the final plan to the COTR for approval no later than 20 business days after Task Order award. The COTR may require changes to the plan at any time during the life of the Task Order. The contractor shall submit their changes within 20 business days of the requested change.

C.1.10 PROPERTY CONTROL

The contractor's property control procedures shall comply with FAR 52.245-5, Government Property (Cost-Reimbursement, Time-and-Material, or Labor-Hour Contracts).

C.1.11 OPERATING ENVIRONMENT

C.1.11.1 Operating Hours

C.1.11.1.1 Hours of Operation and Government Holidays: The normal hours of operation are 8:00 A.M. to 5:00 P.M. Various functions within the Information Technology Services Office require 7X24X365 (366 for leap years) coverage as addressed in Table 2 below and in section C.5.

Table 2 – Operating Hours

Functional Service Area	Work Hours	Required Security Clearances
Application and Management Support Services	8 A.M. to 5 P.M. ¹	Suitability, Secret, Top Secret, Top Secret/SCI
Deployment Support	8 A.M. to 5 P.M.	Suitability, Secret, Top Secret, Top Secret/SCI
Infrastructure Engineering	8 A.M. to 5 P.M.	Suitability, Secret, Top

¹ Monitoring is 24X7X365 (366 for leap years)

Functional Service Area	Work Hours	Required Security Clearances
		Secret, Top Secret/SCI
Testing	8 A.M to 5 P.M.	Suitability, Secret, Top Secret, Top Secret/SCI
Operations and Maintenance for End User Support: Help Desk Desk Side Support	7X24X365 (366 for leap years) 5x12 desk side support operations, with provision that designated VIPs are entitled to on call support	Suitability, Secret, Top Secret, Top Secret/SCI
Video Teleconferencing	8 A.M to 5 P.M. ²	Suitability, Secret, Top Secret, Top Secret/SCI
Satellite/Cable TV Operations	8 A.M to 5 P.M.	Suitability, Secret, Top Secret, Top Secret/SCI
Phone and PBX Operations	8 A.M to 5 P.M. ³	Suitability, Secret, Top Secret, Top Secret/SCI
Network Management Center	7X24X365 (366 for leap years)	Suitability, Secret, Top Secret, Top Secret/SCI
Security Management Center	7X24X365 (366 for leap years)	Suitability, Secret, Top Secret, Top Secret/SCI
Communications Security (COMSEC) Management	7X24X365 (366 for leap years)	Suitability, Secret, Top Secret, Top Secret/SCI
Continuity Management	8 A.M to 5 P.M.	Suitability, Secret, Top Secret, Top Secret/SCI

C.1.11.1.2 The days specified in Table 3 below are the legal public holidays. The contractor will adhere to the Government holiday schedule. If the holiday falls on a Saturday, the recognized Federal holiday is the preceding Friday. If the holiday falls on a Sunday, the recognized Federal holiday is the following Monday.

Table 3 – Federal Holidays

Holiday	Date
New Year's Day	1st day of January
Martin Luther King's Birthday	3rd Monday in January
President's Day	3rd Monday in February
Memorial Day	Last Monday in May

² Limited coverage required 24X7X365 (366 for leap years)

³ Limited support required 24X7X365 (366 for leap years)

PROCUREMENT SENSITIVE

Independence Day	4th of July
Labor Day	1st Monday in September
Columbus Day	2nd Monday in October
Veteran's Day	11th of November
Thanksgiving Day	4th Thursday in November
Christmas Day	25th of December

C.1.11.1.3 Hours of Operation Other Than Normal: There will be mission situations that require the contractor to work other than normal hours. Such scheduling may require accomplishment of contractor work at times other than normal operation hours; the CO, or appropriate Government representative, will approve in writing work outside normal operation hours when required. Overtime shall only be permitted when approved in writing by the CO.

C.1.11.2 Operations Under Adverse Conditions

C.1.11.2.1 Emergencies and Special Events: The contractor shall respond to emergencies as governed by procedures prescribed by the DHS in accordance with its applicable statutes, regulations, orders, policies, and guidelines. The DHS may have the need to extend contractor tour of duties, hours, and bringing on additional cleared contractor personnel in the event of a major emergency. The contractor shall provide surge personnel support, as directed by the CO, in response to emergencies or special events. Emergencies may consist of natural disasters, terrorist threats or events, elevation of the DHS threat level or as designated by the Department. In the event of any emergency, the CO may initiate contractor action by a verbal authorization. The CO will define a task order in a timely manner or as time permits after the emergency is contained or resolved.

C.1.11.2.1.1 Extreme weather conditions and natural disasters (such as tornados, flooding, snow, and ice) may warrant temporary office evacuation or office closure. The contractor shall respond to extreme weather conditions according to DHS direction, and shall inform all employees of these instructions. During normal duty hours, the normal chain of management will provide notification of facility closures. During non-duty hours, local radio and television channels will provide notification. Facility closings shall in no way interfere with the contractor operation and maintenance of the critical systems. All contractor employees identified as essential personnel shall remain on duty or report for duty in accordance with the Emergency Situations and relevant Continuity of Operations (COOP), IT Contingency, IT Disaster Recovery/Business Continuity Plan.

C.1.11.2.1.2 The contractor shall participate in all scheduled and unscheduled fire drills, Shelter in Place, and other scheduled safety and emergency-training exercises, which may necessitate interrupted services unless directed otherwise. The Government will consider such interruptions when assessing contractor performance for the affected period.

PROCUREMENT SENSITIVE

- C.1.11.2.2 **Building Occupant Emergency Plan Compliance:** Contractor personnel shall comply with all building occupant emergency plan activities such as building evacuations and shelter in place.
- C.1.11.2.3 **Personnel Response to IT Continuity Events:** Key contractor personnel and contractor personnel with critical skills shall report to and perform duties at alternate sites during IT continuity events, as directed by the Government. The contractor shall provide personnel resources to respond to IT continuity events. The contractor should consider such things as cross-training and providing personnel who would be able to respond from outside the metropolitan area (i.e. individual with appropriate skill sets who would be unaffected by issues in the Baltimore-Washington metropolitan area).
- C.1.11.2.4 **Performance of Services during Crisis:** The following services are essential during crises declared by the DHS Secretary or the President of the United States. All basic services and operations will continue as directed by the COTR. The contractor shall submit an essential personnel list, to include designated emergency POCs, to the COTR within ten business days after Task Order start and shall update monthly for changes throughout the life of the Task Order. The list shall contain the individual's name, address, home phone number, beeper number or cell phone number, security clearance, and duty title. Upon notification of a crisis by the COTR, the contractor shall perform the essential services identified in the CIO COOP Implementation Plan. The COTR will direct implementation of Services under this provision at any time as required to meet mission requirements. (CDRL C.1.11-1, Essential Personnel Contact List)

C.1.11.3 Travel

- C.1.11.3.1 **Authorization and Restrictions:** Contractor personnel may be required to travel to support the requirements of this Task Order. Long distance and local travel may be required in the Continental United States (CONUS). The Government expects the contractor to have a facility within the Washington DC Metropolitan area. The Government will not reimburse local travel within a 50-mile radius from the contractor's facility or the contractor's assigned duty station. This includes travel, subsistence, and associated labor charges for travel time. The Government will not reimburse travel performed for personal convenience and daily travel to and from work at the contractor's facility. The Government will authorize travel, subsistence, and associated labor charges for travel beyond a 50-mile radius of the contractor's facility or assigned duty station; HOWEVER, the COTR shall previously approve all travel outside the Washington DC Metropolitan area. The Government will reimburse authorized travel in accordance with the Federal Travel Regulation. The Government will not reimburse travel without prior approval from the COTR. The contractor's request for travel shall be in writing or electronic as directed by the COTR and contain the dates, locations and estimated costs of the travel.
- C.1.11.3.2 **Costs:** The contractor shall, to the maximum extent practicable, minimize overall travel costs by taking advantage of discounted airfare rates available through advance purchase. Charges associated with itinerary changes and cancellations under nonrefundable airline tickets are reimbursable as long as the changes are driven by the work requirement. Costs associated with Contractor travel shall be in accordance with FAR Part 31.205-46, Travel Costs

and applicable Federal Travel Regulation. If any travel arrangements cause additional costs to the contract that exceed those previously negotiated, written approval by contract modification issued by the CO is required prior to undertaking such travel. Contractor personnel traveling to support Task order requirements shall provide a Trip Report to the COTR within 2 business days of completing travel. A summary of trips taken within each month shall be included in the monthly reports.

C.1.12 CONTRACT TRANSITION

C.1.12.1 Transition and Phase In Section Intentionally Left Blank

- C.1.12.1.1 Transition Plan: Section Intentionally Left Blank.
- C.1.12.1.2 Transition Tasks: Section Intentionally Left Blank
- C.1.12.1.3 Transition Ramp-up: Section Intentionally Left Blank

C.1.12.2 Phase Out

- C.1.12.2.1 Inventory: At the Phase-out of this Task Order the contractor and Government shall conduct a joint inventory assessment of property accounts for the contractor's staff (i.e. hand receipts of cell phones, blackberries, etc.) to ensure a full accounting of all Government property. The Government will hold the contractor liable for any damaged or lost equipment, and the contractor shall ensure all other Government equipment is in working order.
- C.1.12.2.2 Observations: The contractor shall permit the successor contractor (and the successor contractor's employees) to observe and become familiar with any and all operations specified in this Task Order for a minimum of 90 business days, or for a COTR specified timeframe, prior to the expiration or termination of the Task Order.
- C.1.12.2.3 Maintenance of Systems, Files, and Data: The contractor shall maintain the full operational status of all Government systems and equipment, and continue all current work in progress until the successor contractor assumes full operational responsibility. The contractor shall not destroy, delete, or otherwise dispose of any files or data upon expiration or termination of the Task Order, without prior permission from the COTR.
- C.1.12.2.4 Cooperation: The contractor shall fully cooperate with the successor contractor and the Government so as not to interfere with their work or duties.

C.2 DEFINITIONS AND ACRONYMS

C.2.1 DEFINITIONS

The definitions set forth below are those unique or used in this Task Order. Definitions for technical terms or words which are included in this Task Order can be found in the technical documents referenced in the individual functional areas of the Task Order. The definitions provided below are oriented to DHS's Task Order. In many cases definitions are specific by situation. The total listing of definitions is not all-inclusive, but it has been derived from official publications (e.g., regulations and technical manuals and industry standards) when available.

Note: In the event of a conflict between any definition in this section and a comparable definition in the Federal Acquisition Regulation, the latter shall prevail.

A LAN: The DHS unclassified network

Acceptance, Approved (as Directed, as Permitted, as Required): Where these words or words of similar import are used, it shall be understood that the direction, requirement, permission, approval, or acceptance of the Contracting Officer (CO) or Contracting Officer's Technical Representative (COTR) is intended, unless stated otherwise.

Acceptable Quantity Level (AQL): Represents the required success rate for each output that comprises the total workload. The AQL is reasonable to allow for the possibility of unexpected problems that prevent some outputs from meeting the requirements of the performance standards. The AQL is a percentage value of the number of performances of each output that must adhere to the performance standard set for that output. AQLs are determined based on agency directives or historical records of Government performance.

Accountability: The obligation of both the contractor and the Government to fulfill the requirements of this Task Order. This includes item such as the contractor's responsibility to maintain accurate and complete records of documents, funds and property.

Accreditation: The formal declaration by a Designated Approving Authority (DAA) that an information system (IS) is approved to operate in a particular security mode using a prescribed set of safeguards to an acceptable level of risk.

Approval: The process through which the Government provides authorization to the contractor to proceed with an action. An approved authorization must be in writing.

Availability: A measure of the degree to which an item is in an operable and committable state at the start of any task or mission, when the task or mission is called for at an unknown (random) point in time.

Authentication: A security process designed to establish the validity of a transmission, message or originator or to verify an individual's eligibility to receive specific categories of information.

Authorization: The process of granting or denying access to system objects based on an individual or entities identities, roles or other qualifying characteristics (e.g. clearance level).

Availability period: The amount of time the system(s), or the total system, is functioning so that the customer can get work done.

PROCUREMENT SENSITIVE

Baseline: A specification or product that has been formally reviewed and agreed upon, and thereafter serves as the basis for further development and can be changed only through formal change-control procedures or a type of procedure such as configuration management (CM).

Basic Rate Interface (BRI): A level of service within the Integrated Services Digital Network (ISDN). The BRI includes a number of B-channels and a D-channel; B-channels carry data, voice, and other services and the D-channel carries control and signaling information.

Biennially: One time every two years

Bimonthly: One time every two months

Biweekly: One time every two weeks

C LAN: The DHS Top Secret network

Certificate: Digital documents attesting to the binding of a public key to an individual or other entity. They allow verification of the claim that a given public key does in fact belong to a given individual. Certificates, also called digital certificates, are issued by a Certificate Authority and contain the public key and other identification information relating to the certificate requester.

Certification: Certification is the comprehensive evaluation of the technical and non-technical security features of an Information System (IS) and other safeguards, made in support of the accreditation process, to establish the extent to which a particular design and implementation meets a set of specified security requirements.

Certified Information Systems Security Professional (CISSP): A professional certification in information systems security administered by the International Information Systems Security Certification Consortium (ISC)²®

Channel Service Unit/Data Service Unit (CSU/DSU): A digital-interface device used to connect a router to a digital circuit such as a T1 or T3 line.

Classified: Documents, data, information, systems, products, services, items, etc for which access is limited to those persons having a "need to know" and appropriate security clearance.

Clearance: Authority permitting individuals cooperating in DHS work, and having a legitimate interest therein, access to classified technical information, material, or equipment or admission to restricted areas or facilities where such information or material is located.

Commercial Off The Shelf (COTS): Describes software or hardware products that are ready-made and available for sale to the general public.

Common Operating Environment (COE): A listing of components (hardware and software) that captures the concept of a common or shared operating environment across an enterprise or organization; provides a standard for the organization to be common operating environment (COE) compliant.

Common Vulnerabilities and Exposures (CVE): An index of standardized names for vulnerabilities and other information security exposures. CVE aims to standardize the names for all publicly known vulnerabilities and security exposures. The CVE database is operated by the MITRE corporation, and is sponsored by the Department of Homeland Security.

PROCUREMENT SENSITIVE

Confidentiality: Assurance that information is not disclosed to unauthorized entities or processes.

Configuration Management (CM): A discipline applying technical and administrative direction and surveillance to: (a) identify and document the functional and physical characteristics of a particular item, system, etc; (b) control changes of those characteristics; and (c) record and report changes to processing and implementation status.

Conflict of Interest (COI): According to DHS Clause 1337, "Conflict of interest means that because of other activities or relationships with other persons or organizations, a person or organization is unable or potentially unable to render impartial assistance or advice to the Government, that the person's or organization's objectivity in performing the Task Order is or might be otherwise impaired, or that the person or organization has or might acquire an unfair competitive advantage."

Configuration: The functional or physical characteristics of equipment, systems, hardware or software set forth in technical documentation and achieved in a product.

Conservation: The protection, improvement, and use of natural resources according to principles that will provide optimum public benefit and support of DHS's mission.

Continuity of Operations (COOP). The COOP focuses on restoring and organization's (usually headquarters element) essential functions at an alternate site and performing those functions for up to 30 days before returning to normal operations. Because a COOP addresses headquarters-level issues, it is developed and executed independently from the Business Continuity Plan (BCP). Implementation of a viable COOP capability is mandated by PDD 67, Enduring Constitutional Governmental and Continuity of Government Operations. FEMA, the Federal Government's executive agent for COOP, provides COOP guidance in FPC 65, Federal Executive Branch Continuity of Operations. Standard elements of a COOP include Delegation of Authority statements, Orders of Succession, and Vital Records and Databases. Because the COOP emphasizes the recovery of an organization's operational capability at an alternate site, the plan does not necessarily include IT operations. In addition, minor disruptions that do not require relocation to an alternate site are typically not addressed. However, COOP may include the BCP, Business Resource Plan (BRP), and disaster recovery plan as appendices. (Source: NIST 800-34, Contingency Planning for Information Systems)

Contract Data Requirements List (CDRL). Data required to be submitted by the contractor to the Government. A proper and correct submission of a CDRL is evidenced by the following criteria: completeness, accuracy of data, preparation in accordance with applicable mandatory publication or other prescribing document, signature or initials by the certifying official, and correct and timely turn-in or distribution.

Contract Modification: Any written alteration in the terms and conditions of the contract or Task Order, such as specifications, delivery point, rate of delivery, Task Order period, price, quantity, or other Task Order provisions.

Contracting Officer (CO): An individual appointed in accordance with procedures prescribed by the Federal Acquisition Regulation with the authority to enter into, administer, and terminate contracts and make related determinations and findings.

Contracting Officer's Technical Representative (COTR): The individual or individuals appointed by the Contracting Officer to act as the authorized Government representative and to oversee contractor performance.

PROCUREMENT SENSITIVE

Contractor: The term contractor, as used herein, refers to the principle/prime contractor.

Contractor Furnished Equipment (CFE): That equipment that the contractor includes in its offer in order to perform the requirements of the Task Order, and that is not covered under Government-Furnished Property (GFP).

Contractor-Furnished Property (CFP): Equipment and facilities provided by the Contractor to perform the Task Order requirements.

Corrective Action: Consists of those efforts required to correct reported deficiencies and mitigate reoccurrence of defects.

Critical Design Review (CDR): The CDR is a multi-disciplined technical review to ensure that the system under review can proceed into system fabrication, demonstration, and test; and can meet the stated performance requirements within cost (program budget), schedule (program schedule), risk, and other system constraints. Generally this review assesses the system final design as captured in product specifications for each configuration item in the system, and ensures that each product in the product baseline has been captured in the detailed design documentation.

Customer: Any recipient of a service described in Section 5, Specific Work Requirements of the Task Order.

Damage: A condition that impairs either value or utility of an article; may occur in varying degrees. Property may be damaged in appearance or in expected useful life without rendering it unserviceable or less useful. Damage also shows partial non-serviceability. Usually implies that damage is the result of some act or omission.

Data Integrity: Condition that exists when data is unchanged from its source and has not been accidentally or maliciously modified, altered or destroyed.

Database: A collection of records, in one or more files, which are often coded for rapid search and retrieval via computer.

Defense Message System (DMS): The system of record for organizational messaging used by the Department of Defense. It is a modified commercial-off-the-shelf (COTS) application that provides multimedia messaging, directory, and security services. DMS uses the underlying Defense Information Infrastructure (DII) network and security services in conjunction with National Security Agency (NSA) security products.

Degauss: Destroy information contained in magnetic media by subjecting that media to high-intensity alternating magnetic fields, following which the magnetic fields slowly decrease.

Degausser: Electrical device or hand-held permanent magnet that can generate a high intensity magnetic field to sanitize magnetic storage media.

Denial of Service: Any action or series of actions that prevent any part of a system from functioning in accordance with its intended purpose. This includes any action that causes unauthorized destruction, modification or delay of service.

Desktop Administration: Services provided in the operation and maintenance of an individual's desktop computer. This includes services such as installation of a new system, hardware upgrades, relocation and removal of hardware, installation and upgrade of software applications and operating system. It also includes configuration of hardware and software, backup and restore, performance monitoring and tuning, problem tracking and error detection, needs assessment, procurement, disposal, and inventory management.

PROCUREMENT SENSITIVE

Desktop Computer: Distributed computing resource, either networked or standalone, consisting of a CPU, keyboard, monitor, and a screen manipulation device, such as a mouse. This typically includes PCs, Apple Macintoshes, UNIX based workstations, X-terminals and other terminals. This definition excludes mainframes, supercomputers and midrange computers.

Desktop Configuration: The hardware and software characteristics associated with a desktop computer (UNIX, PC, Macintosh, and X-Terminal). Hardware characteristics include: CPU, RAM, amount of disk storage, size of monitor, cards installed in the system unit, and devices attached directly to the system unit. Software characteristics include: identification of COTs application software in use on the workstation, operating system, and a description of any commonly distributed custom applications.

Digital Video Disk (DVD): An optical disc storage media format that can be used for data storage.

Discrepancy: A variance between contractually required and actual performance.

Disposal: The disposition of excess assets (including intellectual and real property, industrial and personal property) by the Government in accordance with DHS regulations and the FAR.

Document Type Definition (DTD): A DTD defines the legal building blocks of an XML document. It defines the document structure with a list of legal elements.

Downtime: The amount of time when an end user's access to network services is impaired. Downtime for each incident shall be the period between the time of failure and the time that the system is returned to the Government fully operational.

Due Diligence: The purpose of Due Diligence is for the contractor to validate the inventory and environment portrayed during the master Task Order award and account for any changes that have occurred between Task Order award and the Task Order start. If there is a discrepancy found which exceeds parameters, then a due diligence price adjustment will be submitted. The Due Diligence period shall be limited to not more than 20 business days unless a longer period is granted by the CO.

E-Government: One of the five key elements of the President's Management Agenda designed to make better use of information technology (IT) investments to eliminate billions of dollars of wasteful Federal spending, reduce Government's paperwork burden on citizens and businesses, and improve Government response time to citizens. A key goal is for citizens to be able to access Government services and information within three "clicks," when using the Internet.

Electronic Signatures in Global and National Commerce Act (ESIGN): A U.S. Code that facilitates the use of electronic records and signatures in interstate and foreign commerce by ensuring the validity and legal effect of contracts entered into electronically.

Emergency: The reporting of sudden, usually unforeseen, occurrences where life or property are in immediate danger and require immediate action.

Employee: An employee includes both contractor employees and subcontract employees.

Enterprise Acquisition Gateway for Leading Edge Solutions (EAGLE): The DHS contracts for Information Technology (IT) support services that will enable DHS business and program units to accomplish their mission objectives.

PROCUREMENT SENSITIVE

Enterprise Architecture (EA): A description including graphics of the systems and interconnections providing for or supporting various functions. EA defines the physical connection, location, and identification of such key nodes as circuit and network platforms, and allocates system and component performance parameters. Shows how multiple systems within a domain or an operational scenario link and interoperate, and may describe the internal construction or operations of particular systems in the systems architecture.

Enterprise Change Control Board (ECCB): The board responsible for reviewing any incoming change requests, including both enhancements and defects. The first step focuses on triage, where high severity defects are assigned to the support team so that they can be dealt with by a hot fix. Lower severity defects and all enhancement requests will be evaluated by the board in order to determine which change requests are to be acted upon and which systems will be affected so that the change request may be assigned appropriately.

Facilities: Property used for production, maintenance, research, development or testing. It includes plant equipment and real property. It does not include material, special test equipment, special tooling or agency peculiar property.

FAR: Federal Acquisition Regulation.

FASTLANE: FASTLANE is a high speed asynchronous transfer mode (ATM) encryptor for local and wide area network multimedia applications (i.e., voice, video, data, and imagery). FASTLANE supports permanent and switched virtual circuits, point-to-point and point-to-multi-point, simplex and duplex connections. It provides authentication and end-to-end protection of user information up to the Top Secret/Sensitive Compartmented Information level.

Fiscal Year (FY): A period of 12 months beginning 1 October and ending 30 September of the following year. Fiscal year is designated by the calendar year in which it ends.

Government Furnished Equipment (GFE): A term used in this Task Order to mean equipment in the possession of, or directly acquired by, the Government and subsequently made available for the use by the contractor solely in the performance of this Task Order.

Government Furnished Property (GFP): A term used in this Task Order to mean property in the possession of, or directly acquired by, the Government and subsequently made available for the sole use of the contractor in the performance of this Task Order. Facilities, equipment, and materials in possession of, or acquired directly by the Government, and subsequently provided to the contractor.

Government Off The Shelf (GOTS): Software developed for and owned by the Government.

Guidance: A statement of direction such as, rules, laws, regulations, guidelines, and directives.

Heterogeneous: Environment in which platform architectures may differ.

Homogenous: Environment in which platform architecture is the same.

HSDN LAN: The Homeland Secure Data Network that transmits classified information

Information Technology Management (ITM): Activities related to management support of IT related policy development, strategic planning, capital planning, resource management, and special projects.

PROCUREMENT SENSITIVE

Infrastructure: Identifies the top-level design of communications, processing, and operating system (OS) software and describes the performance characteristics needed to meet database and application requirements. It includes processors, OS, service software, and standards profiles that include network diagrams showing communication links with bandwidth, processor locations, and capacities to include hardware builds versus schedule and costs. The active and passive components used to transfer information between two points. Infrastructure includes items such as cable plant, premise wiring, phone switch, routers, hubs, concentrators, Ethernet switches, and antennae.

Inspection: Determination and identification of the condition of equipment, facilities, services, systems and all other work output, with reference to contractual requirements.

Integration: The result of an effort that seamlessly joins two or more similar products (for example, individual system elements, components, modules, processes, databases, or other entities) to produce a new product. The new product functions as a replacement for two or more similar entities or products within a framework or architecture.

Integrator: A public or private sector entity that develops, assembles, and executes a comprehensive solution to complex information technology requirements.

Interoperability: The condition achieved when information can be exchanged directly and satisfactorily between two or more systems or components. The concept of having free and open methods to share data and IT services among different products of a similar functional capability. Interface standards are adhered to for the maintenance of service availability and consistent access methods. The use of proprietary features is discouraged. Functional categories for interoperability standards include: desktop systems; server systems; printing; network communications; word processing, spreadsheet and presentation applications; calendar and scheduling applications; application serving and license management.

Intrusion Detection System: Provides an additional layer of assurance through the monitoring of network activity to detect and report suspicious, unauthorized, or harmful activities.

Inventory Control: The process of managing, cataloging, and accounting for property provided under this Task Order.

Inverse Multiplexor (IMUX): A device that breaks up a high-speed transmission into several low-speed transmissions, and vice versa. It is used to transmit LAN and videoconferencing traffic over lower-speed digital channels.

Joint Inventory: A physical count of assets conducted by the contractor and the Government for establishing the quantity and condition of property accountable to the Contract.

Key Management: The process of managing keys. This includes ensuring that key values generated have the necessary properties and making keys known in advance to the parties that will use them. The process also ensures that keys are protected as necessary against disclosure and/or substitution.

Knowledge Management: The systematic process of finding, selecting, securing, organizing, distilling, and presenting information in a way that maintains an ongoing corporate knowledge.

Local: Policy or information pertaining to a particular DHS facility. For example, local facility policy refers to the specific policies of each of the DHS facility locations.

PROCUREMENT SENSITIVE

Local Area Network (LAN): Data network system used to provide connectivity within a logical boundary. In most cases, the extent of a logical boundary can be defined by the service area associated with an assigned TCP/IP address space. This includes inter- and intra-building cable plant or fiber plant, Metropolitan Area Network connections, backbones, and any active or passive components required to provide service from the desktop up to a LAN or WAN/ISP interface.

Lot Size: Number of units or product of output from which a sample is derived.

Maintenance: The work required to preserve and maintain a real property facility or piece of equipment in such condition that it may be effectively used for its designated functional purpose. Maintenance includes activities such as preventing damage that would be more costly to repair than to prevent, diagnosing failures, and performing corrective actions to ensure proper operation.

Mission Critical Systems: The systems used to support critical functions such as: Emergency Warning Systems, Operational Voice Systems, Operational LAN Systems, Operational Intercommunication Systems, Operational Fire and Security Systems, Secure Voice Systems (COMSEC).

Multiplexor: A device that merges several low-speed signals into one high-speed transmission and vice versa

Network: A collection of Local Area Networks (LAN)s under the administrative control of one organization. Networks typically use backbone technology to interconnect LANs and are themselves interconnected with the transmission system.

Network Interface: A network interface consists of the physical, logical and management connections where there is a distinct change in management responsibility or technical implementation. This can occur between two distinct networks or between a user device and its supporting network.

National Institute of Standards and Technology (NIST): The Federal technology agency that works with industry to develop and apply technology, measurements, and standards.

Normal Wear and Tear: Loss or impairment of appearance, effectiveness, worth, or utility of an item that has occurred solely because of normal and customary use of the item for its intended purpose.

On-Site: Repairs or services performed at a customer's location.

Organization: An administrative structure with a mission. The term is used in a very broad sense throughout this document.

Other Direct Costs (ODC): Costs not previously identified as a direct material cost, direct labor cost, or indirect cost; a cost that can be identified specifically with a final cost objective that the Offeror does not treat as a direct material cost or a direct labor cost.

Personal Computer (PC): Desktop and notebook computers.

Personal Digital Assistant (PDA): A small, portable, hand held computing device. PDAs offer communications capabilities to include voice, e-mail, SMS, text messaging, and web access.

Performance Requirements Summary (PRS): The portion of the Task Order which documents Task Order requirements, the component requirements related to each Task Order requirement, and the standards and measures of performance.

PROCUREMENT SENSITIVE

Performance Standard: A selected characteristic of an output of a work process that can be measured in order to evaluate performance.

Personally Identifying Information (PII): Any piece of information which can potentially be used to uniquely identify, contact, or locate a single person.

Personal Peripherals: Peripheral devices attached directly to individual desktops or workstations. These devices include printers, scanners, plotters, modems, external hard disks, etc.

Phase-in Period: The period(s) during which the contractor contends with the transfer of performance responsibility from the existing provider to the contractor. During this period the contractor shall organize, plan, recruit personnel, train, mobilize, develop procedures, and accomplish all actions necessary to commence performance of the services at the end of the transition period.

Phase-out Period: The approximately 90 business day period prior to completion of the Task Order.

Preventive Maintenance: Systematic and cyclic check, inspection, servicing and repairs of deficiencies, as well as reporting of deficiencies beyond scope of preventative maintenance. Preventative maintenance includes accomplishment of routine maintenance and repair.

Primary Rate Interface (PRI): A telecommunications standard for carrying multiple DSO voice and data transmissions between two physical locations.

Program: An organized set of activities directed toward a common purpose, objective, or goal undertaken or proposed by an Agency to carry out assigned responsibilities. The term is generic and may be applied to many types of activities. Acquisition programs are programs whose purpose is to deliver a capability in response to a specific mission need. Acquisition programs may comprise multiple acquisition projects and other activities necessary to meet the mission need.

Program Manager: The contractor representative who acts as the point of contact (POC) with the Government and coordinates Task Order management.

Project: A single undertaking or task involving maintenance, repair, construction, or equipment-in-place, in which a facility or group of similar facilities are treated as an entity with a finite scope.

Protocols: Protocols are conventions and algorithms for the transmittal of information over the network. Protocols exist at various layers of the stack and are often used to perform a specific function, a unique network service or application. Service protocols work in conjunction with the transport protocols to complete the required function(s). Examples of service protocols are the Simple Mail Transfer Protocol (SMTP), File Transfer Protocol (FTP), and Hypertext Transfer Protocol (HTTP).

Quality Assurance (QA): Actions taken by the Government to inspect or check goods and services to determine that they meet or do not meet requirements of the Task Order. See Quality Assurance Surveillance Plan for further detail.

Quality Assurance Personnel (QAP): The personnel responsible for surveying the contractor's performance.

Quality Assurance Surveillance Plan (QASP): An organized written document used by Government for quality assurance surveillance. Document contains sampling/evaluation guides, checklists, and the Performance Requirements Summary (PRS).

PROCUREMENT SENSITIVE

Quality Control (QC): Those actions taken by a contractor to control the performance of services so they meet the requirements of the Task Order. See Quality Control Plan for further detail.

Quality Control (QC) Plan: The contractor's system to control the equipment, systems, or services so that they meet the requirements of the Task Order.

Random Sample: A sampling method whereby each service output in a lot has an equal chance of being selected.

Remote Access: Logging into a computer system through a network or modem to execute a command or manipulate data on that system.

Remote Communication: The services that allow a remote user to connect with an address assigned out of the DHS's internal assigned address space. Typical examples of this type of connectivity include: asynchronous modem/terminal server/dial-in service, HSDN and ISDN service, and some wireless modem services.

Reportable Incident: Any event, suspected event, or vulnerability that could pose a threat to the integrity, availability, or confidentiality of systems, applications or data. Incidents may result in the possession of unauthorized knowledge, the wrongful disclosure of information, the unauthorized alteration or destruction of data or systems and violation of Federal or state laws. If such violations are detected or suspected, they are to be reported immediately to a security manager.

Requirement: Effort mandated by this Task Order, issued by a DHS contracting officer (CO) and performed as directed by the CO or their representative (COTR) within the scope of the resulting Task Order.

Restricted Area: Those areas designated by DHS that require control of personnel for security reasons and/or equipment for protection of personnel, property and information.

Return to Service: The time taken to resolve the user's problem to the state that the end user has full functionality restored as specified in the Service Level Agreements and performance metrics.

Routine Call: A request for service with a response time as defined in the Technical Exhibits.

Sample: A sample consists of one or more service outputs drawn from a lot, the outputs being chosen at random.

Scheduled Outage: The maintenance, testing, or other contractor-initiated activity that impacts the user's ability to access network services. A scheduled outage is not considered downtime if the outage is not during business hours and occurs during the COTR approved maintenance window timeframe.

Secure Telephone Equipment (STE): STE is the U.S. Government's current encrypted telephone communications system for wired or "landline" communications. It is intended to replace the older STU-III system. STE is designed to use ISDN telephone lines which offer higher speeds of up to 128k bits per second and are all digital. The greater bandwidth allows higher quality voice and can also be utilized for data and fax transmission. STE sets are backwards compatible with STU-III phones.

Secure Telephone Unit, Third generation (STU III): STU III are a line of secure telephones.

PROCUREMENT SENSITIVE

Security Systems: Defined to be only those that directly support a given communication service. Examples of systems that would be included are: policy enforcement points or PEP security systems, phone or fax encryption systems, authentication or certification systems, and World Wide Web or e-mail proxy systems.

Sensitive: Documents, data, information, systems, products, services, items, etc requiring protection and control because of statutory requirements or regulations.

Server Administration: Services provided in the operation and maintenance of servers. This includes services such as installation of a new server and additional hardware, installation and upgrade of software applications and network operating system, and configuration of hardware and software. This also includes account management, backup and restore, performance monitoring and tuning, security monitoring, problem tracking and error detection.

Service Call: Any notification or request for service as defined in the Technical Exhibits.

Service Category: A classification for a group of services associated with a specific functional use of a desktop computer. This is comprised of service characteristics for the type of support needed by an individual performing a specific desktop computer function. A suite of services will be packaged into a service category to define a service level agreement.

Service Delivery Model: A Service Delivery Model places total responsibility on the contractor for all component services and products needed to meet the customer's requirements. The customer then comes to the single contractor and selects from a menu of services that best meet their needs. All services provided are governed by a Service Level Agreement between the contractor and the customer that stipulates service quality measures, pricing, and customer recourse for poor performance.

Service Level: A unit used to identify characteristics and metrics that define a particular type of support to be provided by the Contractor. Multiple service levels may be needed for a type of service, such as hardware maintenance, to provide various degrees of support needed by a computer user.

Service Level Agreement (SLA): An agreement between the CIO's Office and its supported customer to provide services at stated performance level.

Shall: The word "Shall" is used in connection with the contractor and specifies that the provisions are mandatory as defined by the FAR.

Site Offices/Locations: Those support locations, offices, and facilities listed in TE C.1.3-002.

Software Categories: Desktop software is divided into three types: operating system, utilities, and applications. Operating system software includes Windows XP, Windows VISTA, and their successors. Utility programs perform functions such as disk management, file backup/recovery, file compression, memory management, security, and virus protection. Application programs encompass a wide variety of programs required by the end users to perform their work. Examples of programs in this category are word processors, spreadsheets, email, groupware, desktop publishing, programming languages, compilers, data base managers, and engineering tools.

Software Release: The date that a software developer makes their software product publicly available. This date is often used in determining when a software product is deployed to the computer desktop.

PROCUREMENT SENSITIVE

Standard Operating Procedure (SOP): A comprehensive narrative description of methods prepared by either the Government or contractor. A set of instructions covering those features of operations that lend themselves to a definite or standardized procedure without loss of effectiveness. The procedure is applicable unless ordered otherwise.

Supplies: Items needed to equip, maintain, operate, and support the requirements of this Task Order and the resulting Task Order

System: Any entity that has input, process, output and feedback.

Tactical FASTLANE (TACLANE): Tactical FASTLANE® was developed by the National Security Agency (NSA) to provide network communications security on Internet Protocol (IP) and Asynchronous Transfer Mode (ATM) networks for the individual user or for enclaves of users at the same security level.

Task Order: An order placed for services by the CO in accordance with the terms and conditions of the contract.

Task Order Start Date: Effective date of the Task Order and beginning of the Phase-In Period as authorized by the CO at or following Task Order award.

Test Readiness Review (TRR): TRR is a multi-disciplined technical review to ensure that a subsystem or system under review is ready to proceed into formal test. The TRR assesses test objectives, test methods and procedures, scope of tests, and safety and confirms that required test resources have been properly identified and coordinated to support planned tests.

Throughput Capability: The rate at which data can be transferred over a network. The physical connection point into the operating network is able to support transferring information at this rate. It does not necessarily mean that the computer is powerful enough to transfer information at this rate. The performance requirements will correspond to the slower of either the sender or the receiver of the data transfer. The throughput is to be verified with a standard set of hardware and software. The validation procedure of throughput capability shall be performed at any time during the day. If the specifications are not met, the network shall be considered down.

Transport Protocols: Protocols used specifically to provide the data transfer mechanisms necessary to establish and maintain a reliable communications link to transmit data across a network. These protocols are independent of the media and topology of the underlying sub networks.

User: A person, organization, or other entity that employs IT related services provided under this Task Order and the resulting Contract.

Utilities: Electricity, gas, water, sewage disposal, and steam are types of utilities used under the performance of this Task Order.

Vulnerability Assessment/Risk Analysis: Identifying, characterizing, and testing potential security exposures.

Wireless LAN Systems: The components and systems used to provide network connectivity without requiring 100% physical cable plant connectivity. Examples of these are Bluetooth, infrared, laser, and radio based interconnection services.

Workstation: This is a networked or standalone computer. This computer is normally used for calculation or graphics intensive applications. It includes the CPU, monitor, keyboard, and a mouse or other screen manipulation devices.

C.2.2 ACRONYMS

ACRONYM	TITLE
ACD	Automatic Call Directory
ADPE	Automated Data Processing Equipment
AIS	Automated Information System
AMHS	Automated Message Handling System
APO	Accountable Property Officer
ATO	Authorization to Operate
AV	Audio Visual
BA	Bachelor of Arts
BMO	Budget Management Office
BOM	Bill of Materials
BPA	Blanket Purchase Agreement
BRI	Basic Rate Interface
BS	Bachelor of Science
C&A	Certification and Accreditation
CAP	Contractor Acquired Property
CAR	Contract Administration Review
CATV	Cable Television
CBP	Customs and Border Protection
CBT	Computer-based Training
CCB	Change Control Board
CCI	COMSEC Controlled Items
CDR	Critical Design Review
CDRL	Contract Data Requirements List
CFE	Contractor Furnished Equipment

PROCUREMENT SENSITIVE

ACRONYM	TITLE
CFF	Contractor Furnished Facilities
CFO	Chief Financial Officer
CFR	Code of Federal Regulations
CIA	Central Intelligence Agency
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CISSP	Certified Information Systems Security Professional
CM	Configuration Management
CMM	Capabilities Maturity Model
CND	Computer Network Defense
CNPPD	Chemical and Nuclear Preparedness and Protection Division
CO	Contracting Officer
COCO	Contractor Owned, Contractor Operated
COMSEC	Communications Security
CONOPS	Concept of Operations
COOP	Continuity of Operations Plan
COTR	Contracting Officer's Technical Representative
COTS	Commercial Off The Shelf
CPIC	Capital Planning and Investment Control
CSIRT	Computer Security Incident Response Team
CSU/DSU	Channel Service Unit/Data Service Unit
CVAM	Controlled Vulnerability Assessment Methodology
CVE	Common Vulnerabilities and Exposures
DAA	Designated Accrediting Authority

ACRONYM	TITLE
DAC	Discretionary Access Control
DCAA	Defense Contracting Audit Agency
DCID	Director of Central Intelligence Directive
DHS	Department of Homeland Security
DISA	Defense Information Systems Agency
DITSCAP	DoD Information Technology Security Certification and Accreditation Process
DMS	Defense Message System
DR	Disaster Recovery
DoD	Department of Defense
DoS	Denial of Service
DSN	Database Source Networks
DSS	Digital Satellite Service
DTD	Document Type Definition
DVD	Digital Video Disk
EA	Enterprise Architecture
EACOE	Enterprise Architecture Center of Excellence
EAGLE	Enterprise Acquisition Gateway for Leading Edge Solutions
ECCB	Enterprise Change Control Board
ECR	Engineering Change Request
EDI	Electronic Data Interchange
EDMO	Enterprise Data Management Office
EF	Essential Functions
EIWG	Enterprise Interconnection and Policy Working Group
EML	Environmental Measurement Lab

ACRONYM	TITLE
EOD	Entry on Duty
EPA	Environmental Protection Agency
ERG	Engineering Review Group
ESIGN	Electronic Signatures in Global and National Commerce Act
ESM	Enterprise System Management
ET	Eastern Time
EVM	Earned Value Management
FAR	Federal Acquisition Regulation
FDCC	Federal Desktop Core Configuration
FEMA	Federal Emergency Management Agency
FIPS	Federal Information Processing Standards
FFMS	Federal Financial Management System
FISMA	Federal Information Security Management Act
FITSAF	Federal Information Technology Security Assessment Framework
FOIA	Freedom of Information Act
FY	Fiscal Year
FYHSP	Future Years Homeland Security Program
GAO	Government Accountability Office
GFE	Government-Furnished Equipment
GFF	Government-Furnished Facilities
GFP	Government-Furnished Property
GFS	Government-Furnished Services
GISRA	Government Information Security Reform Act
GOGO	Government Owned – Government Operated

ACRONYM	TITLE
GOTS	Government Off The Shelf
GPEA	Government Paperwork Elimination Act
GPO	Group Policy Office
GSA	General Services Administration
HAZMAT	Hazardous Material
HLSEA	Homeland Security Enterprise Architecture
HQ	Headquarters
HSDN	Homeland Secure Data Network
HSHR	Homeland Security Presidential Directive
HSRD	Hot Standby Router Protocol
I&A	Identification and Authentication
IATO	Interim Authorization to Operate
IAVA	Information Assurance & Vulnerability Assessment
IAW	In Accordance With
IC	Intelligence Community
ICE	Immigration and Customs Enforcement
ID	Identification
IDS	Intrusion Detection System
IG	Inspector General
IMAC	Installation, Move, Add, Change
IMAP	Internet Message Access Protocol
IMEI	International Mobile Equipment Identity
IMUX	Inverse Multiplexor
INFOCON	Information Condition

PROCUREMENT SENSITIVE

ACRONYM	TITLE
IP	Internet Protocol
IRB	Investment Review Board
IS	Information Systems
ISA	Interconnection Security Agreement
ISDN	Integrated Services Digital Network
ISO	International Standards Organization
ISSM	Information System Security Manager
ISSO	Information System Security Officer
IT	Information Technology
ITAC	Information Technology Acquisition Center
ITIL	Information Technology Infrastructure Library
JRC	Joint Requirements Council
KDP	Key Decision Points
KPI	Key Performance Indicator
LAN	Local Area Network
LRU	Lowest Replaceable Units
MAN	Metropolitan Area Network
MCSE	Microsoft Certified Systems Engineer
MD	Management Directive
MOM	Microsoft Operations Management
NAC	Nebraska Avenue Complex
NARA	National Archives and Record Administration
NCS	National Communications System
NIST	National Institute of Standards and Technology

ACRONYM	TITLE
NMC	Network Management Center
NSA	National Security Agency
O&M	Operations and Maintenance
OCA	Office of Chief Administrative Officer
OCIO	Office of the Chief Information Officer
OEM	Original Equipment Manufacturer
OIM	Office of Infrastructure Management
OMB	Office of Management and Budget
OPO	Office of Procurement Operations
ORR	Operational Readiness Review
OSHA	Occupational Safety and Health Administration
OST	Order Ship Time
OTAR	Over-The-Air Rekey
OTAT	Over-The-Air Transfer
P3I	Pre-planned Product Improvement
PBX	Private Branch Exchange
PCO	Property Control Officer
PDA	Personal Digital Assistant
PDD	Presidential Decision Directive
PDR	Preliminary Design Review
PEP	Policy Enforcement Point
PII	Personally Identifying Information
PL	Public Law
PRS	Performance Requirements Summary

ACRONYM	TITLE
PM	Project Manager
PMO	Program Management Office
PMP	Project Management Plan
PMR	Program Management Review
POAM	Plan of Action and Milestones
POC	Point of Contact
PRI	Primary Rate Interface
RAM	Responsibilities Assignment Matrix
RFID	Radio Frequency Identification
ROM	Rough Order of Magnitude
S&T	Science and Technology
QAE	Quality Assurance Evaluator
QAP	Quality Assurance Personnel
QASP	Quality Assurance Surveillance Plan
QC	Quality Control
SBU	Sensitive but Unclassified
SCI	Sensitive Compartmentalized Information
SDLC	System Development Life Cycle
SEC DHS	Secretary of the Department of Homeland Security
SIM	Security Information Management
SIPRNET	Secure Internet Protocol Router Network
SLA	Service Level Agreement
SNMP	Simple Network Management Protocol
SMTP	Simple Mail Transfer Protocol

ACRONYM	TITLE
SMC	Security Management Center
SME	Subject Matter Expert
SMS	Systems Management Server
SOP	Standard Operating Procedure
SP	Special Publication
SRR	System Requirements Review
SSA	System Security Administrator
SSAA	Systems Security Authorization Agreement
STE	Secure Telephone Equipment
STU III	Secure Telephone Unit, Third generation
TACLANE	Tactical FASTLANE
TCP/IP	Transmission Control Protocol/Internet Protocol
TDA	Table of Distribution and Allowances
TE	Technical Exhibit
TRM	Technical Reference Model
TRR	Test Readiness Review
TS	Top Secret
TS/SCI	Top Secret Sensitive Compartmented Information
TSA	Transportation Security Administration
TSS	Technical Source Selection
URL	Uniform Resource Locator
U.S.	Unites States
U.S.C.	United States Code
USM	Undersecretary of Management

ACRONYM	TITLE
VIP	Very Important Person
VOIP	Voice Over Internet Protocol
VTC	Video Teleconference
WBS	Work Breakdown Structure
WCMS	Web Content Management System
WSE	Web Services Environment

PROCUREMENT SENSITIVE

C.3 GOVERNMENT – FURNISHED PROPERTY (GFP) AND SERVICES

Government Furnished Property (GFP) is applicable to the performance of this Task Order. The contractor is authorized to use GFP at the Department of Homeland Security for the duration of this Task Order in accordance with the requirements of this Task Order. The Government shall provide, without cost to the contractor, facilities (office space with desk and chair), equipment (computer, access to printer, copier, and fax), materials (all related office supplies), and/or other services necessary to perform the requirements in the Task Order.

C.3.1 SCOPE

This Section describes the property and services the Government will furnish to the contractor for performance of the requirements of this Task Order. The Government will provide to the contractor the following access for use: (1) Government Furnished Property (GFP) for which the contractor is responsible and accountable; and (2) property only made available to the contractor, as listed below in this section. The contractor shall take all reasonable precautions and such other actions as may be directed by the Government, or in the absence of such direction, in accordance with sound business practice to safeguard and protect Government property in the contractor's possession or custody listed in this section. The contractor shall accept Government-provided automated information systems (AIS) hardware and software without exception. Government Furnished Equipment (GFE) may include Government-leased equipment or Government-owned equipment. Refusal to accept some or all of the GFP offered by the Government shall not relieve the contractor from Task Order performance, but will relieve the Government from the obligation of providing the same or similar GFP at a future date.

The contractor shall not use GFP or services for any other purpose than those described in this Task Order. The contractor shall not remove GFP from DHS facilities or other supported areas without review and written approval of the CO or authorized representative. The provisions affecting GFP under this section shall be IAW FAR 52.245-5. The Government may direct the contractor to develop and /or revise milestones for joint inventory and transfer of GFP.

C.3.1.1 Government-Furnished Property

C.3.1.1.1 The Government intends to share space with the contractor personnel in the Government facilities indicated in TE C.3.1-002 or as designed by the Government for the duration of this Task Order and only for the performance of this Task Order. This is not considered Government Furnished Property (GFP) requiring property administration IAW FAR 45 plus Supplements.

C.3.1.1.2 Marking Property: The contractor shall not mark or affix any decals, emblems or signs portraying the contractor's name or logo to Government Equipment, Facilities, or Property except as directed by the COTR.

C.3.1.2 Government-Furnished Services

C.3.1.2.1 Telephone Service: The Government will furnish telephone service at contractor-occupied Government sites to include local and long-distance calls.

C.3.1.2.1.1 The contractor shall comply with DHS rules and regulations regarding telephone use. The contractor shall reimburse the Government the cost of unofficial telephone service (e.g., telephone service not incidental to performance of the Task Order).

PROCUREMENT SENSITIVE

C.3.1.2.1.2 The contractor shall obtain prior Government review and written approval before connecting or disconnecting any Contractor Furnished Equipment (CFE) to Government-furnished communications systems or equipment.

C.3.1.2.2 Local Area Network (LAN): The Government will provide limited access to the existing LAN at contractor-occupied Government facilities to include E-Mail capability. The contractor shall not use the LAN for purposes other than for work required under this Task Order.

C.3.1.2.3 Paper Products: The Government will make available containers in shared Government facilities for the collection of recyclable paper.

C.3.1.2.4 Reporting Discrepancies in Performance of Government Furnished Service Contracts: The contractor shall report discrepancies in performance of Government-provided services to the CO or COTR.

C.3.1.3 Supplies and Materials

C.3.1.3.1 Existing Levels of Supplies and Materials: The Government will make available existing Government owned parts, supplies and material to the contractor for use in the performance of the requirements of this Task Order. The Government will furnish the existing levels of Government supplies and materials to the contractor and the contractor shall provide existing levels of Government supplies and materials to the Government during phase-out. The Government will furnish replacement materials required to maintain the serviceability of production equipment on a time and materials basis. The government will furnish all items to the contractor as GFE to use under this Task Order. DHS purchases all hardware, software, warranties and parts using the FirstSource contract.

C.3.1.4 Government-Furnished Equipment (GFE)

The Government will provide GFE (such as telecommunications, computers, network components, storage devices, software, and peripherals) to the contractor to complete the duties of this Task Order with the exception of equipment for the Help Desk and unclassified Test Lab.

C.3.1.4.1 Equipment Offered for Contractor Use: The Government will furnish property from the Product Guide provided at TE C.3.1-001. Original Equipment Manufacturer (OEM) Software is provided at TE C.3.1-002. The result of the last inventory of equipment in the metropolitan Washington D.C. area and other select locations is provided at TE C.3.1-003.

C.3.1.4.2 Contractor Accountability

C.3.1.4.2.1 Transfer of Accountability: The contractor shall become accountable for GFE when assigned.

C.3.1.4.2.2 Property Administration: The contractor shall perform property administration in accordance with FAR Part 45.

C.3.1.4.2.3 Report of Government Property: The contractor shall prepare and submit to the COTR an annual Report of Government Property as directed by the COTR. (CDRL C.3.1-2, Government Property Report – Annual)

C.3.1.4.3 Turn-In and Replacement

PROCUREMENT SENSITIVE

- C.3.1.4.3.1 Turn-In of GFE: The contractor shall prepare a recommendation for excess when GFE is no longer required or suitable for its intended use, or has reached the end of its technical life. The contractor shall provide these recommendations to the COTR who will make the final determination of the disposition of the equipment. Upon approval, the contractor shall process the items in accordance with applicable Federal regulations, and Department of Homeland Security policies and regulations. All Government furnished property and IT equipment identified in this Task Order shall remain the property of the Government.
- C.3.1.4.3.2 Replacement of GFE: The contractor shall coordinate with the CO for replacement of GFE. Upon approval by the CO, the item(s) of equipment to be replaced will be deleted from the GFE listing. If required to maintain performance standards, the Government will provide comparable GFE replacement. The contractor shall contact the Help Desk for problems regarding computers and peripherals. The Government will replace computers and peripherals.
- C.3.1.4.4 Initial Inventory Assessment and Accountability
- C.3.1.4.4.1 Initial Inventory Procedures:
- C.3.1.4.4.2 The contractor shall conduct inventory of government property such as keys; property received from the designated property control officers; and materiel items of work in progress; e.g., items in various stages of repair. This provision does not preclude prior inspection of GFP by the contractor. The operational or conditional status of all GFF and on-site GFE shall be determined and the contractor shall record any item found to be broken or not suitable for its intended purpose. The contractor shall keep the inventory listing current. (CDRL C.3.1-3, Government Property Inventory-Initial)
- C.3.1.4.4.3 The contractor shall inspect all GFE at the time of the inventory. The contractor shall note all valid discrepancies, and the Government may correct the discrepancies by one or more of the following methods at the Government's option. The Government may elect not to provide equipment to the contractor; or may correct noted discrepancies prior to performance period start date; or may require the contractor to repair discrepancies subject to reimbursement by the Government. The COTR will determine validity.
- C.3.1.4.5 Withdrawal of GFE: The Government retains the right to withdraw any GFE at any time during the performance of the Task Order. When possible, the Government will provide at least 30 business days notice of the impending withdrawal of GFE when deemed necessary or appropriate.
- C.3.1.4.6 Equipment and Software Manuals: After the inventory, the Government will turn over to the contractor equipment operating manuals presently maintained by the Government. The contractor shall update these documents as new issues are published. Updated manuals are the property of the Government upon completion or termination of this Task Order.

C.4 CONTRACTOR – FURNISHED PROPERTY AND SERVICES

C.4.1 SCOPE

The contractor shall furnish all materials, supplies, tools, services, temporary work places, and equipment required to perform this Task Order, except for the items specifically identified as Government-Furnished in Section C.3 of this Task Order.

C.4.1.1 Contractor-Furnished Facilities (CFF)

The Government will provide those facilities and installed equipment as listed and identified in Section C.3 of this Task Order. The contractor shall not place, construct, or otherwise provide additional buildings or facilities on DHS premises without prior CO approval. The contractor shall provide the Help Desk facility. The contractor may provide Test Lab facilities and the associated hardware and software via a separate logical follow-on Task Order for the Test Lab requirements specified in this Task Order.

C.4.1.1.1 CFF Listing: The contractor shall provide to the CO or COTR an initial and updated list of Contractor Owned, Contractor Operated (COCO) facilities/real property used in performance of this Task Order. The contractor shall provide the location of the Help Desk and Test Lab used in performance of this Task Order to the CO or COTR. (CDRL C.4.1-1, Contractor Owned, Contractor Operated Facilities List (used in Task Order performance)).

C.4.1.1.2 Keys, Ciphers, Combinations, and Security Clearances: The contractor shall maintain records identifying those members of the contractor's workforce at Government facilities who shall be authorized the use of keys, codes, ciphers, combinations and security access.

C.4.1.1.3 The contractor may be required to provide additional storage space for IT equipment and services associated with this Task Order.

PROCUREMENT SENSITIVE

C.5 SCOPE OF WORK

The Information Technology Services Office provides support for DHS operations at various facilities and locations in, and around, the Metropolitan Washington D.C. area and at locations throughout the U.S. The number of supported locations is projected to increase throughout the U.S. TE C.1.2-002 provides facility locations and TE C.1.3-002 provides the projected number of seats by Fiscal Year (FY) for each of the three Local Area Networks (LANs).

In performing the Scope of Work identified herein, the contractor shall conduct all operations support for Information Technology Services Office with a proactive and technologically aggressive methodology. The methodology shall identify more effective, efficient or alternative forms of new IT advancements that would provide a heightened level of performance for DHS operations. The contractor shall forecast new IT trends and update, brief, and coordinate with DHS management to provide a comprehensive system of knowledge disclosure. The contractor shall use information from market research and market analysis findings to identify new or updated IT technologies, equipment, and data acquisition and availability as well as advancements in hardware, software and supporting system infrastructure. The contractor, as part of full knowledge transfer and disclosure shall perform subjective and comparative analysis to existing DHS technology identifying advancements and efficiencies. If authorized by the COTR, the contractor shall perform and conduct operational and theoretical performance evaluations of current IT capabilities with contractor identified, proposed or updated IT advancements.

C.5.1 APPLICATIONS MANAGEMENT, SUPPORT, AND DEVELOPMENT

The contractor shall manage and maintain all deployed applications for full functionality and continuous availability on all Department of Homeland Security (DHS) systems. The Government defines continuous availability as full functionality of all applications from the desktop client. All applications are run on DHS Data Center Servers. The contractor shall maintain full functionality of file and data storage and retrieval, printing, remote access, and messaging services to authorized users. A list of the supported applications is provided in the Product Guide Software Section at TE C.3.1-001, Government Furnished Equipment.

C.5.1.1 Application Management Services

- C.5.1.1.1 The contractor shall manage and support required applications, provide reporting and documentation deliverables, and a single-point of accountability. The nature of applications maintenance for COTS operating systems and software is to provide patches, pushes, and OEM updates.
- C.5.1.1.2 The contractor shall provide software development/tailoring services as required to facilitate the creation and/or migration of applications into enterprise environments to include the Web Services Environment (WSE) for DHSOnline and DHSInteractive, the Department's intranet and extranet portals. A list of the current custom applications is provided at TE 5.1-001.
 - C.5.1.1.2.1 Requirement Analysis: The contractor shall provide requirement elicitation, analysis and management services in support of applications/databases/systems. The products of this effort are requirement documentation.
- C.5.1.1.3 Functionality Enhancement: The contractor shall provide the support effort of application development. Activities include defect correction, software tailoring to develop functionality enhancements and activities such as user profile management and training.

PROCUREMENT SENSITIVE

C.5.1.1.4 The contractor shall develop a proposed applications consolidation and rationalization plan to provide a utility computing platform. The contractor shall submit the plan to the COTR for approval. (CDRL C.5.1-1, Applications Consolidation and Rationalization Plan)

C.5.1.1.4.1 The contractor's plan shall comply with DHS enterprise configuration and change management requirements.

C.5.1.2 Status and Availability of Major Applications on the Network

C.5.1.2.1 As required for determining network status, the contractor shall provide DHS an Up/Down Status Report of Major Applications on the Network indicating the availability and functionality of applications for end users. Up/Down Status refers to network and server applications and not to desktop-resident applications. This report shall include an up/down status of all network and server applications.

C.5.1.2.2 The contractor shall provide the COTR access to NMC systems for real-time status of all major applications integral to the network at all times.

C.5.1.3 Application Maintenance and Operation Documentation

C.5.1.3.1 The contractor shall provide on a weekly basis, status reports for DHS applications that cover the following data points

- Funding level
- Significant Events/Outages
- Summary of O&M activity

C.5.1.3.1.1 The contractor shall also provide a root cause analysis report (within 48 hours of the incident) to the Government following any outages on DHS Applications. The report shall include the following:

- Root cause of outage
- Remediation activities
- Mitigation activities
- Recommendation for platform enhancement to prevent recurrence

C.5.1.4 Application Database and Systems Maintenance

The contractor shall establish and maintain an application maintenance schedule. The contractor shall coordinate with the Government to schedule any application maintenance downtime sufficiently in advance to enable smooth operations during maintenance windows. Any scheduled jobs, any automated processes (Chronologic Jobs that operate at predefined time intervals or that occur following notifications), or periodically timed or batched tasks shall also be considered applications.

C.5.1.4.1 The contractor shall identify the requirements for and install upgrades, updates, service packs, and patches.

C.5.1.4.2 The contractor shall maintain security protection and reliability updates on operating systems.

C.5.1.4.3 The contractor shall identify and notify the COTR of any upgrades, updates, service packs, and patches determined to be incompatible with system or application specifications and proceed as directed by the COTR.

PROCUREMENT SENSITIVE

C.5.1.4.4 The contractor shall provide recommendation for preempting and/or resolving any system performance issues.

C.5.1.5 Performance Trends of Major Applications on the Network

C.5.1.5.1 When requested by the Government, the contractor shall provide DHS a Performance Trend of Major Applications on the Network Report. (CDRL C.5.1-5, Performance Trend of Major Applications on the Network Report)

C.5.1.5.2 The contractor shall also maintain and provide historical data on the performance of each application to DHS in the form of trend reports. DHS will use these reports to assess the performance of each application. Data for trend reports shall be maintained in the knowledge database.

C.5.1.5.3 The contractor shall collect, maintain and update this data, along with all other knowledge that can be used to enhance IT operations, in a COTR accessible knowledge database; data shall include date and time.

C.5.1.6 Enterprise Desk Application Licensing

C.5.1.6.1 The contractor shall evaluate the available and pre-existing DHS enterprise software license agreements and shall make use of them to the extent possible and practical.

C.5.1.6.2 The contractor shall track and deploy all software licenses required to perform the DHS mission and provide a list of the licenses to the COTR. The COTR may direct the contractor to administer the purchase of software on behalf of the Government off of DHS designated licensing Task Order vehicles.

C.5.1.7 Collaborative Applications

C.5.1.7.1 The contractor shall make recommendation on purchases to support collaborate applications and functionality. The DHS will consider the recommendations and purchase approved collaborative applications through FirstSource and provide the applications as GFE

C.5.1.7.2 The collaborative applications are items such as the following:

- Secure e-mail for authorized users
- A comprehensive suite of software tools to improve authorized users' abilities to share and collaborate on secure data both on DHS systems and on authorized, interconnected networks

C.5.1.8 Application Development

The contractor shall provide Application Development services as directed by the COTR. Application Development services shall be accomplished in response to Logical Follow-On Task Orders on a case by case basis.

C.5.1.9 Ensure New Acquisitions Include Common Security Configurations

The contractor shall comply with Office of Management and Budget policy memorandum M-07-11, "Implementation of Commonly Accepted Security Configurations for Windows Operating Systems" which states: "agencies with these operating systems (Windows XP and VISTA) and/or plans to upgrade to these operating systems must adopt these standard security configurations by February 1, 2008." The standards are as follows:

- The contractor shall certify applications are fully functional and operate correctly as intended on systems using the Federal Desktop Core Configuration (FDCC). This

PROCUREMENT SENSITIVE

includes Internet Explorer 7 configured to operate on Windows XP and Vista (in Protected Mode on Vista).

- For the Windows XP settings see http://csrc.nist.gov/itsec/guidance_WinXP.html
- For the Windows Vista settings see http://csrc.nist.gov/itsec/guidance_vista.html
- The standard installation, operating, maintenance, update, and/or patching of software shall not alter the configuration settings from the approved FDCC configuration. The information technology should also use the Windows Installer Service for installation to the default “program files” director and should be able to silently install and uninstall
- Application designed for normal end user shall run in the standard user context without elevated system administration privileges.

C.5.2 DEPLOYMENT SUPPORT

C.5.2.1 Provide Deployment Support

The Government shall require deployment support services for short-term and long-term deployment projects. The contractor shall provide deployment support for all DHS sites, including sites requiring Sensitive but Unclassified (SBU), Homeland Secure Data Network (HSDN), and Top Secret access, with seamless conversion from any existing network assets, failover capability, high availability during transition and operation, and temporary relocation support. The contractor shall perform installation planning and scheduling, site documentation preparation (e.g. configuration drawings), equipment staging, installation, and checkout for DHS sites. The Government will provide a technical project manager for each deployment project.

C.5.2.1.1 The contractor shall apply and adhere to IT Project Management policies and procedures for all deployment projects.

C.5.2.1.2 The contractor shall collect and document customer requirements, review the scope of the effort with the customer, and determine the required equipment and mutually agreed upon pricing for delivery of those services.

C.5.2.1.3 The contractor shall develop a Deployment Project Plan for each project and submit to the Government Operations and Maintenance (O&M) and/or Engineering Branch Chief as applicable for approval.

C.5.2.1.4 The contractor shall develop a Rough Order of Magnitude (ROM) for the proposed services as part of the Deployment Project Plan, which the Government will use to develop additional task orders for build-out and deployment services under this Task Order. This initial tasking or the specific build-out task establishes the performance levels for subsequent task orders.

C.5.2.1.5 The contractor shall conduct site surveys, prepare site reports, network diagrams, develop bill of materials (BOM), and any other required documentation associated with the completed site survey.

C.5.2.1.6 The contractor shall evaluate, complete, and submit to the Government Operations and Maintenance (O&M) and/or Engineering Branch Chief as applicable for approval, a review and report on proposed workspace to determine if the existing facilities infrastructure can adequately support the communications and information technology equipment.)

C.5.2.1.7 The contractor shall provide the COTR and the customer organization with a trip report.

PROCUREMENT SENSITIVE

C.5.2.1.8 The contractor shall prepare a detailed site report for each site that identifies equipment, internal and external interconnects, site integration plan, and site drawings and submit it to the Government Operations and Maintenance (O&M) and/or Engineering Branch Chief as applicable for approval when requested.

C.5.2.1.9 The contractor shall install new, enhanced, or replacements of hardware and/or software and the physical infrastructure, as required (e.g., wiring, cable plant) for DHS and other federal agencies systems and facilities as directed by the COTR.

C.5.2.2 Develop Deployment Plan Template

The contractor shall develop the DHS Deployment Plan Template and submit to the COTR for approval. (CDRL C.5.2-5, DHS Deployment Plan Template) Using the approved template, the contractor shall develop, maintain, update and implement specific Deployment Project Plans.

C.5.2.2.1 The contractor Deployment Plan shall, at a minimum, address the following:

- Deploy and maintain a stable and highly available system in accordance with appropriate performance standards
- Utilize highly trained maintenance technicians and systems engineers to minimize repair calls and promote minimal user disruption
- Demonstrate the availability to support geographically dispersed deployments.
- Provide special support for reviewing of cabling plans throughout current and potential locations

C.5.2.3 Site Activation

Upon COTR direction, the contractor shall execute the Government approved solution identified in accordance with the Deployment Project Plan to ensure seamless installation/integration. The contractor shall develop a formal acceptance process and submit to the COTR for approval. (CDRL C.5.2-6, Site Acceptance Process) The contractor shall provide Test Plans and Test Results to the Government Operations and Maintenance (O&M) and/or Engineering Branch Chief as applicable. (

C.5.2.4 Facilities Modifications

The contractor shall provide facility modification services, when requested by the COTR, in accordance with all applicable executive orders, presidential directives, other federal and DHS laws, federal orders, management policies, handbooks, guidelines, processes, and procedures. All facility modifications shall be integral to and necessary for the successful performance of the IT services provided under this Task Order.

C.5.2.4.1 The contractor shall identify and coordinate complete facilities infrastructure modifications according to the approved plan(s).

C.5.2.5 Installation and Checkout

C.5.2.5.1 The contractor shall perform installations and checkouts in accordance with the Deployment Project Plan.

C.5.2.5.2 To provide seamless transition services and promote high system availability, the contractor shall perform onsite installation checks for all deployed equipment. These checks shall verify system and network operation

PROCUREMENT SENSITIVE

and capability and be completed with results provided within ten days of system move or transition.

- C.5.2.5.3 The contractor shall provide to the COTR, a summary of results in accordance with the Deployment Project Plan or as requested in a Status Report

C.5.2.6 Transition to O&M

- C.5.2.6.1 The contractor shall transition to O&M processes in accordance with DHS policy and procedure.

C.5.2.7 Engineering and Project Management

- C.5.2.7.1 The contractor shall provide engineering and project management support for DHS deployment projects.
- C.5.2.7.2 The contractor shall attend and participate at project related meetings to resolve operational problems and issues as directed.

C.5.3 INFRASTRUCTURE ENGINEERING SERVICES**C.5.3.1 On-site Engineering Team**

The contractor shall provide a dedicated on-site engineering team that performs services to support DHS projects (e.g., new architecture or infrastructure designs, new deployments of network/systems, etc.), and provide support for operation and maintenance activities (maintenance of infrastructure, maintain stability of environment, monitoring, and technology refreshment etc.).

- C.5.3.1.1 The contractor Engineering Team Leader, and other technical personnel as appropriate, shall attend all meetings as directed by the COTR and contribute to specific technical working groups, change control boards and change management boards set up to address engineering operations and issues with DHS Components and other Government agencies. The contractor shall structure the technical requirements/knowledge base of the team based on the current needs of DHS.

C.5.3.2 Systems Engineering Support

The contractor shall perform the design, testing, implementation, configuration validation, operation, maintenance, administration, management, backup, and recovery of DHS IT infrastructure systems, to include servers and storage devices, with an overarching system engineering function used to guide and direct the overall value and effectiveness of the system. This function shall provide support to further refine and improve on the solution as technology, business needs, and the DHS IT infrastructure mission evolve.

Projects may consist of the building and deployment of new networks and infrastructure components such as databases, servers of many types, network storage devices, other network components, and desktops/workstations, as well as the removal of existing network features and infrastructure components. Projects may include features, which require the installation and removal of hardware such as switches, servers and routers, databases, servers of many types, storage devices, desktops/workstations and installation and un-installation of infrastructure components. Projects also may include addition and removal of security features such as antivirus, auditing tools, and policy enforcement points (PEP)s. The contractor shall complete all work in each DHS environment classification: Unclassified, Secret and Top Secret.

Engineering projects include tasks such as the following:

- E-mail and messaging services
- File share services
- Active directory services
- Storage area network services
- Backup and archive technologies
- Blackberry and wireless technologies
- Management, configuration and utility servers
- Network configuration and planning
- Client platform designs including software images and hardware configurations
- New infrastructure designs and user rollout support
- Network and server enhancements based on recommended best practices, and technical assessments

C.5.3.3 Engineering Projects

The contractor can expect to perform the following types of engineering projects:

- C.5.3.3.1 The contractor shall provide network engineering services associated with the replacement of infrastructure components or the implementation of improvements to the deployed network infrastructure planned or initiated by DHS.
- C.5.3.3.2 The contractor shall engineer, all telecommunication, Local Area Network (LAN), Wide Area Network (WAN) circuits and connectivity to DHS systems with Government organizations and designated DHS business partners.
- C.5.3.3.3 The contractor shall perform Client Configuration Management Engineering, develop and manage the approved images and overlays on those devices managed by the contractor including engineering, building, deploying and maintaining DHS approved images for all LANs.
- C.5.3.3.4 The contractor shall provide Engineer and Build Solutions for deployments and engineering project management support for deployments of new facilities and upgrades of existing facilities throughout the DHS. Possible deployment projects include both new facilities and upgrades to existing facilities.
- C.5.3.3.5 The contractor shall conduct technology refreshment projects in accordance with DHS guidance and upon approval of the COTR.
- C.5.3.3.5.1 The contractor shall recommend new products and technology for supporting all layers of the IT infrastructure architecture.
- C.5.3.3.6 The contractor shall perform the engineering design for the Security Management Center (SMC) and design all systems to ensure positive authentication of each user before granting system access. The SMC in this form does not exist today, and the contractor shall propose a solution for this requirement.
- C.5.3.3.6.1 The contractor shall perform support for sustaining forensics within the SMC.

PROCUREMENT SENSITIVE

C.5.3.3.7 The contractor shall provide Video Tele-Conferencing Engineering Support to include design, conduct market research and document video capabilities needed in accordance with their assigned engineering support duties.

C.5.3.3.7.1 The contractor shall make recommendations to the Government for acquiring video conferencing system hardware and software and for improvements to existing systems.

C.5.3.3.8 The contractor shall perform Satellite/Cable TV Engineering including design, implement, and document facility and individual television infrastructure.

C.5.3.3.9 The contractor shall perform Phone and Private Branch Exchange (PBX) Engineering including design, implement, and document the telephony infrastructure.

C.5.3.3.10 The contractor shall provide engineering support for implementing and integrating applications developed by external DHS Contractors or internal DHS employees into DHS data centers.

C.5.3.3.11 The contractor shall provide engineering support for Continuity of Operations (COOP) and Disaster Recovery (DR) to ensure DHS functions and capabilities are not lost or diminished during periods when services or components are unavailable.

C.5.3.3.12 The contractor shall provide Security Architecture Engineering Support. The DHS security architecture provides policy enforcement support for all network enclaves. The contractor shall abide by and follow all Government and DHS directives regarding the selection of security products, the configuration and hardening of operating systems, and for all cryptographic devices.

C.5.3.3.12.1 The contractor shall assist the Government in continuously updating and enhancing the DHS security architecture throughout the life of the Task Order.

C.5.3.3.12.2 The contractor shall implement an Identification and Authentication (I&A) system for all users and shall implement a strong capability for administrative and remote users.

C.5.3.3.12.3 The contractor shall implement a Discretionary Access Control (DAC) capability providing need-to-know based access for each COTR specified user of the applicable systems.

C.5.3.4 Engineering Process and Methodology

C.5.3.4.1 The contractor shall use an engineering development lifecycle methodology consistent with ITIL framework to support projects initiated by DHS. The contractor's methodology shall include the following as a minimum:

- Requirements Definition
- Detailed Systems Design Document
- DHS Enterprise Configuration Board Review
- System Testing

PROCUREMENT SENSITIVE

- Operational instructions
- Train operations personnel in new processes or activities as required
- Implementation Instructions and Document Delivery to Deployment and Operations
- Engineering Change Request (ECR) as required
- Obtain Operations Sign-off on Change and Deliver Documentation
- Concept of Operations (CONOPS)
- Project Implementation
- O&M Assistance

C.5.3.4.2 Configuration Management (CM)

C.5.3.4.2.1 The contractor shall support CM Boards and Project Teams through activities and deliverables such as project status reports, design documents, design validation, migration planning, service delivery guidance, and implementation support documents.

C.5.3.4.2.2 The contractor shall develop, maintain, update, and implement CM plans and procedures; control configuration baselines and conduct functional and physical configuration audits and formal qualifications reviews.

C.5.3.4.2.3 The contractor shall submit proposed changes to DHS systems or to project baselines, to the Change Control Board (CCB) and the Engineering Review Group (ERG), maintain a record of all submitted and approved changes, and maintain a schedule of deliverables showing both the scheduled and actual delivery dates.

C.5.3.4.2.4 The contractor shall develop, maintain, update, and implement a Configuration Management Data Base (CMDB), an engineering release system, a configuration item development record (including the configuration index and change status listing), configuration status accounting, and support the CCB.

C.5.3.4.2.5 The contractor shall maintain configuration management of all images and provide Gold Copy images to the Government as a deliverable to this task within five business days of any approved changes.

C.5.4 TESTING**C.5.4.1 Test Support and Documentation**

The contractor shall establish and operate a test environment to perform hardware, software and systems testing. The test environment shall include testing for engineered systems including networks, video, and phone systems. The contractor shall supply systems engineering oversight, identification of readiness criteria for all system milestones, and verification and validation oversight to include test success criteria, test plans, and requirements verification traceability to demonstrate that all implementations meet requirements as stated in the requirements database. The contractor shall propose a test environment architecture and a standardized test template that supports DHS engineering projects. This support shall also include the development of individual test plans for each individual test project approved by the COTR.

C.5.4.1.1 The contractor's test template shall define the scope and approach for testing and acceptance. At a minimum, the template shall address the

PROCUREMENT SENSITIVE

following: initial receipt of hardware and software, unit level testing of software components for any developed software, hardware and software integration and installation testing, and system end-to-end testing in a simulated operational environment.

C.5.4.1.1.1 The contractor's test template shall also include methodology and a systematic approach for testing external interfaces to agencies and entities.

C.5.4.1.1.2 The test template shall describe the roles and responsibilities of the contractor, the DHS program office, users, stakeholders, and external systems, the test facilities used for each testing event, and the data and sources used during testing events. The template shall describe the test plans and procedures developed for each testing event, the testing events and sequences (schedule) in which they will occur, and the integration of the testing events and the security certification and accreditation activities. The contractor performing IT-NOVA O&M shall complete all of the documentation required for C&A. IT-NOVA Program Management Office personnel shall accomplish the actual C&A.

C.5.4.2 Test and Development Lab

The contractor may be required to establish, operate and maintain a test laboratory, using CFE, to support the DHS IT Infrastructure Systems. The contractor may provide its' own existing test lab to support this effort. The test lab shall be located in the Washington DC Metro area, and a segment of the test lab shall be capable of handling tests of Top Secret information. The Government will determine the exact requirements of this facility after the Task Order is awarded. The contractor shall provide personnel to operate and maintain a Government provided classified test lab in an undetermined Government facility. The Government will provide more information on the location and requirements of the classified test lab as it becomes available.

C.5.4.2.1 The contractor shall provide support to developers and customers performing integration and test activities. The contractor shall provide support during the hours of 8:00 am ET to 5:00 pm ET, Monday – Friday, excluding Federal holidays. The contractor shall also provide support after hours, on weekends and on Federal holidays for purposes such as deployments, maintenance and extended testing support as directed by the COTR.

C.5.4.2.2 The contractor shall make configuration changes in the test laboratory and production environments at the direction of the COTR. The contractor shall plan for future configuration changes and production deployments in coordination with the COTR. The contractor shall make configuration changes in compliance with security policies and procedures and change control procedures. Configuration changes shall be in accordance with controlled and repeatable procedures established by the contractor and approved by the COTR.

C.5.4.2.3 The contractor shall document test procedures and configurations performed by the contractor relating to the support of testing activities.

C.5.4.2.4 The contractor shall track the status of actions and tasks performed by them in support of testing activities.

C.5.4.2.5 The contractor shall notify the COTR regarding any issues or risks that affect the performance of current or scheduled test activities. The contractor

PROCUREMENT SENSITIVE

shall notify the COTR within three business days of discovery of an identified issue or risk that could affect performance of the test activities. The contractor shall provide the COTR a complete description of the issue, diagnosis, resolution actions undertaken, and the impact on the timeframe for test activities.

- C.5.4.2.6 The contractor shall perform Microsoft Exchange and Active Directory Configurations activities such as configuring Exchange and Active Directory; installing software; verifying currency of installed software; and configuring security settings, databases, and user accounts and permissions.
- C.5.4.2.7 The contractor shall install communications and network infrastructure components to support test requirements.
- C.5.4.2.8 The contractor shall create, update and maintain standard workstation images, commonly referred to as ghosts, to support deployment to the desktop. The images shall meet all stated standards for "as-is" current production environment and "to-be" production environment. The contractor shall provide the Integration and Testing with the standard mechanism for delivery of the application to the desktop.
- C.5.4.2.9 The contractor shall maintain web based applications in the test environment by performing activities such as installing upgrades, patches and service packs, assigning user names and passwords, and assigning user permissions.
- C.5.4.2.10 The contractor shall provide support to the Testing Lab by performing activities such as reviewing new application architecture, verifying that the application architecture supports the current DHS environment, and submitting findings to the COTR.
- C.5.4.2.11 The contractor shall perform a production readiness review in order to determine whether a system is ready for deployment into the production environment.

C.5.5 OPERATIONS AND MAINTENANCE FOR END USER SUPPORT

C.5.5.1 End User and Desk Side Support

The contractor shall provide a detailed End User and Desk Side Support Concept of Operations that includes elements such as a detailed description of processes, procedures, policies, WBS, organization chart, work flow, detailed performance metrics, and evaluation criteria for the entire Help Desk operations including Tier 1, 2 and 3, and field site support (CDRL C.5.5-1, End User and Desk Side Support Concept of Operations).

The End User and Desk Side Support Concept of Operations Plan shall demonstrate a proactive and aggressive methodology to pursue new IT technological advancements and trends applicable to help desk and desk side support such as conducting frequent and thorough market research and analysis of new IT technologies and equipment including software based upon a subjective and comparative analysis to existing DHS technology. If authorized by the COTR, the contractor shall perform and conduct operational and theoretical performance evaluations of current IT capabilities with contractor proposed IT advancements.

PROCUREMENT SENSITIVE

The contractor's Concept of Operations Plan shall meet the following minimum requirements: Provide continuous operation 7X24X365 (366 for leap years) helpdesk and 5x12 desk side support operations, with provision that designated VIPs are entitled to on call support, that includes call center support, Network Systems Monitoring, Tier 1 (Help Desk Services) including remote desktop management for Commercial Off The Shelf (COTS) and Government Off The Shelf (GOTS) applications and Tier 2 "(Desk Side Support) services as well as Tier 3 Engineering support for diagnosing and resolving end user problems unresolved by the second-level analysts. The Government reserves all rights stated for review and personnel disposition. TE C.5.5-001 provides one year's monthly Help Desk Ticket Data workload. The Following represents a portion of the workload for 2006 O&M services:

Category	Workload
LAN – A E-mail Messages	72,335,644
LAN – A Support Requests	86,565
LAN – A Active Accounts	5,976
LAN – HSDN E-mail Message	1,105,254
LAN – HSDN Support Requests	3,104
LAN – HSDN Active Accounts	1,894
LAN – C E-mail Messages	767,307
LAN – C Support Requests	11,029
LAN – C Active Accounts	1,350
VTC Sessions	2,292
Unclassified Voice Conference Bridge	21,628
DMS Messages	228,413
AMHS Messages	517,611
Secure Fax	18,988
PBX Support	16,059
Total E-mail Messages	74,208,205
Support Requests	100,698

C.5.5.1.1 Help Desk Operations through Tier 3 Engineering Support: The contractor shall design the Help Desk to act as the primary interface to the end users of various COTS and custom-developed applications. DHS currently has email and telephonic help desk contact capabilities. The contractor shall propose the contact methods (e.g. phone, fax, web, e-mail, chat) for contacting the help desk. The contractor shall provide seamless call distribution and call

PROCUREMENT SENSITIVE

management support. In accomplishing this function, the DHS requires the contractor to provide a comprehensive, state-of-the-art, Help Desk solution that aligns with industry best practices, and that represents the best value to the Department and the Government.

- C.5.5.1.1.1 The contractor shall provide the help desk facility and its associated IT infrastructure at a location(s) that is located at least 50 miles outside of the metropolitan Washington D.C. area and inside the continental U.S.
- C.5.5.1.2 The contractor shall design, implement, and maintain a DHS approved COTS enterprise help desk system capable of interfacing and reporting to DHS systems as required. Additionally, this system shall provide a knowledge base for use by Tier 2, and 3 technicians and provide self-help for end users. All data generated, stored, and maintained in the system remains the property of the Government.
- C.5.5.1.3 The contractor shall provide on-site and field office support comprised of personnel with appropriate level of security clearances who will resolve complex technical problems of laptops, desktops, network peripheral devices, network components, storage devices, and troubleshooting of various software- and hardware-related issues.
- C.5.5.1.4 The contractor shall provide infrastructure advanced operational support and infrastructure services to DHS. The contractor shall perform troubleshooting to isolate the source of, diagnose and/or resolve, or assist in the resolution of IT and telecommunications problems (end-to-end).

C.5.5.2 Maintenance

- C.5.5.2.1 The contractor shall develop a Preventative Maintenance Plan, Preventative Maintenance Policies and Preventative Maintenance Procedures for all DHS IT and telecommunications fixed and mobile systems/equipment. The contractor shall provide to the COTR the plan within 40 business days of Task Order start, the policies within 60 business days and the procedures within 120 business days. (CDRL C.5.5-2, Preventative Maintenance Plan, Policies and Procedures)
- C.5.5.2.2 The contractor shall perform preventative maintenance on DHS system components in accordance with the DHS approved Preventative Maintenance Plan, policies and procedures. This includes personnel to perform the support and maintenance of data center assets, except for OEM warranty and maintenance agreements. For all new installations, system upgrades or routine maintenance the contractor shall complete all requested administrative requirements and reports to the CCB for approval prior to implementation. All information shall be presented to the COTR.
 - C.5.5.2.2.1 The contractor shall coordinate with the Government to schedule any system maintenance downtime sufficiently in advance to enable smooth operations during maintenance windows.
- C.5.5.2.3 The contractor shall maintain the Microsoft Systems Management Server (SMS) Deployment solution, or newer equivalent technology, to support the management and distribution of changes to the DHS computing environment. Using this technology the contractor shall:

PROCUREMENT SENSITIVE

- C.5.5.2.3.1 Perform software pushes and security patch management; provide an accurate account of software usage; and inventory network devices.
- C.5.5.2.3.2 Create, maintain and update application packages.
- C.5.5.2.3.3 If system changes are required the contractor shall follow the established DHS Change Control and Security Review processes prior to implementation.

C.5.6 VIDEO TELECONFERENCING**C.5.6.1 Video Teleconferencing (VTC)**

The contractor shall engineer, operate, and maintain Video teleconferencing and multimedia services and equipment. The contractor shall support customers who receive core services and customers who receive enterprise-level service as depicted in TE C.1.2-002. Conferencing and multimedia equipment includes support for secure and non-secure bridging systems, display and projection systems, electronic whiteboards, audio systems, DVD and video recording and replay, video switching systems, control systems, and video cameras. A list of the type of VTC equipment supported is provided at TE C.3.1-001, Government Furnished Equipment.

- C.5.6.1.1 The contractor shall provide 7X24X365 (366 for leap years) support for set up and operation of VTC and multimedia systems for DHS buildings, provide user level maintenance support for VTC and multi-media systems, and operate video conferences at multiple locations.
- C.5.6.1.2 The contractor shall maintain, setup, monitor, and troubleshoot video equipment for users. The contractor shall assist customers with the use of video conferencing systems by providing personal instruction in the use of control interfaces and procedures.
- C.5.6.1.3 The contractor shall schedule and monitor all video teleconferencing sessions.
- C.5.6.1.4 The contractor shall maintain an inventory of video conferencing equipment owned and leased by DHS.
- C.5.6.1.5 The contractor shall maintain a DHS video conferencing contact list.
- C.5.6.1.6 The contractor shall maintain and operate a VTC management platform.
- C.5.6.1.7 The contractor shall install/replace and configure video conferencing equipment required by DHS Component customers.
- C.5.6.1.8 The contractor shall complete all work in each DHS environment classification: Unclassified, Secret and Top Secret.

C.5.7 SATELLITE/CABLE TELEVISION OPERATIONS

The contractor shall engineer, operate, and maintain satellite/cable television services and equipment.

C.5.7.1 Operations

- C.5.7.1.1 The contractor shall complete all work in each DHS environment classification, Unclassified, Secret, Top Secret, and Top Secret/SCI.
- C.5.7.1.2 The contractor shall perform periodic testing to ensure system operations.

PROCUREMENT SENSITIVE

- C.5.7.1.3 The contractor shall set up and maintain channel alignment of the head-in systems, coordinate system expansion and reconfiguration, interface and coordinate with the Digital Satellite Service (DSS) and cable contractors as necessary for maintenance and system reconfiguration.
- C.5.7.1.4 The contractor shall maintain, setup, monitor, and troubleshoot satellite and/or cable TV equipment for users, assist customers with the use of satellite and/or cable TV systems by providing personal instruction in the use of control interfaces and procedures.
- C.5.7.1.5 The contractor shall maintain and update an inventory of satellite and/or cable TVs and associated peripheral, connectivity and installation components and make available for COTR review upon request.
- C.5.7.1.6 The contractor shall develop, maintain, update and implement a DHS satellite and/or cable TV contact list.
- C.5.7.1.7 The contractor shall install/replace and configure satellite and/or cable TV equipment as directed by the COTR or DHS Component customers.

C.5.8 VOICE COMMUNICATIONS AND MESSAGING

The contractor shall engineer, operate, and maintain voice communications, messaging services and equipment.

C.5.8.1 Private Branch Exchange (PBX) Infrastructure

The contractor shall provide administrative, operational, and management support for the DHS headquarters and associate component telecommunications. The contractor shall install, maintain and support the PBX Infrastructure within the Washington DC metropolitan area. This infrastructure includes components such as an Integrated Services Digital Network (ISDN), Voice over Internet Protocol (VOIP), analogue, digital and other communication devices at specified levels of classification. The contractor shall use FTS 2001 currently and transition to Networx for Phone and PBX operations.

- C.5.8.1.1 The contractor shall manage, update and make changes to systems.
- C.5.8.1.2 The contractor shall install, maintain, setup, monitor, and troubleshoot phone and PBX equipment for users, assist customers with the use of phone systems by providing personal instruction in the use of control interfaces and procedures, and install/replace and configure phone and PBX equipment required by DHS Headquarters and Component customers.
- C.5.8.1.3 The contractor shall maintain an inventory of phone and PBX equipment owned and leased by DHS.
- C.5.8.1.4 The contractor shall perform management and scheduling for conference bridges at unclassified and secure levels
- C.5.8.1.5 The contractor shall complete all work in each DHS environment classification: Unclassified, Secret and Top Secret.
- C.5.8.1.6 The contractor shall provide handset installation and configuration.
- C.5.8.1.7 The contractor shall develop, maintain, update, implement and report on phone and PBX services such as providing the following: A DHS Dial Plan, Telephone Infrastructure Cabling plant (infrastructure) documentation, port

PROCUREMENT SENSITIVE

utilization reports, load balancing reports, route pattern reports. (CDRL C.5.8-1, Phone and PBX Services Report)

C.5.8.1.7.1 The contractor shall maintain all documentation and records of telephony infrastructure.

C.5.8.1.7.2 The contractor shall ensure all telephony infrastructure components conform to a standardized set-up and design and provide redundancy.

C.5.8.1.8 The contractor shall continuously (or as directed) refresh the PBX, conference bridges and all tools and technologies for providing this support so that the Government is ensured the best value for its investment, to include all systems upgrades and patches to current release levels.

C.5.8.2 Telephone Switchboard Operations Center

The contractor shall provide contiguous hours 24X7X365 Telephone Switchboard Operation Center services for the DHS headquarters to The Secretary of the DHS, executive staff, employees, DHS contractors, and the public. The monthly call volume for the last year is provided at TE C.5.8-001.

C.5.8.2.1 Section intentionally left blank.

C.5.8.2.2 Section intentionally left

C.5.8.2.2.1 Section intentionally left blank.

C.5.8.2.2.2 The contractor shall create a proposed ACD and submit it to the COTR by November 15, 2008 (has already occurred). The contractor shall make changes to the proposed ACD as directed by the COTR and make the ACD operational within 10 business day of final approval. The ACD shall be subject to COTR directed changes throughout the life of the Task Order. (CDRL C.5.8-3, Automatic Call Directory)

C.5.8.2.3 The contractor shall provide an employee and office call directory service to DHS or DHS agency callers and connect callers who are members of the public to the requested/appropriate office or individual (phone extensions shall not be provided to the public).

C.5.8.2.3.1 The contractor shall develop, maintain, update and implement an office and personnel directory.

C.5.8.2.3.2 The contractor shall use the current office and personnel directory and the DHS Personal Profile data in Microsoft Outlook to identify phone extensions.

C.5.8.2.4 The contractor shall operate the teleconference bridge and will schedule teleconferences as requested and provide confirmation of scheduling to the requesters.

C.5.8.2.5 The contractor shall assign an operations center project manager who will report to the Director of the DHS Executive Service Center. The contractor shall have a supervisor for the switchboard.

C.5.8.2.6 The contractor shall provide automated reports monthly to the COTR on call pattern statistics. (CDRL C.5.8-4, Call Pattern Statistics Report – Monthly) The reports shall include the following:

PROCUREMENT SENSITIVE

- Call volume by day of week and duty hours (8:00 am to 7:00 pm ET) and non-duty hours.
- Aggregate monthly call volume from internal (DHS) and external (public) sources
- Aggregate monthly call volume of external calls and the specific ACD option selected

C.5.8.2.7 The contractor shall develop, maintain, update and implement a Continuity of Operations (COOP) Plan for Switchboard Operations. (CDRL C.5.8-5, Switchboard COOP Plan)

C.5.8.2.8 The contractor shall train its staff on switchboard operations.

C.5.8.2.8.1 The training shall cover DHS call handling policy, equipment use, use and maintenance of references, and routing of calls to the appropriate office or person.

C.5.8.2.8.2 The contractor shall develop, maintain, update and implement a training lesson plan and materials for the handling of calls in a professional manner and tone of voice. The contractor shall submit the initial and all updated lesson plans to the COTR for review and approval prior to using for training.

C.5.8.2.9 The contractor shall make recommendations necessary for upgrading the switchboard operation.

C.5.8.3 Voice Over Internet Protocol (VOIP)

The contractor shall facilitate the DHS transition and implementation of VOIP.

C.5.8.4 Unified Messaging

The contractor shall facilitate the DHS transition and implementation of unified messaging.

C.5.9 NETWORK MANAGEMENT CENTER (NMC)

C.5.9.1 NMC Operations

The contractor shall monitor, manage, and perform problem resolution support of all DHS HQ components, which consist of network circuits and devices, computer systems, applications, and databases/file servers. The purpose of the Network Management Center is to monitor systems 7X24X365 (366 for leap years). The NMC/SMC facility is not currently built and the Government anticipates completion at the Nebraska Avenue Complex located in Washington, DC, Building 100, second floor during the second quarter of FY08. The NMC/SMC will be located and maintained in a SCIF environment. The contractor shall use the NMC/SMC to monitor and manage all three network enclaves using industry standard applications and shall segregate; both logically and physically, maintain and operate NMC systems by security classification level. The contractor shall ensure that the NMC interfaces with the DHS Network Operations Center (NOC), including escalation procedures. The NOC is managed by Customs and Border Protection (CBP) and it is responsible for the the enterprise level issues that affect all components of the Department. The contractor shall operate and maintain the primary and backup NMC to monitor the following functions on a 7X24X365 (366 for leap years) basis:

- Network operations

PROCUREMENT SENSITIVE

- Security operations
 - Help Desk operations
- C.5.9.1.1 The contractor shall respond to network related problems and notify the COTR as specified in the DHS Escalation Policy. The contractor shall work in conjunction and cooperate with other LAN personnel and contractors supporting other IT infrastructure areas in order to respond to alarms, diagnose problems, and escalate issues to DHS NMC for fast, effective response before they cause costly unscheduled downtime or poor performance.
- C.5.9.1.2 The contractor shall monitor all network devices, environmental systems or peripheral devices which are managed or monitored using Simple Network Management Protocol (SNMP) and diagnostics tools currently in place, and to include any future additions to the hardware configuration to quickly detect, track, isolate, and resolve problems.
- C.5.9.1.3 The contractor shall perform troubleshooting techniques to isolate the source of, diagnose and/or resolve, or assist in the resolution of network problems (end-to-end) and root cause analysis.
- C.5.9.1.4 The contractor shall develop and submit the NMC Standard Operating Procedures (SOP) to the COTR for review and approval. (CDRL C.5.9-1, NMC Standard Operating Procedures)
- C.5.9.1.5 The contractor shall operate the NMC and support DHS COOP exercises. The contractor shall perform tests as requested by the COTR quarterly, at a minimum and as required by the DHS COOP Policy to verify failover from primary to backup NMC without any disruption of operational capability.
- C.5.9.1.6 The contractor shall identify the requirements for and install upgrades, updates, service packs, and patches.
- C.5.9.1.7 The contractor shall maintain security protection and reliability updates on operating systems.
- C.5.9.1.8 The contractor shall identify and notify the COTR of any upgrades, updates, service packs, and patches determined to be incompatible with system or application specifications and proceed as directed by the COTR.
- C.5.9.1.9 The contractor shall monitor system operability and functionality, identify abnormal performance and degradation and complete resolution actions and return the system to normal performance.
- C.5.9.1.10 The contractor shall monitor system capacity, maintain normal performance, and prevent system degradation resulting from usage exceeding system capacity.
- C.5.9.1.11 The contractor shall operate the NMC to respond to changes in loads on the network as necessary, in response to higher threat levels.
- C.5.9.1.12 The contractor shall report on the network and systems infrastructure using a GFE Enterprise Management Tool. The contractor shall report on network and system status as directed by COTR to include Network Diagrams that identify enterprise building, floor, room, rack and system for HQ and field sites.
- C.5.9.1.13 The contractor shall notify and update the Help Desk of any network or system infrastructure issue or problem detected or managed by the NMC.

PROCUREMENT SENSITIVE

- C.5.9.1.14 The contractor shall manage status, errors, and inbound and outbound traffic statistics of all routing interfaces, bandwidth utilization, and errors of all inbound and outbound LAN /WAN circuits.
- C.5.9.1.15 The contractor shall manage the LAN/WAN routing protocol between the routers; perform port management, network capacity management (including planning and trending), and configuration management.
- C.5.9.1.16 The contractor shall maintain configuration LAN/WAN change documentation, and continually update schematics to reflect current network architectures.
- C.5.9.1.17 The contractor shall support terminal equipment associated with special circuits as required and shall maintain and monitor connections to LAN tail sites.
- C.5.9.1.18 The contractor shall maintain and monitor the secure wide area network connection to existing and/or future connections to other Intelligence Community's networks.
- C.5.9.1.19 NMC/SMC management shall provide Network Metrics Reports to the COTR.
- C.5.9.1.20 The contractor shall maintain the outbound and inbound Internet access to ensure full operational capability for internal and external user contiguous hours access to the Internet 24X7X365 (366 for leap years) except during periods of Government approved planned outage. The contractor shall provide outbound access connectivity for the DHS staff to the Internet. The contractor shall provide In-bound public access connectivity to the DHS Public Website.
- C.5.9.1.21 The contractor shall monitor Internet access, identify, and resolve interruptions to the Internet service. The contractor shall perform upgrades, implement changes, and install patches to components on the Internet servers. These shall include middleware updates, new Database Source Networks (DSNs), application updates, application additions, patches and hot fixes.
- C.5.9.1.21.1 The contractor shall perform upgrades, implement changes and install patches to components of the Web Content Management System (WCMS), which publishes finished web site updates to the public web site.
- C.5.9.1.21.2 The contractor shall perform all maintenance that will disrupt or could disrupt the availability of Internet services only during planned outage periods.
- C.5.9.1.21.3 The contractor shall maintain logs of Internet activity and make available for review as requested by the COTR.
- C.5.9.1.22 The contractor shall develop and utilize a system to receive, respond and resolve technical inquiries from the public regarding access to the DHS Website (currently <http://www.dhs.gov>). The DHS Webmaster receives inquires from the public and will forward those requiring technical assistance to the contractor. The DHS Webmaster will provide the requirements for technical assistance and establish a timeline, in conjunction with the contractor, for completion of the development, set-up and operation of the Public Interface Activities technical assistance system.

PROCUREMENT SENSITIVE

- C.5.9.1.22.1 The contractor shall post Internet notices alerting those accessing the DHS Website of interruptions or other problems causing degradation of access.
- C.5.9.1.23 The contractor shall provide Web page content assistance for authorized users, developers or content providers. The contractor assistance shall include verifying approval of the request for assistance, preparation of the content, complying with the requirements of Section 508, and deploying the content.
- C.5.9.1.24 The contractor shall adhere to the DHS perspective in Enterprise Interconnection and Policy Working Group (EIWG) with the DOD to facilitate the technical issues and governance processes related to the interconnection between the Secure Internet Protocol Router Network (SIPRNET) and DHS secure networks, address operational problems and assist in extending capabilities to federal information sharing initiatives.
- C.5.9.1.24.1 The contractor shall attend meetings of and contribute to specific technical operational working groups set up to address engineering and operations issues with DoD and other Governmental agencies, and leverage the contractor knowledge and resources with the Intelligence Community (IC) to ensure that DHS is aligned with emerging IC systems engineering and technology solutions.

C.5.10 SECURITY MANAGEMENT CENTER (SMC)

The DHS SMC shall provide continuous security monitoring to detect all potential adverse events within all DHS network and computer systems. The SMC shall provide day-to-day operations and maintenance of the DHS defense-in-depth security infrastructure. At Contract award, GFE will be provided to assist in Security structure build-out. The SMC in this form does not exist today, and the contractor shall propose a solution for this requirement. (See paragraph C.5.9.1 for the location and status of the NMC/SMC.)

C.5.10.1 SMC Operations

The contractor shall centrally manage DHS Information Technology Services Office Security Management. The SMC shall be co-located with the NMC to provide a fully integrated operations and security management function.

- C.5.10.1.1 The contractor shall provide security system administration, key management, security audit and analysis, security incident reporting and response, security intrusion detection, system vulnerability assessment, responding to Information Security Vulnerability Notices (ISVMs), the most recent anti-virus signature updates, and end-user support to resolve security issues.
- C.5.10.1.2 The contractor shall prepare a DHS Information Technology Services Office Security Management Approach and SOPs, Checklists and a DHS Information Technology Services Office Security Plan, for operations within the SMC, and submit to the COTR for approval. (CDRL C.5.10-1, Information Technology Services Office Security Management Approach and SOPs, Checklists and DHS Information Technology Services Office Security Plan)
- C.5.10.1.3 The contractor shall staff the SMC with subject matter experts to act as analysts to support 7X24X365 (366 for leap years) monitoring and response capability.

PROCUREMENT SENSITIVE

- C.5.10.1.4 The contractor shall identify the requirements for and install upgrades, updates, service packs, and patches.
- C.5.10.1.5 The contractor shall maintain security protection and reliability updates on operating systems.
- C.5.10.1.6 The contractor shall identify and notify the COTR of any upgrades, updates, service packs, and patches determined to be incompatible with system or application specifications and proceed as directed by the COTR.
- C.5.10.1.7 The contractor shall monitor system operability and functionality, identify abnormal performance and degradation and complete resolution actions to return the systems to normal performance.
- C.5.10.1.8 The contractor shall monitor system capacity, maintain normal performance, and prevent system degradation resulting from usage exceeding system capacity.

C.5.10.2 Vulnerability Assessment

- C.5.10.2.1 The contractor shall perform threat and vulnerability assessments on all information system assets, including Public Facing operational IT systems, as part of its sustaining Security Systems Administration. The contractor shall generate a Vulnerability Assessment Report following each assessment that lists the vulnerabilities discovered, and their impact/threat to the network (high, medium, and low). The contractor's security team shall present high threat vulnerabilities and suggested mitigations to the Government prior to leaving the sites. The report shall include mitigation recommendations for all other vulnerabilities identified. The SMC shall report the status of actions to correct the high threat vulnerabilities to the System Security Administrators (SSAs), security manager, and the ISSO/ISSM on a monthly basis.
- C.5.10.2.2 The contractor shall identify specific security weaknesses on target systems, and provide recommended techniques and/or improvements to strengthen the security of the target system.
- C.5.10.2.3 The contractor shall scan DHS systems using GFE or vulnerability tools approved by the Government.
- C.5.10.2.4 The contractor's vulnerability assessment capability shall identify unauthorized access points or potential implementation weaknesses.
- C.5.10.2.5 The contractor shall define and audit PEP policy and determine how the PEP handles application(s) traffic such as web, email, or telnet. Additionally, the integrated security team's DHS PEP Management Policy shall describe PEP updates and management.
- C.5.10.2.6 The contractor shall identify, review and analyze the vulnerabilities associated with each application and the cost-benefits associated with the methods used for securing the applications and provide the findings to the COTR. (CDRL C.5.10-3, Application Vulnerability Cost-Benefit Analysis)
- C.5.10.2.7 The contractor shall develop a DHS PEP policy that identifies the necessary network applications, vulnerabilities associated with these applications, creation of applications traffic matrices identifying protection methods, and PEP rule-sets based on applications traffic matrices.

C.5.10.3 Security Information Management (SIM) & Security Management Capability

PROCUREMENT SENSITIVE

SIM is an automated capability that provides for the collection, analysis, alerting, reporting, and trending for all of the system components within a computing environment.

C.5.10.3.1 The contractor shall establish, operate, and maintain an Information Technology Services Office security management capability suitable for the real-time monitoring and assessment of all assigned assets in accordance with DHS MD 4300 and Security Architecture Volume 2. Examples of these assets are PEPs, virtual private networks, routers, switches, server and end system computing elements. Additionally, the system shall collect event input from the IDS, anti-virus, and network management systems. DHS HQ shall procure initial GFE for all LAN environments. The contractor should propose tools to address capabilities that may not be either fully procured or implemented by the government prior to the award of IT NOVA. DHS determined that the ESM and other enterprise security management products manufactured by ArcSight will form the nucleus of the DHS HQ SIM.

C.5.10.3.2 The SMC shall be responsible for day-to-day operations and maintenance of the defense-in-depth security infrastructure. The SMC shall be co-located with the Information Technology Services Office NMC to provide a fully integrated operations and security management functions.

C.5.10.4 Security Systems Administration

The contractor shall manage and monitor all DHS security components including intrusion detection systems (IDSs) and PEPs. Security systems shall use an automated delivery function to the maximum extent possible to push anti-virus software signature updates to the desktops and provide the results to Information Technology Services Office NMC/SMC management for analysis. Security systems administration shall include the following:

C.5.10.4.1 The contractor shall monitor DHS systems for intrusion activity, and be prepared to take appropriate steps to mitigate any suspected intrusion while maintaining the availability of the system for all authorized users.

C.5.10.4.2 The contractor shall conduct computer forensics, law enforcement evidence collection and preservation efforts in support of the system.

C.5.10.4.3 The contractor shall conduct assessments quarterly (or as directed) at all major nodes, such as gateways and regional centers where data is stored and report the results of such findings to the COTR and the **ESD Security Manager**.

C.5.10.4.4 The contractor shall perform anti-virus scans of the entire DHS networks in accordance with the proscribed procedures in DHS Approved Maintenance Downtime as described in Section C.5.6.4.

C.5.10.5 Security Change Management

The contractor shall centrally manage and control the implementation of corrective patches and service packs.

C.5.10.5.1 For all new installations, system upgrades or routine maintenance, the contractor shall complete all requested administrative requirements and testing prior to submission to CCB for approval.

PROCUREMENT SENSITIVE

C.5.10.5.2 The contractor shall assess DHS directed security patches or service packs before implementation to verify the need to implement and the impact upon the system.

C.5.10.5.3 The contractor, in coordination with DHS, shall determine the schedule for deploying Information Assurance and Vulnerability Alerts (IAVAs), patches, and service packs.

C.5.10.5.4 The contractor shall provide monthly reports to the appropriate COTR on the success of the patch/service pack deployment, and any issues preventing completion. (CDRL C.5.10-4, Patch/Service Pack Deployment Report)

C.5.10.6 Security Log Access, Retention and Review

C.5.10.6.1 In accordance with applicable DHS directives, the contractor shall maintain all security logs for the required retention period. Access to these logs shall be restricted to ISSM approved personnel.

C.5.10.6.2 The contractor shall record all accesses to these logs, including an audit history of reads, changes, and deletions.

C.5.10.6.3 The contractor shall protect logs under these restrictions to include all security logs (PEP, IDS, anti-virus), as well as domain controller, and all management systems as directed by the ISSM/ISSO.

C.5.10.6.4 The contractor shall perform reviews and provide monthly reports (or as directed) on all system logs included within the Monthly Workload Report.

C.5.10.7 System Security Administrators

The contractor shall provide all System Security Administrators (SSA). Each SSA is an extension of the SMC in providing security oversight, monitoring, and reporting for DHS and is the principal POC for all security issues and support of Government ISSMs and ISSOs.

C.5.10.8 Data Spills and Response

The contractor shall employ guards and gateways to monitor, prevent, detect, respond, report and correct the unauthorized release of Secret or TS/SCI data.

C.5.10.9 Incident Response

The contractor shall create and maintain the capability to respond rapidly to any network event that could affect the Information Assurance /Information Protection posture of DHS. The contractor shall create and maintain SOPs and checklists to cover events such as network intrusions, data spills, introduction of malicious software, Denial of Service (DoS) incidents, inappropriate network use, etc. The contractor shall base these SOPs and checklists upon existing DHS directives and guidance.

C.5.10.9.1 The contractor shall maintain a trained Computer Security Incident Response Team (CSIRT), which may include systems administrators and other personnel. The contractor shall develop policy and processes related to the establishment and generation of the CSIRT. The CSIRT shall maintain a digital forensics capability that establishes and maintains an evidentiary chain of custody.

C.5.10.9.2 The contractor shall utilize all available audit logs to support forensics activities, and shall develop SOPs for the conduct of forensics investigations

PROCUREMENT SENSITIVE

that shall be submitted to the COTR for approval. (CDRL C.5.10-6, Forensic Investigation SOPs)

C.5.10.9.3 The contractor shall follow established reporting procedures when providing initial notification to the SSAs, Security Manager, ISSO, and Information System Security Manager (ISSM) of any network event or incident.

C.5.10.9.4 The contractor shall provide Event and Incident Reports to the Government as directed in the DOD-Dir.8500 Series Computer Network Defense (CND). The Continuity of Operations Plan shall detail non-IT incident response, as identified in HSPD-5 and the DHS Initial National Response Plan.

C.5.10.10 Information Condition (INFOCON) Management

In response to potential threats to the DHS (and U.S. infrastructure assets in general), the Secretary of the DHS (SECDHS) may direct the elevation of the protection levels of the network and IT assets through the implementation of INFOCON levels. The INFOCON level is determined based upon an assessment of risk to the DHS networks. When directed by DHS, the Designated Accrediting Authority (DAA) will approve specific measures of protection for the networks.

C.5.10.10.1 The contractor shall implement INFOCON conditions within the DHS, and will track the attainment of the directed INFOCON level across the networks.

C.5.10.10.2 The contractor shall assist in the coordination of DHS INFOCON levels and that of external entities such as DOD as directed by the COTR.

C.5.10.10.3 The contractor shall develop, submit to the COTR for approval and follow SOPs and checklists to track the changes in INFOCON level and the attainment of the directed INFOCON. (CDRL C.5.10-8, INFOCON Level SOPs and Checklists)

C.5.10.10.4 The Information Technology Services Office SMC shall create SOPs based upon DHS policies to support the DHS Computer Network Defense Continuity of Operations Plan.

C.5.11 COMMUNICATIONS SECURITY (COMSEC) MANAGEMENT**C.5.11.1 COMSEC Security**

C.5.11.1.1 The contractor shall provide on-site 7X24X365 (366 for leap years) COMSEC Support for services such as installation maintenance and administration of messaging systems (e.g., DMS, AMHS, receipt, transmission and/or distribution of all forms of communication media such as: faxes, messages, correspondence, etc).

C.5.11.1.2 The contractor shall operate encryption systems to support secure voice and video systems as required and assist Government personnel with receipt, inventory control, deployment, and securing of encryption systems. The contractor shall assist users in the operations of secure facsimile systems, and perform user level maintenance.

C.5.11.1.3 The contractor shall receive, distribute, inventory and administrator COMSEC account material.

C.5.11.1.4 The contractor shall perform COMSEC technical tasks such as maintaining and updating messaging systems, installation and maintenance of all cryptographic equipment (e.g., TACLANE, FASTLANE, and KIV-7).

PROCUREMENT SENSITIVE

C.5.11.1.5 The contractor shall provide a COMSEC Plan to address implementation and operational details in accordance with DHS and NSA policies and procedures and provide to the COTR. (CDRL C.5.11-1, COMSEC Plan)

C.5.11.1.6 The contractor shall establish and manage a COMSEC account in accordance with DHS guidelines and procedures.

C.5.11.1.7 The contractor shall manage, update and maintain the Information Technology Services Office SMC COMSEC account and COMSEC controlled items (CCI) and all keying material.

C.5.12 OTHER COMMUNICATIONS OPERATIONS**C.5.12.1 Emergency Notification System**

The contractor shall program and operate Emergency Notification System (Communicator) and:

C.5.12.1.1 The contractor shall provide user training as required.

C.5.12.1.2 The contractor shall interface and coordinate with the vendor for maintenance and software upgrades.

C.5.12.1.3 The contractor shall provide data entry and system backup as required.

C.5.12.2 Executive Telecommunications Support

The contractor shall provide contiguous hours 24x7x365 secure and non-secure IT and communications services and support for the Secretary of the Department of Homeland Security (DHS), the Deputy Secretary and other designated DHS executive staff while they are traveling outside of the National Capital Area (NCA).

C.5.12.2.1 The contractor shall provide daily operations support for fixed and mobile IT/Telecom equipment such as the following tasks:

- Manage and control inventory
- Operate, test, troubleshoot, and maintain equipment
- Operate and ensure capability of mobile IT/Telecom vehicle
- Maintain proficiency on existing and future IT/Telecom systems
- Assist in design, development, analysis, integration, and evaluation of IT/Telecom systems
- Plan and perform preventive maintenance inspections on IT/Telecom equipment that is installed at the ETS NAC facility, installed in secure mobile vehicle platforms, and used while traveling
- Perform equipment lifecycle management
- Perform COMSEC and project management support
- Synthesize customer needs with commercially available IT products into requirements that will allow the implementation of engineered IT/Telecom systems and processes
- Provide operational assistance to DHS Senior Executives and staff

C.5.12.2.2 The contractor shall provide travel operations support such as:

- Coordinate with DHS staff advance arrival personnel at the travel sites
- Transport IT/Telecommunications equipment to and from travel sites

PROCUREMENT SENSITIVE

- Conduct site survey(s) for installation of travel systems
- Install and remove IT/Telecom equipment from trip site
- Provide point-to-point telecom support to travel teams
- Coordinate their own travel logistics arrangements

C.5.13 TRAINING

The contractor shall provide professional, technical and end-user training. The contractor shall provide the training support for DHS IT operations to include user applications and network access, system administration, and security. The contractor shall develop training plans for DHS personnel, system users, and contractor personnel. The training plans shall be submitted to the COTR for approval prior to implementation. (CDRL C.5.13-1, Training Plan) The contractor shall maintain an electronic record of all training courses conducted and who attended.

C.5.13.1 System Administrator Training

The contractor shall provide appropriate training, training materials, and help desk support for the applications provided for DHS. The contractor shall work with the Government to develop a Training Plan that addresses the delivery of training to supervisors, and system administrators. The plan shall be in conformance with the SOPs and SLAs.

C.5.13.1.1 The contractor shall provide the training curriculum and training materials for DHS applications and desktops. The training materials shall be suitable for both users and system administrators, and adopted from existing training materials for legacy applications integrated into DHS service.

C.5.13.1.2 The contractor shall provide the delivery of the user training through a "train-the-trainer" approach to the maximum extent possible. The contractor shall provide training directly to the users at either contractor facilities or Government facilities.

C.5.13.1.2.1 The contractor shall provide DHS training through training delivery methods such as the following:

- Direct delivery of the training to user and system administrators at DHS facilities or other locations as directed by the Government
- Direct delivery of special user training to personnel who will then act as trainers in the field
- Delivery of training to user through computer-based training (CBT) or other distance learning techniques that the contractor has found effective

C.5.13.1.3 The contractor shall provide documentation and manuals for COTS products that have them.

C.5.13.2 Security Training

The contractor shall develop, document, and administer a Security Training Plan and Curriculum providing annual required security awareness and operational security refresher training. Delivered training elements shall comply with DHS and other relevant external agency directives and policies for enforcement of Government security provisions. The appropriate COTR will review and approve the training curriculum prior to implementation. Implementation of the training may be either through instructed

sessions or via computer-based self-paced training. The contractor may elect to provide this training in incremental elements depending upon component usage, and the training may be delivered via computer-based training, help files or instructed sessions following Government approval.

C.5.13.2.1 The contractor shall provide training to users and operators to facilitate the usage of security components within the network and on the desktop.

C.5.13.3 End-User Training

The contractor shall develop, document, and conduct end-user training on all COTS, GOTS, and unique software. The appropriate COTR will review and approve the training curriculum prior to implementation. Implementation of the training may be either through instructed sessions or via computer-based self-paced training. The contractor may elect to provide this training in incremental elements depending upon component usage, and may be delivered via computer-based training, help files or instructed sessions following Government approval.

C.5.14 WIRELESS SERVICES MANAGEMENT

The Contractor shall provide support to ESD Wireless Services (WS) to include wireless coordination support, frequency management support, and frequency spectrum planning.

C.5.14.1 Wireless Coordination Support

The Contractor shall support ESD Wireless Services in facilitating the coordination of DHS wireless investments through the DHS Wireless Working Group (WWG). The Contractor shall perform the following tasks:

C.5.14.1.1 The contractor shall provide support to include the development and tracking of program metrics, development and execution of program strategy, development of program governance documentation (e.g., MD4100 updates) and reporting.)

C.5.14.1.2 The contractor shall support the WWG through process development, development of Governance documentation and templates, facilitation of meetings, and managing communications.

C.5.14.1.3 The contractor shall provide technical and operational subject matter expertise to support IT acquisition reviews and WWG investment/resource coordination efforts.

C.5.14.2 Frequency Management Support

The contractor shall perform frequency management functions as follows.

C.5.14.2.1 Provide proficient technical expertise for Spectrun Software tools and products such as Spectrum XXI and ATDI Hertz Warfare.

C.5.14.2.2 Assist with the daily selection, coordination, and processing of all radio frequency authorizations in support of DHS components. The selected/approved frequencies shall be registered by the contractor in the Government Master File, GMF.

PROCUREMENT SENSITIVE

- C.5.14.2.3 Assist in the development of frequency plans that meet new communications requirements and improve methodologies for interoperability among the DHS components and key federal, state, and local partners.
- C.5.14.2.4 Ensure that systems will neither cause nor receive harmful interference to or from other authorized users when placed in their intended operational environments.
- C.5.14.2.5 Ensure accuracy of all frequency assignments by conducting "five-year-reviews" or "ten-year reviews" as required by NTIA regulations of all DHS GMF records.

C.5.14.3 Frequency Spectrum Planning

The contractor shall support Spectrum Planning as follows:

- C.5.14.3.1 Develop and recommend frequency changes to eliminate technical incompatibilities, improve interoperability, and reduce and/or eliminate interference.
- C.5.14.3.2 Refine the nationwide channel plan with the support of the WWG to include identifying frequencies and developing a logical structure for nationwide channels (e.g., component specific channels, DHS common channels, interoperability channels).
- C.5.14.3.3 Develop a nationwide strategy to define optimal geographic spacing for frequency reuse zones; identify the number of frequencies needed for a successful regional/zone system design, use temporary transition frequencies (if required), and use permanent narrowband frequencies of the new wireless systems.
- C.5.14.3.4 Prepare equipment and system certification documentation as required by NTIA regulations.
- C.5.14.3.5 Coordinate new, proposed frequencies within DHS and with other federal departments and government agencies.
- C.5.14.3.6 Prepare spectrum Planning analyses and documentation as directed including documentation for spectrum management support of the National Response Framework (NRF) Emergency Support Function #2 – Communications (ESF #2).

C.5.14.4 Security Support

- C.5.14.4.1 The contractor shall prepare a DHS Information Technology Services Office (ITSO), Enterprise Services Division (ESD) Security Management Approach and SOPs, Checklists and a DHS Information Technology Services Office Security Plan, for ESD operations, and submit to the COTR for approval within 60 days of Modification P00001 (9/10/08).
- C.5.14.4.2 The contractor shall identify and notify the COTR and the ESD Security Manager of any upgrades, updates, service packs, and patches determined to be incompatible with system or application specifications and proceed as directed by the COTR.

PROCUREMENT SENSITIVE

C.5.14.4.3 The contractor shall identify specific security weaknesses on target systems, and provide recommended techniques and/or improvements to strengthen the security of the target system.

C.5.14.4.9 For all new installations, system upgrades or routine maintenance, the contractor shall ensure all requested administrative requirements, compliance with DHS Security Architecture and hardening guidance. The contractor shall test to ensure that installation will be able to sustain and /or improve the operational and security posture of the systems prior to submission to CCB for approval.

C.5.14.4.10 The contractor, in coordination with DHS, shall determine the schedule for deploying Information Assurance and Vulnerability Alerts (IAVAs), patches, and service packs and document completion to the COTR and the ESD Security Manager.

C.5.14.4.11 The contractor shall provide monthly reports to the appropriate COTR and the ESD Security Manager on the success of the patch/service pack deployment, and any issues preventing completion. (CDRL C.5.10-4, Patch/Service Pack Deployment Report)

C.5.14.4.12 The contractor shall provide Weekly quad reports, in accordance with ITSO Standards, to the ESD Security Manager and other appropriate Technical Point of Contacts as directed by the COTR.

C.5.14.4.13 In response to potential threats to the DHS (and U.S. infrastructure assets in general), the Secretary of the DHS (SEC DHS) may direct the elevation of the protection levels of the network and IT assets through the implementation of INFOCON levels. The INFOCON level is determined based upon an assessment of risk to the DHS networks. When directed by DHS, the Designated Accrediting Authority (DAA) will approve specific measures of protection for the networks.

C.5.14.4.14 The contractor shall implement INFOCON conditions within the DHS, and will track the attainment of the directed INFOCON level across the networks.

C.5.14.4.15 The contractor shall assist in the coordination of DHS INFOCON levels and that of external entities such as DOD as directed by the ESD Security Manager and the COTR.

C.5.14.4.16 The contractor shall develop, submit to the COTR for approval and follow SOPs and checklists to track the changes in INFOCON level and the attainment of the directed INFOCON. (CDRL C.5.10-8, INFOCON Level SOPs and Checklists)

C.5.14.4.17 The Information Technology Services Office SMC shall create SOPs based upon DHS policies to support the DHS Computer Network Defense Continuity of Operations Plan.

C.5.14.5 Data Center Infrastructure

C.5.14.5.1 The contractor will perform as the single point of contact for the Component, Managed Service Provider(s) (MSP) and DHS Data and Application Services Program Management Office. In this capacity the Contractor will "manage" the day-to-day interaction with the MSP to ensure the business needs of the Component are being satisfied.

C.5.14.5.2 Component Point of Contact for data center Operations and Maintenance

- Define/monitor Service Level Agreement's (SLA) required by the Component.

PROCUREMENT SENSITIVE

- Escalate the systemic problems experienced by components to the DHS Data and Application Services Program Management Office
- Collaborate with IT Service Delivery on application deployment
- Educate IT Infrastructure on Component business.
- Define and support business continuity requirements at the Data Centers

C.5.14.5.3 Component IT Strategic Planning

- Develop standards for migration planning
- Develop and collaborate in the development of IT Infrastructure Strategies with IT planning and architecture.
- Provide input into IT planning and architecture on potential uses of emerging technologies on the conduct of Component Business.
- Define new requirements to IT planning and architecture.

C.5.14.5.4 Interact with the Managed Service Provider's Relationship Manager for:

- Transition and migration planning
- Day-to-day service delivery activities

C.5.14.5.5 Interact with the Component's Infrastructure Leader for

- Physical consolidation planning and implementation
- Day-to-day service delivery activities
- Monitor component migration plan

C.5.14.6 Office Management

C.5.14.6.1 The contractor shall take initiative to identify, respond to problems, and propose solutions for issues that have a potential negative impact to the mission environment. The contractor shall analyze the operational environment, identify and propose solutions to improve the efficiency and effectiveness of the Information Technology Services Office.

C.5.14.6.2 Administrative Services: The contractor shall perform all related administrative services required to perform services such as, material requisitioning, documentation Quality Control (QC), status and tracking of ESD reports, develop and review correspondence for executive formatting/appropriateness; develop travel requests, develop and execute travel reimbursements, time and attendance monitoring, meeting coordination/scheduling and reception. The contractor shall maintain accurate and complete records, files, and libraries of or access to documents to such as Federal, state, and local regulations, codes, laws, technical manuals, manufacturer's instructions, Standard Operating Procedures (SOPs), and recommendations, which are necessary and related to the functions being performed. The contractor shall support DHS during audits and inspections, and provide support and responses to audit and inspection items (internal and external).

C.5.14.6.3 Submittal of Reports and Information: The contractor shall compile data, prepare required reports, and submit information as directed by the COTR. The reports include daily, weekly, monthly and annual reports the contractor shall submit at the specified time.

PROCUREMENT SENSITIVE

C.5.14.6.4 Ad hoc Requirements: Upon notification from the Government, the contractor shall provide management and technical information to the Government such as: (CDRL C.1.4-1, Ad hoc Requirements)

- Technical evaluation of suggestions
- Input for staff studies
- Fact sheets
- Audits
- Congressional inquiries
- One-time reports
- Recommendations for amending, revising, or originating Government regulations or policies within the scope of this Task Order
- Information requested by the CO/COTR on other interfacing Task Orders that support this effort

C.5.14.6.5 Paper File Archiving. The contractor shall prepare all correspondence in and maintain all files using DHS specific, and generally accepted commercial industry standards. All files, records, and documents maintained in the performance of this Task Order are Government property and the contractor shall return them upon completion or termination of the work.

C.5.14.6.6

C.5.14.6.7 Document Management: For all deliverables within this Task Order, the contractor shall implement document management to include version control and comment resolution such that each release has clear inventory of comments accepted/rejected as part of the version.

C.5.15 IT CONTINUITY MANAGEMENT

The contractor shall perform continuity management actions affecting the Information Technology Service Office and all of its functions including the Network Management Center, Security Management Center, Front Office, Enterprise Business Management Office, Infrastructure Information Systems Security Manager (ISSM), Mission Critical Infrastructure Operations (MCIO), Enterprise Application Delivery and Operations, IT Continuity Management, Business Office Operations, Infrastructure Transformation Office, Wireless Management Office, and all network and telecommunications components. The contractor shall also provide continuity management and redundancy capability of the Help Desk.

These programs/offices have 46 recoverable essential functions (EFs) with alternate site operations occurring at two sites as a minimum. The sites, to include redundant NMC, and SMC, are provided by DHS. EFs concern DHS, state/local Governments, law enforcement, and other executive branch directorates, and agencies. The DHS Continuity Planning framework is provided at TE C.5.15-001.

The contractor shall provide IT integration capability for all departmental, intergovernmental, and non-governmental organizations (NGO) applications used on the LANs.

C.5.15.1 Continuity Assessment

PROCUREMENT SENSITIVE

C.5.15.1.1 The contractor shall perform an initial baseline analysis of existing IT continuity plans and programs. (CDRL C.5.15-1, Business Continuity Initial Assessment)

C.5.15.1.2 After completing the baseline analysis, and its approval by the COTR, the contractor shall evaluate the baseline against the Business Continuity Framework to determine operational gaps. The contractor shall document the findings of the gap analysis and submit the findings to the COTR within 60 business days of the baseline analysis approval by the COTR. (CDRL C.5.15-2, Business Continuity Framework Gap Analysis)

C.5.15.2 Continuity Planning

C.5.15.2.1 The contractor shall facilitate strategic planning with programs and offices annually, or as directed by the COTR. The outcome of the strategic planning is the Multi-Year Strategic Program Management Plan containing continuity planning goals and objectives to include performance measures for the period. (CDRL C.5.15-3, Multi-Year Strategic Program Management Plan)

C.5.15.2.2 The contractor shall update and maintain annually, or as directed by the COTR, the CIO COOP Implementation Plan. The contractor shall provide the document to the COTR for approval. (CDRL C.5.15-4, CIO COOP Implementation Plan)

C.5.15.2.3 The contractor shall develop, maintain, update and implement the Incident Response and Management Plan, containing management activist and emergency response and escalation procedures. The contractor shall update the plan annually or as directed by the COTR, based on threat/exposure/business continuity strategy. (CDRL C.5.15-5, Incident Response and Management Plan)

C.5.15.2.4 The contractor shall develop, maintain, update and implement the CIO Operational Recovery Plan and IT Disaster Recovery/Business Continuity Plans, at least annually for offices/programs. (CDRL C.5.15-6, CIO Operational Recovery Plan and IT Disaster Recovery/Business Continuity Plan)

C.5.15.3 Continuity Reviews and Coordination

C.5.15.3.1 The contractor shall participate in Enterprise Architecture Center of Excellence (EACOE) reviews, Enterprise Change Control Board (ECCB) reviews, and other compliance activities to identify the impact of these bodies' decisions and actions on IT continuity planning and advise these bodies' on continuity planning considerations. The contractor shall document the reviews continuity planning impacts and provide comments in accordance with the guidelines provided by the appropriate board.

C.5.15.3.2 The contractor shall schedule, plan and conduct a bi-weekly meeting of designated stake holders to discuss and coordinate requirements for the development and maintenance of the Disaster Recovery and IT Contingency Plan and coordinate the plans and activities for conducting COOP Exercises. The meeting participants shall also coordinate the actions taken to address findings resulting from COOP exercises. The contractor shall provide meeting minutes to the COTR within three business days of the meeting.

C.5.15.4 Continuity Program Administration

PROCUREMENT SENSITIVE

- C.5.15.4.1 The contractor shall develop, maintain, update and implement IT continuity policy, guidance, methodologies and tools. Updates shall occur at least annually, in response to Homeland Security Presidential Directives (HSPDs), or as directed by the COTR. (CDRL C.5.15-8, Continuity Policy, Guidance, Methodologies and Tools)
- C.5.15.4.2 The contractor shall update and maintain, at the direction of the COTR, the list of CIO essential functions and critical IT/telecommunication networks, systems, facilities, and critical positions. (CDRL C. 5.15-9, Essential Functions, Critical IT/Telecommunication Networks, Systems, Facilities, and Critical Positions List)
- C.5.15.4.3 The contractor shall annually, or when significant changes occur to the essential function(s) or DHS IT infrastructure perform a continuity management review. Changes shall result in a threat and vulnerability exposure, Risk Assessment, Interdependency Analysis, Business Impact Analysis. The contractor shall ensure re-use of existing information when performing the aforementioned tasks. The contractor shall prepare a report and executive briefing identifying risk to the CIO. (CDRL C.5.15-10, Continuity Management Review)
- C.5.15.4.4 The contractor shall conduct a review of the CIO COOP Implementation program, Operational Recovery/IT Contingency Plans, observe related tests, and provide feedback on program compliance in accordance with all applicable executive orders, presidential directives, other federal and DHS laws, federal orders management policies, handbooks, guidelines, processes, and procedures, as directed by the COTR.
- C.5.15.4.5 The contractor shall develop executive briefings as directed by COTR.

C.5.15.5 Testing and Exercises

- C.5.15.5.1 The contractor shall develop test plans and provide training on the test/exercise plans annually or as directed by COTR
- C.5.15.5.2 The contractor shall participate in test/exercises and the after-action test/exercise reviews and document issues in an After Action Report

C.5.15.6 Electronic Records

- C.5.15.6.1 The contractor shall develop, maintain, update and implement the electronic vital records program to ensure critical records from all three networks are stored off premise. Records range from paper-based documents to the latest electronic-storage media.
- C.5.15.6.2 The off-site storage location(s) shall be located at least 50 miles from the production site, outside of the impact area of the production site, and inside the continental U.S.
- C.5.15.6.3 The frequency of records back-up is dependent on the record type and COTR direction.
- C.5.15.6.4 The retrievable and fully operational time frames shall fulfill the performance requirements for critical and non-critical systems as identified in Table 1 of the Task Order, Continuity of Government Condition (COGCON) level activation/reconstitution timeframes, or as designated by the COTR.

C.5.15.6.5 The contractor shall test and ensure the records are retrievable and usable at least quarterly. The contractor shall provide a test report to the COTR within five business days of completing the test. (CDRL C.5.15-14, Electronic Vital Records Program Test Report.

C.6 APPLICABLE LAWS, PUBLICATIONS, AND FORMS

C.6.1 GENERAL INFORMATION

C.6.1.1 Applicable Publications and Forms

- C.6.1.1.1 Most Government publications listed are available electronically and the Government will provide the non-electronic versions at the start of the Task Order. The contractor shall maintain a copy of all required publications listed in this Section and Technical Exhibits in accordance with Section C.1. The contractor shall post supplements or amendments to listed publications from any organizational level issued during the life of the Task Order as required.
- C.6.1.1.2 The contractor shall establish continuing publication requirements with the DHS publication distribution office. The contractor shall have customer accounts for all publications listed in this Task Order.
- C.6.1.1.3 The contractor shall immediately implement changes to publications that result in a decrease or no change to the Task Order price. Prior to implementing any revision, supplement, or amendment that may result in an increase in Task Order price, the contractor shall submit a price proposal to the COTR and obtain approval. The contractor shall submit said price proposal within 20 business days from the date the contractor receives notice of the revision, supplement, or amendment-giving rise to the increase in cost of performance. Failure of the contractor to submit a price proposal within 20 business days from the date of receipt of any change shall entitle the Government to require performance in accordance with such change at no increase in Task Order price.
- C.6.1.1.4 The contractor shall ensure that all publications are posted and up-to-date. Upon completion of the Task Order, the contractor shall return to the Government all issued publications.

C.6.1.2 Publication Conflict Resolution

- C.6.1.2.1 If there is a conflict between Section C and the cited references, Section C shall control.
- C.6.1.2.2 Any task set forth in any such reference which will call for the exercise of discretionary Government authority that cannot be delegated, will be subject to the final approval of the Government official having such authority.
- C.6.1.2.3 All publications and forms will be current issue. The contractor shall use existing stocks of forms until depleted.
- C.6.1.2.4 The publications and documents listed in this Section are current with dates as of the writing of this Task Order, not necessarily date of Task Order award. The Government will not modify this section of the Task Order during the tenure of the Task Order unless a Contract Price change is required based upon a new documentary requirement.

C.6.2 FEDERAL PUBLICATIONS

C.6.2.1 Federal Regulation and Guidelines

All supplies and services provided under this Task Order shall conform to the applicable Federal Information Processing Standards Publications (FIPS PUBS) as specified on Web site <http://www.itl.nist.gov/fipspubs/>. The contractor shall also comply with

PROCUREMENT SENSITIVE

Electronic and Information Technology Standards as specified on Web site
<http://www.section508.gov/index.cfm?FuseAction=Content&ID=3>

- Government Paperwork Elimination Act (GPEA)
<http://www.whitehouse.gov/omb/fedreg/gpea2.html>
- Federal Acquisition Regulation
- Records management guidance for agencies implementing electronic signature technologies <http://www.nara.gov/records/policy/gpea.html>
- Electronic Signatures in Global and National Commerce Act (ESIGN)
<http://www.whitehouse.gov/omb/memoranda/m00-15.html>
- OMB Circular A130
<http://www.whitehouse.gov/OMB/circulars/a130/a130.html>

C.6.3 OTHER PUBLICATIONS

C.6.3.1 U.S. Congress-Public Law (PL) and United States Code (U.S.C.)

- PL 107-347 Section III, Federal Information Security Management Act (FISMA) of 2002, 2002
- PL 107-305, Cyber Security Research and Development Act of 2002
- PL 96-456, Classified Information Procedures Act of 1980
- 5 U.S.C. 552, Freedom of Information Act; Public Information; Agency Rules, Opinions, Orders, Records, and Proceedings, 1967
- 5 U.S.C. 552a, Privacy Act; Records Maintained on Individuals, 1974
- 18 U.S.C. 1029, Fraud and Related Activity in Connection with Access Devices
- 18 U.S.C. 1030, Fraud and Related Activity in Connection with Computers
- 40 U.S.C. 1401 et seq., P.L. 104-106, Clinger Cohen Act of 1996 (Information Technology and Management Reform Act of 1996)
- 44 U.S.C. 3534, Federal Agency Responsibilities
- 44 U.S.C. 3535, Annual Independent Evaluation
- 44 U.S.C. 3537, Authorization of Appropriations
- 44 U.S.C. 3541, P.L. 107-296, Federal Information Security Management Act of 2002 (FISMA)
- 44 U.S.C. 3546, Federal Information Security Incident Center

C.6.3.2 Executive Orders—Office of Management and Budget (OMB), Homeland Security Presidential Directive (HSPD) and Presidential Decision Directive

- HSPD-7, Critical Infrastructure Identification, Prioritization, and Protection, 2004
- HSPD-20 National Continuity Policy, 2007
- OMB Policy Memorandum M-07-11, Implementation of Commonly Accepted Security Configurations for Windows Operating Systems.
- OMB Memorandum M-07-18, Ensuring New Acquisitions Include Common Security Configurations
- OMB Circular A-130, Appendix III, Security of Federal Automated Information Systems, 2000

PROCUREMENT SENSITIVE

C.6.3.3 DHS Management Directive (MD)

The DHS Interactive web site contains the DHS MDs

- DHS MD 0000 Organization of the Office of the Secretary of Homeland Security
- DHS MD 0002 Operational Integration Staff
- DHS MD 0003 Acquisition Line of Business Integration and Management
- DHS MD 0004 Administrative Service Line of Business Integration and Management
- DHS MD 0005 Financial Management Line of Business Integration and Management
- DHS MD 0006 Human Capital Line of Business Integration and Management
- DHS MD 0007.1 Information Technology Integration and Management
- DHS MD 0475 Information Collection Program
- DHS MD 0480.1 Ethics/Standards of Conduct
- DHS MD 0490.1 Federal Register Notices and Rules
- DHS MD 0550.1 Record Management
- DHS MD 0560 Real Property Management Program
- DHS MD FORM 560-1 (3/05): Custody Receipt for Personal Property/Property Pass
- DHS MD FORM 560-3 (3/05): Property Transfer Receipt
- DHS MD 0565 Personal Property Management Directive
- DHS MD 0590 Mail Management Program
- DHS MD 0720.1 Small Business Acquisition Program
- DHS MD 0731 Strategically Sourced Commodities Policy and Procedures
- DHS MD 0760.1 Purchase Card Program
- DHS MD 0780 Contracting Officer's Technical Representative (COTR) Certification, Appointment & Responsibilities
- DHS MD 0782 Acquisition Certification Requirement for Program Managers
- DHS MD 0783 Ordering Official Certification
- DHS MD 0784 Acquisition Oversight Program
- DHS MD 1120 Capitalization and Inventory of Personal Property
- DHS MD 1130.1 Electronic Funds Transfer for Disbursements, Collections and Deposits
- DHS MD 1190.1 Billings and Collections
- DHS MD 1210.1 Vendor Maintenance
- DHS MD 1330 Planning, Programming, Budgeting and Execution
- DHS MD 1400 Investment Review Process
 - Enclosure 1: Definitions
 - Enclosure 2: Guiding Principles
 - Enclosure 3: Exhibit 300 Light

PROCUREMENT SENSITIVE

- Enclosure 4: Request for MRC Review
- Enclosure 5: IT Investment Review
- Enclosure 6: Business Case Scoring Template
- Enclosure 7: Phases and Business Case Elements
- DHS MD 1510.1 Travel for Official Government Business
- DHS MD 1560.2 Payment for Official Travel Expenses by Non-Federal Sources
- DHS MD 3120.2 Employment of Non-Citizens
- DHS MD 4010.2 Section 508 Program Management Office & Electronic and Information Technology Accessibility
 - Appendix A: Software Applications and Operating Systems
 - Appendix B: Web-Based Intranet and Internet Information and Applications
 - Appendix C: Telecommunications Products
 - Appendix D: Video and Multimedia Products
 - Appendix E: Self Contained, Closed Products
 - Appendix F: Desktop and Portable Computers
 - Appendix G: Functional Performance Criteria
 - Appendix H: Information, Documentation and Support
- DHS MD 4030 Geospatial Management Office
- DHS MD 4100.1 Wireless Management Office
- DHS MD 4200.1 IT Capital Planning and Investment Control (CPIC) and Portfolio Management
 - Attachment 1: Guide to Information Technology Capital Planning and Investment Control
- DHS MD 4300.1 Information Technology Systems Security
- DHS MD 4400.1 DHS Web (Internet, Intranet, and Extranet Information) and Information Systems
- DHS MD 4500.1 DHS E-Mail Usage
- DHS MD 4510 Domain Names
- DHS MD 4600.1 Personal Use of Government Office Equipment
- DHS MD 4700.1 Personal Communications Device Distribution
- DHS MD 4800 Telecommunications Operations
 - Attachment A: Frequently Asked Questions (FAQs)
 - Attachment B: Nomination and Designation of Designated Agency Representative (DAR) for Telecommunications Services
 - Attachment C: Designated Agency Representative (DAR) for Telecommunications Services Function Requirements
- DHS MD 4900 Individual Use and Operation of DHS Information Systems/ Computers
 - Attachment A: Information Systems/Computer Access Agreement

PROCUREMENT SENSITIVE

- Attachment B: Logon Screen
- DHS MD 5110.1 Environmental Compliance Program
- DHS MD 5120.1 Environmental Management Program
- DHS MD 5200.1 Occupational Safety and Health Programs
- DHS MD 8200.1 Information Quality
- DHS MD 9300.1 Continuity of Operations Programs and Continuity of Government Functions
- DHS MD 11000 Office of Security
- DHS MD 11005 Suspending Access to DHS Facilities, Sensitive Information, and IT Systems
- DHS MD 11020.1 Issuance of Access Control Media
- DHS MD 11021 Portable Electronic Devices in SCI Facilities
- DHS MD 11030.1 Physical Protection of Facilities and Real Property
- DHS MD 11041 Protection of Classified National Security Information Program Management
- DHS MD 11042.1 Safeguarding Sensitive But Unclassified (For Official Use Only) Information
- DHS MD 11043 Sensitive Compartmented Information Program Management
- DHS MD 11044 Protection of Classified National Security Information Classification Management
- DHS MD 11045 Protection of Classified National Security Information: Accountability, Control, and Storage
- DHS MD 11046 Open Storage Area Standards for Collateral Classified Information
- DHS MD 11047 Protection of Classified National Security Information Transmission & Transportation
- DHS MD 11048 Suspension, Denial, and Revocation of Access to Classified Information
- DHS MD 11049 Protection of Classified National Security Information: Security Violations and Infractions
- DHS MD 11050.2 Personnel Security and Suitability Program
- DHS MD 11051 Department of Homeland Security SCIF Escort Procedures
- DHS MD 11052 Internal Security Program
- DHS MD 11053 Security Education, Training, and Awareness Program Directive
- DHS MD 11056.1 Sensitive Security Information (SSI)
- DHS MD 11060.1 Operations Security Program
- DHS MD 11080 Security Line of Business Integration and Management

C.6.3.4 DHS Regulations

- Homeland Security Acquisition Regulation 305.242-71

C.6.3.5 DHS Guides

- DHS SCG OS-001 (IT), Security Classification Guide – Homeland Security Data Network, February 2004
- DHS SCG OS-002 (IT), Security Classification Guide – National Security IT Systems Certification and Accreditation, March 2004

C.6.3.6 National Institute of Standards and Technology (NIST), Special Publications

The web site www.nist.gov contains the NIST publications

- 800-18, Guide for Developing Security Plans for Information Technology Systems, 1998
- 800-23, Guideline to Federal Organizations on Security Assurance and Acquisition/Use of Tested/Evaluated Products, 2000
- 800-26, Revised NIST SP 800-26 System Questionnaire with NIST SP 800-53 References and Associated Security Control Mappings, 2005
- 800-27, Engineering Principles for Information Technology Security (A Baseline for Achieving Security), Revision A, 2004
- 800-30, Risk Management Guide for Information Technology Systems, 2002
- 800-31, Intrusion Detection Systems (IDS), 2001
- 800-34, Contingency Planning Guide for Information Technology Systems, 2002
- 800-35, Guide to Information Technology Security Services, 2003
- 800-36, Guide to Selecting Information Security Products, 2003
- 800-37, Guide for the Security Certification and Accreditation of Federal Information Systems, 2004
- 800-40, Procedures for Handling Security Patches, 2002
- 800-41, Guidelines on PEPs and PEP Policy, 2002
- 800-42, Guideline on Network Security Testing, 2003
- 800-45, Guidelines on Electronic Mail Security, 2002
- 800-47, Guide for Interconnecting Information Technology Systems, 2002
- 800-50, Building an Information Technology Security Awareness and Training Program, 2003
- 800-51, Use of the Common Vulnerabilities and Exposures (CVE) Vulnerability Naming Scheme, 2002
- 800-53, Recommended Security Controls for Federal Information Systems, 2005
- 800-55, Security Metrics Guide for Information Technology Systems, 2003
- 800-59, Guideline for Identifying an Information System as a National Security System, 2003
- 800-60, Guide for Mapping Types of Information and Information Systems to Security Categories, 2004

- 800-61, Computer Security Incident Handling Guide, 2004
- 800-64, Security Considerations in the Information System Development Life Cycle, 2004
- 800-65, Integrating Security into the Capital Planning and Investment Control Process, 2005
- 800-68, Draft NIST Special Publication 800-68, Guidance for Securing Microsoft Windows XP Systems for IT Professionals: A NIST Security Configuration Checklist, 2004
- 800-70, The NIST Security Configuration Checklists Program

C.6.3.7 Federal Information Processing Standards Publications (FIPS PUBS)

The web site <http://www.itl.nist.gov/fipspubs/> contains FIPS publications.

- FIPS 199, Standards for Security Categorization of Federal Information and Information Systems, 2003

C.6.4 FORMS

DHS will provide electronically a comprehensive list of all forms upon Task Order award. DHS will provide a URL address to access the DHS website for forms.

C.7 TECHNICAL EXHIBITS

Technical Exhibit Title Numbering System:

A Technical Exhibit (TE) is titled in relation to the Section from which it is first referenced and its order among TEs in that Section. For example, Section 3.1 has three Technical Exhibits titled TE C.3.1.-001, TE C.3.1-002, and TE C.3.1.-003.

TE Page Numbering System:

Since Section C.7 provides all Technical Exhibits except those maintained on the DHS Interactive website, all TEs are page numbered in relation to their TE title. For example, page one of TE C.5.2.-001 is shown as page number TE C.5.2.-001-01 to indicate that it is the first page of TE C.5.2.-001 from Task Order Section 5.2.

List of Technical Exhibits:

TE	Description	Task Order Paragraph
<u>C.1.2-001</u>	DHS Organization Chart	<u>C.1.2</u>
<u>C.1.2-002</u>	Locations Supported Summary (Sensitive But Unclassified)	<u>C.1.2, C.5.6.1</u>
<u>C.1.2-003</u>	DHS OCIO Organization Chart	<u>C.1.2</u>
<u>C.1.3-002</u>	Seats by Fiscal Year (FY) for LAN – A	<u>C.1.3.1.1, C.5</u>
<u>C.1.3-002</u>	Seats by Fiscal Year (FY) for LAN – HSDN	<u>C.1.3.1.1, C.5</u>
<u>C.1.3-002</u>	Seats by Fiscal Year (FY) for LAN – C	<u>C.1.3.1.1, C.5</u>
<u>C.1.6-001</u>	Performance Requirements Summary	<u>C.1.6.1, C.1.6.1.2, C.1.9.1.1</u>
<u>C.1.6-002</u>	Plans developed, maintained, and updated by Contractor	<u>C.1.6.2.4</u>
<u>C.1.7-001</u>	Key Personnel Positions and Descriptions	<u>C.1.7.1.2</u>
<u>C.1.12-001</u>	Current Contracts Period of Performance	<u>C.1.12.1.1</u>
<u>C.1.12.002</u>	Projects	<u>C.1.12.1.1</u>
<u>C.3.1-001</u>	Government Furnished Equipment Product Guide of IT Equipment & Software	<u>C.3.1.4.1, C.5, C.5.1, C.5.6.1</u>
<u>C.3.1-002</u>	Government Furnished Equipment Software	<u>C.3.1.4.1</u>
<u>C.3.1-003</u>	Government Furnished Equipment Inventory	<u>C.3.1.4.1</u>
<u>C.3.1-004</u>	Government Furnished Facilities	<u>C.3.1.4.1</u>
<u>C.5.1-001</u>	DHS Custom Applications	<u>C.5.1.1.2</u>
<u>C.5.5-001</u>	Help Desk Ticket volume	<u>C.5.5.1</u>
<u>C.5.8-001</u>	Switchboard Call Volume	<u>C.5.8.2</u>
<u>C.5.15-001</u>	Continuity Planning Framework	<u>C.5.15.1</u>

AMENDMENT OF SOLICITATION/MODIFICATION OF CONTRACT

CONTRACT ID CODE

PAGE OF PAGES

1 3

2. AMENDMENT/MODIFICATION NO. P00005		3. EFFECTIVE DATE 02/01/2009		4. REQUISITION/PURCHASE REQ. NO. RUIO-09-HS039		5. PROJECT NO. (If applicable)	
6. ISSUED BY U.S. Dept. of Homeland Security Office of Procurement Operations Information Tech. Acquisition Div. Murray Lane, SW Building 410 Washington DC 20528		CODE DHS/OPO/ITAC		7. ADMINISTERED BY (If other than item 6) U.S. Dept. of Homeland Security Office of Procurement Operations Information Tech. Acquisition Div. 245 Murray Lane, SW Building 410 Washington DC 20528		CODE DHS/OPO/ITAC	
8. NAME AND ADDRESS OF CONTRACTOR (Inc., street, county, State and ZIP Code) LOCKHEED MARTIN SERVICES INC 2339 ROUTE 70 WEST FLOOR 3W CHERRY HILL NJ 080023315				<input checked="" type="checkbox"/> 9A. AMENDMENT OF SOLICITATION NO. <input type="checkbox"/> 9B. DATED (SEE ITEM 11)			
CODE 8052583730000 FACILITY CODE				<input checked="" type="checkbox"/> 10A. MODIFICATION OF CONTRACT/ORDER NO. HSHQDC-06-D-00017 HSHQDC-08-J-00138 <input type="checkbox"/> 10B. DATED (SEE ITEM 11) 06/02/2008			

11. THIS ITEM ONLY APPLIES TO AMENDMENTS OF SOLICITATIONS

The above numbered solicitation is amended as set forth in item 14. The hour and date specified for receipt of Offers is extended, is not extended. Offers must acknowledge receipt of this amendment prior to the hour and date specified in the solicitation or as amended, by one of the following methods: (a) By completing items 8 and 15, and returning _____ copies of the amendment; (b) By acknowledging receipt of this amendment on each copy of the offer submitted; or (c) By separate letter or telegram which includes a reference to the solicitation and amendment numbers. FAILURE OF YOUR ACKNOWLEDGEMENT TO BE RECEIVED AT THE PLACE DESIGNATED FOR THE RECEIPT OF OFFERS PRIOR TO THE HOUR AND DATE SPECIFIED MAY RESULT IN REJECTION OF YOUR OFFER. If by virtue of this amendment you desire to change an offer already submitted, such change may be made by telegram or letter, provided each telegram or letter makes reference to the solicitation and this amendment, and is received prior to the opening hour and date specified.

12. ACCOUNTING AND APPROPRIATION DATA (If required)

See Schedule

13. THIS ITEM ONLY APPLIES TO MODIFICATION OF CONTRACTS/ORDERS. IT MODIFIES THE CONTRACT/ORDER NO. AS DESCRIBED IN ITEM 14.

CHECK ONE	A. THIS CHANGE ORDER IS ISSUED PURSUANT TO: (Specify authority) THE CHANGES SET FORTH IN ITEM 14 ARE MADE IN THE CONTRACT ORDER NO. IN ITEM 10A.
	B. THE ABOVE NUMBERED CONTRACT/ORDER IS MODIFIED TO REFLECT THE ADMINISTRATIVE CHANGES (such as changes in paying office, appropriation date, etc.) SET FORTH IN ITEM 14, PURSUANT TO THE AUTHORITY OF FAR 43.103(b).
X	C. THIS SUPPLEMENTAL AGREEMENT IS ENTERED INTO PURSUANT TO AUTHORITY OF: FAR 43.103(a)(3) and Mutual Agreement of Both Parties
	D. OTHER (Specify type of modification and authority)

E. IMPORTANT: Contractor is not, is required to sign this document and return 1 copies to the issuing office.



14. DESCRIPTION OF AMENDMENT/MODIFICATION (Organized by UCF section headings, including solicitation/contract subject matter where feasible.)

DUNS Number: 805258373+0000

The purpose of this modification to Task Order HSHQDC-08-J-00138 is to extend the Base Year period of performance and to authorize five (5) Task Order Unique Labor Categories at no additional cost to the government. In addition, a new Task Order Contracting Officer is named.

Period of Performance: 06/01/2008 to 01/31/2013

Except as provided herein, all terms and conditions of the document referenced in item 9A or 10A, as heretofore changed, remains unchanged and in full force and effect.

15A. NAME AND TITLE OF SIGNER (Type or print) Andreas Hansen Jr Mgr Contract		16A. NAME AND TITLE OF CONTRACTING OFFICER (Type or print) Rebecca A. Taylor	
15B. CONTRACTOR OFFER FOR 		15C. DATE SIGNED 1/30/09	
16B. UNITED STATES OF AMERICA 		16C. DATE SIGNED JAN 30 2009	

540-01-152-8070
as edition unusable

STANDARD FORM 30 (REV. 10-83)
Prescribed by GSA
FAR (48 CFR) 53.243

Accordingly, the following changes are hereby made to Task Order HSHQDC-08-J-00138:

1. Revise **Section F.1 - TASK ORDER TERM** to read:

Base Year: The task order term is revised **from** June 1, 2008 through January 31, 2009 **to read** June 1, 2008 through April 10, 2009. If exercised, the period of performance for the option years is revised to read as follows:

- Option 1: Revised **from** February 1, 2009 through January 31, 2010
To read April 11, 2009 through January 31, 2010
- Option 2: February 1, 2010 through January 31, 2011 (No Change)
- Option 3: February 1, 2011 through January 31, 2012 (No Change)
- Option 4: February 1, 2012 through January 31, 2013 (No Change)

2. The contractor will utilize Option Year 1 rates for all labor categories during the extended Base Year performance period from February 1, 2009 through April 10, 2009.

3. Revise **Section G.1 - TO CONTRACTING OFFICER (TO CO)** as follows:

Change TO Contracting Officer from:

NAME: Charles Conrad
 PHONE NO.: (202) 447-5554
 EMAIL: charles.conrad@dhs.gov

Change TO Contracting Officer to read:

NAME: Rebecca A. Taylor
 PHONE NO.: (202) 447-5480
 EMAIL: rebecca.a.taylor@dhs.gov

4. Delete **Section G.2 - TO ADMINISTRATIVE CONTRACTING OFFICER (TO ACO)** in its entirety. Section G.2 will remain blank as a place holder in the task order.
5. Add five (5) IT-NOVA Task Order Unique Labor Categories to enable the contractor to recruit and retain personnel with Top Secret/Secured Compartmented Information (TS/SCI) clearance levels. IT-NOVA Task Order Unique Labor Category titles and rates are shown at Table 1.

Table 1.	Government Site Rates				
<u>IT-NOVA Task Order Unique Labor Categories</u>	Base Year	Option Year 1	Option Year 2	Option Year 3	Option Year 4
Applications Engineer (Senior) Business Process Reengineering Spec (Senior) Computer Systems Analyst (Senior) Information Engineer (Principal) Information Technology Senior Consultant	(b) (4)				

6. The total amount of Base Year Contract Line Item Numbers (CLINS) 0001 through 0009 remains unchanged at \$35,868,230.00.
7. The value and total amount funded/obligated to the task order remains unchanged at \$35,868,230.00
8. The ceiling for this task order remains unchanged at \$288,499,204.00.
9. The following proposals submitted by the contractor are hereby incorporated into this task order to form an integral part of this contract, which proposals are entitled:
 - “IT-NOVA - Lockheed Martin Revised Re-Baseline Proposal” dated January 29, 2009;
 - “IT-NOVA – Lockheed Martin Revised Pricing Model” dated January 29, 2009;
 - “Lockheed Martin Proposal for Additional Labor Categories” dated December 11, 2008.
10. All other terms and conditions remain the same.



January 28, 2009.

Department of Homeland Security (DHS)
Office of Procurement Operations/ITAC
245 Murray Drive
Building 410
Washington, DC 20528

Mod # 5
Attachment # 1

Attention: Rebecca Taylor, Contracting Officer
Subject: **IT-NOVA – HSHQDC-06-D-00017/HSHQDC-07-J-00138**
Reference: IT-NOVA - Lockheed Martin (LM) Revised Re-Baseline Proposal

Dear Ms. Taylor:

Lockheed Martin (LM) is pleased to enclose a re-baseline proposal. Please be advised that:

- LM has revised the proposal in consideration of adding five (5) new labor categories to the full scope of the task order (across all applicable PWS sections).
- LM has proposed a labor mix that does not exceed the existing NTE ceiling.
- The attached proposal assumes option year one pricing commencing February 1, 2009.
- The attached proposal contains a blend of actual, estimated, and projected data.
- The five new labor categories have been separated in the proposal to enable ease of review and identification.
- In consideration of the ceiling threshold LM has priced out according to the highest proposed labor category, with the intent that during the course of the performance period LM will seek to hire against all labor categories. LM will continuously work with the government to integrate the labor categories as needed.
- LM has satisfied the government's request to propose as many labor categories that may be utilized throughout the life of the task order. It is possible that LM will not utilize each proposed labor category during the base period of the task order. However as previously mentioned, in coordination with the government, LM plans to incorporate labor categories as needed throughout the life of the task order.

Should you have any further questions or concerns please feel free to contact me at 301-352-2640 or via email at (b) (4)

Sincerely,

Zanetta Williams
Zanetta Williams, CPCM
Sr. Staff, Contracts



I. Overview

Adjustments to PWS category skill mixes were made to numerous PWS elements with the understanding that by PWS and at the Task Order level the Contract value would remain unchanged. The justifications for all proposed changes are written below in the individual detail of the PWS elements. Overall IT NOVA program PWS summaries of the changes are identified in the table below.

Original Bid			Repriced Proposal		
PWS	Name	FTEs	PWS	Name	FTEs
C.1,3,4	Program Mgmt Office (PMO)	(b) (4)	C.1,3,4	Program Mgmt Office (PMO)	(b) (4)
C.5.1	Applications Mgmt Services		C.5.1	Applications Mgmt Services	
C.5.2	Deployment Support		C.5.2	Deployment Support	
C.5.3	Infrastructure Engineering Services		C.5.3	Infrastructure Engineering Services	
C.5.4	Testing		C.5.4	Testing	
C.5.5	Operations & Maintenance		C.5.5	Operations & Maintenance	
C.5.6	Video Teleconferencing		C.5.6	Video Teleconferencing	
C.5.7	Satellite/Cable TV Operations		C.5.7	Satellite/Cable TV Operations	
C.5.8	Phone & PBX Operations		C.5.8	Phone & PBX Operations	
C.5.9	Network Mgmt Center (NMC)		C.5.9	Network Mgmt Center (NMC)	
C.5.10	Security Mgmt Center (SMC)		C.5.10	Security Mgmt Center (SMC)	
C.5.11	COMSEC Security		C.5.11	COMSEC Security	
C.5.12	Other Communications Operations		C.5.12	Other Communications Operations	
C.5.13	Training		C.5.13	Training	
C.5.14	Wireless Mgmt		C.5.14	Wireless Mgmt	
C.5.15	Continuity Mgmt		C.5.15	Continuity Mgmt	
Sub			Sub		
Totals			Totals		

The proposed changes to the current staffing levels were developed based upon our current experience through actual daily tasking. The development of the new labor mix for the various PWS elements was the result of the inclusion of 5 additional EAGLE labor categories to the IT-NOVA Task Order:

- Applications Engineer (Senior)
- Business Process Reengineering Spec (Senior)
- Computer Systems Analyst (Senior)
- Information Engineer (Principal)
- Information Technology Senior Consultant

(b) (4)

(b) (4)

The proposed changes are designed to take advantage of operational efficiencies expected from the deployment of new technology, personnel with new skill sets and the re-engineering effort of process and procedures.

(b) (4)

(b) (4)

(b) (4)

(b) (4)

(b) (4)

(b) (4)

(b) (4)

The complexity of the DHS/HQ operating environment mandates processes that are highly integrated with DHS/HQ, its subordinate components, and operating partners such as CBP. These processes, whether automated or manual must ensure the integrity of the systems and the inherent dependencies during normal operations, issue resolution, and system enhancements. In order to ensure this integrity and to achieve required operational efficiencies, it is imperative that each process and procedure be effective, robust, and maintains the dependencies of each operating partner.

The proposed exchange of labor categories will through the focused re-engineering effort and streamlining of current process and procedures in order to achieve the operational efficiencies expected from existing technology, the deployment of new technology, and the availability of human resources.

Lockheed Martin Proposal For Additional Labor Categories



Mod #5
Attachment #3

**Department of Homeland Security
Office of the Chief Information Officer (OCIO)
Information Technology Services Office
HQ Services Division**

December 11, 2008

AMENDMENT OF SOLICITATION/MODIFICATION OF CONTRACT		1. CONTRACT ID CODE	PAGE OF PAGES 1 8
2 AMENDMENT/MODIFICATION NO. P00006	3 EFFECTIVE DATE 04/11/2009	4 REQUISITION/PURCHASE REQ. NO.	5. PROJECT NO. (If applicable)
6 ISSUED BY U.S. Dept. of Homeland Security Office of Procurement Operations Information Tech. Acquisition Div. 245 Murray Lane, SW Building 410 Washington DC 20528	CODE DHS/OPO/ITAC	7. ADMINISTERED BY (If other than Item 6) U.S. Dept. of Homeland Security Office of Procurement Operations Information Tech. Acquisition Div. 245 Murray Lane, SW Building 410 Washington DC 20528	CODE DHS/OPO/ITAC
8. NAME AND ADDRESS OF CONTRACTOR (No., street, county, State and ZIP Code) LOCKHEED MARTIN SERVICES INC 2339 ROUTE 70 WEST FLOOR 3W CHERRY HILL NJ 080023315		(x) 9A. AMENDMENT OF SOLICITATION NO.	
CODE 8052583730000		9B. DATED (SEE ITEM 11)	
FACILITY CODE		x 10A. MODIFICATION OF CONTRACT/ORDER NO. HSHQDC-06-D-00017 HSHQDC-08-J-00138	
		10B. DATED (SEE ITEM 13) 06/02/2008	

11. THIS ITEM ONLY APPLIES TO AMENDMENTS OF SOLICITATIONS

The above numbered solicitation is amended as set forth in Item 14. The hour and date specified for receipt of Offers is extended, is not extended. Offers must acknowledge receipt of this amendment prior to the hour and date specified in the solicitation or as amended, by one of the following methods: (a) By completing Items 8 and 15, and returning _____ copies of the amendment; (b) By acknowledging receipt of this amendment on each copy of the offer submitted; or (c) By separate letter or telegram which includes a reference to the solicitation and amendment numbers. FAILURE OF YOUR ACKNOWLEDGEMENT TO BE RECEIVED AT THE PLACE DESIGNATED FOR THE RECEIPT OF OFFERS PRIOR TO THE HOUR AND DATE SPECIFIED MAY RESULT IN REJECTION OF YOUR OFFER. If by virtue of this amendment you desire to change an offer already submitted, such change may be made by telegram or letter, provided each telegram or letter makes reference to the solicitation and this amendment, and is received prior to the opening hour and date specified.

12. ACCOUNTING AND APPROPRIATION DATA (If required)

See Schedule

13. THIS ITEM ONLY APPLIES TO MODIFICATION OF CONTRACTS/ORDERS. IT MODIFIES THE CONTRACT/ORDER NO. AS DESCRIBED IN ITEM 14.

CHECK ONE	A. THIS CHANGE ORDER IS ISSUED PURSUANT TO: (Specify authority) THE CHANGES SET FORTH IN ITEM 14 ARE MADE IN THE CONTRACT ORDER NO. IN ITEM 10A.
	B. THE ABOVE NUMBERED CONTRACT/ORDER IS MODIFIED TO REFLECT THE ADMINISTRATIVE CHANGES (such as changes in paying office, appropriation date, etc.) SET FORTH IN ITEM 14, PURSUANT TO THE AUTHORITY OF FAR 43.103(b)
X	C. THIS SUPPLEMENTAL AGREEMENT IS ENTERED INTO PURSUANT TO AUTHORITY OF FAR 43.103(a)(3) and Mutual Agreement of Both Parties
	D. OTHER (Specify type of modification and authority)

E. IMPORTANT: Contractor is not, is required to sign this document and return 1 copies to the issuing office.

14. DESCRIPTION OF AMENDMENT/MODIFICATION (Organized by UCF section headings, including solicitation/contract subject matter where feasible.)

DUNS Number: 805258373+0000

The purpose of this modification is to extend the base year period of performance through May 3, 2009; incorporate the Lockheed Martin Proposal for Survey, Design, Integration, Deployment and Training of Remedy Asset Management and Change Management Modules; and revise the task order Exhibit 1.700 Key Personnel Listing.

See page 6 for modification details.

Discount Terms:

Net 30

Delivery Location Code: DHS

Continued ...

Except as provided herein, all terms and conditions of the document referenced in Item 9A or 10A, as heretofore changed, remains unchanged and in full force and effect.

15A. NAME AND TITLE OF SIGNER (Type or print) <i>Zaretta Williams, Contract Manager</i>	15C. DATE SIGNED <i>4/10/09</i>	16A. NAME AND TITLE OF CONTRACTING OFFICER (Type or print) Rebecca A. Taylor	16C. DATE SIGNED <i>APR 10 2009</i>
15B. CONTRACTOR/ORDER NO. <i>[Signature]</i> (Signature of person authorized to sign)		16B. UNITED STATES OF AMERICA <i>[Signature]</i> (Signature of Contracting Officer)	

NSM 7540-01-152-6070
Previous edition unusable

STANDARD FORM 30 (REV. 10-83)
Prescribed by GSA
FAR (48 CFR) 53.243

CONTINUATION SHEET

REFERENCE NO. OF DOCUMENT BEING CONTINUED
 HSHQDC-06-D-00017/HSHQDC-08-J-00138/P00006

PAGE OF
 2 8

NAME OF OFFEROR OR CONTRACTOR
 LOCKHEED MARTIN SERVICES INC

ITEM NO (A)	SUPPLIES/SERVICES (B)	QUANTITY (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)
0001	Department of Homeland Security 245 Murray Lane Bldg. 410 Washington DC 20528 FOB: Destination Period of Performance: 06/01/2008 to 01/31/2013 Change Item 0001 to read as follows (amount shown is the obligated amount): Base Year Operations and Maintenance Support Services (HSD) This CLIN shall not exceed the amount of \$29,789,173.00. Funding shall be obligated in the following amounts: 1. Operations and Maintenance Support Services (HSD) \$29,564,505.00 2. Survey, Design, Integration, Deployment and Training of Remedy Asset Management and Change Management Modules \$224,668.00 Period of Performance: 06/01/2008 to 05/03/2009 Accounting Info: RWC8049 RWC WF-99-01-00-000-02-05-0000-00-00-00-00 GE OE 25 84 FY2008 Funded: \$0.00 Accounting Info: SCAC008-000-IX-22-11-02-000-02-05-0000-00-00-00-00 -GE-OE-25-41-EM0122 Funded: \$0.00 Accounting Info: SCAC008-000-IX-22-11-02-000-02-05-0000-00-00-00-00 -GE-OE-25-44-SO0024 Funded: \$0.00 Accounting Info: RWC8049 RWC WF-99-01-00-000-02-05-0000-00-00-00-00 GE OE 25 44 FY2008 Funded: \$0.00 Accounting Info: RWC8049 RWC WF-99-01-00-000-02-05-0000-00-00-00-00 GE OE 31 18 FY2008 Funded: \$0.00 Accounting Info: RWC8049 RWC WF-99-01-00-000-02-05-0000-00-00-00-00 GE OE 25 76 FY2008 Continued ...				0.00

CONTINUATION SHEET

REFERENCE NO OF DOCUMENT BEING CONTINUED
 HSHQDC-06-D-00017/HSHQDC-08-J-00138/P00006

PAGE OF
 3 8

NAME OF OFFEROR OR CONTRACTOR
 LOCKHEED MARTIN SERVICES INC

ITEM NO. (A)	SUPPLIES/SERVICES (B)	QUANTITY (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)
	Funded: \$0.00 Accounting Info: RWC8049 RWC WF-99-01-00-000-02-05-0000-00-00-00-00 GE OE 25 74 FY2008 Funded: \$0.00				
0002	Change Item 0002 to read as follows(amount shown is the obligated amount): Base Year Operations and Maintenance Support Services ODC's HSD NTE \$1,700,000.00 Period of Performance: 06/01/2008 to 05/03/2009 Accounting Info: RWC8049 RWC WF-99-01-00-000-02-05-0000-00-00-00-00 GE OE 25 84 FY2008 Funded: \$0.00 Change Item 0003 to read as follows(amount shown is the obligated amount):				0.00
0003	Base Year Spectrum Support Services ESD NTE \$1,080,000 Period of Performance: 06/01/2008 to 05/03/2009 Accounting Info: WLP007-000-IX-22-12-00-000-02-05-0000-00-00-00-00 GE OE 25 44 WL0032 Funded: \$0.00				0.00
0004	Change Item 0004 to read as follows(amount shown is the obligated amount): Base Year Spectrum ODCs ESD NTE \$20,000 Period of Performance: 06/01/2008 to 05/03/2009 Accounting Info: WLP007-000-IX-22-12-00-000-02-05-0000-00-00-00-00 GE OE 25 44 WL0032 Funded: \$0.00 Continued ...				0.00

CONTINUATION SHEET

REFERENCE NO. OF DOCUMENT BEING CONTINUED
 HSHQDC-06-D-00017/HSHQDC-08-J-00138/P00006

PAGE OF
 4 8

NAME OF OFFEROR OR CONTRACTOR
 LOCKHEED MARTIN SERVICES INC

ITEM NO (A)	SUPPLIES/SERVICES (B)	QUANTITY (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)
0005	Change Item 0005 to read as follows (amount shown is the obligated amount): Base Year Infrastructure Transformation Program (ITP) ESD NTE \$830,916.80 Period of Performance: 06/01/2008 to 05/03/2009 Accounting Info: SCAC007-000-IX-22-11-02-000-02-05-0000-00-00-00-00 -GE-OE-25-44-EP0012 Funded: \$0.00				0.00
0006	Change Item 0006 to read as follows (amount shown is the obligated amount): Base Year Infrastructure Transformation Program ODC's ESD NTE \$40,000 Period of Performance: 06/01/2008 to 05/03/2009 Accounting Info: SCAC007-000-IX-22-11-02-000-02-05-0000-00-00-00-00 (GE) OE 25 44 EP0012 Funded: \$0.00				0.00
0007	Change Item 0007 to read as follows (amount shown is the obligated amount): Base Year Security Support Services ESD NTE \$690,977.20 Period of Performance: 06/01/2008 to 05/03/2009 Amount: \$452,987.00 Accounting Info: IFSR008-000-IX-22-10-05-000-02-05-0000-00-00-00-00 -GE OE 25 44 SC0032 Funded: \$0.00 Amount: \$237,990.20 Accounting Info: OINF008-000-IT-21-14-10-000-02-05-0500-00-00-00-00 -GE OE 25 44 SC0021 Funded: \$0.00 Change Item 0008 to read as follows (amount shown Continued ...				0.00

CONTINUATION SHEET

REFERENCE NO OF DOCUMENT BEING CONTINUED
 HSHQDC-06-D-00017/HSHQDC-08-J-00138/P00006

PAGE OF
 5 8

NAME OF OFFEROR OR CONTRACTOR
 LOCKHEED MARTIN SERVICES INC

ITEM NO (A)	SUPPLIES/SERVICES (B)	QUANTITY (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)
	is the obligated amount):				
0008	Base Year Security Support Services ODC's ESD NTE \$40,000 Period of Performance: 06/01/2008 to 05/03/2009 Accounting Info: OINF008-000-IT-21-14-10-000-02-05-0500-00-00-00-00 -GE OE 25 44 SC0021 Funded: \$0.00				0.00
	Change Item 0009 to read as follows (amount shown is the obligated amount):				
0009	Base Year DHS Headquarters Coop Support and Exercises NTE \$1,677,163 Period of Performance: 06/01/2008 to 05/03/2009 Accounting Info: NONE008-000-MA-20-01-00-000-02-07-0800-00-00-00-00 -GE-OE-25-44-000000 Funded: \$0.00				0.00

Accordingly, the following changes are hereby made to Task Order HSHQDC-08-J-00138:

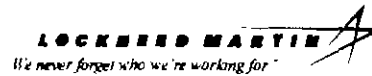
1. The Task Order HSHQDC-08-J-00138 base year period of performance is hereby extended at no cost to the Government. The base year period of performance is hereby changed from June 1, 2008 through April 10, 2009 to June 1, 2008 through May 3, 2009.
2. The Lockheed Martin proposal dated March 20, 2009 for Survey, Design, Integration, Deployment and Training of Remedy Asset Management and Change Management Modules is hereby incorporated into the task order at no additional cost to the Government. The labor costs for the installation of the Survey, Design, Integration, Deployment and Training of Remedy Asset Management and Change Management Modules shall be billed against CLIN 0001 Operations and Maintenance Support Services (HSD) with a total cost not to exceed the amount of \$224,668.00. A sixty (60) calendar day period beginning on April 11, 2009 will be allotted for the Lockheed Martin Survey, Design, Integration, Deployment and Training of Remedy Asset Management and Change Management Modules personnel to clear the DHS Entry on Duty (EOD) process.
3. In accordance with Section I.11 "Key Personnel of Facilities" of the task order, Technical Exhibit 1.700 Key Personnel Listing, effective as of April 7, 2009 is hereby incorporated into this task order. (See Attachment 1)

4. Revise **Section F.1 - TASK ORDER TERM** to read:

Base Year: The task order term is revised **from** June 1, 2008 through April 10, 2009 **to read** June 1, 2008 through May 3, 2009. If exercised, the period of performance for the option years is revised to read as follows:

- Option 1: Revised **from** April 11, 2009 through January 31, 2010
To read May 4, 2009 through January 31, 2010
- Option 2: February 1, 2010 through January 31, 2011 (No Change)
- Option 3: February 1, 2011 through January 31, 2012 (No Change)
- Option 4: February 1, 2012 through January 31, 2013 (No Change)

5. The total amount of Base Year Contract Line Item Numbers (CLINS) 0001 through 0009 remains unchanged at \$35,868,230.00.
6. The value and total amount funded/obligated to the task order remains unchanged at \$35,868,230.00
7. The ceiling for this task order remains unchanged at \$288,499,204.00.
8. All other terms and conditions remain the same.



**Key Personnel for IT-NOVA
As of: 07 April 2009**

Number	Labor Category	Originally Proposed Key Personnel	Interim Proposed Key Personnel (proposed substitutions bolded)	Proposed Key Personnel for Base Period (proposed substitutions bolded)
1	Program Manager	(b)	(4)	(4)
2	Deputy Program Manager			
3	Project Control Specialist			
4	Disaster Recovery Specialist			
5	Deployment Manager			
6	Systems Architect			
7	Systems Engineer			
8	SME Level III			
9	IT Security Specialist Level III			
10	Comm & Network Engineer Level IV			
11	Comm NW Mgr Level III			
12	COMSEC SME Level III			
13	Systems Ops Mgr Level III			
14	Systems Engineer Level III			
15	Help Desk Mgr (RC) Level III			
16	Help Desk Mgr (End User) Level III			
17	Comm Network Engineer Level IV			
18	Voice Comm Mgr Level III			
19	Comm Network Engineer (CATV) Level IV			
20	Bus Cas Analyst Level III			
21	Wireless Communications Executive Comms Manager			
22				
23	Remedy Consideration Trainer			

24	Remedy Consideration Trainer
25	Remedy Consideration Trainer
26	Remedy Consideration Sr. Systems Engineer
27	Remedy Consideration Sr. Systems Engineer
28	Remedy Consideration Systems Engineer



AMENDMENT OF SOLICITATION/MODIFICATION OF CONTRACT		1. CONTRACT ID CODE	PAGE OF PAGES 1 16
2. AMENDMENT/MODIFICATION NO. 00007	3. EFFECTIVE DATE See Block 15C	4. REQUISITION/PURCHASE REQ. NO. RUIO-09-HS059	5. PROJECT NO. (if applicable)
ISSUED BY U.S. Dept. of Homeland Security Office of Procurement Operations Information Tech. Acquisition Div. 245 Murray Lane, SW Building 410 Washington DC 20528	COO DHS/OPO/ITA	7. ADMINISTERED BY (if other than Item 6) U.S. Dept. of Homeland Security Office of Procurement Operations Information Tech. Acquisition Div. 245 Murray Lane, SW Building 410 Washington DC 20528	CODE DHS/OPO/ITA
8. NAME AND ADDRESS OF CONTRACTOR (inc. alt. nat. entity, State and ZIP Code) LOCKHEED MARTIN SERVICES INC 2339 ROUTE 70 WEST FLOOR 3W CHERRY HILL NJ 080023315		(x) 9A. AMENDMENT OF SOLICITATION NO.	9B. DATED (SEE ITEM 11)
CODE 8052583730000	FACILITY CODE	X 10A. MODIFICATION OF CONTRACT/ORDER NO. HSHQDC-06-D-00017 HSHQDC-08-J-00138	10B. DATED (SEE ITEM 13) 06/02/2008

11. THIS ITEM ONLY APPLIES TO AMENDMENTS OF SOLICITATIONS

The above numbered solicitation is amended as set forth in Item 14. The time and date specified for receipt of Offers is extended, is not extended. Offers must acknowledge receipt of this amendment prior to the hour and date specified in this solicitation or as amended, by one of the following methods: (a) By completing Items 8 and 18, and returning copies of the amendment; (b) By acknowledging receipt of this amendment on each copy of the offer submitted; or (c) By separate letter or telegram which includes a reference to the solicitation and amendment numbers. FAILURE OF YOUR ACKNOWLEDGEMENT TO BE RECEIVED AT THE PLACE DESIGNATED FOR THE RECEIPT OF OFFERS PRIOR TO THE HOUR AND DATE SPECIFIED MAY RESULT IN REJECTION OF YOUR OFFER. If by virtue of this amendment you desire to change an offer already submitted, such change may be made by telegram or letter, provided each telegram or letter makes reference to the solicitation and this amendment, and is received prior to the opening hour and date specified.

12. ACCOUNTING AND APPROPRIATION DATA (if required)
See Schedule
Net Increase: \$42,283,315.74

13. THIS ITEM ONLY APPLIES TO MODIFICATION OF CONTRACT/ORDER. IT MODIFIES THE CONTRACT/ORDER NO. AS DESCRIBED IN ITEM 14.

CHECK ONE

A. THIS CHANGE ORDER IS ISSUED PURSUANT TO: (Specify authority) THE CHANGES SET FORTH IN ITEM 14 ARE MADE IN THE CONTRACT ORDER NO. IN ITEM 10A.

B. THE ABOVE NUMBERED CONTRACT/ORDER IS MODIFIED TO REFLECT THE ADMINISTRATIVE CHANGES (such as changes in paying office, appropriation date, etc.) SET FORTH IN ITEM 14, PURSUANT TO THE AUTHORITY OF FAR 43.103(d).

C. THIS SUPPLEMENTAL AGREEMENT IS ENTERED INTO PURSUANT TO AUTHORITY OF:

D. OTHER (Specify type of modification and authority)
X FAR 52.217-9 "Option to Extend the Term of the Contract"

14. DESCRIPTION OF AMENDMENT/MODIFICATION (Organized by UCF as chain headings, including solicitation/contract subject matter where feasible)
E. IMPORTANT: Contractor is not is required to sign the document and return 1 copies to the issuing office.

DUNS Number: 805258373+0010

The purpose of this modification is to exercise Option Year 1 of Task Order HSHQDC-08-J-00138; increase the task order value and amount of obligated funding; delete Section B - Contract Line Item Numbers (CLINS) 0010 through 0025; add re-numbered CLINS to Section B; delete Section C - Statement of Work dated November 26, 2008; incorporate Section C - Statement of Work dated April 15, 2009; and revise Section G.6 - Invoice Requirements.

Lockheed Martin proposal entitled, "IT-NOVA Price Proposal for Option Year 1" dated April 20, 2009 is incorporated into this task order. Accordingly, the following actions are executed through this Modification 00007:
Continued ...

Except as provided herein, all terms and conditions of the document referred to in Item 9A or 9A, as heretofore changed, remains unchanged and in full force and effect.

15A. NAME AND TITLE OF SIGNER (Type or print) Zanetta Williams, Contract Manager	16A. NAME AND TITLE OF CONTRACTING OFFICER (Type or print) Rebecca A. Taylor
15B. CONTRACTOR OFFICIAL SIGNATURE 	16B. UNITED STATES OF AMERICA
15C. DATE SIGNED 4/30/09	16C. DATE SIGNED MAY - 1 2009

NAME OF OFFEROR OR CONTRACTOR
LOCKHEED MARTIN SERVICES INC

ITEM NO (A)	SUPPLIES/SERVICES (B)	QUANTITY (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)
	<p>1. Option Year 1 for the period of May 4, 2009 through January 31, 2010 is hereby exercised. This is done in accordance with FAR 52.217-9 "Option to Extend the Term of the Contract" (March 2000).</p> <p>2. The task order value and amount of funding obligated is hereby increased from \$35,868,230.00 by \$42,283,315.74 to \$78,151,545.74. The Contractor shall not exceed the total obligated funding amount of \$78,151,545.74.</p> <p>3. The ceiling for this task order remains unchanged at \$288,499,204.00.</p> <p>4. Section B - Supplies/Services is revised to delete Contract Line Item Numbers (CLINS) 0010 through 0025 in their entirety. Newly renumbered CLINS 1001 through 1004; 2001 through 2004; 3001 through 3004; and 4001 through 4004 are hereby added to correctly identify CLIN option year numbering.</p> <p>5. Section C - Statement of Work dated November 26, 2008 is hereby deleted in its entirety.</p> <p>6. Section C - Statement of Work dated April 15, 2009 is hereby incorporated into the task order and includes new Section C.9 E Performance Metrics Definition Document.</p> <p>7. Section G.6 - Invoice Requirements is revised to add new subparagraph Section G.6.6 - Billing/Invoice Instructions. (see page 14 of this Modification P00007)</p> <p>8. All other terms and conditions remain unchanged. Discount Terms: Net 30 FOB: Destination Period of Performance: 06/01/2008 to 01/31/2013 Change Item 0010 to read as follows (amount shown is the obligated amount):</p>				
0010	<p>DELETE CLIN - This CLIN has been renumbered. (See CLIN 1001) Option Year 1 Continued ...</p>				0.00

CONTINUATION SHEET

REFERENCE NO OF DOCUMENT BEING CONTINUED
 HSHQDC-06-D-00017/HSHQDC-08-J-00138/P00007

PAGE OF
 3 16

NAME OF OFFEROR OR CONTRACTOR
 LOCKHEED MARTIN SERVICES INC

ITEM NO (A)	SUPPLIES/SERVICES (B)	QUANTITY (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)
	Operations and Maintenance Support Services HSD. Amount: \$0.00 (Option Line Item) Product/Service Code: D399 Product/Service Description: OTHER ADP & TELECOMMUNICATIONS SERVICES Change Item 0011 to read as follows (amount shown is the obligated amount):				
0011	DELETE CLIN - This CLIN has been renumbered. (See CLIN 1002) Option Year 1 Operations and Maintenance Support Services ODCs HSD. NTE \$6,000,000.00 Amount: \$0.00 (Option Line Item) Product/Service Code: D399 Product/Service Description: OTHER ADP & TELECOMMUNICATIONS SERVICES Change Item 0012 to read as follows (amount shown is the obligated amount):				0.00
0012	DELETE CLIN - This CLIN has been renumbered. (See CLIN 1003) Option Year 1 Wireless Management Office ESD Amount: \$0.00 (Option Line Item) Product/Service Code: D399 Product/Service Description: OTHER ADP & TELECOMMUNICATIONS SERVICES Change Item 0013 to read as follows (amount shown is the obligated amount):				0.00
0013	DELETE CLIN - This CLIN has been renumbered. (See CLIN 1004) Option Year 1 Wireless Management Office ODCs ESD Amount: \$0.00 (Option Line Item) Product/Service Code: D399 Product/Service Description: OTHER ADP & TELECOMMUNICATIONS SERVICES Change Item 0014 to read as follows (amount shown is the obligated amount): Continued ...				0.00

CONTINUATION SHEET

REFERENCE NO OF DOCUMENT BEING CONTINUED
 HSHQDC-06-D-00017/HSHQDC-08-J-00138/P00007

PAGE OF
 4 16

NAME OF OFFEROR OR CONTRACTOR
 LOCKHEED MARTIN SERVICES INC

ITEM NO (A)	SUPPLIES/SERVICES (B)	QUANTITY (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)
0014	<p>DELETE CLIN -This CLIN has been renumbered. (See CLIN 2001) Option Year 2 Operations and Maintenance Support Services (HSD) Amount: \$0.00 (Option Line Item)</p> <p>Accounting Info: RWC8049 RWC WF-99-01-00-000-02-05-0000-00-00-00-00 GE OE 25 84 FY2008 Funded: \$0.00</p> <p>Accounting Info: SCAC008-000-IX-22-11-02-000-02-05-0000-00-00-00-00 -GE-OE-25-41-EM0122 Funded: \$0.00</p> <p>Accounting Info: SCAC008-000-IX-22-11-02-000-02-05-0000-00-00-00-00 -GE-OE-25-44-S00024 Funded: \$0.00</p> <p>Accounting Info: RWC8049 RWC WF-99-01-00-000-02-05-0000-00-00-00-00 GE OE 25 44 FY2008 Funded: \$0.00</p> <p>Accounting Info: RWC8049 RWC WF-99-01-00-000-02-05-0000-00-00-00-00 GE OE 31 18 FY2008 Funded: \$0.00</p> <p>Accounting Info: RWC8049 RWC WF-99-01-00-000-02-05-0000-00-00-00-00 GE OE 25 76 FY2008 Funded: \$0.00</p> <p>Accounting Info: RWC8049 RWC WF-99-01-00-000-02-05-0000-00-00-00-00 GE OE 25 74 FY2008 Funded: \$0.00</p> <p>Change Item 0015 to read as follows (amount shown is the obligated amount):</p>				0.00
0015	<p>DELETE CLIN - This CLIN has been renumbered. (See CLIN 2002) Option Year 2 Operations and Maintenance Support Services ODCs HSD Amount: \$0.00 (Option Line Item) Continued ...</p>				0.00

CONTINUATION SHEET

REFERENCE NO OF DOCUMENT BEING CONTINUED
 HSHQDC-06-D-00017/HSHQDC-08-J-00138/P00007

PAGE OF
 5 16

NAME OF OFFEROR OR CONTRACTOR
 LOCKHEED MARTIN SERVICES INC

ITEM NO (A)	SUPPLIES/SERVICES (B)	QUANTITY (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)
	Product/Service Code: D399 Product/Service Description: OTHER ADP & TELECOMMUNICATIONS SERVICES Change Item 0016 to read as follows (amount shown is the obligated amount):				
0016	DELETE CLIN - This CLIN has been renumbered. (See CLIN 2003) Option Year 2 Wireless Management Office ESD Amount: \$0.00 (Option Line Item)				0.00
	Product/Service Code: D399 Product/Service Description: OTHER ADP & TELECOMMUNICATIONS SERVICES Change Item 0017 to read as follows (amount shown is the obligated amount):				
0017	DELETE CLIN - This CLIN has been renumbered. (See CLIN 2004) Option Year 2 Wireless Management Office ODCs ESD Amount: \$0.00 (Option Line Item)				0.00
	Product/Service Code: D399 Product/Service Description: OTHER ADP & TELECOMMUNICATIONS SERVICES Change Item 0018 to read as follows (amount shown is the obligated amount):				
0018	DELETE CLIN - This CLIN has been renumbered. (See CLIN 3001) Option Year 3 Operations and Maintenance Support Services HSD Amount: \$0.00 (Option Line Item)				0.00
	Product/Service Code: D399 Product/Service Description: OTHER ADP & TELECOMMUNICATIONS SERVICES Change Item 0019 to read as follows (amount shown is the obligated amount):				
0019	DELETE CLIN - This CLIN has been renumbered. (See CLIN 3002) Option Year 3 Operations and Maintenance Support Services ODCs Continued ...				0.00

CONTINUATION SHEET

REFERENCE NO. OF DOCUMENT BEING CONTINUED
 HSHQDC-06-D-00017/HSHQDC-08-J-00138/P00007

PAGE OF
 6 16

NAME OF OFFEROR OR CONTRACTOR
 LOCKHEED MARTIN SERVICES INC

ITEM NO (A)	SUPPLIES/SERVICES (B)	QUANTITY (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)
	HSD Amount: \$0.00 (Option Line Item) Product/Service Code: D399 Product/Service Description: OTHER ADP & TELECOMMUNICATIONS SERVICES Change Item 0020 to read as follows (amount shown is the obligated amount):				
0020	DELETE CLIN - This CLIN has been renumbered. (See CLIN 3003) Option Year 3 Wireless Management Office ESD Amount: \$0.00 (Option Line Item) Product/Service Code: D399 Product/Service Description: OTHER ADP & TELECOMMUNICATIONS SERVICES Change Item 0021 to read as follows (amount shown is the obligated amount):				0.00
0021	DELETE CLIN - This CLIN has been renumbered. (See CLIN 3004) Option Year 3 Wireless Management Office ODCs ESD Amount: \$0.00 (Option Line Item) Product/Service Code: D399 Product/Service Description: OTHER ADP & TELECOMMUNICATIONS SERVICES Change Item 0022 to read as follows (amount shown is the obligated amount):				0.00
0022	DELETE CLIN - This CLIN has been renumbered. (See CLIN 4001) Option Year 4 Operations and Maintenance Support Services HSD Amount: \$0.00 (Option Line Item) Product/Service Code: D399 Product/Service Description: OTHER ADP & TELECOMMUNICATIONS SERVICES Change Item 0023 to read as follows (amount shown is the obligated amount):				0.00
0023	DELETE CLIN - This CLIN has been renumbered. (See CLIN 4002) Continued ...				0.00

CONTINUATION SHEET

REFERENCE NO OF DOCUMENT BEING CONTINUED
 HSHQDC-06-D-00017/HSHQDC-08-J-00138/P00007

PAGE OF
 7 16

NAME OF OFFEROR OR CONTRACTOR
 LOCKHEED MARTIN SERVICES INC

ITEM NO (A)	SUPPLIES/SERVICES (B)	QUANTITY (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)
	Option Year 4 Operations and Maintenance Support Services ODCs HSD Amount: \$0.00 (Option Line Item) Product/Service Code: D399 Product/Service Description: OTHER ADP & TELECOMMUNICATIONS SERVICES Change Item 0024 to read as follows (amount shown is the obligated amount):				
0024	DELETE CLIN - This CLIN has been renumbered. (See CLIN 4003) Option Year 4 Wireless Management Office ESD Amount: \$0.00 (Option Line Item) Product/Service Code: D399 Product/Service Description: OTHER ADP & TELECOMMUNICATIONS SERVICES Change Item 0025 to read as follows (amount shown is the obligated amount):				0.00
0025	DELETE CLIN - This CLIN has been renumbered. (See CLIN 4004) Option Year 4 Wireless Management Office ODCs ESD Amount: \$0.00 (Option Line Item) Product/Service Code: D399 Product/Service Description: OTHER ADP & TELECOMMUNICATIONS SERVICES Add Item 1001 as follows:				0.00
1001	Option Year 1 Operation and Maintenance Support Service HSD: PWS Sections: C.1,3,4 and C.5.1 through C.5.13 and C.5.15 NTE \$36,879,910.88 Period of Performance: 05/04/2009 through 01/31/2010 Product/Service Code: D399 Product/Service Description: OTHER ADP & TELECOMMUNICATIONS SERVICES Accounting Info: RWC9049 RWC WF-99-01-00-000-02-05-0400-05-00-00-00 GE OE 25 Continued ...				36,879,910.88

CONTINUATION SHEET

REFERENCE NO. OF DOCUMENT BEING CONTINUED
 HSHQDC-06-D-00017/HSHQDC-08-J-00138/P00007

PAGE OF
 8 16

NAME OF OFFEROR OR CONTRACTOR
 LOCKHEED MARTIN SERVICES INC

ITEM NO (A)	SUPPLIES/SERVICES (B)	QUANTITY (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)
	76 FY2009 Funded: \$3,042,780.43 Accounting Info: RWC9049 RWC WF-99-01-00-000-02-05-0400-05-00-00-00 GE OE 31 18 FY2009 Funded: \$9,360,245.10 Accounting Info: RWC9049 RWC WF-99-01-00-000-02-05-0400-05-00-00-00 GE OE 25 84 FY2009 Funded: \$14,533,729.08 Accounting Info: RWC9049 RWC WF-99-01-00-000-02-05-0400-05-00-00-00 GE OE 25 44 FY2009 Funded: \$8,752,699.29 Accounting Info: RWC9049 RWC WF-99-01-00-000-02-05-0400-05-00-00-00 GE OE 25 74 FY2009 Funded: \$549,861.84 Accounting Info: BCEP-NONE009-000-MA-20-01-00-000-02-07-0800-00-00-00-00-000000 Funded: \$640,595.14 Add Item 1002 as follows:				
1002	Option Year 1 Operation and Maintenance Support Service HSD ODCs (Travel and Direct Materials associated directly with the performance under this task order.): PWS Sections: C.5.1 through C.5.13 and C.5.15 NTE \$2,303,404.86 Period of Performance: 05/04/2009 through 01/31/2010 Product/Service Code: D399 Product/Service Description: OTHER ADP & TELECOMMUNICATIONS SERVICES Accounting Info: RWC9049 RWC WF-99-01-00-000-02-05-0400-05-00-00-00 GE OE 25 41 FY2009 Funded: \$1,500,000.00 Accounting Info: BCEP-NONE009-000-MA-20-01-00-000-02-07-0800-00-00-00-00-000000 Continued ...				2,303,404.86

CONTINUATION SHEET

REFERENCE NO OF DOCUMENT BEING CONTINUED
 HSHQDC-06-D-00017/HSHQDC-08-J-00138/P00007

PAGE OF
 9 16

NAME OF OFFEROR OR CONTRACTOR
 LOCKHEED MARTIN SERVICES INC

ITEM NO (A)	SUPPLIES/SERVICES (B)	QUANTITY (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)
	Funded: \$803,404.86				
1003	Add Item 1003 as follows: Option Year 1 Wireless Management Office ESD: PWS Section: C.5.14 NTE \$2,948,574.72 Period of Performance: 05/04/2009 through 01/31/2010 Product/Service Code: D399 Product/Service Description: OTHER ADP & TELECOMMUNICATIONS SERVICES Accounting Info: SCAC009-000-IX-22-11-02-000-02-05-0400-04-00-00-00-00 -GE-OE-25-76-FY2009 Funded: \$2,565,276.00 Accounting Info: WLP00X-000-IX-22-12-00-000-02-05-0400-04-00-00-00-00 -GE-OE-25-76-FY2009 Funded: \$383,298.72 Add Item 1004 as follows:				2,948,574.72
1004	Option Year 1 Wireless Management Office ESD ODCs (Travel and Direct Materials associated directly with the performance under this task order.): PWS Section: C.5.14 NTE \$151,425.28 Period of Performance: 05/04/2009 through 01/31/2010 Product/Service Code: D399 Product/Service Description: OTHER ADP & TELECOMMUNICATIONS SERVICES Accounting Info: SCAC009-000-IX-22-11-02-000-02-05-0400-04-00-00-00-00 -GE-OE-25-76-FY2009 Funded: \$90,000.00 Accounting Info: WLP00X-000-IX-22-12-00-000-02-05-0400-04-00-00-00-00 -GE-OE-25-76-FY2009 Funded: \$61,425.28 Add Item 2001 as follows:				151,425.28
2001	Option Year 2 Operation and Maintenance Support Service HSD: Continued ...				0.00

CONTINUATION SHEET

REFERENCE NO. OF DOCUMENT BEING CONTINUED
 HSHQDC-06-D-00017/HSHQDC-06-J-00138/P00007

PAGE OF
 10 16

NAME OF OFFEROR OR CONTRACTOR
 LOCKHEED MARTIN SERVICES INC

ITEM NO (A)	SUPPLIES/SERVICES (B)	QUANTITY (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)
	PWS Sections: C.1,3,4 and C.5.1 through C.5.13 and C.5.15 NTE \$51,371,156.00 Period of Performance: 02/01/2010 through 01/31/2011 Amount: \$51,371,156.00 (Option Line Item) Accounting Info: RWC8049 RWC WF-99-01-00-000-02-05-0000-00-00-00-00 GE OE 25 84 FY2008 Funded: \$0.00 Accounting Info: SCAC008-000-IX-22-11-02-000-02-05-0000-00-00-00-00 -GE-OE-25-41-EM0122 Funded: \$0.00 Accounting Info: SCAC008-000-IX-22-11-02-000-02-05-0000-00-00-00-00 -GE-OE-25-44-SO0024 Funded: \$0.00 Accounting Info: RWC8049 RWC WF-99-01-00-000-02-05-0000-00-00-00-00 GE OE 25 44 FY2008 Funded: \$0.00 Accounting Info: RWC8049 RWC WF-99-01-00-000-02-05-0000-00-00-00-00 GE OE 31 18 FY2008 Funded: \$0.00 Accounting Info: RWC8049 RWC WF-99-01-00-000-02-05-0000-00-00-00-00 GE OE 25 76 FY2008 Funded: \$0.00 Accounting Info: RWC8049 RWC WF-99-01-00-000-02-05-0000-00-00-00-00 GE OE 25 74 FY2008 Funded: \$0.00 Add Item 2002 as follows: 2002 Option Year 2 Operation and Maintenance Support Service HSD ODCs (Travel and Direct Materials associated directly with the performance under this task order.): PWS Sections: C.5.1 through C.5.13 and C.5.15.....NTE \$6,000,000.00 Continued ...				0.00

CONTINUATION SHEET

REFERENCE NO OF DOCUMENT BEING CONTINUED
 HSHQDC-06-D-00017/HSHQDC-08-J-00138/P00007

PAGE OF
 11 16

NAME OF OFFEROR OR CONTRACTOR
 LOCKHEED MARTIN SERVICES INC

ITEM NO (A)	SUPPLIES/SERVICES (B)	QUANTITY (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)
	Period of Performance: 02/01/2010 through 01/31/2011 Amount: \$6,000,000.00 (Option Line Item) Product/Service Code: D399 Product/Service Description: OTHER ADP & TELECOMMUNICATIONS SERVICES Add Item 2003 as follows:				
2003	Option Year 2 Wireless Management Office ESD: PWS Section: C.5.14 NTE \$4,115,942.00 Period of Performance: 02/01/2010 through 01/31/2011 Amount: \$4,115,942.00 (Option Line Item) Product/Service Code: D399 Product/Service Description: OTHER ADP & TELECOMMUNICATIONS SERVICES Add Item 2004 as follows:				0.00
2004	Option Year 2 Wireless Management Office ESD ODCs (Travel and Direct Materials associated directly with the performance under this task order.): PWS Section: C.5.14.....NTE \$120,000.00 Period of Performance: 02/01/2010 through 01/31/2011 Amount: \$120,000.00 (Option Line Item) Product/Service Code: D399 Product/Service Description: OTHER ADP & TELECOMMUNICATIONS SERVICES Add Item 3001 as follows:				0.00
3001	Option Year 3 Operation and Maintenance Support Service HSD: PWS Sections: C.1,3,4 and C.5.1 through C.5.13 and C.5.15 NTE \$52,442,323.00 Period of Performance: 02/01/2011 through 01/31/2012 Amount: \$52,442,323.00 (Option Line Item) Product/Service Code: D399 Product/Service Description: OTHER ADP & TELECOMMUNICATIONS SERVICES Add Item 3002 as follows: Continued ...				0.00

CONTINUATION SHEET

REFERENCE NO OF DOCUMENT BEING CONTINUED
 HSHQDC-06-D-00017/HSHQDC-08-J-00138/P00007

PAGE OF
 12 16

NAME OF OFFEROR OR CONTRACTOR
 LOCKHEED MARTIN SERVICES INC

ITEM NO (A)	SUPPLIES/SERVICES (B)	QUANTITY (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)
3002	Option Year 3 Operation and Maintenance Support Service HSD ODCs (Travel and Direct Materials associated directly with the performance under this task order.): PWS Sections: C.5.1 through C.5.13 and C.5.15.....NTE \$6,000,000.00 Period of Performance: 02/01/2011 through 01/31/2012 Amount: \$6,000,000.00 (Option Line Item) Product/Service Code: D399 Product/Service Description: OTHER ADP & TELECOMMUNICATIONS SERVICES Add Item 3003 as follows:				0.00
3003	Option Year 3 Wireless Management Office ESD: PWS Section: C.5.14 NTE \$4,238,554.00 Period of Performance: 02/01/2011 through 01/31/2012 Amount: \$4,238,554.00 (Option Line Item) Product/Service Code: D399 Product/Service Description: OTHER ADP & TELECOMMUNICATIONS SERVICES Add Item 3004 as follows:				0.00
3004	Option Year 3 Wireless Management Office ESD ODCs (Travel and Direct Materials associated directly with the performance under this task order.): PWS Section: C.5.14 NTE \$120,000.00 Period of Performance: 02/01/2011 through 01/31/2012 Amount: \$120,000.00 (Option Line Item) Product/Service Code: D399 Product/Service Description: OTHER ADP & TELECOMMUNICATIONS SERVICES Add Item 4001 as follows:				0.00
4001	Option Year 4 Operation and Maintenance Support Service HSD: PWS Sections: C.1,3,4 and C.5.1 through C.5.13 and C.5.15 NTE \$53,075,751.00 Period of Performance: 02/01/2012 through Continued ...				0.00

CONTINUATION SHEET

REFERENCE NO OF DOCUMENT BEING CONTINUED
 HSHQDC-06-D-00017/HSHQDC-08-J-00138/P00007

PAGE OF
 13 16

NAME OF OFFEROR OR CONTRACTOR
 LOCKHEED MARTIN SERVICES INC

ITEM NO (A)	SUPPLIES/SERVICES (B)	QUANTITY (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)
	01/31/2013 Amount: \$53,075,751.00 (Option Line Item) Product/Service Code: D399 Product/Service Description: OTHER ADP & TELECOMMUNICATIONS SERVICES Add Item 4002 as follows:				
4002	Option Year 4 Operation and Maintenance Support Service HSD ODCs (Travel and Direct Materials associated directly with the performance under this task order.): PWS Sections: C.5.1 through C.5.13 and C.5.15 NTE \$6,000,000.00 Period of Performance: 02/01/2012 through 01/31/2013 Amount: \$6,000,000.00 (Option Line Item) Product/Service Code: D399 Product/Service Description: OTHER ADP & TELECOMMUNICATIONS SERVICES Add Item 4003 as follows:				0.00
4003	Option Year 4 Wireless Management Office ESD: PWS Section: C.5.14 NTE \$4,366,310.00 Period of Performance: 02/01/2012 through 01/31/2013 Amount: \$4,366,310.00 (Option Line Item) Product/Service Code: D399 Product/Service Description: OTHER ADP & TELECOMMUNICATIONS SERVICES Add Item 4004 as follows:				0.00
4004	Option Year 4 Wireless Management Office ESD ODCs (Travel and Direct Materials associated directly with the performance under this task order.): PWS Section: C.5.14 NTE \$120,000.00 Period of Performance: 02/01/2012 through 01/31/2013 Amount: \$120,000.00 (Option Line Item) Product/Service Code: D399 Product/Service Description: OTHER ADP & TELECOMMUNICATIONS SERVICES				0.00

9. Revise Section G.6 – Invoice Requirements by the addition of new subparagraph G.6.6 – Billing/Invoice Instructions, which reads as follows:

G. 6.6 Billing/Invoice Instructions

- A. Billing shall occur at the CLIN level.
1. Billing shall be a representation of the total labor hours and total amount per CLIN (for CLINS with associated labor categories);
 2. The Contractor is allowed to mix approved labor categories, in accordance with the most recent COTR approved staffing plan, as necessary to provide services required under this task order.

B. Invoices shall include two forms per invoice.

Form #1: The cover page shall be the SF1034, Public Voucher for Purchases and Services Other Than Personal

- a. The SF 1034 shall only reference one invoicing period.
- b. The SF 1034 shall include only one invoice number.
- c. The SF 1034 shall only reference CLIN numbers and respective totals for each CLIN
- d. For services supplied, the total amount billed shall include all IT-NOVA Costs incurred per CLIN per the invoicing period and all previous month’s subcontractor costs.

C. **Form #2:** The second page shall be a cost element summary that includes cost details submitted to the Government (separately) within cost detail binders titled "IT-NOVA (insert month) Costs Binder". The cost detail binders shall only be submitted to the task order COTR and CO via hand delivery.

CLIN #	\$ COMMITTED	\$ AWARDED	\$ EXPENDED	\$ UNOBLIGATED	% REMAINING
1001					
1002					
1003					
1004					
TOTAL					

Standard Form 1034 Revised October 1987 Department of the Treasury TFM 4-2000 1034-122		Form #1 PUBLIC VOUCHER FOR PURCHASES AND SERVICES OTHER THAN PERSONAL			VOUCHER NO	
U.S. DEPARTMENT, BUREAU, OR ESTABLISHMENT AND LOCATION		DATE VOUCHER PREPARED		SCHEDULE NO.		
		CONTRACT NUMBER AND DATE		PAID BY		
		REQUISITION NUMBER AND DATE				
PAYEE'S NAME AND ADDRESS		DATE INVOICE RECEIVED		DISCOUNT TERMS		
		PAYEE'S ACCOUNT NUMBER		GOVERNMENT B/L NUMBER		
		SHIPPED FROM		TO		WEIGHT
NUMBER AND DATE OF ORDER	DATE OF DELIVERY OR SERVICE	ARTICLES OR SERVICES <small>(Enter description, item number of contract or Federal supply schedule, and other information deemed necessary)</small>	QUAN-TITY	UNIT PRICE		AMOUNT
				COST	PER	
	(Billing Period)	For Services Supplied. Total amount billed includes all IT-NOVA (Insert Month) costs incurred and all (Insert Month) supporting cost details have been submitted to the Government (separately) as the "IT-NOVA (Insert Month) Costs Binders". Please see attached (Insert Month) Cost Element Summary.				(Overall Total From Cost Element Summary sheet)
<small>(Use continuation sheets if necessary)</small>		<small>(Payee must NOT use the space below)</small>			TOTAL	
PAYMENT:		APPROVED FOR	EXCHANGE RATE	DIFFERENCES		
<input type="checkbox"/> PROVISIONAL		= \$	= \$1 00			
<input type="checkbox"/> COMPLETE		BY ²				
<input type="checkbox"/> PARTIAL						
<input type="checkbox"/> FINAL				Amount verified, correct for		
<input type="checkbox"/> PROGRESS		TITLE		(Signature or initials)		
<input type="checkbox"/> ADVANCE						
Pursuant to authority vested in me, I certify that this voucher is correct and proper for payment.						
_____ <small>(Date)</small>		_____ <small>(Authorized Certifying Officer)²</small>			_____ <small>(Title)</small>	
ACCOUNTING CLASSIFICATION						
CHECK NUMBER		ON ACCOUNT OF U.S. TREASURY		CHECK NUMBER		ON (Name of bank)
CASH		DATE		PAYEE ³		
\$						
¹ When stated in foreign currency, insert name of currency. ² If the ability to certify and authority to approve are combined in one person, one signature only is necessary, otherwise the approving officer will sign in the space provided, over his official title. ³ When a voucher is recorded in the name of a company or corporation, the name of the person writing the company or corporate name, as well as the capacity in which he signs, must appear. For example: "John Doe Company, per John Smith, Secretary" or "Treasurer" as the case may be.					PER	
					TITLE	

Previous edition usable

NSN 7650-00-634-4206

PRIVACY ACT STATEMENT

The information requested on this form is required under the provisions of 31 U.S.C. 82b and 82c, for the purpose of disbursing Federal money. The information requested is to identify the particular creditor and the amounts to be paid. Failure to furnish this information will hinder discharge of the payment obligation.

Form #2
Sample Cost Element

VOUCHER #

(Month)
COST ELEMENT SUMMARY

Program Name:	IT NOVA
Delivery Order #:	HSHQDC-08-J-00138
Base Year PoP:	
Month:	
Task Order Number	

June Regular Voucher

Billing Period:	CLIN Title	Total Labor Hours	Total Dollar Amount
1001			
(0010)			
1002			
(0011)			
1003			
(0012)			
1004			
(0013)			
Total Amount:			

Cost Incurred in June Volume

Voucher #	Voucher Date	Amount	Page #
Total			

Overall Total	
----------------------	--

AMENDMENT OF SOLICITATION/MODIFICATION OF CONTRACT		1 CONTRACT ID CODE	PAGE OF PAGES 1 2
2 AMENDMENT/MODIFICATION NO P00008	3 EFFECTIVE DATE 07/27/2009	4 REQUISITION/PURCHASE REQ NO RUIO-09-HS130	5 PROJECT NO (if applicable)
6 ISSUED BY U.S. Dept. of Homeland Security Office of Procurement Operations Information Tech. Acquisition Div. 245 Murray Lane, SW Building 410 Washington DC 20528	CODE DHS/OPO/ITAC	7 ADMINISTERED BY (if other than item 6) U.S. Dept. of Homeland Security Office of Procurement Operations Information Tech. Acquisition Div. 245 Murray Lane, SW Building 410 Washington DC 20528	CODE DHS/OPO/ITAC
8 NAME AND ADDRESS OF CONTRACTOR (No. street, county, State and ZIP Code) LOCKHEED MARTIN SERVICES INC 2339 ROUTE 70 WEST FLOOR 3W CHERRY HILL NJ 080023315		(x) 9A AMENDMENT OF SOLICITATION NO	
		9B DATED (SEE ITEM 11)	
		X 10A MODIFICATION OF CONTRACT/ORDER NO HSHQDC-06-D-00017 HSHQDC-08-J-00138	
		10B DATED (SEE ITEM 13) 06/02/2008	
CODE 8052583730000	FACILITY CODE		

11. THIS ITEM ONLY APPLIES TO AMENDMENTS OF SOLICITATIONS

The above numbered solicitation is amended as set forth in Item 14. The hour and date specified for receipt of Offers is extended, is not extended.
Offers must acknowledge receipt of this amendment prior to the hour and date specified in the solicitation or as amended, by one of the following methods: (a) By completing items 8 and 15, and returning _____ copies of the amendment; (b) By acknowledging receipt of this amendment on each copy of the offer submitted; or (c) By separate letter or telegram which includes a reference to the solicitation and amendment numbers. FAILURE OF YOUR ACKNOWLEDGEMENT TO BE RECEIVED AT THE PLACE DESIGNATED FOR THE RECEIPT OF OFFERS PRIOR TO THE HOUR AND DATE SPECIFIED MAY RESULT IN REJECTION OF YOUR OFFER. If by virtue of this amendment you desire to change an offer already submitted, such change may be made by telegram or letter, provided each telegram or letter makes reference to the solicitation and this amendment, and is received prior to the opening hour and date specified.

12 ACCOUNTING AND APPROPRIATION DATA (if required)

See Schedule

13. THIS ITEM ONLY APPLIES TO MODIFICATION OF CONTRACTS/ORDERS. IT MODIFIES THE CONTRACT/ORDER NO. AS DESCRIBED IN ITEM 14.

CHECK ONE	A THIS CHANGE ORDER IS ISSUED PURSUANT TO: (Specify authority) THE CHANGES SET FORTH IN ITEM 14 ARE MADE IN THE CONTRACT ORDER NO. IN ITEM 10A.
X	B THE ABOVE NUMBERED CONTRACT/ORDER IS MODIFIED TO REFLECT THE ADMINISTRATIVE CHANGES (such as changes in paying office, appropriation date, etc.) SET FORTH IN ITEM 14, PURSUANT TO THE AUTHORITY OF FAR 43.103(b).
	C THIS SUPPLEMENTAL AGREEMENT IS ENTERED INTO PURSUANT TO AUTHORITY OF:
	D OTHER (Specify type of modification and authority)

E. IMPORTANT: Contractor is not, is required to sign this document and return _____ copies to the issuing office.

14 DESCRIPTION OF AMENDMENT/MODIFICATION (Organized by UCF section headings, including solicitation/contract subject matter where feasible.)

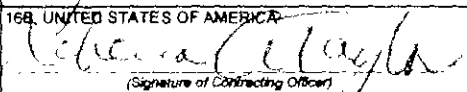
DUNS Number: 805258373+0000

The purpose of this administrative modification is to (1) name a new Contracting Officer's Technical Representative (COTR) and Task Manager; (2) state a new billing address; (3) add updated Contract Security Classification Specification DD Form 254s; and (4) add revised Key Personnel Listing to Task Order HSHQDC-08-J-00138.

See Page 2 for modification details.

Period of Performance: 06/01/2008 to 01/31/2013

Except as provided herein, all terms and conditions of the document referenced in Item 9A or 10A, as heretofore changed, remains unchanged and in full force and effect.

15A NAME AND TITLE OF SIGNER (Type or print)		16A NAME AND TITLE OF CONTRACTING OFFICER (Type or print) Rebecca A. Taylor	
15B CONTRACTOR/OFFEROR (Signature of person authorized to sign)	15C DATE SIGNED	16B UNITED STATES OF AMERICA  (Signature of Contracting Officer)	16C DATE SIGNED JUL 27 2009

540-01-152-9070

Previous edition unusable

STANDARD FORM 30 (REV 10-83)
Prescribed by GSA
FAR (48 CFR) 53.243

SF-30 CONTINUATION SHEET

1. Revise **Section G.3.2 - COTR Designation** to remove Lattia Baker and designate Gerald R. Warren as the Task Order COTR. Mr. Warren may be contacted as follows:

Name: Gerald R. (Rob) Warren
Phone: 202-447-0644
Email: Gerald.Warren@dhs.gov

2. Gregory Capella is hereby designated Task Manager for oversight on **Section C.5.1 - Applications Management, Support, and Development** portion of the task order. Mr Capella may be contacted as follows:

Name: Gregory Capella
Phone: 202-447-0644
Email: Gregory.Capella@dhs.gov

3. Revise **Section G.7 – Electronic Invoice Submission** as follows:

Change From: Electronic invoices must be submitted to: www.DOB-Invoices@DHS.GOV within thirty (30) days of services rendered.


Change to Read: Electronic invoices must be submitted to: OFO-Invoice@DHS.GOV within thirty (30) days of services rendered.

4. In accordance with **Section I.11 - Key Personnel or Facilities**, revised key personnel listing is hereby incorporate into this task order, titled, "Key Personnel for IT-NOVA as of 24 June 2009". (see Attachment 1)
5. Add fourteen (14) DoD Contract Security Classification Specifications (DD Forms 254) to the task order that were revised by the DHS Office of Security. (see Attachment 2)
6. The value and total amount funded/obligated to the task order remains unchanged at \$78,151,545.74.
7. The ceiling for this task order remains unchanged at \$288,499,204.00.
8. All other terms and conditions remain unchanged.

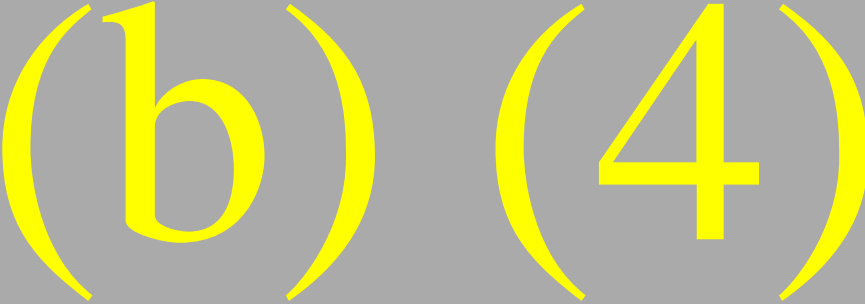


Key Personnel for IT-NOVA
 As of: 24 June 2009

Number	Labor Category	Originally Proposed Key Personnel	Interim Proposed Key Personnel (proposed substitutions bolded)	Proposed Key Personnel for Base Period (proposed substitutions bolded)
1	Program Manager	(b)	(4)	(4)
2	Deputy Program Manager			
3	Project Control Specialist			
4	Disaster Recovery Specialist			
5	Deployment Manager			
6	Systems Architect			
7	Systems Engineer			
8	SME Level III			
9	IT Security Specialist Level III			
10	Comm & Network Engineer Level IV			
11	Comm NW Mgr Level III			
12	COMSEC SME Level III			
13	Systems Ops Mgr Level III			
14	Systems Engineer Level III			
15	Help Desk Mgr (RC) Level III			
16	Help Desk Mgr (End User) Level III			
17	Comm Network Engineer Level IV			
18	Voice Comm Mgr Level III			
19	Comm Network Engineer (CATV) Level IV			
20	Bus Cas Analyst Level III			
21	Wireless Communications			
22	Executive Comms Manager			
23	Remedy Consideration Trainer			

24	Remedy Consideration Trainer	
25	Remedy Consideration Trainer	
26	Remedy Consideration Sr. Systems Engineer	
27	Remedy Consideration Sr. Systems Engineer	
28	Remedy Consideration Systems Engineer	
29	Remedy Consideration Systems Engineer	
30	Remedy Consideration Systems Engineer	
31	Remedy Consideration Systems Engineer	

ATTACHMENT 2 – 56 pages
Updated Contract Security Classification Specifications (DD FORM 254s)

Page	Subcontractor Name
	

DEPARTMENT OF DEFENSE CONTRACT SECURITY CLASSIFICATION SPECIFICATION		1. CLEARANCE AND SAFEGUARDING	
The requirements of the DoD Industrial Security Manual apply to all aspects of this effort)		a. FACILITY CLEARANCE REQUIRED SECRET	
		b. LEVEL OF SAFEGUARDING REQUIRED N/A	
2. THIS SPECIFICATION IS FOR: (X and complete as applicable)		3. THIS SPECIFICATION IS: (X and complete as applicable)	
1. PRIME CONTRACT NUMBER HSHQDC-06-D-00017 HQHSDC-08-J-00138		<input type="checkbox"/> a. ORIGINAL (Complete Date in all cases)	Date (YYMMDD) 20071210
2. SUBCONTRACT NUMBER 6012244		<input checked="" type="checkbox"/> b. REVISED (Supersedes all previous specs)	Revision No 2 Date (YYMMDD) 20090113
3. INFORMATION OR OTHER NUMBER		<input type="checkbox"/> c. FINAL (Complete Item 5 in all cases)	Date (YYMMDD)
4. IS THIS A FOLLOW-ON CONTRACT? <input checked="" type="checkbox"/> YES <input type="checkbox"/> NO. If Yes complete the following			
a. Classified material received or generated under HSHQDC-06-D-00017 HQHSDC-07-J-00739 (Preceding Contract Number) is transferred to this follow-on contract			
5. IS THIS A FINAL DD FORM 254? <input type="checkbox"/> YES <input checked="" type="checkbox"/> NO. If Yes complete the following			
a. Release to the contractor's request dated _____ retention of the identified classified material is authorized for the period of _____			
6. CONTRACTOR (Include Commercial and Government Entity (CAGE) Code)			
a. NAME, ADDRESS, AND ZIP CODE LOCKHEED MARTIN SERVICES, INC 3333 ROUTE 70 WEST CHERRY HILL NJ 08002-1315		b. CAGE CODE 77609	c. COGNIZANT SECURITY OFFICE (Name, Address, and Zip Code) DEFENSE SECURITY SERVICE 307 FELLOWSHIP ROAD STE 115 MT LAUREL, NJ 08054-1233
7. SUBCONTRACTOR			
(b) (4)		b. CAGE CODE 3Y798	c. COGNIZANT SECURITY OFFICES (Name, Address, and Zip Code) DEFENSE SECURITY SERVICE 127 DODD BLVD. LANGLEY AFB, VA 23665-1906
8. ACTUAL PERFORMANCE			
a. Description Department of Homeland Security (DHS) various assignments within the Washington, DC metropolitan area		b. CAGE CODE	c. COGNIZANT SECURITY OFFICE (Name, Address, and Zip Code)
9. GENERAL IDENTIFICATION OF THIS PROCUREMENT			
10. Provide IT Operations & Maintenance technical support to Lockheed Martin in support of the IT-NOVA DHS Eagle Task Order. This is in response to Lockheed Martin's requirements to provide support to IT Operations Maintenance and O&M for the DHS Headquarters and Components directly supported by the DHS OCIO.			
10. THIS CONTRACT WILL REQUIRE ACCESS TO:		11. IN PERFORMING THIS CONTRACT, THE CONTRACTOR WILL:	
COMSEC INFORMATION	YES <input checked="" type="checkbox"/> NO <input type="checkbox"/>	a. HAVE ACCESS TO CLASSIFIED INFORMATION ONLY AT ANOTHER CONTRACTOR'S FACILITY OR A GOVERNMENT ACTIVITY	YES <input checked="" type="checkbox"/> NO <input type="checkbox"/>
RESTRICTED DATA	YES <input type="checkbox"/> NO <input checked="" type="checkbox"/>	b. RECEIVE CLASSIFIED DOCUMENTS ONLY	YES <input type="checkbox"/> NO <input checked="" type="checkbox"/>
TECHNICAL SKETCH/WEAPON DESIGN INFORMATION	YES <input type="checkbox"/> NO <input checked="" type="checkbox"/>	c. RECEIVE AND GENERATE CLASSIFIED MATERIAL	YES <input type="checkbox"/> NO <input checked="" type="checkbox"/>
UNCLASSIFIED RESTRICTED DATA	YES <input type="checkbox"/> NO <input checked="" type="checkbox"/>	d. FABRICATE, MODIFY, OR STORE CLASSIFIED HARDWARE	YES <input type="checkbox"/> NO <input checked="" type="checkbox"/>
PROSECUTION INFORMATION	YES <input type="checkbox"/> NO <input checked="" type="checkbox"/>	e. PERFORM SERVICES ONLY	YES <input type="checkbox"/> NO <input checked="" type="checkbox"/>
RESTRICTED INFORMATION (SCI)	YES <input type="checkbox"/> NO <input checked="" type="checkbox"/>	f. HAVE ACCESS TO U.S. CLASSIFIED INFORMATION OUTSIDE THE U.S., PUERTO RICO, U.S. POSSESSIONS AND TRUST TERRITORIES	YES <input type="checkbox"/> NO <input checked="" type="checkbox"/>
PROSECUTION	YES <input checked="" type="checkbox"/> NO <input type="checkbox"/>	g. BE AUTHORIZED TO USE THE SERVICES OF DEFENSE TECHNICAL INFORMATION CENTER (DTIC) OR OTHER SECONDARY DISTRIBUTION CENTER	YES <input type="checkbox"/> NO <input checked="" type="checkbox"/>
PROSECUTION INFORMATION	YES <input type="checkbox"/> NO <input checked="" type="checkbox"/>	h. REQUIRE A COMSEC ACCOUNT	YES <input type="checkbox"/> NO <input checked="" type="checkbox"/>
PROSECUTION INFORMATION	YES <input type="checkbox"/> NO <input checked="" type="checkbox"/>	i. HAVE A TEMPEST REQUIREMENT	YES <input type="checkbox"/> NO <input checked="" type="checkbox"/>
PROSECUTION INFORMATION	YES <input type="checkbox"/> NO <input checked="" type="checkbox"/>	j. HAVE OPERATIONS SECURITY (OPSEC) REQUIREMENTS	YES <input type="checkbox"/> NO <input checked="" type="checkbox"/>
PROSECUTION INFORMATION	YES <input type="checkbox"/> NO <input checked="" type="checkbox"/>	k. BE AUTHORIZED TO USE THE DEFENSE COURIER SERVICE	YES <input type="checkbox"/> NO <input checked="" type="checkbox"/>
PROSECUTION INFORMATION	YES <input checked="" type="checkbox"/> NO <input type="checkbox"/>	l. OTHER (Specify):	YES <input type="checkbox"/> NO <input checked="" type="checkbox"/>
PROSECUTION INFORMATION	YES <input type="checkbox"/> NO <input checked="" type="checkbox"/>		YES <input type="checkbox"/> NO <input checked="" type="checkbox"/>

DD FORM 254 DEC 1999

PREVIOUS EDITION IS OBSOLETE

12. PUBLIC RELEASE Any information (classified or unclassified) pertaining to this contract shall not be released for public dissemination except as provided by the Industrial Security Manual or unless it has been approved for public release by appropriate U.S. Government authority. Proposed public releases shall be submitted for approval prior to release. Direct Through (Specify) **NONE AUTHORIZED.**

UNLESS CONTRACTOR HAS OBTAINED AUTHORITY TO RELEASE FROM THE DEPARTMENT OF HOMELAND SECURITY, CONTRACTOR SHALL COORDINATE WITH THE COTR AND THE OFFICE OF SECURITY (ASD) ON ALL CHANGES TO THIS GUIDANCE.

The Directorate for Freedom of Information and Security Review, Office of the Assistant Secretary of Defense (Public Affairs) for review. In the case of non DoD User Agencies, requests for disclosure shall be submitted to that agency.

13. SECURITY GUIDANCE The security classification guidance needed for this classified effort is identified below. If any difficulty is encountered in applying this guidance or if any other contributing factor indicates a need for changes in this guidance, the contractor is authorized and encouraged to provide recommended changes to challenge the guidance or the classification assigned to any information or material furnished or generated under this contract. Send all clarifying questions for interpretation of this guidance to the official identified below. Pending final decision, the information involved shall be classified and protected at the highest level of classification assigned or recommended. (Fill in as appropriate for the classified effort. Attach, or forward under separate correspondence, any documents/guidance/extracts referenced herein. Add additional pages as needed to provide complete guidance.)

Ref. Item 10a: COMSEC Access will involve the installation, maintenance, or use of crypto-equipment, systems, or existing material. Access to COMSEC requires a final US Government Clearance. Disclosure to Subcontractor requires prior approval of DHS. The contractor upon award shall contact the DHS COMSEC Control Office if Record (COR) at Commercial (540) 542-3848, to receive current COMSEC guidance.

Ref. Item 10e (2). Personnel: All contractor personnel requiring access to non-SCI Information must be: U.S. Citizens, have been granted a FINAL SECRET security clearance by the U.S. Government, prior to being given any access to such information released or generated under this contract. Immigrant aliens, personnel cleared on an interim basis or personnel holding contractor granted CONFIDENTIAL clearances are not eligible for access to information under this contract. Non-SCI Information associated with this contract shall not be released to subcontractors without the permission of the DHS CSO. Note 10e (1) and 11a. Access to all classified information (SCI) will be at DHS facilities only. For the purposes of this contract, the contractor is not authorized to process and/or store any classified information at contractor locations.

Jose Salazar 1-9-9
 JOSE SALAZAR, DHS OFFICE OF SECURITY
 PROGRAM MANAGER INDUSTRIAL SECURITY
 (902) 447-5346

14. ADDITIONAL SECURITY REQUIREMENTS. Requirements, in addition to ISM requirements, are established for this contract. (If Yes, Yes No identify the pertinent contractual clauses in the contract document itself, or provide an appropriate statement which identifies the additional requirements. Provide a copy of the requirements to the cognizant security office. Use item 13 if additional space is needed.)

15. INSPECTIONS. Elements of this contract are outside the inspection responsibility of the cognizant security office. Yes No Identify, explain and identify specific areas or elements carved out and the activity responsible for inspections. Use item 13 if additional space is needed.)

16. CERTIFICATION AND SIGNATURE Security requirements stated herein are complete and adequate for safeguarding the classified information to be provided or generated under this classified effort. All questions shall be referred to the official named below.

a. FULL NAME OF CERTIFYING OFFICIAL EDWARD J. PINDER	b. TITLE FACILITY SECURITY OFFICER (HOF)	c. TELEPHONE (Include Area Code) (856) 486-5266
---	---	--

ADDRESS (Include Zip Code) LOCKHEED MARTIN SERVICES, INC 400 ROUTE 70 WEST FREE HILL, NJ 08002 <i>Edward J. Pinder</i> 28 JAN 2009	17. REQUIRED DISTRIBUTION	
	<input checked="" type="checkbox"/>	a. CONTRACTOR
	<input checked="" type="checkbox"/>	b. SUBCONTRACTOR
	<input checked="" type="checkbox"/>	c. COGNIZANT SECURITY OFFICE FOR PRIME AND SUBCONTRACTOR
	<input checked="" type="checkbox"/>	d. U.S. ACTIVITY RESPONSIBLE FOR OVERSEAS SECURITY ADMINISTRATION
<input checked="" type="checkbox"/>	e. ADMINISTRATIVE CONTRACTING OFFICER	
<input checked="" type="checkbox"/>	f. OTHERS AS NECESSARY	

FORM 254 (BACK), DEC 1999

CONTINUATION SHEET FOR BLOCK 13.

LOCKHEED MARTIN SERVICES INC 2339 ROUTE 70 WEST FLOOR 3W, CHERRY HILL, NJ 08002-3315
CAGE CODE: 77609 CONTRACT# HSHQDC-06-D-00017 HQHSDC-07-J-00138
SUBCONTRACT#

Ref Item 10j: "Contractors shall control and safeguard FOUO in accordance with DHS Directive (MD 01421), "Safeguarding Sensitive but Unclassified (For Official Use Only) Information," dated Jan 6, 2005. DHS contractors must sign a special Non-Disclosure Agreement before receiving access to FOUO information. Contractors with questions on handling DHS FOUO shall contact DHS OS ASD at (202) 447-5341."

Ref. Item 11a: Contract performance for all work is restricted to DHS Government buildings located in and around the metropolitan area of Washington, D.C., and at other locations in the metropolitan area of Wash DC. All contractor personnel must be U.S. citizens, have been granted a final security clearance by the U.S. Government, have been approved as meeting suitability criteria by DHS CSO, and have been indoctrinated by a Non Disclosure Agreement, Standard Form 312 for this specific program prior to being given any access to such information released or generated under this contract. Immigrant aliens, personnel cleared on an interim basis, or personnel holding contractor granted CONFIDENTIAL clearances, are not eligible for access to classified information released or generated under this contract without the express permission of the CSO through the DHS Personnel Division (DHS/PSD). The contractor and the Contracting Officer Technical Representative or other delegated representative will revalidate all staffing requirements under the contract with the CSO annually or when a revised DD Form 254 is issued, whichever is sooner.

DEPARTMENT OF DEFENSE CONTRACT SECURITY CLASSIFICATION SPECIFICATION		1. CLEARANCE AND SAFEGUARDING	
<i>The requirements of the DoD Industrial Security Manual apply to all aspects of this effort.</i>		a. FACILITY CLEARANCE REQUIRED TOP SECRET	
		b. LEVEL OF SAFEGUARDING REQUIRED NONE	
2. THIS SPECIFICATION IS FOR: (X and complete as applicable)		3. THIS SPECIFICATION IS: (X and complete as applicable)	
<input checked="" type="checkbox"/> a. PRIME CONTRACT NUMBER HSHQDC-06-D-00017 HQHSDC-08-J-00138		<input type="checkbox"/> a. ORIGINAL (Complete date in all cases) Date (YYYYMMDD) 20071210	
<input checked="" type="checkbox"/> b. SUBCONTRACT NUMBER 7200002657		<input checked="" type="checkbox"/> b. REVISED (Supersedes all previous specs) Revision No. 2 Date (YYYYMMDD) 20090113	
<input type="checkbox"/> c. SOLICITATION OR OTHER NUMBER Due Date (YYYYMMDD)		<input type="checkbox"/> c. FINAL (Complete item 3 in all cases) Date (YYYYMMDD)	
4. IS THIS A FOLLOW-ON CONTRACT? <input checked="" type="checkbox"/> YES <input type="checkbox"/> NO. If Yes complete the following			
Classified material received or generated under HSHQDC-06-D-00017 HQHSDC-07-J-00739 (Preceding Contract Number) is transferred to this follow-on contract			
5. IS THIS A FINAL DD FORM 2547 <input type="checkbox"/> YES <input checked="" type="checkbox"/> NO. If Yes complete the following			
In response to the contractor's request dated _____, retention of the identified classified material is authorized for the period of _____.			
6. CONTRACTOR (Include Commercial and Government Entity (CAGE) Code)			
a. NAME, ADDRESS, AND ZIP CODE LOCKHEED MARTIN SERVICES, INC 2339 ROUTE 70 WEST CHERRY HILL, NJ 08002-3315		b. CAGE CODE 77609	c. COORDINANT SECURITY OFFICE (Name, Address, and Zip Code) DEFENSE SECURITY SERVICE 307 FELLOWSHIP ROAD STE 115 MT. LAUREL, NJ 08054-1233
7. SUBCONTRACTOR			
a. NAME, ADDRESS, AND ZIP CODE (b) (4)		b. CAGE CODE 3D0X0	c. COORDINANT SECURITY OFFICES (Name, Address, and Zip Code) DEFENSE SECURITY SERVICE 1250 OAKMEAD PARKWAY, STE 318 SUNNYVALE, CA 94085-4030
8. ACTUAL PERFORMANCE			
a. LOCATION Department of Homeland Security (DHS) various locations within the Washington, DC metropolitan area.		b. CAGE CODE	c. COORDINANT SECURITY OFFICE (Name, Address, and Zip Code)
9. GENERAL IDENTIFICATION OF THIS PROCUREMENT (U) Provide IT Operations & Maintenance technical support to Lockheed Martin in support of the IT-NOVA DHS Eagle Task Order. This is in response to Lockheed Martin's requirements to provide support to IT Operations Maintenance and COOP for the DHS Headquarters and Components directly supported by the DHS OCIO.			
10. THIS CONTRACT WILL REQUIRE ACCESS TO:		11. IN PERFORMING THIS CONTRACT, THE CONTRACTOR WILL:	
a. COMBINATIONS SECURITY (COMSEC) INFORMATION	YES <input checked="" type="checkbox"/> NO <input type="checkbox"/>	a. HAVE ACCESS TO CLASSIFIED INFORMATION ONLY AT ANOTHER CONTRACTOR'S FACILITY OR A GOVERNMENT ACTIVITY	YES <input checked="" type="checkbox"/> NO <input type="checkbox"/>
b. RESTRICTED DATA	YES <input type="checkbox"/> NO <input checked="" type="checkbox"/>	b. RECEIVE CLASSIFIED DOCUMENTS ONLY	YES <input type="checkbox"/> NO <input checked="" type="checkbox"/>
c. CRITICAL NUCLEAR WEAPON DESIGN INFORMATION	YES <input type="checkbox"/> NO <input checked="" type="checkbox"/>	c. RECEIVE AND GENERATE CLASSIFIED MATERIAL	YES <input type="checkbox"/> NO <input checked="" type="checkbox"/>
d. FORMERLY RESTRICTED DATA	YES <input type="checkbox"/> NO <input checked="" type="checkbox"/>	d. FABRICATE, MODIFY, OR STORE CLASSIFIED HARDWARE	YES <input type="checkbox"/> NO <input checked="" type="checkbox"/>
e. INTELLIGENCE INFORMATION:		e. PERFORM SERVICES ONLY	YES <input type="checkbox"/> NO <input checked="" type="checkbox"/>
(1) Sensitive Compartmented Information (SCI)	YES <input checked="" type="checkbox"/> NO <input type="checkbox"/>	f. HAVE ACCESS TO U.S. CLASSIFIED INFORMATION OUTSIDE THE U.S., PUERTO RICO, U.S. POSSESSIONS AND TRUST TERRITORIES	YES <input type="checkbox"/> NO <input checked="" type="checkbox"/>
(2) Non-SCI	YES <input type="checkbox"/> NO <input checked="" type="checkbox"/>	g. BE AUTHORIZED TO USE THE SERVICES OF DEFENSE TECHNICAL INFORMATION CENTER (DTIC) OR OTHER SECONDARY DISTRIBUTION CENTER	YES <input type="checkbox"/> NO <input checked="" type="checkbox"/>
f. SPECIAL ACCESS INFORMATION	YES <input type="checkbox"/> NO <input checked="" type="checkbox"/>	h. REQUIRE A COMSEC ACCOUNT	YES <input type="checkbox"/> NO <input checked="" type="checkbox"/>
g. NATO INFORMATION	YES <input type="checkbox"/> NO <input checked="" type="checkbox"/>	i. HAVE A TEMPEST REQUIREMENT	YES <input type="checkbox"/> NO <input checked="" type="checkbox"/>
h. FOREIGN GOVERNMENT INFORMATION	YES <input type="checkbox"/> NO <input checked="" type="checkbox"/>	j. HAVE OPERATIONS SECURITY (OPSEC) REQUIREMENTS	YES <input type="checkbox"/> NO <input checked="" type="checkbox"/>
i. LIMITED DISSEMINATION INFORMATION	YES <input type="checkbox"/> NO <input checked="" type="checkbox"/>	k. BE AUTHORIZED TO USE THE DEFENSE COURIER SERVICE	YES <input type="checkbox"/> NO <input checked="" type="checkbox"/>
j. FOR OFFICIAL USE ONLY INFORMATION	YES <input checked="" type="checkbox"/> NO <input type="checkbox"/>	l. OTHER (Specify):	YES <input type="checkbox"/> NO <input checked="" type="checkbox"/>
k. OTHER (Specify)	YES <input type="checkbox"/> NO <input checked="" type="checkbox"/>		

DD FORM 254, DEC 1999

PREVIOUS EDITION IS OBSOLETE

12. PUBLIC RELEASE. Any information (classified or unclassified) pertaining to this contract shall not be released for public dissemination except as provided by the Industrial Security Manual or unless it has been approved for public release by appropriate U.S. Government authority. Proposed public releases shall be submitted for approval prior to release Direct Through (Specify) **NONE AUTHORIZED. SCI WILL NOT BE RELEASED TO PUBLIC.**

UNLESS CONTRACTOR HAS OBTAINED AUTHORITY TO RELEASE FROM THE DEPARTMENT OF HOMELAND SECURITY; CONTRACTOR SHALL COORDINATE WITH THE COTR AND THE OFFICE OF SECURITY (ASD) ON ALL CHANGES TO THIS GUIDANCE to the Directorate for Freedom of Information and Security Review, Office of the Assistant Secretary of Defense (Public Affairs)* for review. *In the case of non-DoD User Agencies, requests for disclosure shall be submitted to that agency.

13. SECURITY GUIDANCE. The security classification guidance needed for this classified effort is identified below. If any difficulty is encountered in applying this guidance or if any other contributing factor indicates a need for changes in this guidance, the contractor is authorized and encouraged to provide recommended changes; to challenge the guidance or the classification assigned to any information or material furnished or generated under this contract; and to submit any questions for interpretation of this guidance to the official identified below. Pending final decision, the information involved shall be handled and protected at the highest level of classification assigned or recommended. (FR in as appropriate for the classified effort. Attach, or forward under separate correspondence, any documents/guides/extracts referenced herein. Add additional pages as needed to provide complete guidance.)

Ref. Item 10a: COMSEC Access will involve the installation, maintenance, or use of crypto-equipment, systems, or keying material. Access to COMSEC requires a final US Government Clearance. Disclosure to Subcontractor requires prior approval of DHS. The contractor upon award shall contact the DHS COMSEC Control Office if Record (COR) at commercial (540) 542-3848, to receive current COMSEC guidance.

Ref. Item 10e (1). Personnel: All contractor personnel assigned to this contract shall possess security clearances issued by the Defense Security Service (DSS) commensurate with the level of required access to classified information that is directly in support of this contract. Immigrant aliens, personnel cleared on an interim basis, or personnel holding contractor-generated Confidential clearances are not eligible for access to classified information released or generated under this contract. Contractor personnel who are specifically designated as requiring access to Sensitive Compartmented Information (SCI) must be eligible under the provisions of DCID 6/4 without exception. Personnel will be submitted for access by their DHS manager and verified by their Contract Technical Representative. If approved for access, they will receive an indoctrination briefing by DHS security staff prior to being granted access to SCI. All personnel security be scheduled for debriefing with the DHS SSO by calling (202) 282-8643. Note 10e (1) and 11a. Access to all classified information (SCI) will be at DHS facilities only. For the purposes of this contract, the contractor is not authorized to process and/or store any classified information at contractor locations.

Jose Salazar 1-9-9
 JOSE J. SALAZAR, DHS OFFICE OF SECURITY
 PROGRAM MANAGER INDUSTRIAL SECURITY
 (202) 447-5346

14. ADDITIONAL SECURITY REQUIREMENTS. Requirements, in addition to ISM requirements, are established for this contract. (If Yes, Yes No identify the pertinent contractual clauses in the contract document itself, or provide an appropriate statement which identifies the additional requirements. Provide a copy of the requirements to the cognizant security office. Use Item 13 if additional space is needed.)

15. INSPECTIONS. Elements of this contract are outside the inspection responsibility of the cognizant security office. Yes No (If Yes, explain and identify specific areas or elements carved out and the entity responsible for inspections. Use Item 13 if additional space is needed.)

"DHS/OS/SSBD CONCURS AND APPROVES THE "NEED-TO-KNOW" AT THE SCI LEVEL"
2/14/09 Clearances: Access to Intelligence Information requires a final US Government clearance. Subcontracting requires prior approval of the GCA. Briefings: Special briefings and procedures are required.

16. CERTIFICATION AND SIGNATURE. Security requirements stated herein are complete and adequate for safeguarding the classified information to be released or generated under this classified effort. All questions shall be referred to the official named below.

a. TYPED NAME OF CERTIFYING OFFICIAL EDWARD J. PINDER	b. TITLE FACILITY SECURITY OFFICER (HOF)	c. TELEPHONE (Include Area Code) (856) 486-5266
--	---	--

d. ADDRESS (Include Zip Code)
 LOCKHEED MARTIN SERVICES, INC
 2339 ROUTE 70 WEST
 CHERRY HILL, NJ 08002

e. SIGNATURE
Edward Pinder 28 JAN 2009

17. REQUIRED DISTRIBUTION

<input checked="" type="checkbox"/>	a. CONTRACTOR
<input checked="" type="checkbox"/>	b. SUBCONTRACTOR
<input checked="" type="checkbox"/>	c. COGNIZANT SECURITY OFFICE FOR PRIME AND SUBCONTRACTOR
<input checked="" type="checkbox"/>	d. U.S. ACTIVITY RESPONSIBLE FOR OVERSEAS SECURITY ADMINISTRATION
<input checked="" type="checkbox"/>	e. ADMINISTRATIVE CONTRACTING OFFICER
<input checked="" type="checkbox"/>	f. OTHERS AS NECESSARY

CONTINUATION SHEET FOR BLOCK 13.

**LOCKHEED MARTIN SERVICES INC 2339 ROUTE 70 WEST FLOOR 3W, CHERRY HILL, NJ 08002-3315
CAGE CODE: 77609 CONTRACT# HSHQDC-06-D-00017 HQHSDC-07-J-00138**

Reference Item 10e (1): Access to all Sensitive Compartmented Information (SCI) will be at DHS facilities only. For the purposes of this contract, the contractor is not authorized to process and/or store any classified information at contractor locations.

- a. All SCI will be handled in accordance with special security requirements, which will be furnished by the designated responsible special security office (SSO).
- b. SCI will not be released to contractor employees without specific release approval of the originator of the material as outlined in governing directives; based on prior approval and certification of "need-to-know" by the designated contractor.
- c. All Contractor personnel requiring access to SCI as part of this contract effort must be approved and indoctrinated by DHS. Requests for Access will be submitted by the government project manager who can validate the justification for access.
- d. Inquiries pertaining to classification guidance on SCI will be directed to the Special Security Officer (SSO).
- e. SCI furnished in support of this contract remains the property of the Department of Homeland Security (DHS), agency, or component originator. Upon completion or cancellation of the contract, SCI furnished will be returned to the direct custody of the supporting SSO, or destroyed IAW instructions outlined by the Contract Officer.
- f. Visits by contractor employees will only be certified by DHS when such visits are conducted as part of the contract effort.

Ref Item 10j: "Contractors shall control and safeguard FOUO in accordance with DHS Directive (MD 11042.1) "Safeguarding Sensitive but Unclassified (For Official Use Only) Information," dated Jan 6, 2005. DHS contractors must sign a special Non-Disclosure Agreement before receiving access to FOUO information. Contractors with questions on handling DHS FOUO shall contact DHS OS ASD at (202) 447-5341."

Ref. Item 11a. Contract performance for all SCI work is restricted to DHS Government buildings located in and around the metropolitan area of Washington, D.C., and at other locations in the metropolitan area of Wash DC. All contractor personnel must be U.S. citizens, have been granted a final security clearance by the U.S. Government, have been approved as meeting suitability criteria by DHS CSO, and have been indoctrinated by a Non Disclosure Agreement, Standard Form 312 for this specific program prior to being given any access to such information released or generated under this contract. Immigrant aliens, personnel cleared on an interim basis, or personnel holding contractor granted CONFIDENTIAL clearances, are not eligible for access to classified information released or generated under this contract without the express permission of the CSO through the DHS Personnel Division (DHS/PSD). The contractor and the Contracting Officer Technical Representative or other delegated representative will revalidate all SCI staffing requirements under the contract with the CSO annually or when a revised DD Form 254 is issued, whichever is sooner.
SCI WILL NOT BE RELEASED TO PUBLIC.

DEPARTMENT OF DEFENSE CONTRACT SECURITY CLASSIFICATION SPECIFICATION		1. CLEARANCE AND SAFEGUARDING	
(The requirements of the DoD Industrial Security Manual apply to all aspects of this effort)		a. FACILITY CLEARANCE REQUIRED TOP SECRET	
		b. LEVEL OF SAFEGUARDING REQUIRED NONE	
2. THIS SPECIFICATION IS FOR: (X and complete as applicable)		3. THIS SPECIFICATION IS: (X and complete as applicable)	
a. PRIME CONTRACT NUMBER <input checked="" type="checkbox"/> HSHQDC-06-D-00017 HQHSDC-08-J-00138		a. ORIGINAL (Complete date in all cases)	Date (YYMMDD) 20071210
b. SUBCONTRACT NUMBER <input checked="" type="checkbox"/> 46032242		b. REVISED (Supersedes all previous specs)	Revision No. 2 Date (YYMMDD) 20090112
c. SOLICITATION OR OTHER NUMBER	Date (YYMMDD)	c. FINAL (Complete item 3 in all cases)	Date (YYMMDD)
4. IS THIS A FOLLOW-ON CONTRACT? <input checked="" type="checkbox"/> YES <input type="checkbox"/> NO If Yes complete the following			
Classified material received or generated under <u>HSHQDC-06-D-00017 HQHSDC-07-J-00739</u> (Preceding Contract Number) is transferred to this follow-on contract			
5. IS THIS A FINAL DD FORM 254? <input type="checkbox"/> YES <input checked="" type="checkbox"/> NO. If Yes complete the following			
In response to the contractor's request dated _____, retention of the identified classified material is authorized for the period of _____			
6. CONTRACTOR (Include Commercial and Government Entity (CAGE) Code)			
a. NAME, ADDRESS, AND ZIP CODE LOCKHEED MARTIN SERVICES, INC 2339 ROUTE 70 WEST CHERRY HILL, NJ 08002-3315	b. CAGE CODE 77609	c. COGNIZANT SECURITY OFFICE (Name, Address, and Zip Code) DEFENSE SECURITY SERVICE 307 FELLOWSHIP ROAD STE 115 MT. LAUREL, NJ 08054-1233	
7. SUBCONTRACTOR			
a. NAME, ADDRESS, AND ZIP CODE (b) (4)	b. CAGE CODE 1D2J7	c. COGNIZANT SECURITY OFFICES (Name, Address, and Zip Code) DEFENSE SECURITY SERVICE 14428 ALBEMARLE POINT PLACE, STE 140 CHANTILLY, VA 20151	
8. ACTUAL PERFORMANCE			
a. LOCATION Department of Homeland Security (DHS) various locations within the Washington, DC metropolitan area.	b. CAGE CODE	c. COGNIZANT SECURITY OFFICE (Name, Address, and Zip Code)	
9. GENERAL IDENTIFICATION OF THIS PROCUREMENT (U) Provide IT Operations & Maintenance technical support to Lockheed Martin in support of the IT-NOVA DHS Eagle Task Order. This is in response to Lockheed Martin's requirements to provide support to IT Operations Maintenance and COOP for the DHS Headquarters and Components directly supported by the DHS OCIO.			
10. THIS CONTRACT WILL REQUIRE ACCESS TO:		11. IN PERFORMING THIS CONTRACT, THE CONTRACTOR WILL:	
a. COMMUNICATIONS SECURITY (COMSEC) INFORMATION	YES <input checked="" type="checkbox"/> NO <input type="checkbox"/>	a. HAVE ACCESS TO CLASSIFIED INFORMATION ONLY AT ANOTHER CONTRACTOR'S FACILITY OR A GOVERNMENT ACTIVITY	YES <input checked="" type="checkbox"/> NO <input type="checkbox"/>
b. RESTRICTED DATA	YES <input type="checkbox"/> NO <input checked="" type="checkbox"/>	b. RECEIVE CLASSIFIED DOCUMENTS ONLY	YES <input type="checkbox"/> NO <input checked="" type="checkbox"/>
c. CRITICAL NUCLEAR WEAPON DESIGN INFORMATION	YES <input type="checkbox"/> NO <input checked="" type="checkbox"/>	c. RECEIVE AND GENERATE CLASSIFIED MATERIAL	YES <input type="checkbox"/> NO <input checked="" type="checkbox"/>
d. FORMERLY RESTRICTED DATA	YES <input type="checkbox"/> NO <input checked="" type="checkbox"/>	d. FABRICATE, MODIFY, OR STORE CLASSIFIED HARDWARE	YES <input type="checkbox"/> NO <input checked="" type="checkbox"/>
e. INTELLIGENCE INFORMATION:		e. PERFORM SERVICES ONLY	YES <input type="checkbox"/> NO <input checked="" type="checkbox"/>
(1) Sensitive Compartmented Information (SCI)	YES <input checked="" type="checkbox"/> NO <input type="checkbox"/>	f. HAVE ACCESS TO U.S. CLASSIFIED INFORMATION OUTSIDE THE U.S., PUERTO RICO, U.S. POSSESSIONS AND TRUST TERRITORIES	YES <input type="checkbox"/> NO <input checked="" type="checkbox"/>
(2) Non-SCI	YES <input type="checkbox"/> NO <input checked="" type="checkbox"/>	g. BE AUTHORIZED TO USE THE SERVICES OF DEFENSE TECHNICAL INFORMATION CENTER (DTIC) OR OTHER SECONDARY DISTRIBUTION CENTER	YES <input type="checkbox"/> NO <input checked="" type="checkbox"/>
7. SPECIAL ACCESS INFORMATION	YES <input type="checkbox"/> NO <input checked="" type="checkbox"/>	h. REQUIRE A COMSEC ACCOUNT	YES <input type="checkbox"/> NO <input checked="" type="checkbox"/>
g. NATO INFORMATION	YES <input type="checkbox"/> NO <input checked="" type="checkbox"/>	i. HAVE A "EMPLOY" REQUIREMENT	YES <input type="checkbox"/> NO <input checked="" type="checkbox"/>
h. FOREIGN GOVERNMENT INFORMATION	YES <input type="checkbox"/> NO <input checked="" type="checkbox"/>	j. HAVE OPERATIONS SECURITY (OPSEC) REQUIREMENTS	YES <input type="checkbox"/> NO <input checked="" type="checkbox"/>
i. LIMITED DISSEMINATION INFORMATION	YES <input type="checkbox"/> NO <input checked="" type="checkbox"/>	k. BE AUTHORIZED TO USE THE DEFENSE CARRIER SERVICE	YES <input type="checkbox"/> NO <input checked="" type="checkbox"/>
j. FOR OFFICIAL USE ONLY INFORMATION	YES <input checked="" type="checkbox"/> NO <input type="checkbox"/>	l. OTHER (Specify):	YES <input type="checkbox"/> NO <input checked="" type="checkbox"/>
k. OTHER (Specify)	YES <input type="checkbox"/> NO <input checked="" type="checkbox"/>		

DD FORM 254, DEC 1999

PREVIOUS EDITION IS OBSOLETE.

12 PUBLIC RELEASE. Any information (classified or unclassified) pertaining to this contract shall not be released for public dissemination except as provided by the Industrial Security Manual or unless it has been approved for public release by appropriate U.S. Government authority. Proposed public releases shall be submitted for approval prior to release Direct Through (Specify) **NONE AUTHORIZED. SCI WILL NOT BE RELEASED TO PUBLIC.**

UNLESS CONTRACTOR HAS OBTAINED AUTHORITY TO RELEASE FROM THE DEPARTMENT OF HOMELAND SECURITY, CONTRACTOR SHALL COORDINATE WITH THE COTR AND THE OFFICE OF SECURITY (ASD) ON ALL CHANGES TO THIS GUIDANCE to the Directorate for Freedom of Information and Security Review, Office of the Assistant Secretary of Defense (Public Affairs) for review. (In the case of non-DoD User Agencies, requests for disclosure shall be submitted to that agency)

13 SECURITY GUIDANCE. The security classification guidance needed for this classified effort is identified below. If any difficulty is encountered in applying this guidance or if any other contributing factor indicates a need for changes in this guidance, the contractor is authorized and encouraged to provide recommended changes; to challenge the guidance of the classification assigned to any information or material furnished or generated under this contract, and to submit any questions for interpretation of this guidance to the official identified below. Pending final decision, the information involved shall be handled and protected at the highest level of classification assigned or recommended. (Fill in as appropriate for the classified effort. Attach, or forward under separate correspondence, any documents/guidance/extracts referenced herein. Add additional pages as needed to provide complete guidance.)

Ref. Item 10a: COMSEC Access will involve the installation, maintenance, or use of crypto-equipment, systems, or keying material. Access to COMSEC requires a final US Government Clearance. Disclosure to Subcontractor requires prior approval of DHS. The contractor upon award shall contact the DHS COMSEC Control Office if Record (COR) at commercial (540) 542-3848, to receive current COMSEC guidance.

Ref. Item 10e (1). Personnel: All contractor personnel assigned to this contract shall possess security clearances issued by the Defense Security Service (DSS) commensurate with the level of required access to classified information that is directly in support of this contract. Immigrant aliens, personnel cleared on an interim basis, or personnel holding contractor-generated Confidential clearances are not eligible for access to classified information released or generated under this contract. Contractor personnel who are specifically designated as requiring access to Sensitive Compartmented Information (SCI) must be eligible under the provisions of DCID 6/4 without exception. Personnel will be submitted for access by their DHS manager and verified by their Contract Technical Representative. If approved for access, they will receive an indoctrination briefing by DHS security staff prior to being granted access to SCI. All personnel security be scheduled for debriefing with the DHS SSO by calling (202) 282-8643. Note 10e (1) and 11a. Access to all classified information (SCI) will be at DHS facilities only. For the purposes of this contract, the contractor is not authorized to process and/or store any classified information at contractor locations.

Jose Salazar 1-9-9
 JOSE J. SALAZAR, DHS OFFICE OF SECURITY
 PROGRAM MANAGER INDUSTRIAL SECURITY
 (202) 447-5346

14. ADDITIONAL SECURITY REQUIREMENTS. Requirements, in addition to ISM requirements, are established for this contract. (If Yes, Yes No identify the pertinent contractual clauses in the contract document itself, or provide an appropriate statement which identifies the additional requirements. Provide a copy of the requirements to the cognizant security office. Use Item 13 if additional space is needed.)

15. INSPECTIONS. Elements of this contract are outside the inspection responsibility of the cognizant security office. (If Yes, explain and identify specific areas or elements covered out and the activity responsible for inspections. Use Item 13 if additional space is needed.) Yes No

"DHS/OS/SSPD CONCURS AND APPROVES THE "NEED-TO-KNOW" AT THE SCI LEVEL"
EC 2/10/09 Clearances: Access to intelligence information requires a final US Government clearance. Subcontracting requires prior approval of the GCA. Briefings: Special briefings and procedures are required.

16. CERTIFICATION AND SIGNATURE. Security requirements stated herein are complete and adequate for safeguarding the classified information to be released or generated under this classified effort. All questions shall be referred to the official named below.

a. TYPED NAME OF CERTIFYING OFFICIAL EDWARD J. PINDER	b. TITLE FACILITY SECURITY OFFICER (HOF)	c. TELEPHONE (Include Area Code) (856) 486-5266
--	---	--

d. ADDRESS (Include Zip Code) LOCKHEED MARTIN SERVICES, INC 2339 ROUTE 70 WEST CHERRY HILL, NJ 08002	17. REQUIRED DISTRIBUTION	
	<input checked="" type="checkbox"/>	a. CONTRACTOR
	<input checked="" type="checkbox"/>	b. SUBCONTRACTOR
	<input checked="" type="checkbox"/>	c. COGNIZANT SECURITY OFFICE FOR PRIME AND SUBCONTRACTOR
	<input checked="" type="checkbox"/>	d. U.S. ACTIVITY RESPONSIBLE FOR OVERSEAS SECURITY ADMINISTRATION
	<input checked="" type="checkbox"/>	e. ADMINISTRATIVE CONTRACTING OFFICER
<input checked="" type="checkbox"/>	f. OTHERS AS NECESSARY	

Signature: *Edward Pinder 28 JAN 2009*

DD FORM 254 (BACK), DEC 1999

CONTINUATION SHEET FOR BLOCK 13.

**LOCKHEED MARTIN SERVICES INC 2339 ROUTE 70 WEST FLOOR 3W, CHERRY HILL, NJ 08002-3315
CAGE CODE: 77609 CONTRACT# HSHQDC-06-D-00017 HQHSDC-07-J-00138**

Reference Item 10e (1): Access to all Sensitive Compartmented Information (SCI) will be at DHS facilities only. For the purposes of this contract, the contractor is not authorized to process and/or store any classified information at contractor locations.

- a. All SCI will be handled in accordance with special security requirements, which will be furnished by the designated responsible special security office (SSO).
- b. SCI will not be released to contractor employees without specific release approval of the originator of the material as outlined in governing directives; based on prior approval and certification of "need-to-know" by the designated contractor.
- c. All Contractor personnel requiring access to SCI as part of this contract effort must be approved and indoctrinated by DHS. Requests for Access will be submitted by the government project manager who can validate the justification for access.
- d. Inquiries pertaining to classification guidance on SCI will be directed to the Special Security Officer (SSO).
- e. SCI furnished in support of this contract remains the property of the Department of Homeland Security (DHS), agency, or component originator. Upon completion or cancellation of the contract, SCI furnished will be returned to the direct custody of the supporting SSO, or destroyed IAW instructions outlined by the Contract Officer.
- f. Visits by contractor employees will only be certified by DHS when such visits are conducted as part of the contract effort.

Ref Item 10j: "Contractors shall control and safeguard FOUO in accordance with DHS Directive (MD 11042.1) "Safeguarding Sensitive but Unclassified (For Official Use Only) Information," dated Jan 6, 2005. DHS contractors must sign a special Non-Disclosure Agreement before receiving access to FOUO information. Contractors with questions on handling DHS FOUO shall contact DHS OS ASD at (202) 447-5341."

Ref. Item 11a. Contract performance for all SCI work is restricted to DHS Government buildings located in and around the metropolitan area of Washington, D.C., and at other locations in the metropolitan area of Wash DC. All contractor personnel must be U.S. citizens, have been granted a final security clearance by the U.S. Government, have been approved as meeting suitability criteria by DHS CSO, and have been indoctrinated by a Non Disclosure Agreement, Standard Form 312 for this specific program prior to being given any access to such information released or generated under this contract. Immigrant aliens, personnel cleared on an interim basis, or personnel holding contractor granted CONFIDENTIAL clearances, are not eligible for access to classified information released or generated under this contract without the express permission of the CSO through the DHS Personnel Division (DHS/PSD). The contractor and the Contracting Officer Technical Representative or other delegated representative will revalidate all SCI staffing requirements under the contract with the CSO annually or when a revised DD Form 254 is issued, whichever is sooner. SCI WILL NOT BE RELEASED TO PUBLIC.

DEPARTMENT OF DEFENSE CONTRACT SECURITY CLASSIFICATION SPECIFICATION		1. CLEARANCE AND SAFEGUARDING	
(The requirements of the DoD Industrial Security Manual apply to all aspects of this effort)		a. FACILITY CLEARANCE REQUIRED	
		TOP SECRET	
		b. LEVEL OF SAFEGUARDING REQUIRED	
		NONE	
2. THIS SPECIFICATION IS FOR: (X and complete as applicable)		3. THIS SPECIFICATION IS: (X and complete as applicable)	
<input checked="" type="checkbox"/> a. PRIME CONTRACT NUMBER HSHQDC-06-D-00017 HQHSDC-08-J-00138		<input type="checkbox"/> a. ORIGINAL (Complete date in all cases) Date (YYMMDD) 20071210	
<input checked="" type="checkbox"/> b. SUBCONTRACT NUMBER 46032262		<input checked="" type="checkbox"/> b. REVISED (Supersedees all previous specs) Revision No. 2 Date (YYMMDD) 20090113	
<input type="checkbox"/> c. SDCITATION OR OTHER NUMBER Due Date (YYMMDD)		<input type="checkbox"/> c. FINAL (Complete item 5 in all cases) Date (YYMMDD)	
4. IS THIS A FOLLOW-ON CONTRACT? <input checked="" type="checkbox"/> YES <input type="checkbox"/> NO. If Yes complete the following			
Classified material received or generated under <u>HSHQDC-06-D-00017 HQHSDC-07-J-00739</u> (Preceding Contract Number) is transferred to this follow-on contract			
5. IS THIS A FINAL DD FORM 254? <input type="checkbox"/> YES <input checked="" type="checkbox"/> NO. If Yes complete the following			
In response to the contractor's request dated _____, retention of the identified classified material is authorized for the period of _____			
6. CONTRACTOR (Include Commercial and Government Entity / CAGE Code)			
a. NAME, ADDRESS, AND ZIP CODE LOCKHEED MARTIN SERVICES, INC 2339 ROUTE 70 WEST CHERRY HILL, NJ 08002-3315		b. CAGE CODE 77509	c. COORDINANT SECURITY OFFICE (Name, Address, and Zip Code) DEFENSE SECURITY SERVICE 307 FELLOWSHIP ROAD STE 115 MT. LAUREL, NJ 08054-1233
7. SUBCONTRACTOR			
a. NAME, ADDRESS, AND ZIP CODE (b) (4)		b. CAGE CODE 0VT30	c. COORDINANT SECURITY OFFICES (Name, Address, and Zip Code) DEFENSE SECURITY SERVICE 14428 ALBERMARLE POINT PLACE, STE 140 CHANTILLY, VA 20151
8. ACTUAL PERFORMANCE			
a. LOCATION Department of Homeland Security (DHS) various locations within the Washington, DC metropolitan area.		b. CAGE CODE	c. COORDINANT SECURITY OFFICE (Name, Address, and Zip Code)
9. GENERAL IDENTIFICATION OF THIS PROCUREMENT (U) Provide IT Operations & Maintenance technical support to Lockheed Martin in support of the IT-NOVA DHS Eagle Task Order. This is in response to Lockheed Martin's requirements to provide support to IT Operations Maintenance and COOP for the DHS Headquarters and Components directly supported by the DHS OCIO.			
10. THIS CONTRACT WILL REQUIRE ACCESS TO:			
a. COMMUNICATIONS SECURITY (COMSEC) INFORMATION	YES	NO	11. IN PERFORMING THIS CONTRACT, THE CONTRACTOR WILL:
b. RESTRICTED DATA	<input type="checkbox"/>	<input checked="" type="checkbox"/>	a. HAVE ACCESS TO CLASSIFIED INFORMATION ONLY AT ANOTHER CONTRACTOR'S FACILITY OR A GOVERNMENT ACTIVITY
c. CRITICAL NUCLEAR WEAPON DESIGN INFORMATION	<input type="checkbox"/>	<input checked="" type="checkbox"/>	b. RECEIVE CLASSIFIED DOCUMENTS ONLY
d. FORMERLY RESTRICTED DATA	<input type="checkbox"/>	<input checked="" type="checkbox"/>	c. RECEIVE AND GENERATE CLASSIFIED MATERIAL
e. INTELLIGENCE INFORMATION	<input type="checkbox"/>	<input checked="" type="checkbox"/>	d. FABRICATE, MODIFY, OR STORE CLASSIFIED HARDWARE
(1) Sensitive Compartmented Information (SCI)	<input checked="" type="checkbox"/>	<input type="checkbox"/>	e. PERFORM SERVICES ONLY
(2) Non-SCI	<input type="checkbox"/>	<input checked="" type="checkbox"/>	f. HAVE ACCESS TO U.S. CLASSIFIED INFORMATION OUTSIDE THE U.S., PUERTO RICO, U.S. POSSESSIONS AND TRUST TERRITORIES
f. SPECIAL ACCESS INFORMATION	<input type="checkbox"/>	<input checked="" type="checkbox"/>	g. BE AUTHORIZED TO USE THE SERVICES OF DEFENSE TECHNICAL INFORMATION CENTER (DTIC) OR OTHER SECONDARY DISTRIBUTION CENTER
g. NATO INFORMATION	<input type="checkbox"/>	<input checked="" type="checkbox"/>	h. REQUIRE A COMSEC ACCOUNT
h. FOREIGN GOVERNMENT INFORMATION	<input type="checkbox"/>	<input checked="" type="checkbox"/>	i. HAVE A TEMPEST REQUIREMENT
i. LIMITED DISSEMINATION INFORMATION	<input type="checkbox"/>	<input checked="" type="checkbox"/>	j. HAVE OPERATIONS SECURITY (OPSEC) REQUIREMENTS
j. FOR OFFICIAL USE ONLY INFORMATION	<input checked="" type="checkbox"/>	<input type="checkbox"/>	k. BE AUTHORIZED TO USE THE DEFENSE COURIER SERVICE
k. OTHER (Specify)	<input type="checkbox"/>	<input checked="" type="checkbox"/>	l. OTHER (Specify)

DD FORM 254, DEC 1999

PREVIOUS EDITION IS OBSOLETE.

12 PUBLIC RELEASE. Any information (classified or unclassified) pertaining to this contract shall not be released for public dissemination except as provided by the Industrial Security Manual or unless it has been approved for public release by appropriate U.S. Government authority. Proposed public releases shall be submitted for approval prior to release Direct Through (Specify) **NONE AUTHORIZED. SCI WILL NOT BE RELEASED TO PUBLIC.**

UNLESS CONTRACTOR HAS OBTAINED AUTHORITY TO RELEASE FROM THE DEPARTMENT OF HOMELAND SECURITY, CONTRACTOR SHALL COORDINATE WITH THE COTB AND THE OFFICE OF SECURITY (ASD) ON ALL CHANGES TO THIS GUIDANCE. to the Directorate for Freedom of Information and Security Review, Office of the Assistant Secretary of Defense (Public Affairs)* for review. *In the case of non-DoD User Agencies, requests for disclosure shall be submitted to that agency.

13 SECURITY GUIDANCE. The security classification guidance needed for this classified effort is identified below. If any difficulty is encountered in applying the guidance or if any other contributing factor indicates a need for changes in this guidance, the contractor is authorized and encouraged to provide recommended changes; to challenge the guidance or the classification assigned to any information or material furnished or generated under this contract, and to submit any questions for interpretation of this guidance to the official identified below. Pending final decision, the information involved shall be handled and protected at the highest level of classification assigned or recommended. (Fill in as appropriate for the classified effort. Attach, or forward under separate correspondence, any documents/guides/extracts referenced herein. Add additional pages as needed to provide complete guidance.)

Ref. Item 10a: COMSEC Access will involve the installation, maintenance, or use of crypto-equipment, systems, or keying material. Access to COMSEC requires a final US Government Clearance. Disclosure to Subcontractor requires prior approval of DHS. The contractor upon award shall contact the DHS COMSEC Control Office if Record (COR) at commercial (540) 542-3848, to receive current COMSEC guidance.

Ref. Item 10e (1). Personnel: All contractor personnel assigned to this contract shall possess security clearances issued by the Defense Security Service (DSS) commensurate with the level of required access to classified information that is directly in support of this contract. Immigrant aliens, personnel cleared on an interim basis, or personnel holding contractor-generated Confidential clearances are not eligible for access to classified information released or generated under this contract. Contractor personnel who are specifically designated as requiring access to Sensitive Compartmented Information (SCI) must be eligible under the provisions of DCID 6/4 without exception. Personnel will be submitted for access by their DHS manager and verified by their Contract Technical Representative. If approved for access, they will receive an indoctrination briefing by DHS security staff prior to being granted access to SCI. All personnel security be scheduled for debriefing with the DHS SSO by calling (202) 282-8643. Note 10e (1) and 11a. Access to all classified information (SCI) will be at DHS facilities only. For the purposes of this contract, the contractor is not authorized to process and/or store any classified information at contractor locations.

Jose Salazar
 JOSE J. SALAZAR, DHS OFFICE OF SECURITY
 PROGRAM MANAGER INDUSTRIAL SECURITY
 (202) 447-5346

14. ADDITIONAL SECURITY REQUIREMENTS. Requirements, in addition to ISM requirements, are established for this contract. (If Yes, Yes No identify the pertinent contractual clauses in the contract document itself, or provide an appropriate statement which identifies the additional requirements. Provide a copy of the requirements to the cognizant security office. Use Item 13 if additional space is needed.)

15. INSPECTIONS. Elements of this contract are outside the inspection responsibility of the cognizant security office. (If Yes, explain and identify specific areas or elements carved out and the activity responsible for inspections. Use Item 13 if additional space is needed.) Yes No

"DHS/OS/SSPD CONCURS AND APPROVES THE "NEED-TO-KNOW" AT THE SCI LEVEL"

2/10/09 Clearances: Access to intelligence information requires a final US Government clearance. Subcontracting requires prior approval of the GCA. Briefings: Special briefings and procedures are required.

16. CERTIFICATION AND SIGNATURE. Security requirements stated herein are complete and adequate for safeguarding the classified information to be released or generated under this classified effort. All questions shall be referred to the official named below.

a. TYPED NAME OF CERTIFYING OFFICIAL EDWARD J. PINDER	b. TITLE FACILITY SECURITY OFFICER (HOF)	c. TELEPHONE (Include Area Code) (856) 486-5266
--	---	--

d. ADDRESS (Include Zip Code) LOCKHEED MARTIN SERVICES, INC 2339 ROUTE 70 WEST CHERRY HILL, NJ 08002	17. REQUIRED DISTRIBUTION <input checked="" type="checkbox"/> a. CONTRACTOR <input checked="" type="checkbox"/> b. SUBCONTRACTOR <input checked="" type="checkbox"/> c. COGNIZANT SECURITY OFFICE FOR PRIME AND SUBCONTRACTOR <input checked="" type="checkbox"/> d. U.S. ACTIVITY RESPONSIBLE FOR OVERSEAS SECURITY ADMINISTRATION <input checked="" type="checkbox"/> e. ADMINISTRATIVE CONTRACTING OFFICER <input checked="" type="checkbox"/> f. OTHERS AS NECESSARY
---	--

DD FORM 254 (BACK), DEC 1999

CONTINUATION SHEET FOR BLOCK 13.

**LOCKHEED MARTIN SERVICES INC 2339 ROUTE 70 WEST FLOOR 3W, CHERRY HILL, NJ 08002-3315
CAGE CODE: 77609 CONTRACT# HSHQDC-06-D-00017 HQHSDC-07-J-00138**

Reference Item 10e (1): Access to all Sensitive Compartmented Information (SCI) will be at DHS facilities only. For the purposes of this contract, the contractor is not authorized to process and/or store any classified information at contractor locations.

- a. All SCI will be handled in accordance with special security requirements, which will be furnished by the designated responsible special security office (SSO).
- b. SCI will not be released to contractor employees without specific release approval of the originator of the material as outlined in governing directives; based on prior approval and certification of "need-to-know" by the designated contractor.
- c. All Contractor personnel requiring access to SCI as part of this contract effort must be approved and indoctrinated by DHS. Requests for Access will be submitted by the government project manager who can validate the justification for access.
- d. Inquiries pertaining to classification guidance on SCI will be directed to the Special Security Officer (SSO).
- e. SCI furnished in support of this contract remains the property of the Department of Homeland Security (DHS), agency, or component originator. Upon completion or cancellation of the contract, SCI furnished will be returned to the direct custody of the supporting SSO, or destroyed IAW instructions outlined by the Contract Officer.
- f. Visits by contractor employees will only be certified by DHS when such visits are conducted as part of the contract effort.

Ref Item 10j: "Contractors shall control and safeguard FOUO in accordance with DHS Directive (MD 11042.1) "Safeguarding Sensitive but Unclassified (For Official Use Only) Information," dated Jan 6, 2005. DHS contractors must sign a special Non-Disclosure Agreement before receiving access to FOUO information. Contractors with questions on handling DHS FOUO shall contact DHS OS ASD at (202) 447-5341."

Ref. Item 11a. Contract performance for all SCI work is restricted to DHS Government buildings located in and around the metropolitan area of Washington, D.C., and at other locations in the metropolitan area of Wash DC. All contractor personnel must be U.S. citizens, have been granted a final security clearance by the U.S. Government, have been approved as meeting suitability criteria by DHS CSO, and have been indoctrinated by a Non Disclosure Agreement, Standard Form 312 for this specific program prior to being given any access to such information released or generated under this contract. Immigrant aliens, personnel cleared on an interim basis, or personnel holding contractor granted CONFIDENTIAL clearances, are not eligible for access to classified information released or generated under this contract without the express permission of the CSO through the DHS Personnel Division (DHS/PSD). The contractor and the Contracting Officer Technical Representative or other delegated representative will revalidate all SCI staffing requirements under the contract with the CSO annually or when a revised DD Form 254 is issued, whichever is sooner. SCI WILL NOT BE RELEASED TO PUBLIC.

DEPARTMENT OF DEFENSE CONTRACT SECURITY CLASSIFICATION SPECIFICATION		1. CLEARANCE AND SAFEGUARDING	
(The requirements of the DoD Industrial Security Manual apply to all aspects of this effort)		<input checked="" type="checkbox"/> FACILITY CLEARANCE REQUIRED TOP SECRET	
		<input type="checkbox"/> LEVEL OF SAFEGUARDING REQUIRED NONE	
2. THIS SPECIFICATION IS FOR: (X and complete as applicable)		3. THIS SPECIFICATION IS: (X and complete as applicable)	
<input checked="" type="checkbox"/> a. PRIME CONTRACT NUMBER HSHQDC-06-D-00017 HQHSDC-08-J-00138	<input type="checkbox"/> b. ORIGINAL (Complete date in all cases) Date (YYMMDD) 20071210	<input checked="" type="checkbox"/> d. SUBCONTRACT NUMBER 46032302	<input checked="" type="checkbox"/> d. REVISED (Supersedes all previous specs) Revision No. 2 Date (YYMMDD) 20090113
<input type="checkbox"/> c. SOLICITATION OR OTHER NUMBER Due Date (YYMMDD)	<input type="checkbox"/> e. FINAL (Complete Item 5 in all cases) Date (YYMMDD)		
4. IS THIS A FOLLOW-ON CONTRACT? <input checked="" type="checkbox"/> YES <input type="checkbox"/> NO. If Yes complete the following			
Classified material received or generated under <u>HSHQDC-06-D-00017 HQHSDC-07-J-00739</u> (Preceding Contract Number) is transferred to this follow-on contract			
5. IS THIS A FINAL DD FORM 254? <input type="checkbox"/> YES <input checked="" type="checkbox"/> NO. If Yes complete the following			
In response to the contractor's request dated _____, retention of the identified classified material is authorized for the period of _____			
6. CONTRACTOR (Include Commercial and Government Entity (CAGE) Code)			
a. NAME, ADDRESS, AND ZIP CODE LOCKHEED MARTIN SERVICES, INC 2339 ROUTE 70 WEST CHERRY HILL, NJ 08002-3315	b. CAGE CODE 77609	c. COGNIZANT SECURITY OFFICE (Name, Address, and Zip Code) DEFENSE SECURITY SERVICE 307 FELLOWSHIP ROAD STE 115 MT. LAUREL, NJ 08054-1233	
7. SUBCONTRACTOR			
a. NAME, ADDRESS, AND ZIP CODE (b) (4)	b. CAGE CODE 1EEX6	c. COGNIZANT SECURITY OFFICES (Name, Address, and Zip Code) DEFENSE SECURITY SERVICE 938 ELKRIDGE LANDING ROAD, STE 310 LINTHICUM, MD 21090-2917	
8. ACTUAL PERFORMANCE			
a. LOCATION Department of Homeland Security (DHS) various locations within the Washington, DC metropolitan area.	b. CAGE CODE	c. COGNIZANT SECURITY OFFICE (Name, Address, and Zip Code)	
9. GENERAL IDENTIFICATION OF THIS PROCUREMENT (U) Provide IT Operations & Maintenance technical support to Lockheed Martin in support of the IT-NOVA DHS Eagle Task Order. This is in response to Lockheed Martin's requirements to provide support to IT Operations Maintenance and COOP for the DHS Headquarters and Components directly supported by the DHS OCIO.			
10. THIS CONTRACT WILL REQUIRE ACCESS TO:			
a. COMMUNICATIONS SECURITY (COMSEC) INFORMATION	YES <input checked="" type="checkbox"/> NO <input type="checkbox"/>	11. IN PERFORMING THIS CONTRACT, THE CONTRACTOR WILL:	
b. RESTRICTED DATA	YES <input type="checkbox"/> NO <input checked="" type="checkbox"/>	a. HAVE ACCESS TO CLASSIFIED INFORMATION ONLY AT ANOTHER CONTRACTOR'S FACILITY OR A GOVERNMENT ACTIVITY	YES <input checked="" type="checkbox"/> NO <input type="checkbox"/>
c. CRITICAL NUCLEAR WEAPON DESIGN INFORMATION	YES <input type="checkbox"/> NO <input checked="" type="checkbox"/>	b. RECEIVE CLASSIFIED DOCUMENTS ONLY	YES <input type="checkbox"/> NO <input checked="" type="checkbox"/>
d. FORMERLY RESTRICTED DATA	YES <input type="checkbox"/> NO <input checked="" type="checkbox"/>	c. RECEIVE AND GENERATE CLASSIFIED MATERIAL	YES <input type="checkbox"/> NO <input checked="" type="checkbox"/>
e. INTELLIGENCE INFORMATION: (1) Sensitive Compartmented Information (SCI)	YES <input checked="" type="checkbox"/> NO <input type="checkbox"/>	d. FABRICATE, MODIFY, OR STORE CLASSIFIED HARDWARE	YES <input type="checkbox"/> NO <input checked="" type="checkbox"/>
(2) Non-SCI	YES <input type="checkbox"/> NO <input checked="" type="checkbox"/>	e. PERFORM SERVICES ONLY	YES <input type="checkbox"/> NO <input checked="" type="checkbox"/>
f. SPECIAL ACCESS INFORMATION	YES <input type="checkbox"/> NO <input checked="" type="checkbox"/>	f. HAVE ACCESS TO U.S. CLASSIFIED INFORMATION OUTSIDE THE U.S., PUERTO RICO, U.S. POSSESSIONS AND TRUST TERRITORIES	YES <input type="checkbox"/> NO <input checked="" type="checkbox"/>
g. NATO INFORMATION	YES <input type="checkbox"/> NO <input checked="" type="checkbox"/>	g. BE AUTHORIZED TO USE THE SERVICES OF DEFENSE TECHNICAL INFORMATION CENTER (DTIC) OR OTHER SECONDARY DISTRIBUTION CENTER	YES <input type="checkbox"/> NO <input checked="" type="checkbox"/>
h. FOREIGN GOVERNMENT INFORMATION	YES <input type="checkbox"/> NO <input checked="" type="checkbox"/>	h. REQUIRE A COMSEC ACCOUNT	YES <input type="checkbox"/> NO <input checked="" type="checkbox"/>
i. LIMITED DISSEMINATION INFORMATION	YES <input type="checkbox"/> NO <input checked="" type="checkbox"/>	i. HAVE A TELEPOST REQUIREMENT	YES <input type="checkbox"/> NO <input checked="" type="checkbox"/>
j. FOR OFFICIAL USE ONLY INFORMATION	YES <input checked="" type="checkbox"/> NO <input type="checkbox"/>	j. HAVE OPERATIONS SECURITY (OPSEC) REQUIREMENTS	YES <input type="checkbox"/> NO <input checked="" type="checkbox"/>
k. OTHER (Specify)	YES <input type="checkbox"/> NO <input checked="" type="checkbox"/>	k. BE AUTHORIZED TO USE THE DEFENSE COURIER SERVICE	YES <input type="checkbox"/> NO <input checked="" type="checkbox"/>
		l. OTHER (Specify)	YES <input type="checkbox"/> NO <input checked="" type="checkbox"/>

12 PUBLIC RELEASE. Any information (classified or unclassified) pertaining to this contract shall not be released for public dissemination except as provided by the Industrial Security Manual or unless it has been approved for public release by appropriate U.S. Government authority. Proposed public releases shall be submitted for approval prior to release Direct Through (Specify) NONE AUTHORIZED. SCI WILL NOT BE RELEASED TO PUBLIC.

UNLESS CONTRACTOR HAS OBTAINED AUTHORITY TO RELEASE FROM THE DEPARTMENT OF HOMELAND SECURITY; CONTRACTOR SHALL COORDINATE WITH THE COTR AND THE OFFICE OF SECURITY (ASD) ON ALL CHANGES TO THIS GUIDANCE. to the Directorate for Freedom of Information and Security Review, Office of the Assistant Secretary of Defense (Public Affairs) for review. In the case of non-DoD User Agencies, requests for disclosure shall be submitted to that agency.

13 SECURITY GUIDANCE. The security classification guidance needed for this classified effort is identified below. If any difficulty is encountered in applying this guidance or if any other contributing factor indicates a need for changes in this guidance, the contractor is authorized and encouraged to provide recommended changes to challenge the guidance or the classification assigned to any information or material furnished or generated under this contract, and to submit any questions for interpretation of this guidance to the official identified below. Pending final decision, the information involved shall be handled and protected at the highest level of classification assigned or recommended. (Fill in as appropriate for the classified effort. Attach, or forward under separate correspondence, any documents/guides/extracts referenced herein. Add additional pages as needed to provide complete guidance.)

Ref. Item 10a: COMSEC Access will involve the installation, maintenance, or use of crypto-equipment, systems, or keying material. Access to COMSEC requires a final US Government Clearance. Disclosure to Subcontractor requires prior approval of DHS. The contractor upon award shall contact the DHS COMSEC Control Office if Record (COR) at commercial (540) 542-3848, to receive current COMSEC guidance.

Ref. Item 10e (1). Personnel: All contractor personnel assigned to this contract shall possess security clearances issued by the Defense Security Service (DSS) commensurate with the level of required access to classified information that is directly in support of this contract. Immigrant aliens, personnel cleared on an interim basis, or personnel holding contractor-generated Confidential clearances are not eligible for access to classified information released or generated under this contract. Contractor personnel who are specifically designated as requiring access to Sensitive Compartmented Information (SCI) must be eligible under the provisions of DCID 6/4 without exception. Personnel will be submitted for access by their DHS manager and verified by their Contract Technical Representative. If approved for access, they will receive an indoctrination briefing by DHS security staff prior to being granted access to SCI. All personnel security be scheduled for debriefing with the DHS SSO by calling (202) 282-8643. Note 10e (1) and 11a. Access to all classified information (SCI) will be at DHS facilities only. For the purposes of this contract, the contractor is not authorized to process and/or store any classified information at contractor locations.

Jose Salazar 1-9-9
 JOSE J. SALAZAR, DHS OFFICE OF SECURITY
 PROGRAM MANAGER INDUSTRIAL SECURITY
 (202) 447-5346

14. ADDITIONAL SECURITY REQUIREMENTS. Requirements, in addition to ISM requirements, are established for this contract. (If Yes, Yes No identify the pertinent contractual clauses in the contract document itself, or provide an appropriate statement which identifies the additional requirements. Provide a copy of the requirements to the cognizant security office. Use item 13 if additional space is needed.)

15 INSPECTIONS. Elements of this contract are outside the inspection responsibility of the cognizant security office. (If Yes, explain and identify specific areas or elements carved out and the activity responsible for inspections. Use item 13 if additional space is needed.) Yes No
 DHS/OSS/SSB CONCURS AND APPROVES THE "NEED-TO-KNOW" AT THE SCI LEVEL
2/10/09, Clearances: Access to Intelligence information requires a final US Government clearance. Subcontracting requires prior approval of the GCA. Briefings: Special briefings and procedures are required.

16. CERTIFICATION AND SIGNATURE. Security requirements stated herein are complete and adequate for safeguarding the classified information to be released or generated under this classified effort. All questions shall be referred to the official named below.

a. TYPED NAME OF CERTIFYING OFFICIAL EDWARD J. PINDER	b. TITLE FACILITY SECURITY OFFICER (HOF)	c. TELEPHONE (include Area Code) (856) 486-5266
--	---	--

d. ADDRESS (include Zip Code) LOCKHEED MARTIN SERVICES, INC 2339 ROUTE 70 WEST CHERRY HILL, NJ 08002 e. SIGNATURE <i>Edward J. Pinder 28 JAN 2009</i>	17. REQUIRED DISTRIBUTION	
	<input checked="" type="checkbox"/>	a. CONTRACTOR
	<input checked="" type="checkbox"/>	b. SUBCONTRACTOR
	<input checked="" type="checkbox"/>	c. COGNIZANT SECURITY OFFICE FOR PRIME AND SUBCONTRACTOR
	<input checked="" type="checkbox"/>	d. U.S. ACTIVITY RESPONSIBLE FOR OVERSEAS SECURITY ADMINISTRATION
	<input checked="" type="checkbox"/>	e. ADMINISTRATIVE CONTRACTING OFFICER
	<input checked="" type="checkbox"/>	f. OTHERS AS NECESSARY

CONTINUATION SHEET FOR BLOCK 13.

**LOCKHEED MARTIN SERVICES INC 2339 ROUTE 70 WEST FLOOR 3W, CHERRY HILL, NJ 08002-3315
CAGE CODE 77609 CONTRACT# HSHQDC-06-D-00017 HQHSDC-07-J-00138**

Reference Item 10e (1): Access to all Sensitive Compartmented Information (SCI) will be at DHS facilities only. For the purposes of this contract, the contractor is not authorized to process and/or store any classified information at contractor locations.

- a. All SCI will be handled in accordance with special security requirements, which will be furnished by the designated responsible special security office (SSO).
- b. SCI will not be released to contractor employees without specific release approval of the originator of the material as outlined in governing directives; based on prior approval and certification of "need-to-know" by the designated contractor.
- c. All Contractor personnel requiring access to SCI as part of this contract effort must be approved and indoctrinated by DHS. Requests for Access will be submitted by the government project manager who can validate the justification for access.
- d. Inquiries pertaining to classification guidance on SCI will be directed to the Special Security Officer (SSO).
- e. SCI furnished in support of this contract remains the property of the Department of Homeland Security (DHS), agency, or component originator. Upon completion or cancellation of the contract, SCI furnished will be returned to the direct custody of the supporting SSO, or destroyed IAW instructions outlined by the Contract Officer.
- f. Visits by contractor employees will only be certified by DHS when such visits are conducted as part of the contract effort.

Ref Item 10j: "Contractors shall control and safeguard FOUO in accordance with DHS Directive (MD 11042.1) "Safeguarding Sensitive but Unclassified (For Official Use Only) Information," dated Jan 6, 2005. DHS contractors must sign a special Non-Disclosure Agreement before receiving access to FOUO information. Contractors with questions on handling DHS FOUO shall contact DHS OS ASD at (202) 447-5341."

Ref. Item 11a. Contract performance for all SCI work is restricted to DHS Government buildings located in and around the metropolitan area of Washington, D.C., and at other locations in the metropolitan area of Wash DC. All contractor personnel must be U.S. citizens, have been granted a final security clearance by the U.S. Government, have been approved as meeting suitability criteria by DHS CSO, and have been indoctrinated by a Non Disclosure Agreement, Standard Form 312 for this specific program prior to being given any access to such information released or generated under this contract. Immigrant aliens, personnel cleared on an interim basis, or personnel holding contractor granted CONFIDENTIAL clearances, are not eligible for access to classified information released or generated under this contract without the express permission of the CSO through the DHS Personnel Division (DHS/PSD). The contractor and the Contracting Officer Technical Representative or other delegated representative will revalidate all SCI staffing requirements under the contract with the CSO annually or when a revised DD Form 254 is issued, whichever is sooner.
SCI WILL NOT BE RELEASED TO PUBLIC.

DEPARTMENT OF DEFENSE CONTRACT SECURITY CLASSIFICATION SPECIFICATION		1. CLEARANCE AND SAFEGUARDING	
(The requirements of the DoD Industrial Security Manual apply to all aspects of this effort)		a. FACILITY CLEARANCE REQUIRED TOP SECRET	
		b. LEVEL OF SAFEGUARDING REQUIRED NONE	
2. THIS SPECIFICATION IS FOR: (X and complete as applicable)		3. THIS SPECIFICATION IS: (X and complete as applicable)	
a. PRIME CONTRACT NUMBER <input checked="" type="checkbox"/> HSHQDC-06-D-00017 HQHSDC-08-J-00138		a. ORIGINAL (Complete date in all cases) <input type="checkbox"/>	
b. SUBCONTRACT NUMBER <input checked="" type="checkbox"/> 46032247		b. REVISED (Supersedes all previous specs) Revision No. 2	
c. SOLICITATION OR OTHER NUMBER Due Date (YYMMDD)		c. FINAL (Complete item 5 in all cases) Date (YYMMDD)	
4. IS THIS A FOLLOW-ON CONTRACT? <input checked="" type="checkbox"/> YES <input type="checkbox"/> NO. If Yes complete the following			
Classified material received or generated under <u>HSHQDC-06-D-00017 HQHSDC-07-J-00739</u> (Preceding Contract Number) is transferred to this follow-on contract			
5. IS THIS A FINAL DD FORM 254? <input type="checkbox"/> YES <input checked="" type="checkbox"/> NO. If Yes complete the following			
In response to the contractor's request dated _____, retention of the identified classified material is authorized for the period of _____			
6. CONTRACTOR (Include Commercial and Government Entity (CAGE) Code)			
a. NAME, ADDRESS, AND ZIP CODE LOCKHEED MARTIN SERVICES, INC 2339 ROUTE 70 WEST CHERRY HILL, NJ 08002-3315		b. CAGE CODE 77609	c. COGNIZANT SECURITY OFFICE (Name, Address, and Zip Code) DEFENSE SECURITY SERVICE 307 FELLOWSHIP ROAD STE 115 MT. LAUREL, NJ 08054-1233
7. SUBCONTRACTOR		c. COGNIZANT SECURITY OFFICES (Name, Address, and Zip Code)	
a. NAME, ADDRESS, AND ZIP CODE (b) (4)		b. CAGE CODE LJU52	d. DEFENSE SECURITY SERVICE 1340 BRADDOCK PLACE, 5 TH FLOOR ALEXANDRIA, VA 22314
8. ACTUAL PERFORMANCE			
a. LOCATION Department of Homeland Security (DHS) various locations within the Washington, DC metropolitan area.		b. CAGE CODE	c. COGNIZANT SECURITY OFFICE (Name, Address, and Zip Code)
9. GENERAL IDENTIFICATION OF THIS PROCUREMENT (U) Provide IT Operations & Maintenance technical support to Lockheed Martin in support of the IT-NOVA DHS Eagle Task Order. This is in response to Lockheed Martin's requirements to provide support to IT Operations Maintenance and COOP for the DHS Headquarters and Components directly supported by the DHS OCIO.			
10. THIS CONTRACT WILL REQUIRE ACCESS TO:		11. IN PERFORMING THIS CONTRACT, THE CONTRACTOR WILL:	
a. COMMUNICATIONS SECURITY (COMSEC) INFORMATION	YES <input checked="" type="checkbox"/> NO <input type="checkbox"/>	a. HAVE ACCESS TO CLASSIFIED INFORMATION ONLY AT ANOTHER CONTRACTOR'S FACILITY OR A GOVERNMENT ACTIVITY	YES <input checked="" type="checkbox"/> NO <input type="checkbox"/>
b. RESTRICTED DATA	<input type="checkbox"/> YES <input checked="" type="checkbox"/> NO	b. RECEIVE CLASSIFIED DOCUMENTS ONLY	<input type="checkbox"/> YES <input checked="" type="checkbox"/> NO
c. CRITICAL NUCLEAR WEAPON DESIGN INFORMATION	<input type="checkbox"/> YES <input checked="" type="checkbox"/> NO	c. RECEIVE AND GENERATE CLASSIFIED MATERIAL	<input type="checkbox"/> YES <input checked="" type="checkbox"/> NO
d. FORMERLY RESTRICTED DATA	<input type="checkbox"/> YES <input checked="" type="checkbox"/> NO	d. FABRICATE, MODIFY, OR STORE CLASSIFIED HARDWARE	<input type="checkbox"/> YES <input checked="" type="checkbox"/> NO
e. INTELLIGENCE INFORMATION:	<input checked="" type="checkbox"/> YES <input type="checkbox"/> NO	e. PERFORM SERVICES ONLY	<input type="checkbox"/> YES <input checked="" type="checkbox"/> NO
(1) Sensitive Compartmented Information (SCI)	<input checked="" type="checkbox"/> YES <input type="checkbox"/> NO	f. HAVE ACCESS TO U.S. CLASSIFIED INFORMATION OUTSIDE THE U.S., PUERTO RICO, U.S. POSSESSIONS AND TRUST TERRITORIES	<input type="checkbox"/> YES <input checked="" type="checkbox"/> NO
(2) Non-SCI	<input type="checkbox"/> YES <input checked="" type="checkbox"/> NO	g. BE AUTHORIZED TO USE THE SERVICES OF DEFENSE TECHNICAL INFORMATION CENTER (DTIC) OR OTHER SECONDARY DISTRIBUTION CENTER	<input type="checkbox"/> YES <input checked="" type="checkbox"/> NO
f. SPECIAL ACCESS INFORMATION	<input type="checkbox"/> YES <input checked="" type="checkbox"/> NO	h. REQUIRE A COMSEC ACCOUNT	<input type="checkbox"/> YES <input checked="" type="checkbox"/> NO
g. NATO INFORMATION	<input type="checkbox"/> YES <input checked="" type="checkbox"/> NO	i. HAVE A TEMPEST REQUIREMENT	<input type="checkbox"/> YES <input checked="" type="checkbox"/> NO
h. FOREIGN GOVERNMENT INFORMATION	<input type="checkbox"/> YES <input checked="" type="checkbox"/> NO	j. HAVE OPERATIONS SECURITY (OPSEC) REQUIREMENTS	<input type="checkbox"/> YES <input checked="" type="checkbox"/> NO
i. LIMITED DISSEMINATION INFORMATION	<input type="checkbox"/> YES <input checked="" type="checkbox"/> NO	k. BE AUTHORIZED TO USE THE DEFENSE COURIER SERVICE	<input type="checkbox"/> YES <input checked="" type="checkbox"/> NO
j. FOR OFFICIAL USE ONLY INFORMATION	<input checked="" type="checkbox"/> YES <input type="checkbox"/> NO	l. OTHER (Specify):	<input type="checkbox"/> YES <input checked="" type="checkbox"/> NO
k. OTHER (Specify)	<input type="checkbox"/> YES <input checked="" type="checkbox"/> NO		

12 PUBLIC RELEASE. Any information (classified or unclassified) pertaining to this contract shall not be released for public dissemination except as provided by the Industrial Security Manual or unless it has been approved for public release by appropriate U.S. Government authority. Proposed public releases shall be submitted for approval prior to release Direct Through (Specify) **NONE AUTHORIZED. SCI WILL NOT BE RELEASED TO PUBLIC.**
UNLESS CONTRACTOR HAS OBTAINED AUTHORITY TO RELEASE FROM THE DEPARTMENT OF HOMELAND SECURITY, CONTRACTOR SHALL COORDINATE WITH THE COTR AND THE OFFICE OF SECURITY (ASD) ON ALL CHANGES TO THIS GUIDANCE. (to the Directorate for Freedom of Information and Security Review, Office of the Assistant Secretary of Defense (Public Affairs) for review. (In the case of non-DoD User Agencies, requests for disclosure shall be submitted to that agency.)

13 SECURITY GUIDANCE. The security classification guidance needed for this classified effort is identified below. If any difficulty is encountered in applying this guidance or if any other contributing factor indicates a need for changes in this guidance, the contractor is authorized and encouraged to provide recommended changes; to challenge the guidance or the classification assigned to any information or material furnished or generated under this contract, and to submit any questions for interpretation of this guidance to the official identified below. Pending final decision, the information involved shall be handled and protected at the highest level of classification assigned or recommended. (Fill in as appropriate for the classified effort. Attach, or forward under separate correspondence, any documents/guides/extracts referenced herein. Add additional pages as needed to provide complete guidance.)

Ref. Item 10a: COMSEC Access will involve the installation, maintenance, or use of crypto-equipment, systems, or keying material. Access to COMSEC requires a final US Government Clearance. Disclosure to Subcontractor requires prior approval of DHS. The contractor upon award shall contact the DHS COMSEC Control Office if Record (COR) at commercial (540) 542-3848, to receive current COMSEC guidance.

Ref. Item 10e (1). Personnel: All contractor personnel assigned to this contract shall possess security clearances issued by the Defense Security Service (DSS) commensurate with the level of required access to classified information that is directly in support of this contract. Immigrant aliens, personnel cleared on an interim basis, or personnel holding contractor-generated Confidential clearances are not eligible for access to classified information released or generated under this contract. Contractor personnel who are specifically designated as requiring access to Sensitive Compartmented Information (SCI) must be eligible under the provisions of DCID 6/4 without exception. Personnel will be submitted for access by their DHS manager and verified by their Contract Technical Representative. If approved for access, they will receive an indoctrination briefing by DHS security staff prior to being granted access to SCI. All personnel security be scheduled for debriefing with the DHS SSO by calling (202) 282-8643. Note 10e (1) and 11a. Access to all classified information (SCI) will be at DHS facilities only. For the purposes of this contract, the contractor is not authorized to process and/or store any classified information at contractor locations.

Jose Salazar 199
 JOSE SALAZAR, DHS OFFICE OF SECURITY
 PROGRAM MANAGER INDUSTRIAL SECURITY
 (202) 447-5346

14. ADDITIONAL SECURITY REQUIREMENTS. Requirements, in addition to ISM requirements, are established for this contract. (If Yes, Yes No identify the pertinent contractual clauses in the contract document itself, or provide an appropriate statement which identifies the additional requirements. Provide a copy of the requirements to the cognizant security office. Use Item 13 if additional space is needed.)

15. INSPECTIONS. Elements of this contract are outside the inspection responsibility of the cognizant security office. Yes No (If Yes, explain and identify specific areas or elements covered and the activity responsible for inspections. Use Item 13 if additional space is needed.)
"DHS/OS/ASPD CONCURS AND APPROVES THE 'NEED-TO-KNOW' AT THE SCI LEVEL"
2/10/09 Clearances: Access to intelligence information requires a final US Government clearance
 Subcontracting requires prior approval of the GCA. Briefings: Special briefings and procedures are required.

16. CERTIFICATION AND SIGNATURE. Security requirements stated herein are complete and adequate for safeguarding the classified information to be released or generated under this classified effort. All questions shall be referred to the official named below.

a. TYPED NAME OF CERTIFYING OFFICIAL EDWARD J. PINDER		b. TITLE FACILITY SECURITY OFFICER (HOF)	c. TELEPHONE (Include Area Code) (856) 486-5266
3. ADDRESS (Include Zip Code) LOCKHEED MARTIN SERVICES, INC 2339 ROUTE 70 WEST CHERRY HILL, NJ 08002		17. REQUIRED DISTRIBUTION	
* SIGNATURE <i>Edward J. Pinder 26 JAN 2009</i> DD FORM 254 (BACK), DEC 1999		<input checked="" type="checkbox"/> a. CONTRACTOR	
		<input checked="" type="checkbox"/> b. SUBCONTRACTOR	
		<input checked="" type="checkbox"/> c. COGNIZANT SECURITY OFFICE FOR PRIME AND SUBCONTRACTOR	
		<input checked="" type="checkbox"/> d. U.S. ACTIVITY RESPONSIBLE FOR OVERSEAS SECURITY ADMINISTRATION	
		<input checked="" type="checkbox"/> e. ADMINISTRATIVE CONTRACTING OFFICER	
		<input checked="" type="checkbox"/> f. OTHERS AS NECESSARY	

CONTINUATION SHEET FOR BLOCK 13.

**LOCKHEED MARTIN SERVICES INC 2339 ROUTE 70 WEST FLOOR 3W, CHERRY HILL, NJ 08002-3315
CAGE CODE 77609 CONTRACT# HSHQDC-08-D-00017 HQHSDC-07-J-00138**

Reference Item 10e (1): Access to all Sensitive Compartmented Information (SCI) will be at DHS facilities only. For the purposes of this contract, the contractor is not authorized to process and/or store any classified information at contractor locations.

- a. All SCI will be handled in accordance with special security requirements, which will be furnished by the designated responsible special security office (SSO).
- b. SCI will not be released to contractor employees without specific release approval of the originator of the material as outlined in governing directives; based on prior approval and certification of "need-to-know" by the designated contractor.
- c. All Contractor personnel requiring access to SCI as part of this contract effort must be approved and indoctrinated by DHS. Requests for Access will be submitted by the government project manager who can validate the justification for access.
- d. Inquiries pertaining to classification guidance on SCI will be directed to the Special Security Officer (SSO).
- e. SCI furnished in support of this contract remains the property of the Department of Homeland Security (DHS), agency, or component originator. Upon completion or cancellation of the contract, SCI furnished will be returned to the direct custody of the supporting SSO, or destroyed IAW instructions outlined by the Contract Officer.
- f. Visits by contractor employees will only be certified by DHS when such visits are conducted as part of the contract effort.

Ref Item 10j: "Contractors shall control and safeguard FOUO in accordance with DHS Directive (MD 11042.1) "Safeguarding Sensitive but Unclassified (For Official Use Only) Information," dated Jan 6, 2005. DHS contractors must sign a special Non-Disclosure Agreement before receiving access to FOUO information. Contractors with questions on handling DHS FOUO shall contact DHS OS ASD at (202) 447-5341."

Ref. Item 11a. Contract performance for all SCI work is restricted to DHS Government buildings located in and around the metropolitan area of Washington, D.C., and at other locations in the metropolitan area of Wash DC. All contractor personnel must be U.S. citizens, have been granted a final security clearance by the U.S. Government, have been approved as meeting suitability criteria by DHS CSO, and have been indoctrinated by a Non Disclosure Agreement, Standard Form 312 for this specific program prior to being given any access to such information released or generated under this contract. Immigrant aliens, personnel cleared on an interim basis, or personnel holding contractor granted CONFIDENTIAL clearances, are not eligible for access to classified information released or generated under this contract without the express permission of the CSO through the DHS Personnel Division (DHS/PSD). The contractor and the Contracting Officer Technical Representative or other delegated representative will revalidate all SCI staffing requirements under the contract with the CSO annually or when a revised DD Form 254 is issued, whichever is sooner. SCI WILL NOT BE RELEASED TO PUBLIC.

DEPARTMENT OF DEFENSE CONTRACT SECURITY CLASSIFICATION SPECIFICATION		1. CLEARANCE AND SAFEGUARDING	
(The requirements of the DoD Industrial Security Manual apply to all aspects of this effort)		a. FACILITY CLEARANCE REQUIRED TOP SECRET	
		b. LEVEL OF SAFEGUARDING REQUIRED NONE	
THIS SPECIFICATION IS FOR: (X and complete as applicable)		3. THIS SPECIFICATION IS: (X and complete as applicable)	
PRIME CONTRACT NUMBER HSHQDC-08-D-00017 HQHSDC-08-J-00138		a. ORIGINAL (Complete date in all cases) Date (YYMMDD) 20071210	
SUB CONTRACT NUMBER 100-0000		b. REVISED (Supersedes all previous specs) Revision No 2 Date (YYMMDD) 20090113	
MODIFICATION OR OTHER NUMBER		c. FINAL (Complete item 3 in all cases) Date (YYMMDD)	
4. THIS A FINAL DD FORM 2547? <input type="checkbox"/> YES <input checked="" type="checkbox"/> NO. If Yes complete the following			
Classified information derived or generated under HSHQDC-08-D-00017 HQHSDC 07-J-00739 (Preceding Contract Number) is transferred to this follow-on contract			
5. THIS A FINAL DD FORM 2547? <input type="checkbox"/> YES <input checked="" type="checkbox"/> NO. If Yes complete the following			
6. Release to a contractor's request dated _____ retention of the identified classified material is authorized for the period of _____			
7. PRIME CONTRACTOR (Include Commercial and Government Entity (CAGE) Code)			
NAME, ADDRESS, AND ZIP CODE LOCKHEED MARTIN SERVICES, INC 100 ROUTE 75 WEST MURKYS HILL NJ 08002 3315		b. CAGE CODE 77609	c. COGNIZANT SECURITY OFFICE (Name, Address, and Zip Code) DEFENSE SECURITY SERVICE 307 FELLOWSHIP ROAD STE 115 MT. LAUREL, NJ 08054-1233
SUB CONTRACTOR		b. CAGE CODE	c. COGNIZANT SECURITY OFFICES (Name, Address, and Zip Code)
(b) (4)		1U305	DEFENSE SECURITY SERVICE 14428 ALBEMARLE POINT PLACE, STE 140 CHANTILLY, VA 20151
8. NATURAL PERFORMANCE		b. CAGE CODE	c. COGNIZANT SECURITY OFFICE (Name, Address, and Zip Code)
Department of Homeland Security (DHS) various projects with in the Washington, DC metropolitan area			
9. GENERAL IDENTIFICATION OF THIS PROCUREMENT			
Provide IT Operations & Maintenance technical support to Lockheed Martin in support of the IT-NOVA DHS Eagle Task Order. This is in response to Lockheed Martin's requirements to provide support to IT Operations Maintenance and COOP at the DHS headquarters and Components directly supported by the DHS OCIO.			
10. THIS CONTRACT WILL REQUIRE ACCESS TO:			
CLASSIFIED INFORMATION (COMSEC)	YES <input checked="" type="checkbox"/>	NO <input type="checkbox"/>	11. IN PERFORMING THIS CONTRACT, THE CONTRACTOR WILL:
SECRET DATA	<input type="checkbox"/>	<input checked="" type="checkbox"/>	a. HAVE ACCESS TO CLASSIFIED INFORMATION ONLY AT ANOTHER CONTRACTOR'S FACILITY OR A GOVERNMENT ACTIVITY <input checked="" type="checkbox"/>
SECRET/CONTROL DESIGN INFORMATION	<input type="checkbox"/>	<input checked="" type="checkbox"/>	b. RECEIVE CLASSIFIED DOCUMENTS ONLY <input type="checkbox"/>
SECRET/CONTROL DESIGN DATA	<input type="checkbox"/>	<input checked="" type="checkbox"/>	c. RECEIVE AND GENERATE CLASSIFIED MATERIAL <input type="checkbox"/>
SECRET/CONTROL INFORMATION	<input type="checkbox"/>	<input checked="" type="checkbox"/>	d. FABRICATE, MODIFY OR STORE CLASSIFIED HARDWARE <input type="checkbox"/>
SECRET/CONTROL Information (SCI)	<input checked="" type="checkbox"/>	<input type="checkbox"/>	e. PERFORM SERVICES ONLY <input type="checkbox"/>
SECRET INFORMATION	<input type="checkbox"/>	<input checked="" type="checkbox"/>	f. HAVE ACCESS TO U.S. CLASSIFIED INFORMATION OUTSIDE THE U.S. PUERTO RICO, U.S. POSSESSIONS AND TRUST TERRITORIES <input type="checkbox"/>
SECRET INFORMATION	<input type="checkbox"/>	<input checked="" type="checkbox"/>	g. BE AUTHORIZED TO USE THE SERVICES OF DEFENSE TECHNICAL INFORMATION CENTER (DTIC) OR OTHER SECONDARY DISTRIBUTION CENTER <input type="checkbox"/>
SECRET INFORMATION	<input type="checkbox"/>	<input checked="" type="checkbox"/>	h. REQUIRE A COMSEC ACCOUNT <input type="checkbox"/>
SECRET INFORMATION	<input type="checkbox"/>	<input checked="" type="checkbox"/>	i. HAVE A TEMPEST REQUIREMENT <input type="checkbox"/>
SECRET GOVERNMENT INFORMATION	<input type="checkbox"/>	<input checked="" type="checkbox"/>	j. HAVE OPERATIONS SECURITY (OPSEC) REQUIREMENTS <input type="checkbox"/>
SECRET GOVERNMENT INFORMATION	<input type="checkbox"/>	<input checked="" type="checkbox"/>	k. BE AUTHORIZED TO USE THE DEFENSE COURIER SERVICE <input type="checkbox"/>
SECRET INFORMATION	<input checked="" type="checkbox"/>	<input type="checkbox"/>	l. OTHER (Specify) <input checked="" type="checkbox"/>
SECRET	<input type="checkbox"/>	<input checked="" type="checkbox"/>	

M 154 DEC 1999

PREVIOUS EDITION IS OBSOLETE

PUBLIC RELEASE. Any information (classified or unclassified) pertaining to this contract shall not be released for public dissemination except as provided by the Industrial Security Manual or unless it has been approved for public release by appropriate U.S. Government authority. Proposed public releases shall be submitted for approval prior to release. Direct Through (Specify) **NONE AUTHORIZED. SCI WILL NOT BE RELEASED TO PUBLIC.**

CONTRACTOR HAS OBTAINED AUTHORITY TO RELEASE FROM THE DEPARTMENT OF HOMELAND SECURITY. CONTRACTOR SHALL COORDINATE WITH THE COTR AND THE OFFICE OF SECURITY (ASD) ON ALL CHANGES TO THIS GUIDANCE. All requests for Freedom of Information and Security Review, Office of the Assistant Secretary of Defense (Public Affairs)* for review and disclosure from DoD User Agencies, requests for disclosure shall be submitted to that agency.

SECURITY GUIDANCE. The security classification guidance needed for this classified effort is identified below. If any difficulty is encountered in applying this guidance or if any other contributing factor indicates a need for changes in this guidance, the contractor is authorized and encouraged to provide unannounced changes to challenge the guidance or the classification assigned to any information or material furnished or generated under this contract. Do not submit any questions for interpretation of this guidance to the official identified below. Pending final decision, the information involved shall be protected and protected at the highest level of classification assigned or recommended. (Fill in as appropriate for the classified effort. Attach, or forward under separate correspondence, any documents/guides/extracts referenced herein. Add additional pages as needed to provide complete guidance.)

Ref. Item 10a: COMSEC Access will involve the installation, maintenance, or use of crypto-equipment, systems, or keying material. Access to COMSEC requires a final US Government Clearance. Disclosure to Subcontractor requires prior approval of DHS. The contractor upon award shall contact the DHS COMSEC Control Office if Record (COR) at Commercial (540) 542-1848, to receive current COMSEC guidance.

Ref. Item 10e (I). **Personnel:** All contractor personnel assigned to this contract shall possess security clearances issued by the Defense Security Service (DSS) commensurate with the level of required access to classified information that is directly in support of this contract. Immigrant aliens, personnel cleared on an interim basis, or personnel holding contractor generated Confidential clearances are not eligible for access to classified information released or generated under this contract. Contractor personnel who are specifically designated as requiring access to Sensitive Compartmented Information (SCI) must be eligible under the provisions of DCID 6/4 without exception. Personnel will be submitted for access by their DHS manager and verified by their Contract Technical Representative. If approved for access, they will receive an indoctrination briefing by DHS security staff prior to being granted access to SCI. All personnel security be handled for debriefing with the DHS SSO by calling (202) 282-8643. Note 10e (I) and 11a. Access to all classified information (SCI) will be at DHS facilities only. For the purposes of this contract, the contractor is not authorized to possess and/or store any classified information at contractor locations.

Jose Salazar 1-9-9
**JOSE J. SALAZAR, DHS OFFICE OF SECURITY
 PROGRAM MANAGER INDUSTRIAL SECURITY
 (202) 447-5346**

14. **ADDITIONAL SECURITY REQUIREMENTS.** Requirements, in addition to ISM requirements, are established for this contract. (If Yes, Yes No. Attach to the pertinent contractual clauses in the contract document itself, or provide an appropriate statement which identifies the additional requirements. Provide a copy of the requirements to the cognizant security office. Use Item 13 if additional space is needed.)

15. **EXCEPTIONS.** Elements of this contract are outside the inspection responsibility of the cognizant security office. (If Yes, Yes No. Attach to the pertinent contractual clauses in the contract document itself, or provide an appropriate statement which identifies the additional requirements. Provide a copy of the requirements to the cognizant security office. Use Item 13 if additional space is needed.)

CONTRACTOR CONCURS AND APPROVES THE "NEED-TO-KNOW" AT THE SCI LEVEL
[Signature] 1/20/09. Clearances: Access to Intelligence information requires a final US Government clearance. Contracting requires prior approval of the GCA. Briefings: Special briefings and procedures are required.

16. **CERTIFICATION AND SIGNATURE.** Security requirements stated herein are complete and adequate for safeguarding the classified information to be created or generated under this classified effort. All questions shall be referred to the official named below.

a. NAME OF CERTIFYING OFFICIAL JOHN J. PINDER	b. TITLE FACILITY SECURITY OFFICER (HOF)	c. TELEPHONE (Include Area Code) (856) 486-5266
---	--	---

17. REQUIRED DISTRIBUTION <input checked="" type="checkbox"/> a. CONTRACTOR <input checked="" type="checkbox"/> b. SUBCONTRACTOR <input checked="" type="checkbox"/> c. COGNIZANT SECURITY OFFICE FOR PRIME AND SUBCONTRACTOR <input checked="" type="checkbox"/> d. U.S. ACTIVITY RESPONSIBLE FOR OVERSEAS SECURITY ADMINISTRATION <input checked="" type="checkbox"/> e. ADMINISTRATIVE CONTRACTING OFFICER <input checked="" type="checkbox"/> f. OTHERS AS NECESSARY	(Name of Contractor) TELEMAN SERVICES INC 100 WEST WASHINGTON ST WASHINGTON DC 20002
	<i>[Signature]</i> 28 JAN 2009 (Date)
	(Signature) (Date)
	(Signature) (Date)
	(Signature) (Date)
	(Signature) (Date)

CONTINUATION SHEET FOR BLOCK 13.

LOCKHEED MARTIN SERVICES INC 2339 ROUTE 70 WEST FLOOR 3W, CHERRY HILL, NJ 08002-3315
CAGE CODE: 77609 CONTRACT# HSHQDC-06-D-00017 HQHSDC-07-J-00138

Reference Item 10e (1): Access to all Sensitive Compartmented Information (SCI) will be at DHS facilities only. For the purposes of this contract, the contractor is not authorized to process and/or store any classified information at contractor locations.

All SCI will be handled in accordance with special security requirements, which will be furnished by the designated responsible special security office (SSO).

SCI will not be released to contractor employees without specific release approval of the originator of the material as outlined in governing directives; based on prior approval and certification of "need-to-know" by the designated contractor.

All Contractor personnel requiring access to SCI as part of this contract effort must be approved and indoctrinated by DHS. Requests for Access will be submitted by the government project manager who can validate the justification for access.

Inquiries pertaining to classification guidance on SCI will be directed to the Special Security Officer (SSO).

SCI furnished in support of this contract remains the property of the Department of Homeland Security (DHS), agency, or component originator. Upon completion or cancellation of the contract, SCI furnished will be returned to the direct custody of the supporting SSO, or destroyed IAW instructions outlined by the Contract Officer.

Visits by contractor employees will only be certified by DHS when such visits are conducted as part of the contract effort.

Ref Item 10j. "Contractors shall control and safeguard FOUO in accordance with DHS Directive (MD 11042.1) "Safeguarding Sensitive but Unclassified (For Official Use Only) Information," dated Jan 6, 2005. DHS contractors must sign a special Non-Disclosure Agreement before receiving access to FOUO information. Contractors with questions on obtaining DHS FOUO shall contact DHS OS ASD at (202) 447-5341."

Ref Item 11a. Contract performance for all SCI work is restricted to DHS Government buildings located in and around the metropolitan area of Washington, D.C., and at other locations in the metropolitan area of Wash DC. All contractor personnel must be U.S. citizens, have been granted a final security clearance by the U.S. Government, have been approved as meeting suitability criteria by DHS CSO, and have been indoctrinated by a Non Disclosure Agreement, DD Form 312 for this specific program prior to being given any access to such information released or generated under this contract. Immigrant aliens, personnel cleared on an interim basis, or personnel holding contractor granted CONFIDENTIAL clearances, are not eligible for access to classified information released or generated under this contract without the express permission of the CSO through the DHS Personnel Division (DHS/PSD). The contractor and the Contracting Officer Technical Representative or other delegated representative will revalidate all SCI staffing requirements under the contract with the CSO annually or when a revised DD Form 254 is issued, whichever is sooner.
SCI WILL NOT BE RELEASED TO PUBLIC.

DEPARTMENT OF DEFENSE CONTRACT SECURITY CLASSIFICATION SPECIFICATION		1 CLEARANCE AND SAFEGUARDING	
The requirements of the DoD Industrial Security Manual apply to all aspects of this effort.		a. FACILITY CLEARANCE REQUIRED TOP SECRET	
		b. LEVEL OF SAFEGUARDING REQUIRED NONE	
2. IDENTIFICATION IS FOR: (X and complete as applicable) a. MODIFICATION NUMBER HSHQDC-06-D-00017 HQHSDC-08-J-00138		3. THIS SPECIFICATION IS: (X and complete as applicable) a. ORIGINAL (Complete date in all cases) Date (YYMMDD) 30071210	
b. CONTRACT NUMBER P000082545		b. REVISED (Supersedes all previous specs) Revision No. Date (YYMMDD) 2 20090113	
c. SUPPLEMENTAL ORDER NUMBER Due Date (YYMMDD)		c. FINAL (Complete item 5 in all cases) Date (YYMMDD)	
4. DOES THIS FOLLOW-ON CONTRACT? <input checked="" type="checkbox"/> YES <input type="checkbox"/> NO. If Yes complete the following Classified material received or generated under HSHQDC-06-D-00017 HQHSDC-07-J-00739 (Preceding Contract Number) is transferred to this follow-on contract.			
5. IS THIS A FINAL DD FORM 2547? <input type="checkbox"/> YES <input checked="" type="checkbox"/> NO. If Yes complete the following In response to the contractor's request dated _____, retention of the identified classified material is authorized for the period of _____.			
6. CONTRACTOR (Include Commercial and Government Entity (CAGE) Code) a. NAME, ADDRESS AND ZIP CODE LOCKHEED MARTIN SERVICES, INC 2349 ROUTE 10 WEST HERRY HILL, NJ 08002-3315		b. CAGE CODE 77609	
c. COGNIZANT SECURITY OFFICE (Name, Address, and Zip Code) DEFENSE SECURITY SERVICE 307 FELLOWSHIP ROAD STE 115 MT. LAUREL, NJ 08054-1233			
7. SUBCONTRACTOR a. NAME, ADDRESS AND ZIP CODE (b) (4)		b. CAGE CODE USDF4	
c. COGNIZANT SECURITY OFFICES (Name, Address, and Zip Code) DEFENSE SECURITY SERVICE P.O. BOX 254036 PATRICK AFB, FL 32925-0036			
8. ACTUAL PERFORMANCE a. DESCRIPTION Department of Homeland Security (DHS) various locations within the Washington, DC metropolitan area.		b. CAGE CODE c. COGNIZANT SECURITY OFFICE (Name, Address, and Zip Code)	
9. GENERAL IDENTIFICATION OF THIS PROCUREMENT DHS Provide IT Operations & Maintenance technical support to Lockheed Martin in support of the IT-NOVA DHS Eagle Task Center. This is in response to Lockheed Martin's requirements to provide support to IT Operations Maintenance and COOP for the DHS Headquarters and Components directly supported by the DHS OCIO.			
10. THIS CONTRACT WILL REQUIRE ACCESS TO:		11. IN PERFORMING THIS CONTRACT, THE CONTRACTOR WILL:	
<input checked="" type="checkbox"/> CLASSIFICATION SECURITY (COMSEC)	<input checked="" type="checkbox"/> YES <input type="checkbox"/> NO	<input checked="" type="checkbox"/> a. HAVE ACCESS TO CLASSIFIED INFORMATION ONLY AT ANOTHER CONTRACTOR'S FACILITY OR A GOVERNMENT ACTIVITY	<input checked="" type="checkbox"/> YES <input type="checkbox"/> NO
<input type="checkbox"/> UNCLASSIFIED DATA	<input type="checkbox"/> YES <input checked="" type="checkbox"/> NO	<input type="checkbox"/> b. RECEIVE CLASSIFIED DOCUMENTS ONLY	<input type="checkbox"/> YES <input checked="" type="checkbox"/> NO
<input type="checkbox"/> UNCLASSIFIED PARACALON DESIGN INFORMATION	<input type="checkbox"/> YES <input checked="" type="checkbox"/> NO	<input type="checkbox"/> c. RECEIVE AND GENERATE CLASSIFIED MATERIAL	<input type="checkbox"/> YES <input checked="" type="checkbox"/> NO
<input type="checkbox"/> EXPORT RESTRICTED DATA	<input type="checkbox"/> YES <input checked="" type="checkbox"/> NO	<input type="checkbox"/> d. FABRICATE, MODIFY, OR STORE CLASSIFIED HARDWARE	<input type="checkbox"/> YES <input checked="" type="checkbox"/> NO
<input type="checkbox"/> RESTRICTED INFORMATION	<input type="checkbox"/> YES <input checked="" type="checkbox"/> NO	<input type="checkbox"/> e. PERFORM SERVICES ONLY	<input type="checkbox"/> YES <input checked="" type="checkbox"/> NO
<input checked="" type="checkbox"/> UNCLASSIFIED INFORMATION (SCI)	<input checked="" type="checkbox"/> YES <input type="checkbox"/> NO	<input type="checkbox"/> f. HAVE ACCESS TO U.S. CLASSIFIED INFORMATION OUTSIDE THE U.S., PUERTO RICO, U.S. POSSESSIONS AND TRUST TERRITORIES	<input type="checkbox"/> YES <input checked="" type="checkbox"/> NO
<input type="checkbox"/> UNCLASSIFIED	<input type="checkbox"/> YES <input checked="" type="checkbox"/> NO	<input type="checkbox"/> g. BE AUTHORIZED TO USE THE SERVICES OF DEFENSE TECHNICAL INFORMATION CENTER (DTIC) OR OTHER SECONDARY DISTRIBUTION CENTER	<input type="checkbox"/> YES <input checked="" type="checkbox"/> NO
<input type="checkbox"/> UNCLASSIFIED INFORMATION	<input type="checkbox"/> YES <input checked="" type="checkbox"/> NO	<input type="checkbox"/> h. REQUIRE A COMSEC ACCOUNT	<input type="checkbox"/> YES <input checked="" type="checkbox"/> NO
<input type="checkbox"/> UNCLASSIFIED INFORMATION	<input type="checkbox"/> YES <input checked="" type="checkbox"/> NO	<input type="checkbox"/> i. HAVE A TEMPEST REQUIREMENT	<input type="checkbox"/> YES <input checked="" type="checkbox"/> NO
<input type="checkbox"/> UNCLASSIFIED INFORMATION	<input type="checkbox"/> YES <input checked="" type="checkbox"/> NO	<input type="checkbox"/> j. HAVE OPERATIONS SECURITY (OPSEC) REQUIREMENTS	<input type="checkbox"/> YES <input checked="" type="checkbox"/> NO
<input type="checkbox"/> UNCLASSIFIED INFORMATION	<input type="checkbox"/> YES <input checked="" type="checkbox"/> NO	<input type="checkbox"/> k. BE AUTHORIZED TO USE THE DEFENSE COURIER SERVICE	<input type="checkbox"/> YES <input checked="" type="checkbox"/> NO
<input type="checkbox"/> UNCLASSIFIED	<input type="checkbox"/> YES <input checked="" type="checkbox"/> NO	<input type="checkbox"/> l. OTHER (Specify):	<input type="checkbox"/> YES <input checked="" type="checkbox"/> NO

DD FORM 254 DE 1999

PREVIOUS EDITION IS OBSOLETE

PUBLIC RELEASE. Any information (classified or unclassified) pertaining to this contract shall not be released for public dissemination except as provided by the Defense Security Manual or unless it has been approved for public release by appropriate U.S. Government authority. Proposed public releases shall be submitted for approval prior to release Direct Through (Specify) **NONE AUTHORIZED. SCI WILL NOT BE RELEASED TO PUBLIC.**

UNLESS CONTRACTOR HAS OBTAINED AUTHORITY TO RELEASE FROM THE DEPARTMENT OF HOMELAND SECURITY, CONTRACTOR SHALL COORDINATE WITH THE COTR AND THE OFFICE OF SECURITY (ASD) ON ALL CHANGES TO THIS GUIDANCE. The Directorate for Freedom of Information and Security Review, Office of the Assistant Secretary of Defense (Public Affairs)* for review. *The use of non-DoD user Agencies' requests for disclosure shall be submitted to that agency.

SECURITY GUIDANCE. The security classification guidance needed for this classified effort is identified below. If any difficulty is encountered in applying the guidance or if any other contributing factor indicates a need for changes in this guidance, the contractor is authorized and encouraged to provide recommended changes, to challenge the guidance or the classification assigned to any information or material furnished or generated under this contract, and to submit any questions for interpretation of this guidance to the official identified below. Pending final decision, the information involved shall be classified and protected at the highest level of classification assigned or recommended. (Fill in as appropriate for the classified effort. Attach or forward under separate correspondence, any documents/guides/extracts referenced herein. Add additional pages as needed to provide complete guidance.)

Ref. Item 10a: COMSEC Access will involve the installation, maintenance, or use of crypto-equipment, systems, or keying material. Access to COMSEC requires a final US Government Clearance. Disclosure to Subcontractor requires prior approval of DHS. The contractor upon award shall contact the DHS COMSEC Control Office of Record (COR) at Commercial (540) 542-3848, to receive current COMSEC guidance.

Ref. Item 10e (1). Personnel: All contractor personnel assigned to this contract shall possess security clearances issued by the Defense Security Service (DSS) commensurate with the level of required access to classified information that is directly in support of this contract. Immigrant aliens, personnel cleared on an interim basis, or personnel holding contractor-generated Confidential clearances are not eligible for access to classified information released or generated under this contract. Contractor personnel who are specifically designated as requiring access to Sensitive Compartmented Information (SCI) must be eligible under the provisions of DCID 6/4 without exception. Personnel will be submitted for review by their DHS manager and verified by their Contract Technical Representative. If approved for access, they will receive an indoctrination briefing by DHS security staff prior to being granted access to SCI. All personnel security be scheduled for debriefing with the DHS SSO by calling (202) 282-8643. **Note 10e (1) and 11a.** Access to all classified information (SCI) will be at DHS facilities only. For the purposes of this contract, the contractor is not authorized to process and/or store any classified information at contractor locations.

Jose Salazar 1-9-9
JOSE J. SALAZAR, DHS OFFICE OF SECURITY
PROGRAM MANAGER INDUSTRIAL SECURITY
 (202) 447-5346

ADDITIONAL SECURITY REQUIREMENTS. Requirements, in addition to ISM requirements, are established for this contract (If Yes, Yes No identify the pertinent contractual clauses in the contract document itself, or provide an appropriate statement which identifies the additional requirements. Provide a copy of the requirements to the cognizant security office. Use item 13 if additional space is needed.)

INSPECTIONS. Elements of this contract are outside the inspection responsibility of the cognizant security office. (Yes, specify and identify specific areas or elements carved out and the activity responsible for inspections. Use item 13 if additional space is needed.) Yes No

DHS/OS/SPD CONCURS AND APPROVES THE "NEED-TO-KNOW" AT THE SCI LEVEL"

2/10/09 **Clearances:** Access to intelligence information requires a final US Government clearance **Access to GCA requires prior approval of the GCA. Briefings:** Special briefings and procedures are required.

CLASSIFICATION AND SIGNATURE. Security requirements stated herein are complete and adequate for safeguarding the classified information to be processed and generated under this classified effort. All questions shall be referred to the official named below.

a. NAME OF CERTIFYING OFFICIAL EDWARD J. PINDER	b. TITLE FACILITY SECURITY OFFICER (HOF)	c. TELEPHONE (Include Area Code) (856) 486-5266
---	--	---

(Include SSN, include Zip Code) SHIELD/MARTIN SERVICES, INC 100 HILL TO WEST MILL HILL, NJ 08902 <i>Edward Pinder 28 JAN 2009</i> J. J. M. 25418A(K) DEC 1999	BY REQUIRED DISTRIBUTION	
	<input checked="" type="checkbox"/>	a. CONTRACTOR
	<input checked="" type="checkbox"/>	b. SUBCONTRACTOR
	<input checked="" type="checkbox"/>	c. COGNIZANT SECURITY OFFICE FOR PRIME AND SUBCONTRACTOR
	<input checked="" type="checkbox"/>	d. U.S. ACTIVITY RESPONSIBLE FOR OVERSEAS SECURITY ADMINISTRATION
	<input checked="" type="checkbox"/>	e. ADMINISTRATIVE CONTRACTING OFFICER
<input checked="" type="checkbox"/>	f. OTHERS AS NECESSARY	

CONTINUATION SHEET FOR BLOCK 13.

LOCKHEED MARTIN SERVICES INC 2339 ROUTE 70 WEST FLOOR 3W, CHERRY HILL, NJ 08002-3315
PAGE CODE 77609 CONTRACT# HSHQDC-08-D-00017 HQHSDC-07-J-00138

Reference Item 10e (1): Access to all Sensitive Compartmented Information (SCI) will be at DHS facilities only. For the purposes of this contract, the contractor is not authorized to process and/or store any classified information at contractor locations.

a. All SCI will be handled in accordance with special security requirements, which will be furnished by the designated responsible special security office (SSO).

b. SCI will not be released to contractor employees without specific release approval of the originator of the material contained in governing directives, based on prior approval and certification of "need-to-know" by the designated contractor.

c. All Contractor personnel requiring access to SCI as part of this contract effort must be approved and indoctrinated by DHS. Requests for Access will be submitted by the government project manager who can validate the justification for access.

d. Inquiries pertaining to classification guidance on SCI will be directed to the Special Security Officer (SSO).

e. SCI furnished in support of this contract remains the property of the Department of Homeland Security (DHS), agency or component originator. Upon completion or cancellation of the contract, SCI furnished will be returned to the direct custody of the supporting SSO, or destroyed IAW instructions outlined by the Contract Officer.

f. Visits by contractor employees will only be certified by DHS when such visits are conducted as part of the contract effort.

Ref. Item 10j: "Contractors shall control and safeguard FOUO in accordance with DHS Directive (MD 11042.1) "Safeguarding Sensitive but Unclassified (For Official Use Only) Information," dated Jan 6, 2005. DHS contractors must sign a special Non-Disclosure Agreement before receiving access to FOUO information. Contractors with questions on handling DHS FOUO shall contact DHS OS ASD at (202) 447-5341."

Ref. Item 11a: Contract performance for all SCI work is restricted to DHS Government buildings located in and around the metropolitan area of Washington, D.C., and at other locations in the metropolitan area of Wash DC. All contractor personnel must be U.S. citizens, have been granted a final security clearance by the U.S. Government, have been approved as meeting suitability criteria by DHS CSO, and have been indoctrinated by a Non Disclosure Agreement, Standard Form 312 for this specific program prior to being given any access to such information released or generated under this contract. Immigrant aliens, personnel cleared on an interim basis, or personnel holding contractor granted CONFIDENTIAL clearances, are not eligible for access to classified information released or generated under this contract without the express permission of the CSO through the DHS Personnel Division (DHS/PSD). The contractor and the Contracting Officer Technical Representative or other delegated representative will revalidate all SCI staffing requirements under the contract with the CSO annually or when a revised DD Form 254 is issued, whichever is sooner. **SCI WILL NOT BE RELEASED TO PUBLIC.**

DEPARTMENT OF DEFENSE CONTRACT SECURITY CLASSIFICATION SPECIFICATION		1. CLEARANCE AND SAFEGUARDING	
(The requirements of the DoD Industrial Security Manual apply to all aspects of this effort)		a. FACILITY CLEARANCE REQUIRED SECRET	
		b. LEVEL OF SAFEGUARDING REQUIRED N/A	
2. THIS SPECIFICATION IS FOR: (X and complete as applicable)		3. THIS SPECIFICATION IS: (X and complete as applicable)	
a. PRIME CONTRACT NUMBER HSHQDC-06-D-00017 HQHSDC-08-J-00138		a. ORIGINAL (Complete date in all cases) Date: (YYMMDD) 20071210	
b. MODIFICATION OR OTHER NUMBER 16012253		b. REVISED (Supersedes all previous specs) Revision No. 2 Date: (YYMMDD) 20090113	
c. DATE (YYMMDD)		c. FINAL (Complete item 3 in all cases) Date: (YYMMDD)	
4. IS THIS A FOLLOW-ON CONTRACT? <input checked="" type="checkbox"/> YES <input type="checkbox"/> NO. If Yes complete the following Classified material received or generated under <u>HSHQDC-06-D-00017 HQHSDC-07-J-00732</u> (Preceding Contract Number) is transferred to this follow-on contract.			
5. IS THIS A FINAL DD FORM 2547 <input type="checkbox"/> YES <input checked="" type="checkbox"/> NO. If Yes complete the following In response to the contractor's request dated _____, retention of the identified classified material is authorized for the period of _____.			
6. CONTRACTOR (Include Commercial and Government Entity) (CAGE Code)			
a. NAME, ADDRESS, AND ZIP CODE LOCKHEED MARTIN SERVICES, INC 3439 ROUTE 70 WEST CHERRY HILL, NJ 08002-3315		b. CAGE CODE 77609	
		c. COGNIZANT SECURITY OFFICE (Name, Address, and Zip Code) DEFENSE SECURITY SERVICE 307 FELLOWSHIP ROAD STE 115 MT. LAUREL, NJ 08054-1233	
7. SUBCONTRACTOR			
a. NAME, ADDRESS, AND ZIP CODE (b) (4)		b. CAGE CODE 0KDD5	
		c. COGNIZANT SECURITY OFFICES (Name, Address, and Zip Code) DEFENSE SECURITY SERVICE 938 ELKRIDGE LANDING ROAD, STE 310 LINTHICUM, MD 21090-2917	
8. ACTUAL PERFORMANCE			
a. LOCATION Department of Homeland Security (DHS) various locations within the Washington, DC metropolitan area.		b. CAGE CODE	
		c. COGNIZANT SECURITY OFFICE (Name, Address, and Zip Code)	
9. GENERAL IDENTIFICATION OF THIS PROCUREMENT (U) Provide IT Operations & Maintenance technical support to Lockheed Martin in support of the IT-NOVA DHS Eagle Peak Order. This is in response to Lockheed Martin's requirements to provide support to IT Operations Maintenance and COOP for the DHS Headquarters and Components directly supported by the DHS OCIO.			
10. THIS CONTRACT WILL REQUIRE ACCESS TO:			
1. COMMUNICATIONS SECURITY (COMSEC) INFORMATION	YES <input checked="" type="checkbox"/>	NO <input type="checkbox"/>	11. IN PERFORMING THIS CONTRACT, THE CONTRACTOR WILL:
2. RESTRICTED DATA	<input type="checkbox"/>	<input checked="" type="checkbox"/>	a. HAVE ACCESS TO CLASSIFIED INFORMATION ONLY AT ANOTHER CONTRACTOR'S FACILITY OR A GOVERNMENT ACTIVITY
3. CRITICAL NUCLEAR WEAPON DESIGN INFORMATION	<input type="checkbox"/>	<input checked="" type="checkbox"/>	b. RECEIVE CLASSIFIED DOCUMENTS ONLY
4. TEMPORARILY RESTRICTED DATA	<input type="checkbox"/>	<input checked="" type="checkbox"/>	c. RECEIVE AND GENERATE CLASSIFIED MATERIAL
5. CONFIDENTIAL INFORMATION	<input type="checkbox"/>	<input checked="" type="checkbox"/>	d. FABRICATE, MODIFY, OR STORE CLASSIFIED HARDWARE
6. SOURCE COMPARTMENTED INFORMATION (SCI)	<input type="checkbox"/>	<input checked="" type="checkbox"/>	e. PERFORM SERVICES ONLY
7. CONTROLLED DATA	<input checked="" type="checkbox"/>	<input type="checkbox"/>	f. HAVE ACCESS TO U.S. CLASSIFIED INFORMATION OUTSIDE THE U.S., PUERTO RICO, U.S. POSSESSIONS AND TRUST TERRITORIES
8. SPECIAL ACCESS INFORMATION	<input type="checkbox"/>	<input checked="" type="checkbox"/>	g. BE AUTHORIZED TO USE THE SERVICES OF DEFENSE TECHNICAL INFORMATION CENTER (DTIC) OR OTHER SECONDARY DISTRIBUTION CENTER
9. CAGE INFORMATION	<input type="checkbox"/>	<input checked="" type="checkbox"/>	h. REQUIRE A COMSEC ACCOUNT
10. NON-GOVERNMENT INFORMATION	<input type="checkbox"/>	<input checked="" type="checkbox"/>	i. HAVE A TEMPEST REQUIREMENT
11. LIMITED DISSEMINATION INFORMATION	<input type="checkbox"/>	<input checked="" type="checkbox"/>	j. HAVE OPERATIONS SECURITY (OPSEC) REQUIREMENTS
12. OFFICIAL SECURITY INFORMATION	<input checked="" type="checkbox"/>	<input type="checkbox"/>	k. BE AUTHORIZED TO USE THE DEFENSE COURIER SERVICE
13. OTHER (Specify)	<input type="checkbox"/>	<input checked="" type="checkbox"/>	l. OTHER (Specify)

FORM 254 DEC 1999

PREVIOUS EDITION IS OBSOLETE.

13. PUBLIC RELEASE. Any information (classified or unclassified) pertaining to this contract shall not be released for public dissemination except as provided by the Industrial Security Manual or unless it has been approved for public release by appropriate U.S. Government authority. Proposed public releases shall be submitted for approval prior to release Direct Through (Specify) **NONE AUTHORIZED.**
UNLESS CONTRACTOR HAS OBTAINED AUTHORITY TO RELEASE FROM THE DEPARTMENT OF HOMELAND SECURITY, CONTRACTOR SHALL COORDINATE WITH THE COTR AND THE OFFICE OF SECURITY (ASD) ON ALL CHANGES TO THIS GUIDANCE.
 In the Directorate for Freedom of Information and Security Review, Office of the Assistant Secretary of Defense (Public Affairs)* for review. In the case of an O&D User Agency, requests for disclosure shall be submitted to that agency.

14. SECURITY GUIDANCE. The security classification guidance needed for this classified effort is identified below. If any difficulty is encountered in applying this guidance or if any other contributing factor indicates a need for changes in this guidance, the contractor is authorized and encouraged to provide recommended changes; to challenge the guidance or the classification assigned to any information or material furnished or generated under this contract; and to submit any questions for interpretation of this guidance to the official identified below. Pending final decision, the information involved shall be treated and protected at the highest level of classification assigned or recommended. (Fill in as appropriate for the classified effort. Attach, or forward under separate correspondence, any documents/guides/extracts referenced herein. Add additional pages as needed to provide complete guidance.)

Ref. Item 10a: COMSEC Access will involve the installation, maintenance, or use of crypto-equipment, systems, or keying material. Access to COMSEC requires a final US Government Clearance. Disclosure to Subcontractor requires prior approval of DHS. The contractor upon award shall contact the DHS COMSEC Control Office if Record (COR) at Commercial (540) 542-3848, to receive current COMSEC guidance.

Ref. Item 10e (2). Personnel: All contractor personnel requiring access to non-SCI Information must be: U.S. Citizens; have been granted a FINAL SECRET security clearance by the U.S. Government, prior to being given any access to such information released or generated under this contract. Immigrant aliens, personnel cleared on an interim basis or personnel holding contractor granted CONFIDENTIAL clearances are not eligible for access to information under this contract. Non-SCI Information associated with this contract shall not be released to subcontractors without the permission of the DHS CSO. Note 10e (1) and 11a. Access to all classified information (SCI) will be at DHS facilities only. For the purposes of this contract, the contractor is not authorized to process and/or store any classified information at contractor locations.

Jose Salazar 1-9-9
 JOSE J. SALAZAR, DHS OFFICE OF SECURITY
 PROGRAM MANAGER INDUSTRIAL SECURITY
 (202) 447-5346

14. ADDITIONAL SECURITY REQUIREMENTS. Requirements, in addition to ISM requirements, are established for this contract. (If Yes, Yes No, identify the pertinent contractual clauses in the contract document itself, or provide an appropriate statement which identifies the additional requirements. Provide a copy of the requirements to the cognizant security office. Use item 13 if additional space is needed.)

15. INSPECTIONS. Elements of this contract are outside the inspection responsibility of the cognizant security office Yes No. (Yes, specify and identify specific areas or elements covered and the security responsible for inspections. Use item 13 if additional space is needed.)

16. CERTIFICATION AND SIGNATURE. Security requirements stated herein are complete and adequate for safeguarding the classified information to be released or generated under this classified effort. All questions shall be referred to the official named below.

a. NAME OF CERTIFYING OFFICIAL EDWARD J. HENDER	b. TITLE FACILITY SECURITY OFFICER (HOF)	c. TELEPHONE (Include Area Code) (856) 486-5266
--	---	--

(Include Zip Code)
 EDWARD J. HENDER
 100 ROUTE 70 WEST
 HERRY HILL, NJ 08002

SIGNATURE
Edward J. Hender 28 JAN 2009

17. REQUIRED DISTRIBUTION	
<input checked="" type="checkbox"/>	a. CONTRACTOR
<input checked="" type="checkbox"/>	b. SUBCONTRACTOR
<input checked="" type="checkbox"/>	c. COGNIZANT SECURITY OFFICE FOR PRIME AND SUBCONTRACTOR
<input type="checkbox"/>	d. U.S. AGENCY RESPONSIBLE FOR OVERSEAS SECURITY ADMINISTRATION
<input type="checkbox"/>	e. ADMINISTRATIVE CONTRACTING OFFICER
<input checked="" type="checkbox"/>	f. OTHERS AS NECESSARY

FF FORM 2541B (ACK) DEC 1999

CONTINUATION SHEET FOR BLOCK 13.

LOCKHEED MARTIN SERVICES INC 2339 ROUTE 70 WEST FLOOR 3W, CHERRY HILL, NJ 08002-3315
CAGE CODE: 77609 CONTRACT# HSHQDC-06-D-00017 HQHSDC-07-J-00138
SUBCONTRACT#

Ref Item 10j: "Contractors shall control and safeguard FOUO in accordance with DHS Directive (MD 421) "Safeguarding Sensitive but Unclassified (For Official Use Only) Information," dated Jan 6, 2005. DHS contractors must sign a special Non-Disclosure Agreement before receiving access to FOUO information. Contractors with questions on handling DHS FOUO shall contact DHS OS ASD at (202) 447-5341."

Ref. Item 11a: Contract performance for all work is restricted to DHS Government buildings located in and around the metropolitan area of Washington, D.C., and at other locations in the metropolitan area of Wash DC. All contractor personnel must be U.S. citizens, have been granted a final security clearance by the U.S. Government, have been approved as meeting suitability criteria by DHS CSO, and have been indoctrinated by a Non Disclosure Agreement, Standard Form 312 for this specific program prior to being given any access to such information released or generated under this contract. Immigrant aliens, personnel cleared on an interim basis, or personnel holding contractor granted CONFIDENTIAL clearances, are not eligible for access to classified information released or generated under this contract without the express permission of the CSO through the DHS Personnel Division (DHS/PSD). The contractor and the Contracting Officer Technical Representative or other delegated representative will revalidate all staffing requirements under the contract with the CSO annually or when a revised DD Form 254 is issued, whichever is sooner.

DEPARTMENT OF DEFENSE CONTRACT SECURITY CLASSIFICATION SPECIFICATION		1. CLEARANCE AND SAFEGUARDING		
<i>The requirements of the DoD Industrial Security Manual apply to all aspects of this effort.</i>		a. FACILITY CLEARANCE REQUIRED TOP SECRET		
		b. LEVEL OF SAFEGUARDING REQUIRED NONE		
2. THIS SPECIFICATION IS FOR: (X and complete as applicable)		3. THIS SPECIFICATION IS: (X and complete as applicable)		
a. ORIGINAL CONTRACT NUMBER HSHQDC-06-D-00017 HQHSDC-08-J-00138		<input type="checkbox"/> a. ORIGINAL (Complete date in all cases) Date (YYMMDD) 20080603		
b. MODIFIED CONTRACT NUMBER 47032243		<input checked="" type="checkbox"/> b. REVISED (Supersedes all previous specs) Revision No. 2 Date (YYMMDD) 20090112		
c. MODIFICATION OR OTHER NUMBER _____		<input type="checkbox"/> c. FINAL (Complete Item 3 in all cases) Date (YYMMDD) _____		
4. IS THIS A FOLLOW-ON CONTRACT? <input checked="" type="checkbox"/> YES <input type="checkbox"/> NO. If Yes complete the following: Classified material received or generated under HSHQDC-06-D-00017 HQHSDC-07-J-00739 (Preceding Contract Number) is transferred to this follow-on contract.				
5. IS THIS A FINAL DD FORM 254? <input type="checkbox"/> YES <input checked="" type="checkbox"/> NO. If Yes complete the following: In response to the contractor's request dated _____, retention of the identified classified material is authorized for the period of _____.				
6. CONTRACTOR (Include Commercial and Government Entity (CAGE) Code)				
a. NAME, ADDRESS, AND ZIP CODE LOCKHEED MARTIN SERVICES, INC 2339 ROUTE 70 WEST CHERRY HILL, NJ 08002 3315		b. CAGE CODE 77609		
		c. COORDINANT SECURITY OFFICE (Name, Address, and Zip Code) DEFENSE SECURITY SERVICE 307 FELLOWSHIP ROAD STE 115 MT. LAUREL, NJ 08054-1233		
7. SUBCONTRACTOR				
a. NAME, ADDRESS, AND ZIP CODE (b) (4)		b. CAGE CODE 3MAD5		
		c. COORDINANT SECURITY OFFICES (Name, Address, and Zip Code) DEFENSE SECURITY SERVICE 938 ELKRIDGE LANDING ROAD, STE 310 LINTHICUM, MD 21090-2917		
8. ACTUAL PERFORMANCE				
a. LOCATION Department of Homeland Security (DHS) various locations within the Washington, DC metropolitan area.		b. CAGE CODE _____		
		c. COORDINANT SECURITY OFFICE (Name, Address, and Zip Code) _____		
9. GENERAL IDENTIFICATION OF THIS PROCUREMENT (a) Provide IT Operations & Maintenance technical support to Lockheed Martin in support of the IT-NOVA DHS Eagle Task Order. This is in response to Lockheed Martin's requirements to provide support to IT Operations Maintenance and COOP for the DHS Headquarters and Components directly supported by the DHS OCIO.				
10. THIS CONTRACT WILL REQUIRE ACCESS TO:				
a. INFORMATION SECURITY (CONSEC) INFORMATION		YES <input checked="" type="checkbox"/> NO <input type="checkbox"/>	11. IN PERFORMING THIS CONTRACT, THE CONTRACTOR WILL:	
b. RESTRICTED DATA		YES <input type="checkbox"/> NO <input checked="" type="checkbox"/>	a. HAVE ACCESS TO CLASSIFIED INFORMATION ONLY AT ANOTHER CONTRACTOR'S FACILITY OR A GOVERNMENT ACTIVITY	
c. UNCLASSIFIED WEAPON DESIGN INFORMATION		YES <input type="checkbox"/> NO <input checked="" type="checkbox"/>	b. RECEIVE CLASSIFIED DOCUMENTS ONLY	
d. UNCLASSIFIED RESTRICTED DATA		YES <input type="checkbox"/> NO <input checked="" type="checkbox"/>	c. RECEIVE AND GENERATE CLASSIFIED MATERIAL	
e. UNCLASSIFIED INFORMATION		YES <input checked="" type="checkbox"/> NO <input type="checkbox"/>	d. FABRICATE, MODIFY OR STORE CLASSIFIED HARDWARE	
f. UNCLASSIFIED INFORMATION (Security Compartmented Information (SCI))		YES <input checked="" type="checkbox"/> NO <input type="checkbox"/>	e. PERFORM SERVICES ONLY	
g. UNCLASSIFIED INFORMATION (SECRET)		YES <input type="checkbox"/> NO <input checked="" type="checkbox"/>	f. HAVE ACCESS TO U.S. CLASSIFIED INFORMATION OUTSIDE THE U.S., PUERTO RICO, U.S. POSSESSIONS AND TRUST TERRITORIES	
h. UNCLASSIFIED INFORMATION (CONFIDENTIAL)		YES <input type="checkbox"/> NO <input checked="" type="checkbox"/>	g. BE AUTHORIZED TO USE THE SERVICES OF DEFENSE TECHNICAL INFORMATION CENTER (DTIC) OR OTHER SECONDARY DISTRIBUTION CENTER	
i. UNCLASSIFIED INFORMATION (UNCLASSIFIED)		YES <input type="checkbox"/> NO <input checked="" type="checkbox"/>	h. REQUIRE A CONSEC ACCOUNT	
j. UNCLASSIFIED INFORMATION (UNCLASSIFIED)		YES <input type="checkbox"/> NO <input checked="" type="checkbox"/>	i. HAVE A TEMPEST REQUIREMENT	
k. UNCLASSIFIED INFORMATION (UNCLASSIFIED)		YES <input type="checkbox"/> NO <input checked="" type="checkbox"/>	j. HAVE OPERATIONS SECURITY (OPSEC) REQUIREMENTS	
l. UNCLASSIFIED INFORMATION (UNCLASSIFIED)		YES <input type="checkbox"/> NO <input checked="" type="checkbox"/>	k. BE AUTHORIZED TO USE THE DEFENSE COURIER SERVICE	
m. UNCLASSIFIED INFORMATION (UNCLASSIFIED)		YES <input type="checkbox"/> NO <input checked="" type="checkbox"/>	l. OTHER (Specify):	

DD FORM 254 DEC 1999

PREVIOUS EDITION IS OBSOLETE

PUBLIC RELEASE. Any information (classified or unclassified) pertaining to this contract shall not be released for public dissemination except as provided by the Industrial Security Manual or unless it has been approved for public release by appropriate U.S. Government authority. Proposed public releases shall be submitted for approval prior to release Direct Through (Specify) **NONE AUTHORIZED. SCI WILL NOT BE RELEASED TO PUBLIC.**

UNLESS CONTRACTOR HAS OBTAINED AUTHORITY TO RELEASE FROM THE DEPARTMENT OF HOMELAND SECURITY, CONTRACTOR SHALL COORDINATE WITH THE COTR AND THE OFFICE OF SECURITY (ASD) ON ALL CHANGES TO THIS GUIDANCE. The Directorate for Freedom of Information and Security Review, Office of the Assistant Secretary of Defense (Public Affairs) for review. In the case of non DoD User Agencies, requests for disclosure shall be submitted to that agency.

SECURITY GUIDANCE. The security classification guidance needed for this classified effort is identified below. If any difficulty is encountered in applying the guidance or if any other contributing factor indicates a need for changes in this guidance, the contractor is authorized and encouraged to provide unclassified changes to challenge the guidance or the classification assigned to any information or material furnished or generated under this contract, and to submit any questions for interpretation of this guidance to the official identified below. Pending final decision, the information involved shall be handled and protected at the highest level of classification assigned or recommended. (Fill in as appropriate for the classified effort. Attach, or forward under cover of correspondence, any documents/guides/extracts referenced herein. Add additional pages as needed to provide complete guidance.)

Ref. Item 19a: COMSEC Access will involve the installation, maintenance, or use of crypto-equipment, systems, or keying material. Access to COMSEC requires a final US Government Clearance. Disclosure to Subcontractor requires prior approval of DHS. The contractor upon award shall contact the DHS COMSEC Control Office if Record (COR) at Commercial (540) 542-3848, to receive current COMSEC guidance.

Ref. Item 10e (1). **Personnel:** All contractor personnel assigned to this contract shall possess security clearances issued by the Defense Security Service (DSS) commensurate with the level of required access to classified information that is directly in support of this contract. Immigrant aliens, personnel cleared on an interim basis, or personnel holding contractor-generated Confidential clearances are not eligible for access to classified information released or generated under this contract. Contractor personnel who are specifically designated as requiring access to Sensitive Compartmented Information (SCI) must be eligible under the provisions of DCID 6/4 without exception. Personnel will be submitted for access by their DHS manager and verified by their Contract Technical Representative. If approved for access, they will receive an indoctrination briefing by DHS security staff prior to being granted access to SCI. All personnel security be scheduled for debriefing with the DHS SSO by calling (202) 282-8643. **Note 10e (1) and 11a.** Access to all classified information (SCI) will be at DHS facilities only. For the purposes of this contract, the contractor is not authorized to access and/or store any classified information at contractor locations.

Jose Selva 1-9-9
JOSE J. ALAZAR, DHS OFFICE OF SECURITY
PROGRAM MANAGER INDUSTRIAL SECURITY
 (202) 447-3446

ADDITIONAL SECURITY REQUIREMENTS: Requirements, in addition to ISM requirements, are established for this contract. (If Yes, Yes No identify the pertinent contractual clauses in the contract document itself, or provide an appropriate statement which identifies the additional requirements. Provide a copy with requirements to the cognizant security office. Use item 13 if additional space is needed.)

INSPECTIONS: Elements of this contract are outside the inspection responsibility of the cognizant security office. (If Yes, Yes No identify the pertinent contractual clauses in the contract document itself, or provide an appropriate statement which identifies the additional requirements. Use item 13 if additional space is needed.)

DHS/OS/SSPD CONCURS AND APPROVES THE "NEED-TO-KNOW" AT THE SCI LEVEL
2/10/09 Clearances: Access to intelligence information requires a final US Government clearance. Contracting requires prior approval of the GCA. Briefings: Special briefings and procedures are required.

VERIFICATION AND SIGNATURE: Security requirements stated herein are complete and adequate for safeguarding the classified information to be used or generated under this classified effort. All questions shall be referred to the official named below.

a. NAME OF BRIEFING OFFICIAL LAWARD J. PINDER	b. TITLE FACILITY SECURITY OFFICER (HOF)	c. TELEPHONE (Include Area Code) (856) 486-5266
---	--	---

d. CONTRACTOR LOCKHEED MARTIN SERVICES, INC 1000 WILLOW WEST HENRY HILL, NJ 08002 <i>Laward Pinder 28 JAN 2009</i>	IF REQUIRED DISTRIBUTION <input checked="" type="checkbox"/> a. CONTRACTOR <input checked="" type="checkbox"/> b. SUBCONTRACTOR <input checked="" type="checkbox"/> c. COGNIZANT SECURITY OFFICE FOR PRIME AND SUBCONTRACTOR <input checked="" type="checkbox"/> d. U.S. ACTIVITY RESPONSIBLE FOR OVERSEAS SECURITY ADMINISTRATION <input checked="" type="checkbox"/> e. ADMINISTRATIVE CONTRACTING OFFICER <input checked="" type="checkbox"/> f. OTHERS AS NECESSARY
---	--

CONTINUATION SHEET FOR BLOCK 13.

**LOCKHEED MARTIN SERVICES INC 2339 ROUTE 70 WEST FLOOR 3W, CHERRY HILL, NJ 08002-3315
PAGE CODE: 77609 CONTRACT# HSHQDC-06-D-00017 HQHSDC-07-J-00138**

Reference Item 10e (1): Access to all Sensitive Compartmented Information (SCI) will be at DHS facilities only. For the purposes of this contract, the contractor is not authorized to process and/or store any classified information at contractor locations

a. All SCI will be handled in accordance with special security requirements, which will be furnished by the designated responsible special security office (SSO).

b. SCI will not be released to contractor employees without specific release approval of the originator of the material as outlined in governing directives; based on prior approval and certification of "need-to-know" by the designated contractor.

c. All Contractor personnel requiring access to SCI as part of this contract effort must be approved and indoctrinated by DHS. Requests for Access will be submitted by the government project manager who can validate the justification for access.

d. Inquiries pertaining to classification guidance on SCI will be directed to the Special Security Officer (SSO).

e. SCI furnished in support of this contract remains the property of the Department of Homeland Security (DHS), Agency, or component originator. Upon completion or cancellation of the contract, SCI furnished will be returned to the direct custody of the supporting SSO, or destroyed IAW instructions outlined by the Contract Officer.

f. Visits by contractor employees will only be certified by DHS when such visits are conducted as part of the contract effort.

Ref Item 10j: "Contractors shall control and safeguard FOUO in accordance with DHS Directive (MD 11042.1) "Safeguarding Sensitive but Unclassified (For Official Use Only) Information," dated Jan 6, 2005. DHS contractors must sign a special Non-Disclosure Agreement before receiving access to FOUO information. Contractors with questions on handling DHS FOUO shall contact DHS OS ASD at (202) 447-5341."

Ref. Item 11a. Contract performance for all SCI work is restricted to DHS Government buildings located in and around the metropolitan area of Washington, D.C., and at other locations in the metropolitan area of Wash DC. All contractor personnel must be U.S. citizens, have been granted a final security clearance by the U.S. Government, have been approved as meeting suitability criteria by DHS CSO, and have been indoctrinated by a Non Disclosure Agreement, standard Form 312 for this specific program prior to being given any access to such information released or generated under this contract. Immigrant aliens, personnel cleared on an interim basis, or personnel holding contractor granted CONFIDENTIAL clearances, are not eligible for access to classified information released or generated under this contract without the express permission of the CSO through the DHS Personnel Division (DHS/PSD). The contractor and the Contracting Officer Technical Representative or other delegated representative will revalidate all SCI staffing requirements under the contract with the CSO annually or when a revised DD Form 254 is issued, whichever is sooner.
SCI WILL NOT BE RELEASED TO PUBLIC.

DEPARTMENT OF DEFENSE CONTRACT SECURITY CLASSIFICATION SPECIFICATION				1. CLEARANCE AND SAFEGUARDING	
<i>(The requirements of the DoD Industrial Security Manual apply to all aspects of this effort)</i>				a. FACILITY CLEARANCE REQUIRED TOP SECRET	
				b. LEVEL OF SAFEGUARDING REQUIRED NONE	
2. THIS SPECIFICATION IS FOR: <i>(X and complete as applicable)</i>		3. THIS SPECIFICATION IS: <i>(X and complete as applicable)</i>			
<input checked="" type="checkbox"/> THIS CONTRACT NUMBER HSHQDC-06-D-00017 HQHSDC-08-J-00138		<input type="checkbox"/> a. ORIGINAL <i>(Complete date in all cases)</i>		Date (YYMMDD) 20081218	
<input type="checkbox"/> PRIOR CONTRACT NUMBER 00000364		<input checked="" type="checkbox"/> b. REVISED <i>(Supersedes all previous specs)</i>		Revision No 1 Date (YYMMDD) 20090113	
<input type="checkbox"/> MODIFICATION OR OTHER NUMBER 00000364		<input type="checkbox"/> c. FINAL <i>(Complete item 5 in all cases)</i>		Date (YYMMDD)	
4. IS THIS A FOLLOW-ON CONTRACT? <input checked="" type="checkbox"/> YES <input type="checkbox"/> NO <i>If Yes complete the following</i> Classified material received or generated under HSHQDC-06-D-00017 HQHSDC-07-J-00739 (Preceding Contract Number) is transferred to this follow-on contract.					
5. IS THIS A FINAL DD FORM 254? <input type="checkbox"/> YES <input checked="" type="checkbox"/> NO <i>If Yes complete the following</i> In response to the contractor's request dated _____, retention of the identified classified material is authorized for the period of _____.					
6. CONTRACTOR <i>(Include Commercial and Government Entity (CAGE) Code)</i>					
a. NAME, ADDRESS, AND ZIP CODE LOCKHEED MARTIN SERVICES, INC 2339 ROUTE 70 WEST CHERRY HILL, NJ 08002-3315		b. CAGE CODE 77609		c. COGNIZANT SECURITY OFFICE <i>(Name, Address, and Zip Code)</i> DEFENSE SECURITY SERVICE 307 FELLOWSHIP ROAD STE 115 MT. LAUREL, NJ 08054-1233	
7. SUBCONTRACTOR					
a. NAME, ADDRESS, AND ZIP CODE (b) (4)		b. CAGE CODE 3FKG0		c. COGNIZANT SECURITY OFFICES <i>(Name, Address, and Zip Code)</i> DEFENSE SECURITY SERVICE 495 SUMMER STREET, STE 300 BOSTON, MA 02210-2192	
8. CENTRAL PERFORMANCE					
a. LOCATION Department of Homeland Security (DHS) various locations within the Washington, DC metropolitan area		b. CAGE CODE		c. COGNIZANT SECURITY OFFICE <i>(Name, Address, and Zip Code)</i>	
9. CENTRAL IDENTIFICATION OF THIS PROCUREMENT (1) Provide IT Operations & Maintenance technical support to Lockheed Martin in support of the IT-NOVA DHS Eagle Task Order. This is in response to Lockheed Martin's requirements to provide support to IT Operations Maintenance and COOP for the DHS Headquarters and Components directly supported by the DHS OCIO.					
10. THIS CONTRACT WILL REQUIRE ACCESS TO:					
<input checked="" type="checkbox"/> COMMUNICATIONS SECURITY (COMSEC)		<input type="checkbox"/> YES <input checked="" type="checkbox"/> NO		11. IN PERFORMING THIS CONTRACT, THE CONTRACTOR WILL:	
<input type="checkbox"/> UNRESTRICTED DATA		<input type="checkbox"/> YES <input checked="" type="checkbox"/> NO		<input checked="" type="checkbox"/> a. HAVE ACCESS TO CLASSIFIED INFORMATION ONLY AT ANOTHER CONTRACTOR'S FACILITY OR A GOVERNMENT ACTIVITY	
<input type="checkbox"/> TECHNICAL NUCLEAR WEAPON DESIGN INFORMATION		<input type="checkbox"/> YES <input checked="" type="checkbox"/> NO		<input type="checkbox"/> b. RECEIVE CLASSIFIED DOCUMENTS ONLY	
<input type="checkbox"/> FINANCIAL RESTRICTED DATA		<input type="checkbox"/> YES <input checked="" type="checkbox"/> NO		<input type="checkbox"/> c. RECEIVE AND GENERATE CLASSIFIED MATERIAL	
<input type="checkbox"/> COMMERCIAL SERVICE INFORMATION		<input type="checkbox"/> YES <input checked="" type="checkbox"/> NO		<input type="checkbox"/> d. FABRICATE, MODIFY, OR STORE CLASSIFIED HARDWARE	
<input checked="" type="checkbox"/> SCIENTIFIC AND TECHNICAL INFORMATION (SCI)		<input type="checkbox"/> YES <input checked="" type="checkbox"/> NO		<input type="checkbox"/> e. PERFORM SERVICES ONLY	
<input type="checkbox"/> OTHER INFORMATION		<input type="checkbox"/> YES <input checked="" type="checkbox"/> NO		<input type="checkbox"/> f. HAVE ACCESS TO U.S. CLASSIFIED INFORMATION OUTSIDE THE U.S., PUERTO RICO, U.S. POSSESSIONS AND TRUST TERRITORIES	
<input type="checkbox"/> PERSONNEL INFORMATION		<input type="checkbox"/> YES <input checked="" type="checkbox"/> NO		<input type="checkbox"/> g. BE AUTHORIZED TO USE THE SERVICES OF DEFENSE TECHNICAL INFORMATION CENTER (DTIC) OR OTHER SECONDARY DISTRIBUTION CENTER	
<input type="checkbox"/> PERSONNEL INFORMATION		<input type="checkbox"/> YES <input checked="" type="checkbox"/> NO		<input type="checkbox"/> h. REQUIRE A COMSEC ACCOUNT	
<input type="checkbox"/> PERSONNEL INFORMATION		<input type="checkbox"/> YES <input checked="" type="checkbox"/> NO		<input type="checkbox"/> i. HAVE A TEMPEST REQUIREMENT	
<input type="checkbox"/> PERSONNEL INFORMATION		<input type="checkbox"/> YES <input checked="" type="checkbox"/> NO		<input type="checkbox"/> j. HAVE OPERATIONS SECURITY (OPSEC) REQUIREMENTS	
<input type="checkbox"/> PERSONNEL INFORMATION		<input type="checkbox"/> YES <input checked="" type="checkbox"/> NO		<input type="checkbox"/> k. BE AUTHORIZED TO USE THE DEFENSE COURIER SERVICE	
<input type="checkbox"/> PERSONNEL INFORMATION		<input type="checkbox"/> YES <input checked="" type="checkbox"/> NO		<input type="checkbox"/> l. OTHER <i>(Specify)</i>	

DD FORM 254 DEC 1999

PREVIOUS EDITION IS OBSOLETE.

13. PUBLIC RELEASE. Any information (classified or unclassified) pertaining to this contract shall not be released for public dissemination except as provided by the Industrial Security Manual or unless it has been approved for public release by appropriate U.S. Government authority. Proposed public releases shall be submitted for approval prior to release Direct Through (Specify) **NONE AUTHORIZED. SCI WILL NOT BE RELEASED TO PUBLIC.**

UNLESS CONTRACTOR HAS OBTAINED AUTHORITY TO RELEASE FROM THE DEPARTMENT OF HOMELAND SECURITY; CONTRACTOR SHALL COORDINATE WITH THE COTR AND THE OFFICE OF SECURITY (ASD) ON ALL CHANGES TO THIS GUIDANCE. The Directorate for Freedom of Information and Security Review, Office of the Assistant Secretary of Defense (Public Affairs) for review. In the case of DoD User Agencies, requests for disclosure shall be submitted to that agency.

14. SECURITY GUIDANCE. The security classification guidance needed for this classified effort is identified below. If any difficulty is encountered in applying this guidance or if any other contributing factor indicates a need for changes in this guidance, the contractor is authorized and encouraged to provide recommended changes, to challenge the guidance or the classification assigned to any information or material furnished or generated under this contract, and to submit any questions for interpretation of this guidance to the official identified below. Pending final decision, the information involved shall be handled and protected at the highest level of classification assigned or recommended. (Fill in as appropriate for the classified effort. Attach, or forward under separate correspondence, any documents/guides/extracts referenced herein. Add additional pages as needed to provide complete guidance.)

Ref. Item 10a: COMSEC Access will involve the installation, maintenance, or use of crypto-equipment, systems, or keying material. Access to COMSEC requires a final US Government Clearance. Disclosure to Subcontractor requires prior approval of DHS. The contractor upon award shall contact the DHS COMSEC Control Office if Record (COR) at commercial (540) 542-3848, to receive current COMSEC guidance.

Ref. Item 10e (1). Personnel: All contractor personnel assigned to this contract shall possess security clearances issued by the Defense Security Service (DSS) commensurate with the level of required access to classified information that is directly in support of this contract. Immigrant aliens, personnel cleared on an interim basis, or personnel holding contractor-generated Confidential clearances are not eligible for access to classified information released or generated under this contract. Contractor personnel who are specifically designated as requiring access to Sensitive Compartmented Information (SCI) must be eligible under the provisions of DCID 6/4 without exception. Personnel will be submitted for access by their DHS manager and verified by their Contract Technical Representative. If approved for access, they will receive an indoctrination briefing by DHS security staff prior to being granted access to SCI. All personnel security be scheduled for debriefing with the DHS SSO by calling (202) 282-8643. **Note 10e (1) and 11a.** Access to all classified information (SCI) will be at DHS facilities only. For the purposes of this contract, the contractor is not authorized to access and/or store any classified information at contractor locations.

Jose Salazar 1-9-9
JOSÉ J. SALAZAR, DHS OFFICE OF SECURITY
PROGRAM MANAGER INDUSTRIAL SECURITY
 (202) 447-5346

14. ADDITIONAL SECURITY REQUIREMENTS. Requirements in addition to ISM requirements, are established for this contract. (If Yes, Yes No identify the pertinent contractual clauses in the contract document itself, or provide an appropriate statement which identifies the additional requirements. Provide a copy of the requirements to the cognizant security office. Use Item 13 if additional space is needed.)

15. INSPECTIONS. Elements of this contract are outside the inspection responsibility of the cognizant security office. Yes No (Specify explaining identity specific areas or elements carved out and the activity responsible for inspections. Use Item 13 if additional space is needed.)

DHS/DSS/SPD CONCURS AND APPROVES THE "NEED-TO-KNOW" AT THE SCI LEVEL
2/10/09 Clearances: Access to Intelligence information requires a final US Government clearance. Contracting requires prior approval of the GCA. Briefings: Special briefings and procedures are required.

16. CERTIFICATION AND SIGNATURE. Security requirements stated herein are complete and adequate for safeguarding the classified information to be released or generated under this classified effort. All questions shall be referred to the official named below.

a. FULL NAME OF CERTIFYING OFFICIAL LAWARD J. PINDER	b. TITLE FACILITY SECURITY OFFICER (HOF)	c. TELEPHONE (Include Area Code) (856) 486-5266
--	--	---

17. REQUIRED DISTRIBUTION CONTRACTOR: RUFFED MARTIN SERVICES, INC 19 RIDDLE RD WEST HERRY HILL, NJ 08002 <i>Edward Pinder 28 JAN 2009</i> (202) 534-3561 DEC 1999	<input checked="" type="checkbox"/> a. CONTRACTOR
	<input checked="" type="checkbox"/> b. SUBCONTRACTOR
	<input checked="" type="checkbox"/> c. COGNIZANT SECURITY OFFICE FOR PRIME AND SUBCONTRACTOR
	<input checked="" type="checkbox"/> d. U.S. ACTIVITY RESPONSIBLE FOR OVERSEAS SECURITY ADMINISTRATION
	<input checked="" type="checkbox"/> e. ADMINISTRATIVE CONTRACTING OFFICER
	<input checked="" type="checkbox"/> f. OTHERS AS NECESSARY

CONTINUATION SHEET FOR BLOCK 13.

LOCKHEED MARTIN SERVICES INC 2339 ROUTE 70 WEST FLOOR 3W, CHERRY HILL, NJ 08002-3315
PAGE CODE 77609 CONTRACT# HSHQDC-08-D-00017 HQHSDC-07-J-00138

Reference Item 10e (1): Access to all Sensitive Compartmented Information (SCI) will be at DHS facilities only. For the purposes of this contract, the contractor is not authorized to process and/or store any classified information at contractor locations.

a. All SCI will be handled in accordance with special security requirements, which will be furnished by the designated responsible special security office (SSO).

b. SCI will not be released to contractor employees without specific release approval of the originator of the material as outlined in governing directives; based on prior approval and certification of "need-to-know" by the designated contractor.

c. All Contractor personnel requiring access to SCI as part of this contract effort must be approved and indoctrinated by DHS. Requests for Access will be submitted by the government project manager who can validate the justification for access.

d. Inquiries pertaining to classification guidance on SCI will be directed to the Special Security Officer (SSO).

e. SCI furnished in support of this contract remains the property of the Department of Homeland Security (DHS), agency, or component originator. Upon completion or cancellation of the contract, SCI furnished will be returned to the direct custody of the supporting SSO, or destroyed IAW instructions outlined by the Contract Officer.

f. Visits by contractor employees will only be certified by DHS when such visits are conducted as part of the contract effort.

Ref Item 10j: "Contractors shall control and safeguard FOUO in accordance with DHS Directive (MD 11042.1) "Safeguarding Sensitive but Unclassified (For Official Use Only) Information," dated Jan 6, 2005. DHS contractors must sign a special Non-Disclosure Agreement before receiving access to FOUO information. Contractors with questions on handling DHS FOUO shall contact DHS OS ASD at (202) 447-5341."

Ref. Item 11a. Contract performance for all SCI work is restricted to DHS Government buildings located in and around the metropolitan area of Washington, D.C., and at other locations in the metropolitan area of Wash DC. All contractor personnel must be U.S. citizens, have been granted a final security clearance by the U.S. Government, have been approved as meeting suitability criteria by DHS CSO, and have been indoctrinated by a Non Disclosure Agreement, Standard Form 312 for this specific program prior to being given any access to such information released or generated under this contract. Immigrant aliens, personnel cleared on an interim basis, or personnel holding contractor granted CONFIDENTIAL clearances, are not eligible for access to classified information released or generated under this contract without the express permission of the CSO through the DHS Personnel Division (DHS/PSD). The contractor and the Contracting Officer Technical Representative or other delegated representative will revalidate all SCI staffing requirements under the contract with the CSO annually or when a revised DD Form 254 is issued, whichever is sooner. **SCI WILL NOT BE RELEASED TO PUBLIC.**

DEPARTMENT OF DEFENSE CONTRACT SECURITY CLASSIFICATION SPECIFICATION		1. CLEARANCE AND SAFEGUARDING	
The requirements of the DoD Industrial Security Manual apply to all aspects of this effort.		a. FACILITY CLEARANCE REQUIRED TOP SECRET	
		b. LEVEL OF SAFEGUARDING REQUIRED NONE	
2. THIS SPECIFICATION IS FOR: (X and complete as applicable)		3. THIS SPECIFICATION IS: (X and complete as applicable)	
a. PRINCIPAL CONTRACT NUMBER HSHQDC-06-D-00017 HQHSDC-08-J-00138		a. ORIGINAL (Complete date in all cases) Date (YYMMDD) 20070928	
b. DDC CONTRACT NUMBER 10002154		b. REVISED (Supersedes all previous specs) Revision No. 2 Date (YYMMDD) 20090112	
c. MODIFICATION OR OTHER NUMBER Due Date (YYMMDD)		c. FINAL (Complete item 5 in all cases) Date (YYMMDD)	
4. IS THIS A FOLLOW-ON CONTRACT? <input checked="" type="checkbox"/> YES <input type="checkbox"/> NO If Yes complete the following			
a. Was the material received or generated under HSHQDC-06-D-00017 HQHSDC-07-J-00739 (Preceding Contract Number) is transferred to this follow-on contract			
5. IS THIS A FINAL DD FORM 254? <input type="checkbox"/> YES <input checked="" type="checkbox"/> NO If Yes complete the following			
a. In response to the contractor's request dated _____ retention of the identified classified material is authorized for the period of _____			
6. CONTRACTOR (Include Commercial and Government Entity (CAGE) Code)		c. COGNIZANT SECURITY OFFICE (Name, Address, and Zip Code)	
a. NAME, ADDRESS, AND ZIP CODE LOCKHEED MARTIN SERVICES, INC 330 ROUTE 75 WEST MURRY HILL, NJ 08002-3315		b. CAGE CODE 77609 DEFENSE SECURITY SERVICE 307 FELLOWSHIP ROAD STE 115 MT. LAUREL, NJ 08054-1233	
7. SUBCONTRACTOR		c. COGNIZANT SECURITY OFFICES (Name, Address, and Zip Code)	
a. NAME, ADDRESS, AND ZIP CODE (b) (4)		b. CAGE CODE 1M7Y6 DEFENSE SECURITY SERVICE 938 ELKRIDGE LANDING ROAD, STE 310 LINTHICUM, MD 21090-2917	
8. INDUSTRY PERFORMANCE		c. COGNIZANT SECURITY OFFICE (Name, Address, and Zip Code)	
a. CAGE CODE		b. CAGE CODE	
b. Name of Homeland Security (DHS) various activities within the Washington, DC metropolitan area.			
9. GENERAL IDENTIFICATION OF THIS PROCUREMENT			
a. Provide IT Operations & Maintenance technical support to Lockheed Martin in support of the IT-NOVA DHS Eagle Task Order. This is in response to Lockheed Martin's requirements to provide support to IT Operations Maintenance and COOP for the DHS headquarters and Components directly supported by the DHS OCIO.			
10. THIS CONTRACT WILL REQUIRE ACCESS TO:		11. IN PERFORMING THIS CONTRACT, THE CONTRACTOR WILL:	
COMMUNICATIONS SECURITY (COMSEC)	YES <input checked="" type="checkbox"/> NO <input type="checkbox"/>	a. HAVE ACCESS TO CLASSIFIED INFORMATION ONLY AT ANOTHER CONTRACTOR'S FACILITY OR A GOVERNMENT ACTIVITY	YES <input checked="" type="checkbox"/> NO <input type="checkbox"/>
CRYPTOGRAPHIC INFORMATION	YES <input type="checkbox"/> NO <input checked="" type="checkbox"/>	b. RECEIVE CLASSIFIED DOCUMENTS ONLY	YES <input type="checkbox"/> NO <input checked="" type="checkbox"/>
RESTRICTED DATA	YES <input type="checkbox"/> NO <input checked="" type="checkbox"/>	c. RECEIVE AND GENERATE CLASSIFIED MATERIAL	YES <input type="checkbox"/> NO <input checked="" type="checkbox"/>
CRITICAL NUCLEAR WEAPON DESIGN INFORMATION	YES <input type="checkbox"/> NO <input checked="" type="checkbox"/>	d. FABRICATE, MODIFY, OR STORE CLASSIFIED HARDWARE	YES <input type="checkbox"/> NO <input checked="" type="checkbox"/>
RESTRICTED DATA	YES <input type="checkbox"/> NO <input checked="" type="checkbox"/>	e. PERFORM SERVICES ONLY	YES <input type="checkbox"/> NO <input checked="" type="checkbox"/>
CRYPTOCRYPT INFORMATION	YES <input checked="" type="checkbox"/> NO <input type="checkbox"/>	f. HAVE ACCESS TO U.S. CLASSIFIED INFORMATION OUTSIDE THE U.S., PUERTO RICO, U.S. POSSESSIONS AND TRUST TERRITORIES	YES <input type="checkbox"/> NO <input checked="" type="checkbox"/>
RESTRICTED DATA	YES <input type="checkbox"/> NO <input checked="" type="checkbox"/>	g. BE AUTHORIZED TO USE THE SERVICES OF DEFENSE TECHNICAL INFORMATION CENTER (DTIC) OR OTHER SECONDARY DISTRIBUTION CENTER	YES <input type="checkbox"/> NO <input checked="" type="checkbox"/>
CRYPTOCRYPT INFORMATION (SCI)	YES <input type="checkbox"/> NO <input checked="" type="checkbox"/>	h. REQUIRE A COMSEC ACCOUNT	YES <input type="checkbox"/> NO <input checked="" type="checkbox"/>
RESTRICTED DATA	YES <input type="checkbox"/> NO <input checked="" type="checkbox"/>	i. HAVE A TEMPEST REQUIREMENT	YES <input type="checkbox"/> NO <input checked="" type="checkbox"/>
CRYPTOCRYPT INFORMATION	YES <input type="checkbox"/> NO <input checked="" type="checkbox"/>	j. HAVE OPERATIONS SECURITY (OPSEC) REQUIREMENTS	YES <input type="checkbox"/> NO <input checked="" type="checkbox"/>
RESTRICTED DATA	YES <input type="checkbox"/> NO <input checked="" type="checkbox"/>	k. BE AUTHORIZED TO USE THE DEFENSE COURIER SERVICE	YES <input type="checkbox"/> NO <input checked="" type="checkbox"/>
CRYPTOCRYPT INFORMATION	YES <input checked="" type="checkbox"/> NO <input type="checkbox"/>	l. OTHER (Specify):	YES <input type="checkbox"/> NO <input checked="" type="checkbox"/>
RESTRICTED DATA	YES <input type="checkbox"/> NO <input checked="" type="checkbox"/>		

PUBLIC RELEASE Any information (classified or unclassified) pertaining to this contract shall not be released for public dissemination except as provided by the Information Security Manual or unless it has been approved for public release by appropriate U.S. Government authority. Proposed public releases shall be submitted for approval prior to release. Direct Through (Specify) **NONE AUTHORIZED. SCI WILL NOT BE RELEASED TO PUBLIC.**

UNLESS CONTRACTOR HAS OBTAINED AUTHORITY TO RELEASE FROM THE DEPARTMENT OF HOMELAND SECURITY, CONTRACTOR SHALL COORDINATE WITH THE COFH AND THE OFFICE OF SECURITY (ASD) ON ALL CHANGES TO THIS GUIDANCE. (The Directorate for Freedom of Information and Security Review, Office of the Assistant Secretary of Defense (Public Affairs)) for review. (In the case of non-DoD User Agencies, requests for disclosure shall be submitted to that agency.)

SECURITY GUIDANCE The security classification guidance needed for this classified effort is identified below. If any difficulty is encountered in applying the guidance or if any other contributing factor indicates a need for changes in this guidance, the contractor is authorized and encouraged to provide recommended changes to challenge the guidance or the classification assigned to any information or material furnished or generated under this contract. Do not submit any questions for interpretation of this guidance to the official identified below. Pending final decision, the information involved shall be protected and protected at the highest level of classification assigned or recommended. (Fill in as appropriate for the classified effort. Attach, or forward under separate transmittence, any documents/guides/extracts referenced herein. Add additional pages as needed to provide complete guidance.)

Ref. Item 10a: COMSEC Access will involve the installation, maintenance, or use of crypto-equipment, systems, or keying material. Access to COMSEC requires a final US Government Clearance. Disclosure to Subcontractor requires prior approval of DHS. The contractor upon award shall contact the DHS COMSEC Control Office if Record (COR) at commercial (540) 542-3848, to receive current COMSEC guidance.

Ref. Item 10e (1). **Personnel:** All contractor personnel assigned to this contract shall possess security clearances issued by the Defense Security Service (DSS) commensurate with the level of required access to classified information that is directly in support of this contract. Immigrant aliens, personnel cleared on an interim basis, or personnel holding contractor-generated Confidential clearances are not eligible for access to classified information released or generated under this contract. Contractor personnel who are specifically designated as requiring access to Sensitive Compartmented Information (SCI) must be eligible under the provisions of DCID 6/4 without exception. Personnel will be submitted for clearance by their DHS manager and verified by their Contract Technical Representative. If approved for access, they will receive indoctrination briefing by DHS security staff prior to being granted access to SCI. All personnel security be maintained for debriefing with the DHS SSO by calling (202) 282-8643. **Note 10e (1) and 11a.** Access to all classified information (SCI) will be at DHS facilities only. For the purposes of this contract, the contractor is not authorized to process and/or store any classified information at contractor locations.

Jose Salazar 1-9-9
 JOSE J. SALAZAR, DHS OFFICE OF SECURITY
 PROGRAM MANAGER INDUSTRIAL SECURITY
 (202) 447-5346

14. ADDITIONAL SECURITY REQUIREMENTS. Requirements, in addition to ISM requirements, are established for this contract. (If Yes, identify the pertinent contractual clauses in the contract document itself, or provide an appropriate statement which identifies the additional requirements. Provide a copy of the requirements to the cognizant security office. Use Item 13 if additional space is needed.) Yes No

15. INSPECTIONS. Elements of this contract are outside the inspection responsibility of the cognizant security office. (List, explain, and identify specific areas or elements covered and the activity responsible for inspections. Use Item 13 if additional space is needed.) Yes No

DHS/OS/SSO CONCURS AND APPROVES THE "NEED-TO-KNOW" AT THE SCI LEVEL"
[Signature] 2/10/09. Clearances: Access to Intelligence information requires a final US Government clearance. Contracting requires prior approval of the GCA. Briefings: Special briefings and procedures are required.

16. VERIFICATION AND SIGNATURE. Security requirements stated herein are complete and adequate for safeguarding the classified information to be processed or generated under this classified effort. All questions shall be referred to the official named below.

a. SIGNED NAME OF CERTIFYING OFFICIAL FORWARD J. BINDER	b. TITLE FACILITY SECURITY OFFICER (HOF)	c. TELEPHONE (Include Area Code) (856) 486-5266
--	---	--

17. REQUIRED DISTRIBUTION <input checked="" type="checkbox"/> a. CONTRACTOR <input checked="" type="checkbox"/> b. SUBCONTRACTOR <input checked="" type="checkbox"/> c. COGNIZANT SECURITY OFFICE FOR PRIME AND SUBCONTRACTOR <input checked="" type="checkbox"/> d. U.S. ACTIVITY RESPONSIBLE FOR OVERSEAS SECURITY ADMINISTRATION <input checked="" type="checkbox"/> e. ADMINISTRATIVE CONTRACTING OFFICER <input checked="" type="checkbox"/> f. OTHERS AS NECESSARY	18. UNLESS INDICATED BY CODE: 18.1. CLASSIFIED MARTIN SERVICES, INC 18.2. 10000 W. STATE ST. WEST 18.3. 10000 W. STATE ST. WEST 18.4. 10000 W. STATE ST. WEST <i>[Signature]</i> 28 JAN 2009
--	---

FORM 254 (BACK), DEC 1999

CONTINUATION SHEET FOR BLOCK 13.

**LOCKHEED MARTIN SERVICES INC 2339 ROUTE 70 WEST FLOOR 3W, CHERRY HILL, NJ 08002-3315
CAGE CODE 77609 CONTRACT# HSHQDC-06-D-00017 HQHSDC-07-J-00138**

Reference Item 10e (1): Access to all Sensitive Compartmented Information (SCI) will be at DHS facilities only. For the purposes of this contract, the contractor is not authorized to process and/or store any classified information at contractor locations.

All SCI will be handled in accordance with special security requirements, which will be furnished by the designated responsible special security office (SSO).

SCI will not be released to contractor employees without specific release approval of the originator of the material as outlined in governing directives; based on prior approval and certification of "need-to-know" by the designated contractor.

All Contractor personnel requiring access to SCI as part of this contract effort must be approved and indoctrinated by DHS. Requests for Access will be submitted by the government project manager who can validate the justification for access.

Inquiries pertaining to classification guidance on SCI will be directed to the Special Security Officer (SSO).

SCI furnished in support of this contract remains the property of the Department of Homeland Security (DHS), agency, or component originator. Upon completion or cancellation of the contract, SCI furnished will be returned to the direct custody of the supporting SSO, or destroyed IAW instructions outlined by the Contract Officer.

Only contractor employees will only be certified by DHS when such visits are conducted as part of the contract effort.

Ref Item 10j. "Contractors shall control and safeguard FOUO in accordance with DHS Directive (MD 11042.1) "Safeguarding Sensitive but Unclassified (For Official Use Only) Information," dated Jan 6, 2005. DHS contractors must enter a special Non-Disclosure Agreement before receiving access to FOUO information. Contractors with questions on handling DHS FOUO shall contact DHS OS ASD at (202) 447-5341."

Ref. Item 11a. Contract performance for all SCI work is restricted to DHS Government buildings located in and around the metropolitan area of Washington, D.C., and at other locations in the metropolitan area of Wash DC. All contractor personnel must be U.S. citizens, have been granted a final security clearance by the U.S. Government, have been approved as meeting suitability criteria by DHS CSO, and have been indoctrinated by a Non Disclosure Agreement, Standard Form 312 for this specific program prior to being given any access to such information released or generated under this contract. Immigrant aliens, personnel cleared on an interim basis, or personnel holding contractor granted CONFIDENTIAL clearances, are not eligible for access to classified information released or generated under this contract without the express permission of the CSO through the DHS Personnel Division (DHS/PSD). The contractor and the Contracting Officer Technical Representative or other delegated representative will revalidate all SCI staffing requirements under the contract with the CSO annually or when a revised DD Form 254 is issued, whichever is sooner.
SCI WILL NOT BE RELEASED TO PUBLIC.

DEPARTMENT OF DEFENSE CONTRACT SECURITY CLASSIFICATION SPECIFICATION		1. CLEARANCE AND SAFEGUARDING	
The requirements of the DoD Industrial Security Manual apply to all aspects of this effort)		a. FACILITY CLEARANCE REQUIRED	
		TOP SECRET	
		b. LEVEL OF SAFEGUARDING REQUIRED	
		SECRET	
2. THIS SPECIFICATION IS FOR: (X and complete as applicable)		3. THIS SPECIFICATION IS: (X and complete as applicable)	
a. PRIME CONTRACT NUMBER HSHQDC-06-D-00017 HQHSDC-08-J-00138		a. ORIGINAL (Complete date in all cases)	
b. REVISION CONTRACT NUMBER P00008		b. REVISED (Supersedes all previous specs)	
c. DD FORM NUMBER OR OTHER NUMBER		Revision No 1	
Due Date (YYMMDD)		Date (YYMMDD) 20090113	
		c. FINAL (Complete item 5 in all cases)	
Date (YYMMDD)		Date (YYMMDD)	
4. IS THIS A FOLLOW-ON CONTRACT? <input checked="" type="checkbox"/> YES <input type="checkbox"/> NO. If Yes complete the following			
a. Has been, here, all received or generated under <u>HSHQDC-06-D-00017 HQHSDC-07-J-00739</u> (Preceding Contract Number) is transferred to this follow-on contract			
5. IS THIS A FINAL DD FORM 2547 <input type="checkbox"/> YES <input checked="" type="checkbox"/> NO. If Yes complete the following			
a. In response to the contractor's request dated _____ retention of the identified classified material is authorized for the period of _____			
6. CONTRACTOR (Include Commercial and Government Entity (CAGE) Code)			
a. NAME, ADDRESS, AND ZIP CODE LOCKHEED MARTIN SERVICES, INC 159 ROUTE 70 WEST MERRY HILL, NJ 08002-3315		b. CAGE CODE 77609	c. COGNIZANT SECURITY OFFICE (Name, Address, and Zip Code) DEFENSE SECURITY SERVICE 307 FELLOWSHIP ROAD STE 115 MT. LAUREL, NJ 08054-1233
7. SUBCONTRACTOR			
a. NAME, ADDRESS, AND ZIP CODE (b) (4)		b. CAGE CODE 0TKN1	c. COGNIZANT SECURITY OFFICES (Name, Address, and Zip Code) DEFENSE SECURITY SERVICE 14428 ALBEMARLE POINT PLACE, SUITE 140 CHANTILLY, VA 20151
8. ACTUAL PERFORMANCE			
a. LOCATION Department of Homeland Security (DHS) various locations within the Washington, DC metropolitan area		b. CAGE CODE	c. COGNIZANT SECURITY OFFICE (Name, Address, and Zip Code)
9. GENERAL IDENTIFICATION OF THIS PROCUREMENT			
a. Provide IT Operations & Maintenance technical support to Lockheed Martin in support of the IT-NOVA DHS Eagle Task Force. This is in response to Lockheed Martin's requirements to provide support to IT Operations Maintenance and COOP at the DHS Headquarters and Components directly supported by the DHS OCIO.			
10. THIS CONTRACT WILL REQUIRE ACCESS TO:			
a. COMMERCIAL AND GOVERNMENT SECURITY (COMSEC)		11. IN PERFORMING THIS CONTRACT, THE CONTRACTOR WILL:	
b. UNCLASSIFIED DATA		a. HAVE ACCESS TO CLASSIFIED INFORMATION ONLY AT ANOTHER CONTRACTOR'S FACILITY OR A GOVERNMENT ACTIVITY	
c. NUCLEAR WEAPON DESIGN INFORMATION		b. RECEIVE CLASSIFIED DOCUMENTS ONLY	
d. UNRESTRICTED DATA		c. RECEIVE AND GENERATE CLASSIFIED MATERIAL	
e. SOURCE INFORMATION		d. FABRICATE, MODIFY, OR STORE CLASSIFIED HARDWARE	
f. SOURCE COMPANIED INFORMATION (SCI)		e. PERFORM SERVICES ONLY	
g. (NSA)		f. HAVE ACCESS TO U.S. CLASSIFIED INFORMATION OUTSIDE THE U.S., PUERTO RICO, U.S. POSSESSIONS AND TRUST TERRITORIES	
h. ACCESS INFORMATION		g. BE AUTHORIZED TO USE THE SERVICES OF DEFENSE TECHNICAL INFORMATION CENTER (DTIC) OR OTHER SECONDARY DISTRIBUTION CENTER	
i. INFORMATION		h. REQUIRE A COMSEC ACCOUNT	
j. STATEMENT INFORMATION		i. HAVE A TEMPEST REQUIREMENT	
k. IDENTIFICATION INFORMATION		j. HAVE OPERATIONS SECURITY (OPSEC) REQUIREMENTS	
l. IDENTIFICATION INFORMATION		k. BE AUTHORIZED TO USE THE DEFENSE COURIER SERVICE	
m. IDENTIFICATION INFORMATION		l. OTHER (Specify):	
n. IDENTIFICATION INFORMATION			

PUBLIC RELEASE Any information (classified or unclassified) pertaining to this contract shall not be released for public dissemination except as provided by the National Security Manual or unless it has been approved for public release by appropriate U.S. Government authority. Proposed public releases shall be submitted for approval prior to release Direct Through (Specify) **NONE AUTHORIZED. SCI WILL NOT BE RELEASED TO PUBLIC.**

UNLESS CONTRACTOR HAS OBTAINED AUTHORITY TO RELEASE FROM THE DEPARTMENT OF HOMELAND SECURITY, CONTRACTOR SHALL COORDINATE WITH THE COFR AND THE OFFICE OF SECURITY (ASD) ON ALL CHANGES TO THIS GUIDANCE.
 (1) The Directorate for Freedom of Information and Security Review, Office of the Assistant Secretary of Defense (Public Affairs)* for review
 (2) The lead of non DoD User Agencies, requests for disclosure shall be submitted to that agency

12. SECURITY GUIDANCE. The security classification guidance needed for this classified effort is identified below. If any difficulty is encountered in applying this guidance or if any other contributing factor indicates a need for changes in this guidance, the contractor is authorized and encouraged to provide recommended changes to challenge the guidance or the classification assigned to any information or material furnished or generated under this contract; and to submit any questions for interpretation of this guidance to the official identified below. Pending final decision, the information involved shall be classified and protected at the highest level of classification assigned or recommended. (Fill in as appropriate for the classified effort. Attach, or forward under separate correspondence, any documents/guides/extracts referenced herein. Add additional pages as needed to provide complete guidance.)

Ref. Item 10a: COMSEC Access will involve the installation, maintenance, or use of crypto-equipment, systems, or keying material. Access to COMSEC requires a final US Government Clearance. Disclosure to Subcontractor requires prior approval of DHS. The contractor upon award shall contact the DHS COMSEC Control Office if Record (COR) at Commercial (540) 542-3848, to receive current COMSEC guidance.

Ref. Item 10e (1). **Personnel:** All contractor personnel assigned to this contract shall possess security clearances issued by the Defense Security Service (DSS) commensurate with the level of required access to classified information that is directly in support of this contract. Immigrant aliens, personnel cleared on an interim basis, or personnel holding contractor-generated Confidential clearances are not eligible for access to classified information released or generated under this contract. Contractor personnel who are specifically designated as requiring access to Sensitive Compartmented Information (SCI) must be eligible under the provisions of DCID 6/4 without exception. Personnel will be submitted for review by their DHS manager and verified by their Contract Technical Representative. If approved for access, they will receive an indoctrination briefing by DHS security staff prior to being granted access to SCI. All personnel security be scheduled for debriefing with the DHS SSO by calling (202) 282-8643. **Note 10e (1) and 11a.** Access to all classified information (SCI) will be at DHS facilities only. For the purposes of this contract, the contractor is not authorized to create and/or store any classified information at contractor locations.

Jose Salazar 1-9-9
JOSE J. SALAZAR, DHS OFFICE OF SECURITY
PROGRAM MANAGER INDUSTRIAL SECURITY
 (602) 447-5346

13. ADDITIONAL SECURITY REQUIREMENTS Requirements, in addition to ISM requirements, are established for this contract. (If Yes, Yes No identify the pertinent contractual clauses in the contract document itself, or provide an appropriate statement which identifies the additional requirements. Provide a copy of the requirements to the cognizant security office. Use item 13 if additional space is needed.)

14. EXCEPTIONS Elements of this contract are outside the inspection responsibility of the cognizant security office Yes No (Specify, explain, and identify specific areas or elements carved out and the activity responsible for inspections. Use item 13 if additional space is needed.)

"DHS/OS/SSPD CONCURS AND APPROVES THE "NEED-TO-KNOW" AT THE SCI LEVEL"
2/10/09 Clearances: Access to Intelligence information requires a final US Government clearance
 Subcontracting requires prior approval of the GCA. Briefings: Special briefings and procedures are required.

15. CERTIFICATION AND SIGNATURE. Security requirements stated herein are complete and adequate for safeguarding the classified information to be released or generated under this classified effort. All questions shall be referred to the official named below.

a. NAME OF CERTIFYING OFFICIAL MURRAY L. PINDER	b. TITLE FACILITY SECURITY OFFICER (HOF)	c. TELEPHONE (Include Area Code) (836) 486-5266
--	---	--

16. CONTRACTOR'S OFFICE DEFENSE MARTIN SERVICES, INC 2000 W. 10TH ST WASHINGTON, DC 20002 <i>28 JAN 2009</i> (FORM 254, BACK), DEC 1999	17. REQUIRED DISTRIBUTION <input checked="" type="checkbox"/> a. CONTRACTOR <input checked="" type="checkbox"/> b. SUBCONTRACTOR <input checked="" type="checkbox"/> c. COGNIZANT SECURITY OFFICE FOR PRIME AND SUBCONTRACTOR <input type="checkbox"/> d. U.S. ACTIVITY RESPONSIBLE FOR OVERSEAS SECURITY ADMINISTRATION <input checked="" type="checkbox"/> e. ADMINISTRATIVE CONTRACTING OFFICER <input checked="" type="checkbox"/> f. OTHERS AS NECESSARY
--	--

CONTINUATION SHEET FOR BLOCK 13.

**LOCKHEED MARTIN SERVICES INC 2339 ROUTE 70 WEST FLOOR 3W, CHERRY HILL, NJ 08002-3315
CAGE CODE: 77609 CONTRACT# HSHQDC-06-D-00017 HQHSDC-07-J-00138**

Reference Item 10e (1): Access to all Sensitive Compartmented Information (SCI) will be at DHS facilities only. For the purposes of this contract, the contractor is not authorized to process and/or store any classified information at contractor locations.

1. All SCI will be handled in accordance with special security requirements, which will be furnished by the designated responsible special security office (SSO).

2. SCI will not be released to contractor employees without specific release approval of the originator of the material as outlined in governing directives, based on prior approval and certification of "need-to-know" by the designated contractor.

3. All Contractor personnel requiring access to SCI as part of this contract effort must be approved and indoctrinated by DHS. Requests for Access will be submitted by the government project manager who can validate the justification for access.

4. Inquiries pertaining to classification guidance on SCI will be directed to the Special Security Officer (SSO).

5. SCI furnished in support of this contract remains the property of the Department of Homeland Security (DHS), agency, or component originator. Upon completion or cancellation of the contract, SCI furnished will be returned to the direct custody of the supporting SSO, or destroyed (AW instructions outlined by the Contract Officer).

6. Visits by contractor employees will only be certified by DHS when such visits are conducted as part of the contract effort.

Ref Item 10j: "Contractors shall control and safeguard FOUO in accordance with DHS Directive (MD 11042.1) "Safeguarding Sensitive but Unclassified (For Official Use Only) Information," dated Jan 6, 2005. DHS contractors must sign a special Non-Disclosure Agreement before receiving access to FOUO information. Contractors with questions on standing DHS FOUO shall contact DHS OS ASD at (202) 447-5341."

Ref. Item 11a: Contract performance for all SCI work is restricted to DHS Government buildings located in and around the metropolitan area of Washington, D.C., and at other locations in the metropolitan area of Wash DC. All contractor personnel must be U.S. citizens, have been granted a final security clearance by the U.S. Government, have been approved as meeting suitability criteria by DHS CSO, and have been indoctrinated by a Non Disclosure Agreement, Standard Form 512 for this specific program prior to being given any access to such information released or generated under this contract. Immigrant aliens, personnel cleared on an interim basis, or personnel holding contractor granted CONFIDENTIAL clearances, are not eligible for access to classified information released or generated under this contract without the express permission of the CSO through the DHS Personnel Division (DHS/PSD). The contractor and the Contracting Officer Technical Representative or other delegated representative will revalidate all SCI staffing requirements under the contract with the CSO annually or when a revised DD Form 254 is issued, whichever is sooner.
SCI WILL NOT BE RELEASED TO PUBLIC.

DEPARTMENT OF DEFENSE CONTRACT SECURITY CLASSIFICATION SPECIFICATION		1. CLEARANCE AND SAFEGUARDING	
The requirements of the DoD Industrial Security Manual apply to all aspects of this effort.		a. FACILITY CLEARANCE REQUIRED TOP SECRET	
		b. LEVEL OF SAFEGUARDING REQUIRED NONE	
2. THIS SPECIFICATION IS FOR: (X and complete as applicable)		3. THIS SPECIFICATION IS: (X and complete as applicable)	
a. PRIME CONTRACT NUMBER HSHQDC-06-D-00017 HQHSDC-08-J-00138		a. ORIGINAL (Complete date in all cases) Date (YYMMDD) 20070928	
b. SUBCONTRACT NUMBER 4603226J		b. REVISED (Supersedes all previous specs) Revision No 2 Date (YYMMDD) 20090113	
c. IDENTIFICATION OR OTHER NUMBER Due Date (YYMMDD)		c. FINAL (Complete item 3 in all cases) Date (YYMMDD)	
4. IS THIS A FOLLOW-ON CONTRACT? <input checked="" type="checkbox"/> YES <input type="checkbox"/> NO If Yes complete the following			
a. All material received or generated under <u>HSHQDC-06-D-00017 HQHSDC-07-J-00739</u> (Preceding Contract Number) is transferred to this follow-on contract			
5. IS THIS A FINAL DD FORM 264? <input type="checkbox"/> YES <input checked="" type="checkbox"/> NO. If Yes complete the following			
a. In response to the contractor's request dated _____, retention of the identified classified material is authorized for the period of _____			
6. CONTRACTOR (Include Commercial and Government Entity (CAGE) Code) NAME, ADDRESS, AND ZIP CODE LOCKHEED MARTIN SERVICES, INC 290 FORTGE TO WEST PERRY HILL, NJ 08002-3315		b. CAGE CODE 77609	
		c. COGNIZANT SECURITY OFFICE (Name, Address, and Zip Code) DEFENSE SECURITY SERVICE 307 FELLOWSHIP ROAD STE 115 MT LAUREL, NJ 08054-1233	
7. SUBCONTRACTOR NAME, ADDRESS, AND ZIP CODE (b) (4)		b. CAGE CODE 46CUI	
		c. COGNIZANT SECURITY OFFICES (Name, Address, and Zip Code) DEFENSE SECURITY SERVICE 14428 ALBEMARLE POINT PLACE, SUITE 140 CHANTILLY, VA 20151	
8. ACTUAL PERFORMANCE BY OR FOR Department of Homeland Security (DHS) various operations within the Washington, DC metropolitan area		b. CAGE CODE	
		c. COGNIZANT SECURITY OFFICE (Name, Address, and Zip Code)	
9. GENERAL IDENTIFICATION OF THIS PROCUREMENT This provides IT Operations & Maintenance technical support to Lockheed Martin in support of the IT-NOVA DHS Eagle Task Order. This is in response to Lockheed Martin's requirements to provide support to IT Operations Maintenance and COOP at the DHS Headquarters and Components directly supported by the DHS OCIO.			
10. THIS CONTRACT WILL REQUIRE ACCESS TO:		11. IN PERFORMING THIS CONTRACT, THE CONTRACTOR WILL:	
CLASSIFIED INFORMATION SECURITY (COMSEC)	YES <input checked="" type="checkbox"/> NO <input type="checkbox"/>	a. HAVE ACCESS TO CLASSIFIED INFORMATION ONLY AT ANOTHER CONTRACTOR'S FACILITY OR A GOVERNMENT ACTIVITY	YES <input checked="" type="checkbox"/> NO <input type="checkbox"/>
RESTRICTED DATA	YES <input type="checkbox"/> NO <input checked="" type="checkbox"/>	b. RECEIVE CLASSIFIED DOCUMENTS ONLY	YES <input type="checkbox"/> NO <input checked="" type="checkbox"/>
DEFENSE NUCLEAR WEAPON DESIGN INFORMATION	YES <input type="checkbox"/> NO <input checked="" type="checkbox"/>	c. RECEIVE AND GENERATE CLASSIFIED MATERIAL	YES <input type="checkbox"/> NO <input checked="" type="checkbox"/>
EXACTLY RESTRICTED DATA	YES <input type="checkbox"/> NO <input checked="" type="checkbox"/>	d. FABRICATE, MODIFY OR STORE CLASSIFIED HARDWARE	YES <input type="checkbox"/> NO <input checked="" type="checkbox"/>
DEFENSE INTELLIGENCE INFORMATION	YES <input type="checkbox"/> NO <input checked="" type="checkbox"/>	e. PERFORM SERVICES ONLY	YES <input type="checkbox"/> NO <input checked="" type="checkbox"/>
DEFENSIVE COMPARTEMENTED INFORMATION (SCI)	YES <input checked="" type="checkbox"/> NO <input type="checkbox"/>	f. HAVE ACCESS TO U.S. CLASSIFIED INFORMATION OUTSIDE THE U.S., PUERTO RICO, U.S. POSSESSIONS AND TRUST TERRITORIES	YES <input type="checkbox"/> NO <input checked="" type="checkbox"/>
SECRET	YES <input type="checkbox"/> NO <input checked="" type="checkbox"/>	g. BE AUTHORIZED TO USE THE SERVICES OF DEFENSE TECHNICAL INFORMATION CENTER (DTIC) OR OTHER SECONDARY DISTRIBUTION CENTER	YES <input type="checkbox"/> NO <input checked="" type="checkbox"/>
SECRET ACCESS INFORMATION	YES <input type="checkbox"/> NO <input checked="" type="checkbox"/>	h. REQUIRE A COMSEC ACCOUNT	YES <input type="checkbox"/> NO <input checked="" type="checkbox"/>
SECRET INFORMATION	YES <input type="checkbox"/> NO <input checked="" type="checkbox"/>	i. HAVE A TEMPEST REQUIREMENT	YES <input type="checkbox"/> NO <input checked="" type="checkbox"/>
DEFENSE GOVERNMENT INFORMATION	YES <input type="checkbox"/> NO <input checked="" type="checkbox"/>	j. HAVE OPERATIONS SECURITY (OPSEC) REQUIREMENTS	YES <input type="checkbox"/> NO <input checked="" type="checkbox"/>
DEFENSE GOVERNMENT INFORMATION	YES <input type="checkbox"/> NO <input checked="" type="checkbox"/>	k. BE AUTHORIZED TO USE THE DEFENSE COURIER SERVICE	YES <input type="checkbox"/> NO <input checked="" type="checkbox"/>
DEFENSE GOVERNMENT INFORMATION	YES <input checked="" type="checkbox"/> NO <input type="checkbox"/>	l. OTHER (Specify)	YES <input type="checkbox"/> NO <input checked="" type="checkbox"/>
SECRET	YES <input type="checkbox"/> NO <input checked="" type="checkbox"/>		

CONTINUATION SHEET FOR BLOCK 13.

**LOCKHEED MARTIN SERVICES INC 2339 ROUTE 70 WEST FLOOR 3W, CHERRY HILL, NJ 08002-3315
CAGE CODE 77609 CONTRACT# HSHQDC-08-D-00017 HQHSDC-07-J-00138**

Reference Item 10e (1): Access to all Sensitive Compartmented Information (SCI) will be at DHS facilities only. For the purposes of this contract, the contractor is not authorized to process and/or store any classified information at contractor locations.

- a. All SCI will be handled in accordance with special security requirements, which will be furnished by the designated responsible special security office (SSO).
- b. SCI will not be released to contractor employees without specific release approval of the originator of the material as outlined in governing directives; based on prior approval and certification of "need-to-know" by the designated contractor.
- c. All Contractor personnel requiring access to SCI as part of this contract effort must be approved and indoctrinated by DHS. Requests for Access will be submitted by the government project manager who can validate the justification for access.
- d. Inquiries pertaining to classification guidance on SCI will be directed to the Special Security Officer (SSO).
- e. SCI furnished in support of this contract remains the property of the Department of Homeland Security (DHS), agency, or component originator. Upon completion or cancellation of the contract, SCI furnished will be returned to the direct custody of the supporting SSO, or destroyed IAW instructions outlined by the Contract Officer.
- f. Visits by contractor employees will only be certified by DHS when such visits are conducted as part of the contract effort.

Ref Item 10j: "Contractors shall control and safeguard FOUO in accordance with DHS Directive (MD 11042.1) regarding Sensitive but Unclassified (For Official Use Only) Information," dated Jan 6, 2005. DHS contractors must sign a special Non-Disclosure Agreement before receiving access to FOUO information. Contractors with questions on obtaining DHS FOUO shall contact DHS OS ASD at (202) 447-5341."

Ref. Item 11a. Contract performance for all SCI work is restricted to DHS Government buildings located in and around the metropolitan area of Washington, D.C., and at other locations in the metropolitan area of Wash DC. All contractor personnel must be U.S. citizens, have been granted a final security clearance by the U.S. Government, have been approved as meeting suitability criteria by DHS CSO, and have been indoctrinated by a Non Disclosure Agreement, standard Form 312 for this specific program prior to being given any access to such information released or generated under this contract. Immigrant aliens, personnel cleared on an interim basis, or personnel holding contractor granted CONFIDENTIAL clearances, are not eligible for access to classified information released or generated under this contract without the express permission of the CSO through the DHS Personnel Division (DHS/PSD). The contractor and the Contracting Officer Technical Representative or other delegated representative will revalidate all SCI staffing requirements under the contract with the CSO annually or when a revised DD Form 254 is issued, whichever is sooner.
SCI WILL NOT BE RELEASED TO PUBLIC.

AMENDMENT OF SOLICITATION/MODIFICATION OF CONTRACT		1 CONTRACT ID CODE	PAGE OF PAGES 1 2
2 AMENDMENT/MODIFICATION NO P00009	3 EFFECTIVE DATE 09/04/2009	4 REQUISITION/PURCHASE REQ. NO RUPA-09-00034	5 PROJECT NO (if applicable)
6 ISSUED BY Dept. of Homeland Security Office of Procurement Operations Information Tech. Acquisition Div. 245 Murray Lane, SW Building 410 Washington DC 20528	CODE DHS/OPO/ITAC	7 ADMINISTERED BY (if other than Item 6) U.S. Dept. of Homeland Security Office of Procurement Operations Information Tech. Acquisition Div. 245 Murray Lane, SW Building 410 Washington DC 20528	CODE DHS/OPO/ITAC
8 NAME AND ADDRESS OF CONTRACTOR (No., street, county, State and ZIP Code) LOCKHEED MARTIN SERVICES INC 2339 ROUTE 70 WEST FLOOR 3W CHERRY HILL NJ 080023315		(X) 9A AMENDMENT OF SOLICITATION NO	
CODE 8052583730000 FACILITY CODE		9B DATED (SEE ITEM 11)	
		X 10A MODIFICATION OF CONTRACT/ORDER NO HSHQDC-06-D-00017 HSHQDC-08-J-00138	
		10B DATED (SEE ITEM 13) 06/02/2008	

11. THIS ITEM ONLY APPLIES TO AMENDMENTS OF SOLICITATIONS

The above numbered solicitation is amended as set forth in Item 14. The hour and date specified for receipt of Offers is extended, is not extended.
Offers must acknowledge receipt of this amendment prior to the hour and date specified in the solicitation or as amended, by one of the following methods: (a) By completing Items 8 and 15, and returning _____ copies of the amendment; (b) By acknowledging receipt of this amendment on each copy of the offer submitted; or (c) By separate letter or telegram which includes a reference to the solicitation and amendment numbers. FAILURE OF YOUR ACKNOWLEDGEMENT TO BE RECEIVED AT THE PLACE DESIGNATED FOR THE RECEIPT OF OFFERS PRIOR TO THE HOUR AND DATE SPECIFIED MAY RESULT IN REJECTION OF YOUR OFFER. If by virtue of this amendment you desire to change an offer already submitted, such change may be made by telegram or letter, provided each telegram or letter makes reference to the solicitation and this amendment, and is received prior to the opening hour and date specified.

12 ACCOUNTING AND APPROPRIATION DATA (if required)

See Schedule

13. THIS ITEM ONLY APPLIES TO MODIFICATION OF CONTRACTS/ORDERS. IT MODIFIES THE CONTRACT/ORDER NO. AS DESCRIBED IN ITEM 14.

CHECK ONE	A THIS CHANGE ORDER IS ISSUED PURSUANT TO (Specify authority) THE CHANGES SET FORTH IN ITEM 14 ARE MADE IN THE CONTRACT ORDER NO IN ITEM 10A.
X	B THE ABOVE NUMBERED CONTRACT/ORDER IS MODIFIED TO REFLECT THE ADMINISTRATIVE CHANGES (such as changes in paying office, appropriation date, etc) SET FORTH IN ITEM 14, PURSUANT TO THE AUTHORITY OF FAR 43.103(b)
	C THIS SUPPLEMENTAL AGREEMENT IS ENTERED INTO PURSUANT TO AUTHORITY OF:
	D OTHER (Specify type of modification and authority)

E. IMPORTANT: Contractor is not, is required to sign this document and return _____ 0 _____ copies to the issuing office

14 DESCRIPTION OF AMENDMENT/MODIFICATION (Organized by UCF section headings, including solicitation/contract subject matter where feasible.)


DUNS Number: 805258373+0000

The purpose of this administrative modification is to: (1) Name an Alternate Contracting Officer's Technical Representative (COTR); (2) Revise Statement of Work Section C.7 - Technical Exhibits; and (3) Add two subcontractor Contract Security Classification Specification DD Form 254s.

See Page 2 for modification details.

Period of Performance: 06/01/2008 to 01/31/2013

Except as provided herein, all terms and conditions of the document referenced in Item 9A or 10A, as heretofore changed, remains unchanged and in full force and effect

15A NAME AND TITLE OF SIGNER (Type or print)	16A NAME AND TITLE OF CONTRACTING OFFICER (Type or print) Rebecca A. Taylor
15B CONTRACTOR/OFFEROR (Signature of person authorized to sign)	15C DATE SIGNED
16B UNITED STATES OF AMERICA  (Signature of Contracting Officer)	16C DATE SIGNED SEP - 4 2009

SF-30 CONTINUATION SHEET

1. Revise **Section G.3.2 - COTR Designation** to designate Roger Kessler as Alternate COTR in the absence of COTR, Gerald R. Warren. Mr. Kessler may be contacted as follows:

Name: Roger Kessler
Phone: 866-459-5385
Email: Roger.Kessler@hhs.gov

2. At **Section C.7 – Technical Exhibits**, the **List of Technical Exhibits** on Page C-93 of the IT-NOVA statement of work is revised to delete Technical Exhibit TE C. 1.12-002, entitled, “Current Contracts Period of Performance” in its entirety. Accordingly, delete Page C-93 dated 4/15/09 in its entirety and insert revised Page C-93 dated 9/4/09. (See Attachment 1)
3. Revise **ATTACHMENT 2 – Contract Security Classification Specifications (DD FORM 254)** shown at **Modification P00008** to add two more subcontractor names to the list: About Web, LLC and EMC 2 Corporation. (See Attachment 2)
4. The value and total amount funded/obligated to the task order remains unchanged at \$78,151,545.74.
5. The ceiling for this task order remains unchanged at \$288,499,204.00.
6. All other terms and conditions remain unchanged.

PROCUREMENT SENSITIVE

C.1 TECHNICAL EXHIBITS

Technical Exhibit Title Numbering System:

A Technical Exhibit (TE) is titled in relation to the Section from which it is first referenced and its order among TEs in that Section. For example, Section 3.1 has three Technical Exhibits titled TE C.3.1.-001, TE C.3.1-002, and TE C.3.1.-003.

TE Page Numbering System:

Since Section C.7 provides all Technical Exhibits except those maintained on the DHS Interactive website, all TEs are page numbered in relation to their TE title. For example, page one of TE C.5.2.-001 is shown as page number TE C.5.2.-001-01 to indicate that it is the first page of TE C.5.2.-001 from Task Order Section 5.2.

List of Technical Exhibits:

TE	Description	Task Order Paragraph
C 1 2-001	DHS Organization Chart	C 1 2
C 1 2-002	Locations Supported Summary (Sensitive But Unclassified)	C 1 2, C 5 6 1
C 1 2-003	DHS OCIO Organization Chart	C 1 2
C 1 3-003	Seats by Fiscal Year (FY) for LAN – A	C 1 3 1 1, C 5
C 1 3-003	Seats by Fiscal Year (FY) for LAN – HSDN	C 1 3 1 1, C 5
C 1 3-003	Seats by Fiscal Year (FY) for LAN – C	C 1 3 1 1, C 5
C 1 6-001	Performance Requirements Summary	C 1 6 1, C 1 6 1 2, C 1 9 1 1
C 1 6-002	Plans developed, maintained, and updated by Contractor	C 1 6 2 4
C 1 7-001	Key Personnel Positions and Descriptions	C 1 7 1 2
C 3 1-001	Government Furnished Equipment Product Guide of IT Equipment & Software	C 3 1 4 1, C 5, C 5 1, C 5 6 1
C 3 1 004	Government Furnished Facilities	C 3 1 4 1
C 5 1-001	DHS Custom Applications	C 5 1 1 2
C 5 15-001	Continuity Planning Framework	C 5 15 1

ATTACHMENT 2
Contract Security Classification Specifications (DD FORM 254s)

ATTACHMENT 2 at MODIFICATION P00008 is revised to add two more names to list of Contract Security Classification Specifications (DD FORM 254s):

- (b) (4) - New pages 57 to 60
- (b) (4) – New pages 61 to 63

Page	Subcontractor Name
2	(b) (4)
6	
10	
14	
18	
22	
26	
30	
34	
38	
41	
45	
49	
53	
57	
61	

DEPARTMENT OF DEFENSE CONTRACT SECURITY CLASSIFICATION SPECIFICATION		1. CLEARANCE AND SAFEGUARDING	
(The requirements of the DoD Industrial Security Manual apply to all aspects of this effort)		a. FACILITY CLEARANCE REQUIRED TOP SECRET	
		b. LEVEL OF SAFEGUARDING REQUIRED NONE	
2. THIS SPECIFICATION IS FOR: (Of and complete as applicable)		3. THIS SPECIFICATION IS: (Of and complete as applicable)	
a. PRIME CONTRACT NUMBER <input checked="" type="checkbox"/> HSHQDC-06-D-00017 HQHSDC-08-J-00138		a. ORIGINAL (Complete date in all cases) <input checked="" type="checkbox"/> Date (YYYYMMDD) 20090714	
b. SUBCONTRACT NUMBER <input checked="" type="checkbox"/> 7200005343		b. REVISED (Supersede all previous specs) <input type="checkbox"/> Revision No. _____ Date (YYYYMMDD) _____	
c. SOLICITATION OR OTHER NUMBER _____ Due Date (YYYYMMDD) _____		c. FINAL (Complete item 5 if all cases) <input type="checkbox"/> Date (YYYYMMDD) _____	
4. IS THIS A FOLLOW-ON CONTRACT? <input checked="" type="checkbox"/> YES <input type="checkbox"/> NO. If Yes complete the following			
Classified material received or generated under <u>HSHQDC-06-D-00017 HQHSDC-07-J-00739</u> (Preceding Contract Number) is transferred to this follow-on contract			
5. IS THIS A FINAL DD FORM 2847? <input type="checkbox"/> YES <input checked="" type="checkbox"/> NO. If Yes complete the following			
In response to the contractor's request dated _____, retention of the identified classified material is authorized for the period of _____.			
6. CONTRACTOR (Include Commercial and Government Entity (CAGE) Code)			
a. NAME, ADDRESS, AND ZIP CODE LOCKHEED MARTIN SERVICES, INC 2339 ROUTE 70 WEST CHERRY HILL, NJ 08002-3315		b. CAGE CODE 77609	c. COORDINATE SECURITY OFFICE (Name, Address, and Zip Code) DEFENSE SECURITY SERVICE 307 FELLOWSHIP ROAD STE 115 MT. LAUREL, NJ 08054-1233
7. SUBCONTRACTOR			
a. NAME, ADDRESS, AND ZIP CODE (b) (4)		b. CAGE CODE 1TYL2	c. COORDINATE SECURITY OFFICES (Name, Address, and Zip Code) DEFENSE SECURITY SERVICE 938 Elkridge Landing Rd, Ste 310 Linthicum, MD 21090-2917
8. ACTUAL PERFORMANCE			
a. LOCATION Department of Homeland Security (DHS) various locations within the Washington, DC metropolitan area. HQ ONLY		b. CAGE CODE	c. COORDINATE SECURITY OFFICE (Name, Address, and Zip Code)
9. GENERAL IDENTIFICATION OF THIS PROCUREMENT (U) Provide IT Operations & Maintenance technical support to Lockheed Martin in support of the IT-NOVA DHS Eagle Task Order. This is in response to Lockheed Martin's requirements to provide support to IT Operations Maintenance and COOP for the DHS Headquarters and Components directly supported by the DHS OCIO.			
10. THIS CONTRACT WILL REQUIRE ACCESS TO:		11. IN PERFORMING THIS CONTRACT, THE CONTRACTOR WILL:	
a. COMMUNICATIONS SECURITY (COMSEC) INFORMATION	YES <input checked="" type="checkbox"/> NO <input type="checkbox"/>	a. HAVE ACCESS TO CLASSIFIED INFORMATION ONLY AT ANOTHER CONTRACTOR'S FACILITY OR A GOVERNMENT ACTIVITY	YES <input checked="" type="checkbox"/> NO <input type="checkbox"/>
b. RESTRICTED DATA	<input type="checkbox"/> <input checked="" type="checkbox"/>	b. RECEIVE CLASSIFIED DOCUMENTS ONLY	<input type="checkbox"/> <input checked="" type="checkbox"/>
c. CRITICAL NUCLEAR WEAPON DESIGN INFORMATION	<input type="checkbox"/> <input checked="" type="checkbox"/>	c. RECEIVE AND GENERATE CLASSIFIED MATERIAL	<input type="checkbox"/> <input checked="" type="checkbox"/>
d. FORMERLY RESTRICTED DATA	<input type="checkbox"/> <input checked="" type="checkbox"/>	d. FABRICATE, COPY, OR STORE CLASSIFIED HARDWARE	<input type="checkbox"/> <input checked="" type="checkbox"/>
e. INTELLIGENCE INFORMATION	<input checked="" type="checkbox"/> <input type="checkbox"/>	e. PERFORM SERVICES ONLY	<input type="checkbox"/> <input checked="" type="checkbox"/>
(1) Sensitive Compartmental Information (SCI)	<input checked="" type="checkbox"/> <input type="checkbox"/>	f. HAVE ACCESS TO U.S. CLASSIFIED INFORMATION OUTSIDE THE U.S., PUERTO RICO, U.S. POSSESSIONS AND TRUST TERRITORIES	<input type="checkbox"/> <input checked="" type="checkbox"/>
(2) Non-SCI	<input type="checkbox"/> <input checked="" type="checkbox"/>	g. BE AUTHORIZED TO USE THE SERVICES OF DEFENSE TECHNICAL INFORMATION CENTER (DTIC) OR OTHER SECONDARY DISTRIBUTION CENTER	<input type="checkbox"/> <input checked="" type="checkbox"/>
f. SPECIAL ACCESS INFORMATION	<input type="checkbox"/> <input checked="" type="checkbox"/>	h. REQUIRE A COMSEC ACCOUNT	<input type="checkbox"/> <input checked="" type="checkbox"/>
g. NATO INFORMATION	<input type="checkbox"/> <input checked="" type="checkbox"/>	i. HAVE A TEMPEST REQUIREMENT	<input type="checkbox"/> <input checked="" type="checkbox"/>
h. FOREIGN GOVERNMENT INFORMATION	<input type="checkbox"/> <input checked="" type="checkbox"/>	j. HAVE OPERATIONS SECURITY (OPSEC) REQUIREMENTS	<input type="checkbox"/> <input checked="" type="checkbox"/>
i. LIMITED DISSEMINATION INFORMATION	<input type="checkbox"/> <input checked="" type="checkbox"/>	k. BE AUTHORIZED TO USE THE DEFENSE COUNSEL SERVICE	<input type="checkbox"/> <input checked="" type="checkbox"/>
j. FOR OFFICIAL USE ONLY INFORMATION	<input checked="" type="checkbox"/> <input type="checkbox"/>	l. OTHER (Specify):	<input type="checkbox"/> <input checked="" type="checkbox"/>
k. OTHER (Specify)	<input type="checkbox"/> <input checked="" type="checkbox"/>		

DD FORM 254, DEC 1999

PREVIOUS EDITION IS OBSOLETE.

12. **PUBLIC RELEASE.** Any information (classified or unclassified) pertaining to this contract shall not be released for public dissemination except as provided by the Industrial Security Manual or unless it has been approved for public release by appropriate U.S. Government authority. Proposed public releases shall be submitted for approval prior to release Direct Through (Specify) **NONE AUTHORIZED. SCI WILL NOT BE RELEASED TO PUBLIC.**
UNLESS CONTRACTOR HAS OBTAINED AUTHORITY TO RELEASE FROM THE DEPARTMENT OF HOMELAND SECURITY, CONTRACTOR SHALL COORDINATE WITH THE COTR AND THE OFFICE OF SECURITY (ASD) ON ALL CHANGES TO THIS GUIDANCE to the Directorate for Freedom of Information and Security Review, Office of the Assistant Secretary of Defense (Public Affairs) for review. *In the case of non-DoD User Agencies, requests for disclosure shall be submitted to that agency.

13. **SECURITY GUIDANCE.** The security classification guidance needed for this classified effort is identified below. If any difficulty is encountered in applying this guidance or if any other contributing factor indicates a need for changes in this guidance, the contractor is authorized and encouraged to provide recommended changes: to challenge the guidance or the classification assigned to any information or material furnished or generated under this contract; and to submit any questions for interpretation of this guidance to the official identified below. Pending final decision, the information involved shall be handled and protected at the highest level of classification assigned or recommended. (Fill in as appropriate for the classified effort. Attach, or forward under separate correspondence, any documents/guidance/extracts referenced herein. Add additional pages as needed to provide complete guidance.)

Ref. Item 10a: COMSEC Access will involve the installation, maintenance, or use of crypto-equipment, systems, or keying material. Access to COMSEC requires a final US Government Clearance. Disclosure to Subcontractor requires prior approval of DHS. The contractor upon award shall contact the DHS COMSEC Control Office if Record (COR) at commercial (540) 542-3848, to receive current COMSEC guidance.

Ref. Item 10e (1). Personnel: All contractor personnel assigned to this contract shall possess security clearances issued by the Defense Security Service (DSS) commensurate with the level of required access to classified information that is directly in support of this contract. Immigrant aliens, personnel cleared on an interim basis, or personnel holding contractor-generated Confidential clearances are not eligible for access to classified information released or generated under this contract. Contractor personnel who are specifically designated as requiring access to Sensitive Compartmented Information (SCI) must be eligible under the provisions of DCID 6/4 without exception. Personnel will be submitted for access by their DHS manager and verified by their Contract Technical Representative. If approved for access, they will receive an indoctrination briefing by DHS security staff prior to being granted access to SCI. All personnel security be scheduled for debriefing with the DHS SSO by calling (202) 282-8643. Note 10e (1) and 11a. Access to all classified information (SCI) will be at DHS facilities only. For the purposes of this contract, the contractor is not authorized to process and/or store any classified information at contractor locations.

Jose

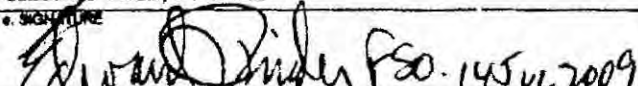
JOSE J. SALAZAR, DHS OFFICE OF SECURITY
PROGRAM MANAGER INDUSTRIAL SECURITY
 (202) 447-5346

14. **ADDITIONAL SECURITY REQUIREMENTS.** Requirements, in addition to ISM requirements, are established for this contract. (If Yes, Yes No identify the pertinent contractual clauses in the contract document itself, or provide an appropriate statement which identifies the additional requirements. Provide a copy of the requirements to the cognizant security office. Use item 13 if additional space is needed.)

15. **INSPECTIONS.** Elements of this contract are outside the inspection responsibility of the cognizant security office. (If Yes, explain and identify specific areas or elements carved out and the activity responsible for inspections. Use item 13 if additional space is needed.) Yes No
"DHS/OS/SSPD CONCURS AND APPROVES THE "NEED-TO-KNOW" AT THE SCI LEVEL"
 Clearances: Access to Intelligence Information requires a final US Government clearance. Subcontracting requires prior approval of the GCA. Briefings: Special briefings and procedures are required.

16. **CERTIFICATION AND SIGNATURE.** Security requirements stated herein are complete and adequate for safeguarding the classified information to be released or generated under this classified effort. All questions shall be referred to the official named below.

a. TYPED NAME OF CERTIFYING OFFICIAL EDWARD J. PINDER	b. TITLE FACILITY SECURITY OFFICER (HOF)	c. TELEPHONE (include Area Code) (856) 486-5266
--	---	--

d. ADDRESS (include Zip Code) LOCKHEED MARTIN SERVICES, INC 2339 ROUTE 70 WEST CHERRY HILL, NJ 08002	17. REQUIRED DISTRIBUTION	
	e. SIGNATURE  FSO-145 VL 2009	<input checked="" type="checkbox"/> a. CONTRACTOR <input checked="" type="checkbox"/> b. SUBCONTRACTOR <input checked="" type="checkbox"/> c. COGNIZANT SECURITY OFFICE FOR PRIME AND SUBCONTRACTOR <input checked="" type="checkbox"/> d. U.S. ACTIVITY RESPONSIBLE FOR OVERSEAS SECURITY ADMINISTRATION <input checked="" type="checkbox"/> e. ADMINISTRATIVE CONTRACTING OFFICER <input checked="" type="checkbox"/> f. OTHERS AS NECESSARY

DD FORM 254 (BACK) DEC 1999

CONTINUATION SHEET FOR BLOCK 13.

**LOCKHEED MARTIN SERVICES INC 2339 ROUTE 70 WEST FLOOR 3W, CHERRY HILL, NJ 08002-3315
CAGE CODE: 77809 CONTRACT# HSHQDC-06-D-00017 HQHSDC-07-J-00138**

Reference Item 10e (1): Access to all Sensitive Compartmented Information (SCI) will be at DHS facilities only. For the purposes of this contract, the contractor is not authorized to process and/or store any classified information at contractor locations.

- a. All SCI will be handled in accordance with special security requirements, which will be furnished by the designated responsible special security office (SSO).
- b. SCI will not be released to contractor employees without specific release approval of the originator of the material as outlined in governing directives; based on prior approval and certification of "need-to-know" by the designated contractor.
- c. All Contractor personnel requiring access to SCI as part of this contract effort must be approved and indoctrinated by DHS. Requests for Access will be submitted by the government project manager who can validate the justification for access.
- d. Inquiries pertaining to classification guidance on SCI will be directed to the Special Security Officer (SSO).
- e. SCI furnished in support of this contract remains the property of the Department of Homeland Security (DHS), agency, or component originator. Upon completion or cancellation of the contract, SCI furnished will be returned to the direct custody of the supporting SSO, or destroyed IAW instructions outlined by the Contract Officer.
- f. Visits by contractor employees will only be certified by DHS when such visits are conducted as part of the contract effort.

Ref Item 10j: "Contractors shall control and safeguard FOUO in accordance with DHS Directive (MD 11042.1) "Safeguarding Sensitive but Unclassified (For Official Use Only) Information," dated Jan 6, 2005. DHS contractors must sign a special Non-Disclosure Agreement before receiving access to FOUO information. Contractors with questions on handling DHS FOUO shall contact DHS OS ASD at (202) 447-5341."

Ref. Item 11a. Contract performance for all SCI work is restricted to DHS Government buildings located in and around the metropolitan area of Washington, D.C., and at other locations in the metropolitan area of Wash DC. All contractor personnel must be U.S. citizens, have been granted a final security clearance by the U.S. Government, have been approved as meeting suitability criteria by DHS CSO, and have been indoctrinated by a Non Disclosure Agreement, Standard Form 312 for this specific program prior to being given any access to such information released or generated under this contract. Immigrant aliens, personnel cleared on an interim basis, or personnel holding contractor granted CONFIDENTIAL clearances, are not eligible for access to classified information released or generated under this contract without the express permission of the CSO through the DHS Personnel Division (DHS/PSD). The contractor and the Contracting Officer Technical Representative or other delegated representative will revalidate all SCI staffing requirements under the contract with the CSO annually or when a revised DD Form 254 is issued, whichever is sooner. SCI WILL NOT BE RELEASED TO PUBLIC.

**DEPARTMENT OF DEFENSE
CONTRACT SECURITY CLASSIFICATION SPECIFICATION**

(The requirements of the DoD Industrial Security Manual apply to all aspects of this effort)

1. CLEARANCE AND SAFEGUARDING

a. FACILITY CLEARANCE REQUIRED
TOP SECRET

b. LEVEL OF SAFEGUARDING REQUIRED
NONE

2. THIS SPECIFICATION IS FOR: (X and complete as applicable)		3. THIS SPECIFICATION IS: (X and complete as applicable)	
<input checked="" type="checkbox"/> a. FRAME CONTRACT NUMBER HSHQDC-06-D-00017 HQHSDC-08-J-00138	<input checked="" type="checkbox"/> a. ORIGINAL (Complete date in all cases) Date (YYMMDD) 20090721	<input type="checkbox"/> b. SUBCONTRACT NUMBER 7200004982	<input type="checkbox"/> b. REVISED (Supersedes all previous specs) Revision No. Date (YYMMDD)
<input type="checkbox"/> c. SOLICITATION OR OTHER NUMBER Due Date (YYMMDD)	<input type="checkbox"/> c. FINAL (Complete item 3 in all cases) Date (YYMMDD)		

4. IS THIS A FOLLOW-ON CONTRACT? YES NO. If Yes complete the following
Classified material received or generated under HSHQDC-06-D-00017 HQHSDC-07-J-00739 (Preceding Contract Number) is transferred to this follow-on contract

5. IS THIS A FINAL DD FORM 254? YES NO. If Yes complete the following
In response to the contractor's request dated _____, retention of the identified classified material is authorized for the period of _____.

6. CONTRACTOR (Include Commercial and Government Entity (CAGE) Code)

a. NAME, ADDRESS, AND ZIP CODE LOCKHEED MARTIN SERVICES, INC 2339 ROUTE 70 WEST CHERRY HILL, NJ 08002-3315	b. CAGE CODE 77609	c. COGNIZANT SECURITY OFFICE (Name, Address, and Zip Code) DEFENSE SECURITY SERVICE 307 FELLOWSHIP ROAD STE 115 MT. LAUREL, NJ 08054-1233
---	-----------------------	--

7. SUBCONTRACTOR

a. NAME, ADDRESS, AND ZIP CODE (b) (4)	b. CAGE CODE 06CT2	c. COGNIZANT SECURITY OFFICES (Name, Address, and Zip Code) DEFENSE SECURITY SERVICE 14428 Albemarle Point Place, Ste 140 Chantilly, VA 20151
--	-----------------------	--

8. ACTUAL PERFORMANCE LOCATION

Department of Homeland Security (DHS) various locations within the Washington, DC metropolitan area.	b. CAGE CODE	c. COGNIZANT SECURITY OFFICE (Name, Address, and Zip Code)
--	--------------	--

9. GENERAL IDENTIFICATION OF THIS PROCUREMENT
(U) Provide IT Operations & Maintenance technical support to Lockheed Martin in support of the IT-NOVA DHS Eagle Task Order. This is in response to Lockheed Martin's requirements to provide support to IT Operations Maintenance and COOP for the DHS Headquarters and Components directly supported by the DHS OCIO.

10. THIS CONTRACT WILL REQUIRE ACCESS TO:	YES	NO	11. IN PERFORMING THIS CONTRACT, THE CONTRACTOR WILL:	YES	NO
a. COMMUNICATIONS SECURITY (COMSEC) INFORMATION	<input checked="" type="checkbox"/>	<input type="checkbox"/>	a. HAVE ACCESS TO CLASSIFIED INFORMATION ONLY AT ANOTHER CONTRACTOR'S FACILITY OR A GOVERNMENT ACTIVITY	<input checked="" type="checkbox"/>	<input type="checkbox"/>
b. RESTRICTED DATA	<input type="checkbox"/>	<input checked="" type="checkbox"/>	b. RECEIVE CLASSIFIED DOCUMENTS ONLY	<input type="checkbox"/>	<input checked="" type="checkbox"/>
c. CRITICAL NUCLEAR WEAPON DESIGN INFORMATION	<input type="checkbox"/>	<input checked="" type="checkbox"/>	c. RECEIVE AND GENERATE CLASSIFIED MATERIAL	<input type="checkbox"/>	<input checked="" type="checkbox"/>
d. FORMERLY RESTRICTED DATA	<input type="checkbox"/>	<input checked="" type="checkbox"/>	d. FABRICATE, MODIFY, OR STORE CLASSIFIED HARDWARE	<input type="checkbox"/>	<input checked="" type="checkbox"/>
e. INTELLIGENCE INFORMATION	<input checked="" type="checkbox"/>	<input type="checkbox"/>	e. PERFORM SERVICES ONLY	<input type="checkbox"/>	<input checked="" type="checkbox"/>
(1) Sensitive Compartmented Information (SCI)	<input checked="" type="checkbox"/>	<input type="checkbox"/>	f. HAVE ACCESS TO U.S. CLASSIFIED INFORMATION OUTSIDE THE U.S., PUERTO RICO, U.S. POSSESSIONS AND TRUST TERRITORIES	<input type="checkbox"/>	<input checked="" type="checkbox"/>
(2) Non-SCI	<input type="checkbox"/>	<input checked="" type="checkbox"/>	g. BE AUTHORIZED TO USE THE SERVICES OF DEFENSE TECHNICAL INFORMATION CENTER (DTIC) OR OTHER SECONDARY DISTRIBUTION CENTER	<input type="checkbox"/>	<input checked="" type="checkbox"/>
f. SPECIAL ACCESS INFORMATION	<input type="checkbox"/>	<input checked="" type="checkbox"/>	h. REQUIRE A COMSEC ACCOUNT	<input type="checkbox"/>	<input checked="" type="checkbox"/>
g. NATO INFORMATION	<input type="checkbox"/>	<input checked="" type="checkbox"/>	i. HAVE A TEMPEST REQUIREMENT	<input type="checkbox"/>	<input checked="" type="checkbox"/>
h. FOREIGN GOVERNMENT INFORMATION	<input type="checkbox"/>	<input checked="" type="checkbox"/>	j. HAVE OPERATIONS SECURITY (OPSEC) REQUIREMENTS	<input type="checkbox"/>	<input checked="" type="checkbox"/>
i. LIMITED DISSEMINATION INFORMATION	<input type="checkbox"/>	<input checked="" type="checkbox"/>	k. BE AUTHORIZED TO USE THE DEFENSE COURIER SERVICE	<input type="checkbox"/>	<input checked="" type="checkbox"/>
j. FOR OFFICIAL USE ONLY INFORMATION	<input checked="" type="checkbox"/>	<input type="checkbox"/>	l. OTHER (Specify):	<input type="checkbox"/>	<input checked="" type="checkbox"/>
k. OTHER (Specify):	<input type="checkbox"/>	<input checked="" type="checkbox"/>			

12. PUBLIC RELEASE. Any information (classified or unclassified) pertaining to this contract shall not be released for public dissemination except as provided by the Industrial Security Manual or unless it has been approved for public release by appropriate U.S. Government authority. Proposed public releases shall be submitted for approval prior to release Direct Through (Specify) **NONE AUTHORIZED. SCI WILL NOT BE RELEASED TO PUBLIC.**

UNLESS CONTRACTOR HAS OBTAINED AUTHORITY TO RELEASE FROM THE DEPARTMENT OF HOMELAND SECURITY, CONTRACTOR SHALL COORDINATE WITH THE COTR AND THE OFFICE OF SECURITY (ASD) ON ALL CHANGES TO THIS GUIDANCE. to the Directorate for Freedom of Information and Security Review, Office of the Assistant Secretary of Defense (Public Affairs) for review. *In the case of non-DoD User Agencies, requests for disclosure shall be submitted to that agency

13. SECURITY GUIDANCE. The security classification guidance needed for this classified effort is identified below. If any difficulty is encountered in applying this guidance or if any other contributing factor indicates a need for changes in this guidance, the contractor is authorized and encouraged to provide recommended changes: to challenge the guidance or the classification assigned to any information or material furnished or generated under this contract; and to submit any questions for interpretation of this guidance to the official identified below. Pending final decision, the information involved shall be handled and protected at the highest level of classification assigned or recommended. (Fill in as appropriate for the classified effort. Attach, or forward under separate correspondence, any documents/guides/extracts referenced herein. Add additional pages as needed to provide complete guidance.)

Ref. Item 10a: COMSEC Access will involve the installation, maintenance, or use of crypto-equipment, systems, or keying material. Access to COMSEC requires a final US Government Clearance. Disclosure to Subcontractor requires prior approval of DHS. The contractor upon award shall contact the DHS COMSEC Control Office if Record (COR) at commercial (540) 542-3848, to receive current COMSEC guidance.

Ref. Item 10e (1). Personnel: All contractor personnel assigned to this contract shall possess security clearances issued by the Defense Security Service (DSS) commensurate with the level of required access to classified information that is directly in support of this contract. Immigrant aliens, personnel cleared on an interim basis, or personnel holding contractor-generated Confidential clearances are not eligible for access to classified information released or generated under this contract. Contractor personnel who are specifically designated as requiring access to Sensitive Compartmented Information (SCI) must be eligible under the provisions of DCID 6/4 without exception. Personnel will be submitted for access by their DHS manager and verified by their Contract Technical Representative. If approved for access, they will receive an indoctrination briefing by DHS security staff prior to being granted access to SCI. All personnel security be scheduled for debriefing with the DHS SSO by calling (202) 282-8643. **Note 10e (1) and 11a.** Access to all classified information (SCI) will be at DHS facilities only. For the purposes of this contract, the contractor is not authorized to process and/or store any classified information at contractor locations.

Jose J. Salazar
**JOSE J. SALAZAR, DHS OFFICE OF SECURITY
 PROGRAM MANAGER INDUSTRIAL SECURITY
 (202) 447-5346**

14. ADDITIONAL SECURITY REQUIREMENTS. Requirements, in addition to ISM requirements, are established for this contract. (If Yes, Yes No identify the pertinent contractual clauses in the contract document itself, or provide an appropriate statement which identifies the additional requirements. Provide a copy of the requirements to the cognizant security office. Use Item 13 if additional space is needed.)

15. INSPECTIONS. Elements of this contract are outside the inspection responsibility of the cognizant security office. (If Yes, explain and identify specific areas or elements carved out and the activity responsible for inspections. Use Item 13 if additional space is needed.) Yes No

"DHS/SOS/SSPD CONCURS AND APPROVES THE "NEED-TO-KNOW" AT THE SCI LEVEL"

Jose J. Salazar Clearances: Access to Intelligence information requires a final US Government clearance. Subcontracting requires prior approval of the GCA. Briefings: Special briefings and procedures are required.

16. CERTIFICATION AND SIGNATURE. Security requirements stated herein are complete and adequate for safeguarding the classified information to be released or generated under this classified effort. All questions shall be referred to the official named below.

a. TYPED NAME OF CERTIFYING OFFICIAL EDWARD J. PINDER	b. TITLE FACILITY SECURITY OFFICER (HOF)	c. TELEPHONE (Include Area Code) (856) 486-5266
--	---	--

d. ADDRESS (Include Zip Code)
 LOCKHEED MARTIN SERVICES, INC
 2339 ROUTE 70 WEST
 CHERRY HILL, NJ 08002

17. REQUIRED DISTRIBUTION

<input checked="" type="checkbox"/>	a. CONTRACTOR
<input checked="" type="checkbox"/>	b. SUBCONTRACTOR
<input checked="" type="checkbox"/>	c. COGNIZANT SECURITY OFFICE FOR PRIME AND SUBCONTRACTOR
<input checked="" type="checkbox"/>	d. U.S. ACTIVITY RESPONSIBLE FOR OVERSEAS SECURITY ADMINISTRATION
<input checked="" type="checkbox"/>	e. ADMINISTRATIVE CONTRACTING OFFICER
<input checked="" type="checkbox"/>	f. OTHERS AS NECESSARY

e. SIGNATURE
Edward J. Pinder FSO. 22-JUN-2009

CONTINUATION SHEET FOR BLOCK 13.

**LOCKHEED MARTIN SERVICES INC 2339 ROUTE 70 WEST FLOOR 3W, CHERRY HILL, NJ 08002-3315
CAGE CODE: 77609 CONTRACT# HSHQDC-06-D-00017 HQHSDC-07-J-00138**

Reference Item 10e (1): Access to all Sensitive Compartmented Information (SCI) will be at DHS facilities only. For the purposes of this contract, the contractor is not authorized to process and/or store any classified information at contractor locations.

- a. All SCI will be handled in accordance with special security requirements, which will be furnished by the designated responsible special security office (SSO).
- b. SCI will not be released to contractor employees without specific release approval of the originator of the material as outlined in governing directives; based on prior approval and certification of "need-to-know" by the designated contractor.
- c. All Contractor personnel requiring access to SCI as part of this contract effort must be approved and indoctrinated by DHS. Requests for Access will be submitted by the government project manager who can validate the justification for access.
- d. Inquiries pertaining to classification guidance on SCI will be directed to the Special Security Officer (SSO).
- e. SCI furnished in support of this contract remains the property of the Department of Homeland Security (DHS), agency, or component originator. Upon completion or cancellation of the contract, SCI furnished will be returned to the direct custody of the supporting SSO, or destroyed IAW instructions outlined by the Contract Officer.
- f. Visits by contractor employees will only be certified by DHS when such visits are conducted as part of the contract effort.

Ref Item 10j: "Contractors shall control and safeguard FOUO in accordance with DHS Directive (MD 11042.1) "Safeguarding Sensitive but Unclassified (For Official Use Only) Information," dated Jan 6, 2005. DHS contractors must sign a special Non-Disclosure Agreement before receiving access to FOUO information. Contractors with questions on handling DHS FOUO shall contact DHS OS ASD at (202) 447-5341."

Ref. Item 11a. Contract performance for all SCI work is restricted to DHS Government buildings located in and around the metropolitan area of Washington, D.C., and at other locations in the metropolitan area of Wash DC. All contractor personnel must be U.S. citizens, have been granted a final security clearance by the U.S. Government, have been approved as meeting suitability criteria by DHS CSO, and have been indoctrinated by a Non Disclosure Agreement, Standard Form 312 for this specific program prior to being given any access to such information released or generated under this contract. Immigrant aliens, personnel cleared on an interim basis, or personnel holding contractor granted CONFIDENTIAL clearances, are not eligible for access to classified information released or generated under this contract without the express permission of the CSO through the DHS Personnel Division (DHS/PSD). The contractor and the Contracting Officer Technical Representative or other delegated representative will revalidate all SCI staffing requirements under the contract with the CSO annually or when a revised DD Form 254 is issued, whichever is sooner.
SCI WILL NOT BE RELEASED TO PUBLIC.

AMENDMENT OF SOLICITATION/MODIFICATION OF CONTRACT		1 CONTRACT ID CODE	PAGE OF PAGES 1 8
2 AMENDMENT/MODIFICATION NO P00010	3 EFFECTIVE DATE See Block 16C	4 REQUISITION/PURCHASE REQ NO RUIO-09-HS142	5 PROJECT NO (If applicable)
6 ISSUED BY U.S. Dept. of Homeland Security Office of Procurement Operations Information Tech. Acquisition Div. 245 Murray Lane, SW Building 410 Washington DC 20528	CODE DHS/OPO/ITAC	7 ADMINISTERED BY (If other than Item 6) U.S. Dept. of Homeland Security Office of Procurement Operations Information Tech. Acquisition Div. 245 Murray Lane, SW Building 410 Washington DC 20528	CODE DHS/OPO/ITAC
8 NAME AND ADDRESS OF CONTRACTOR (No. street, county, State and ZIP Code) LOCKHEED MARTIN SERVICES INC 2339 ROUTE 70 WEST FLOOR 3W CHERRY HILL NJ 080023315		(x) 9A AMENDMENT OF SOLICITATION NO	9B DATED (SEE ITEM 11)
CODE 8052583730000 FACILITY CODE		X 10A MODIFICATION OF CONTRACT/ORDER NO HSHQDC-06-D-00017 HSHQDC-08-J-00138	10B DATED (SEE ITEM 13) 06/02/2008

11. THIS ITEM ONLY APPLIES TO AMENDMENTS OF SOLICITATIONS

The above numbered solicitation is amended as set forth in Item 14. The hour and date specified for receipt of Offers is extended. is not extended. Offers must acknowledge receipt of this amendment prior to the hour and date specified in the solicitation or as amended, by one of the following methods: (a) By completing Items 8 and 15, and returning _____ copies of the amendment; (b) By acknowledging receipt of this amendment on each copy of the offer submitted; or (c) By separate letter or telegram which includes a reference to the solicitation and amendment numbers. FAILURE OF YOUR ACKNOWLEDGEMENT TO BE RECEIVED AT THE PLACE DESIGNATED FOR THE RECEIPT OF OFFERS PRIOR TO THE HOUR AND DATE SPECIFIED MAY RESULT IN REJECTION OF YOUR OFFER. If by virtue of this amendment you desire to change an offer already submitted, such change may be made by telegram or letter, provided each telegram or letter makes reference to the solicitation and this amendment, and is received prior to the opening hour and date specified.

12 ACCOUNTING AND APPROPRIATION DATA (If required) Net Increase: \$2,918,860.00
See Schedule

13. THIS ITEM ONLY APPLIES TO MODIFICATION OF CONTRACTS/ORDERS. IT MODIFIES THE CONTRACT/ORDER NO. AS DESCRIBED IN ITEM 14.

CHECK ONE	A THIS CHANGE ORDER IS ISSUED PURSUANT TO (Specify authority) THE CHANGES SET FORTH IN ITEM 14 ARE MADE IN THE CONTRACT ORDER NO. IN ITEM 10A
	B THE ABOVE NUMBERED CONTRACT/ORDER IS MODIFIED TO REFLECT THE ADMINISTRATIVE CHANGES (such as changes in paying office, appropriation date, etc.) SET FORTH IN ITEM 14, PURSUANT TO THE AUTHORITY OF FAR 43.103(b)
X	C THIS SUPPLEMENTAL AGREEMENT IS ENTERED INTO PURSUANT TO AUTHORITY OF FAR 43.103(a)(3)
	D OTHER (Specify type of modification and authority)

E. IMPORTANT: Contractor is not. is required to sign this document and return 1 copies to the issuing office

14 DESCRIPTION OF AMENDMENT/MODIFICATION (Organized by UCF section headings, including solicitation/contract subject matter where feasible)

DUNS Number: 805258373+0000

1. The purpose of this modification is to provide additional funding to Contract Line Item Number (CLIN) 1002 - Option Year 1: Operation and Maintenance Support Service HSD ODCs. The funding will support purchases of new/renewal software licenses and travel.

2. In addition, FAR Clause 52.232-22, "Limitation of Funds" is added to new Section I.15 and Section B.3.1(d).

See Pages 2-7 for continuation of modification details.

Continued ...

Except as provided herein, all terms and conditions of the document referenced in Item 9A or 10A, as heretofore changed, remains unchanged and in full force and effect

15A NAME AND TITLE OF SIGNER (Type or print) Zanetta Williams Contracts Mgr.	15B CONTRACTOR/OFFEROR 	15C DATE SIGNED 9/25/09	16A NAME AND TITLE OF CONTRACTING OFFICER (Type or print) Rebecca A. Taylor	16B UNITED STATES OF AMERICA 	16C DATE SIGNED SEP 25 2009
---	----------------------------	----------------------------	--	----------------------------------	--------------------------------

NSN 7540-01-152-8070
Previous edition unusable

STANDARD FORM 30 (REV. 10-83)
Prescribed by GSA
FAR (48 CFR) 53.243

CONTINUATION SHEET

REFERENCE NO OF DOCUMENT BEING CONTINUED
 HSHQDC-06-D-00017, HSHQDC-08-J-00138/P00010

PAGE 2 OF 8

NAME OF OFFEROR OR CONTRACTOR
 LOCKHEED MARTIN SERVICES INC

MNO A)	SUPPLIES/SERVICES (B)	QUANTITY (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)
1002	<p>Discount Terms: Net 30 FOB: Destination Period of Performance: 06/01/2008 to 01/31/2013</p> <p>Change Item 1002 to read as follows (amount shown is the obligated amount):</p> <p>Option Year 1 Operation and Maintenance Support Service HSD ODCs (Travel and Direct Materials associated directly with the performance under this task order.): PWS Sections: C.5.1 through C.5.13 and C.5.15</p> <p>This Modification P00010 provides \$2,918,860.00 in additional funding to support travel and new/renewal software licenses as described at pages 6-8, "Modification to Task Order HSHQDC-08-J-00138, IT-NOVA O&M Contract". The \$2,918,860.00 is earmarked as follows:</p> <p>Travel.....\$78,400.65 Software Licenses.....\$2,840,459.35</p> <p>The Not-to-Exceed (NTE) amount of CLIN 1002 is increased from \$2,303,404.86 by \$2,918,860.00 to \$5,222,264.86.</p> <p>Period of Performance: 05/04/2009 through 01/31/2010 Product/Service Code: D399 Product/Service Description: OTHER ADP & TELECOMMUNICATIONS SERVICES</p> <p>Accounting Info: RWC9049 RWC WF-99-01-00-000-02-05-0400-05-00-00-00 GE OE 25 41 FY2009 Funded: \$0.00</p> <p>Accounting Info: BCEF-NONE009-000-MA-20-01-00-000-02-07-0800-00-00-00-00-000000 Funded: \$0.00</p> <p>Accounting Info: RWC9049-RWC-WR-99-01-00-000-02-05-0400-05-00-00-00 -GE-OE-25-41-FY2009 Funded: \$2,918,860.00</p>				2,918,860.00

SF-30 CONTINUATION SHEET

1. Add FAR Clause 52.232-22, entitled "Limitation of Funds" to **new Section I.15**. In accordance with Homeland Security Acquisition Manual (HSAM) 3032.702, incremental funding for Cost-Reimbursement contracts or for the Material portion of a Time and Materials type contract is allowed, provided Clause 52.232-22 is included as appropriate. The new section reads as follows:

I.15 FAR 52.232-22 LIMITATION OF FUNDS (APR 1984)

(a) The parties estimate that performance of this contract will not cost the Government more than (1) the estimated cost specified in the Schedule or, (2) if this is a cost-sharing contract, the Government's share of the estimated cost specified in the Schedule. The Contractor agrees to use its best efforts to perform the work specified in the Schedule and all obligations under this contract within the estimated cost, which, if this is a cost-sharing contract, includes both the Government's and the Contractor's share of the cost.

(b) The Schedule specifies the amount presently available for payment by the Government and allotted to this contract, the items covered, the Government's share of the cost if this is a cost-sharing contract, and the period of performance it is estimated the allotted amount will cover. The parties contemplate that the Government will allot additional funds incrementally to the contract up to the full estimated cost to the Government specified in the Schedule, exclusive of any fee. The Contractor agrees to perform, or have performed, work on the contract up to the point at which the total amount paid and payable by the Government under the contract approximates but does not exceed the total amount actually allotted by the Government to the contract.

(c) The Contractor shall notify the Contracting Officer in writing whenever it has reason to believe that the costs it expects to incur under this contract in the next 60 days, when added to all costs previously incurred, will exceed 75 percent of (1) the total amount so far allotted to the contract by the Government or, (2) if this is a cost-sharing contract, the amount then allotted to the contract by the Government plus the Contractor's corresponding share. The notice shall state the estimated amount of additional funds required to continue performance for the period specified in the Schedule.

(d) Sixty days before the end of the period specified in the Schedule, the Contractor shall notify the Contracting Officer in writing of the estimated amount of additional funds, if any, required to continue timely performance under the contract or for any further period specified in the Schedule or otherwise agreed upon, and when the funds will be required.

(e) If, after notification, additional funds are not allotted by the end of the period specified in the Schedule or another agreed-upon date, upon the Contractor's written request the Contracting Officer will terminate this contract on that date in accordance with the provisions of the Termination clause of this contract. If the Contractor estimates that the funds available will allow it to continue to discharge its obligations beyond that date, it may specify a later date in its request, and the Contracting Officer may terminate this contract on that later date.

(f) Except as required by other provisions of this contract, specifically citing and stated to be an exception to this clause—

(1) The Government is not obligated to reimburse the Contractor for costs incurred in excess of the total amount allotted by the Government to this contract; and

(2) The Contractor is not obligated to continue performance under this contract (including actions under the Termination clause of this contract) or otherwise incur costs in excess of—

(i) The amount then allotted to the contract by the Government or;

(ii) If this is a cost-sharing contract, the amount then allotted by the Government to the contract plus the Contractor's corresponding share, until the Contracting Officer notifies the Contractor in writing that the amount allotted by the Government has been increased and specifies an increased amount, which shall then constitute the total amount allotted by the Government to this contract.

(g) The estimated cost shall be increased to the extent that (1) the amount allotted by the Government or, (2) if this is a cost-sharing contract, the amount then allotted by the Government to the contract plus the Contractor's corresponding share, exceeds the estimated cost specified in the Schedule. If this is a cost-sharing contract, the increase shall be allocated in accordance with the formula specified in the Schedule.

(h) No notice, communication, or representation in any form other than that specified in paragraph (f)(2) of this clause, or from any person other than the Contracting Officer, shall affect the amount allotted by the Government to this contract. In the absence of the specified notice, the Government is not obligated to reimburse the Contractor for any costs in excess of the total amount allotted by the Government to this contract, whether incurred during the course of the contract or as a result of termination.

(i) When and to the extent that the amount allotted by the Government to the contract is increased, any costs the Contractor incurs before the increase that are in excess of—

(1) The amount previously allotted by the Government or;

(2) If this is a cost-sharing contract, the amount previously allotted by the Government to the contract plus the Contractor's corresponding share, shall be allowable to the same extent as if incurred afterward, unless the Contracting Officer issues a termination or other notice and directs that the increase is solely to cover termination or other specified expenses.

(j) Change orders shall not be considered an authorization to exceed the amount allotted by the Government specified in the Schedule, unless they contain a statement increasing the amount allotted.

(k) Nothing in this clause shall affect the right of the Government to terminate this contract. If this contract is terminated, the Government and the Contractor shall negotiate an equitable distribution of all property produced or purchased under the contract, based upon the share of costs incurred by each.

(l) If the Government does not allot sufficient funds to allow completion of the work, the Contractor is entitled to a percentage of the fee specified in the Schedule equalling the percentage of completion of the work contemplated by this contract.

(End of clause)

2. Revise paragraph (d) ODCs at **Section B.3.1 Time and Material Labor** to add FAR Clause 52.232-22 Limitation of Funds; which section will read as follows:

(d) ODCs. During the life of the task order, the Government may order Other Direct Costs (ODCs) in an amount not to exceed \$74 million for each 12 month performance period. Each ODC Contract Line Item Number (CLIN) and dollar amount represents a quarterly allocation and is optional. It is anticipated that ODCs will be funded quarterly using Working Capital Funds; hence, ODCs under this task order are subject to FAR 52.232.18-Availability of Funds **and FAR 52.232-22-Limitation of Funds**. ODCs shall be reimbursed **subject to FAR clause 52.232-22**. ODCs consist of materials, subcontractor (other than labor) and task order-related travel costs, i.e., relocation and

temporary duty (TDY) to include travel, lodging and meals. The ODC percentages are indicated on the Section B.5 Labor Rate Table under the ODC rates. Deployment orders will include quantity of hours required at the proposed rates herein for each labor category, plus materials (ODCs) and the fixed ODC markup percentages. The cost of general-purpose items required for the conduct of the Contractor's normal business operations will not be considered an allowable ODC in the performance of work under this task order. See also Section G and Section H for limitations on materials and mandatory support documentation. Profit is not allowed on ODCs under this task order. All travel costs associated with this task order, if applicable, shall be in accordance with the Federal Travel Regulations (see Section G).

3. The value and total amount funded/obligated to the task order is increased from \$78,151,545.74 by \$2,918,860.00 to \$80,070,405.74.
4. The ceiling for this task order remains unchanged at \$288,499,204.00.
5. All other terms and conditions remain unchanged.

**Modification to Task Order HSHQDC-08-J-00138
IT-NOVA O&M Contract**

Period of Performance:
May 4, 2009 – January 31, 2010
(Effective date for this requirement: September 25, 2009)

Travel – \$78,400.65

Travel in this contract is in support of the following:

- Training
- Conferences
- Deployment Support
- Overseas Travel

Per direction of the COTR, travel may include but is not limited to:

- Site A for DHS Coop Exercises
- Designated Federal Security Events
- Various Sites outside the Washington Metropolitan Area to include EPIC – El Paso, TX; Atlantic City, NJ; Immigration and Customs Enforcement’s TIC facility in Stennis, MS; Data Center 1; Data Center 2
- Over-seas travel – London, England (COMSEC)
- Conferences/Training – Charlotte, NC; Boston, MA; San Diego, CA; Orlando, FL

Software Licenses -- (b) (4)

Below are the existing and new software identified to support the DHS mission. The Contractor affirms that there is not any known travel costs associated with the installation of software. These software licenses are described and broken down as follows:

- **Renewal Software Licenses**
 - (b) (4) – Annual maintenance costs for telephone systems at Vermont Ave., Glebe Road, New York Ave., 7th & D Street, Fairfax Drive, 1125 15th Street, Nebraska Ave.
 - (b) (4) (archiving of emails, reducing online storage), NetBackup (software used to backup the DHS HQ environment).
 - (b) (4) [Redacted]
Manager. First year maintenance and upgrades included.
 - (b) (4) [Redacted]

(b) (4)

- (b) (4) in for active directory per enabled user account license/maintenance. First year maintenance and upgrades includes.

- **New Software Licenses**

- (b) (4) device manager is an integral part of the end-to-end nature of the total solution by giving help desk personnel and administrators of the BlackBerry® Enterprise Solution access to real-time information about BlackBerry smart phones, enabling them to find lost or stolen handsets, proactively monitor and diagnose issues, and audit devices for rogue third party applications – all leading to significant cost savings, improved service levels and corporate compliance.
- (b) (4) – Virtual Private Network (VPN) software supporting remote users and tele-work initiative.
- (b) (4) Professional Edition. Provides utilities to model, edit, transform, and debug XML related technologies. This software also offers file converter, debuggers, support for (b) (4), and major databases.
- (b) (4) (b) (4) is an administrative tool that allows easy integration and reporting of Active Directory + Exchange 200x into a single tool, allowing administrative changes to multiple accounts and domains in a few mouse clicks.
- (b) (4) is a software application suite that manages network equipment. (b) (4) can do the following:
 1. Performance monitoring
 2. Netflow monitoring
 3. IP Address management
 4. Engineering Technical tools
 5. Network Equipment Config Management
 6. Network Equipment Syslog Management
- (b) (4)
- (b) (4) (b) (4) is a file archiving solution that can be used as a data migration or tiered solution. This software based tool can run as a policy engine via limits to tier storage off to another location based on set policies.
- (b) (4)
 - (1) (b) (4) Software tool that can be used to monitor and manage DMX arrays along with other arrays. This software tool allows for alerts and specialized reports to be created also.
 - (2) (b) (4) this software tool utilizes the function of de-duplication on servers.

New Projects –

- (b) (4)
 - This will provide the licenses for the existing (b) (4) and hardware platforms.