ORDER FOR SUPPLIES OR SERVICES

IMPORTANT: Mark all packages and papers with contract and/or order numbers.

PAGE OF PAGES: 1 | 47

1. DATE OF ORDER

2. CONTRACT NO. *(If any)*
HSHQDC-13-D-E2075

3. ORDER NO.
HSSCCG-17-J-00003

4. REQUISITION/REFERENCE NO.
CISOIT17005

5. ISSUING OFFICE *(Address correspondence to)*
USCIS Contracting Office
Department of Homeland Security
70 Kimball Avenue
South Burlington VT 05403

6. SHIP TO:

a. NAME OF CONSIGNEE
Department of Homeland Security

b. STREET ADDRESS
US Citizenship & Immigration Svcs
Office of Information Technology
111 Massachusetts Ave, NW
Suite 5000

c. CITY
Washington

d. STATE
DC

e. ZIP CODE
20529

f. SHIP VIA

7. TO:

a. NAME OF CONTRACTOR
SEVATEC INC

b. COMPANY NAME

c. STREET ADDRESS
3112 FAIRVIEW PARK DRIVE

d. CITY
FALLS CHURCH

e. STATE
VA

f. ZIP CODE
220424504

8. TYPE OF ORDER

□ a. PURCHASE
REFERENCE YOUR:

Please furnish the following on the terms and conditions specified on both sides of this order and on the attached sheet, if any, including delivery as indicated.

☒ b. DELIVERY
Except for billing instructions on the reverse, this delivery order is subject to instructions contained on this side only of this form and is issued subject to the terms and conditions of the above-numbered contract.

9. ACCOUNTING AND APPROPRIATION DATA
See Schedule

10. REQUISITIONING OFFICE
USCIS Contracting Office

11. BUSINESS CLASSIFICATION *(Check appropriate box(es))*
☒ a. SMALL □ b. OTHER THAN SMALL □ c. DISADVANTAGED □ d. WOMEN-OWNED □ e. HUBZone
□ f. SERVICE-DISABLED VETERAN-OWNED □ g. WOMEN-OWNED SMALL BUSINESS (WOSB) ELIGIBLE UNDER THE WOSB PROGRAM □ h. EDWOSB

12. F.O.B. POINT
Destination

13. PLACE OF
a. INSPECTION
Destination
b. ACCEPTANCE
Destination

14. GOVERNMENT B/L NO.

15. DELIVER TO F.O.B. POINT ON OR BEFORE *(Date)*

16. DISCOUNT TERMS
Net 30

17. SCHEDULE *(See reverse for Rejections)*

ITEM NO. (a)	SUPPLIES OR SERVICES (b)	QUANTITY ORDERED (c)	UNIT (d)	UNIT PRICE (e)	AMOUNT (f)	QUANTITY ACCEPTED (g)
	DUNS Number: 132599668+0000 | Transformation, Integration & Configuration Services (TICS II) This order is subject to the Terms and Continued ...					

18. SHIPPING POINT

19. GROSS SHIPPING WEIGHT

20. INVOICE NO.

17(h) TOTAL (Cont. pages)
$[redacted]

SEE BILLING INSTRUCTIONS ON REVERSE

21. MAIL INVOICE TO:

a. NAME
See Invoicing Instructions

b. STREET ADDRESS (or P.O. Box)

c. CITY

d. STATE

e. ZIP CODE

17(i) GRAND TOTAL
$[redacted]

22. UNITED STATES OF AMERICA BY *(Signature)*
21Apr17

23. NAME *(Typed)*
SHAWN T. JENKINS
TITLE: CONTRACTING/ORDERING OFFICER

AUTHORIZED FOR LOCAL REPRODUCTION
PREVIOUS EDITION NOT USABLE

ORDER FOR SUPPLIES OR SERVICES
SCHEDULE - CONTINUATION

PAGE NO
2

IMPORTANT: Mark all packages and papers with contract and/or order numbers.

DATE OF ORDER	CONTRACT NO.	ORDER NO.
	HSHQDC-13-D-E2075	HSSCCG-17-J-00003

ITEM NO. (a)	SUPPLIES/SERVICES (b)	QUANTITY ORDERED (c)	UNIT (d)	UNIT PRICE (e)	AMOUNT (f)	QUANTITY ACCEPTED (g)
	Conditions of the Contractor's EAGLE II contract. AAP Number: 2016031771 DO/DPAS Rating: NONE Period of Performance: 06/03/2017 to 06/02/2019					
0001	Transition-In Accounting Info: ITINTCG TIC EP 20-05-00-000 23-20-0500-00-00-00-00 GE-31-24-00 000000 Funded: [redacted]	[redacted]	[redacted]	[redacted]	[redacted]	
0002	[redacted] Accounting Info: ITINTCG TIC EP 20-05-00-000 23-20-0500-00-00-00-00 GE-31-24-00 000000 Funded: [redacted]	[redacted]	[redacted]	[redacted]	[redacted]	
0003	[redacted] Accounting Info: ITINTCG TIC EP 20-05-00-000 23-20-0500-00-00-00-00 GE-31-24-00 000000 Funded: [redacted]	[redacted]	[redacted]	[redacted]	[redacted]	
0004	[redacted] Accounting Info: ITINTCG TIC EP 20-05-00-000 23-20-0500-00-00-00-00 GE-31-24-00 000000 Funded: [redacted]	[redacted]	[redacted]	[redacted]	[redacted]	
0005	[redacted] Amount: [redacted] [redacted] Anticipated Exercise Date: 60 Days After Award Accounting Info: Continued ...	[redacted]	[redacted]	[redacted]	0.00	

TOTAL CARRIED FORWARD TO 1ST PAGE (ITEM 17(H)) ▷ [redacted]

ORDER FOR SUPPLIES OR SERVICES
SCHEDULE - CONTINUATION

IMPORTANT: Mark all packages and papers with contract and/or order numbers.

DATE OF ORDER	CONTRACT NO.	ORDER NO.
	HSHQDC-13-D-E2075	HSSCCG-17-J-00003

ITEM NO. (a)	SUPPLIES/SERVICES (b)	QUANTITY ORDERED (c)	UNIT (d)	UNIT PRICE (e)	AMOUNT (f)	QUANTITY ACCEPTED (g)
	Funded: $0.00					
1002	[redacted] Amount: [redacted](Option Line Item) Anticipated Exercise Date: Accounting Info: Funded: $0.00	[redacted]	[redacted]	[redacted]	0.00	
1003	[redacted] Amount: [redacted](Option Line Item) Anticipated Exercise Date: Accounting Info: Funded: $0.00	[redacted]	[redacted]	[redacted]	0.00	
1004	[redacted] Amount: [redacted](Option Line Item) Anticipated Exercise Date:	[redacted]	[redacted]	[redacted]	0.00	
1005	[redacted] Amount: $[redacted] Option Line Item) Anticipated Exercise Date:	[redacted]	[redacted]	[redacted]	0.00	
2002	[redacted] Amount: [redacted](Option Line Item) Anticipated Exercise Date: Accounting Info: Funded: $0.00	[redacted]	[redacted]	[redacted]	0.00	
2003	[redacted] Amount: $[redacted](Option Line Item) Anticipated Exercise Date: Accounting Info: Funded: $0.00	[redacted]	[redacted]	[redacted]	0.00	
2004	[redacted] Amount: [redacted]Option Line Continued ...	[redacted]	[redacted]	[redacted]	0.00	

TOTAL CARRIED FORWARD TO 1ST PAGE (ITEM 17(H)) ▷ $0.00

ORDER FOR SUPPLIES OR SERVICES
SCHEDULE - CONTINUATION

PAGE NO
4

IMPORTANT: Mark all packages and papers with contract and/or order numbers.

DATE OF ORDER	CONTRACT NO.	ORDER NO.
	HSHQDC-13-D-E2075	HSSCCG-17-J-00003

ITEM NO. (a)	SUPPLIES/SERVICES (b)	QUANTITY ORDERED (c)	UNIT (d)	UNIT PRICE (e)	AMOUNT (f)	QUANTITY ACCEPTED (g)
	Item) Anticipated Exercise Date:					
2005	[redacted] Amount: [redacted]Option Line Item) Anticipated Exercise Date: Contracting Officer Representative (COR): Sheila Murali sheila.m.murali@uscis.dhs.gov 202-272-0930 Contract Specialist (CS): Hollie Walsh hollie.l.walsh@uscis.dhs.gov 802-872-4649 Contracting Officer (CO): Shawn Jenkins shawn.t.jenkins@uscis.dhs.gov The total amount of award: [redacted] The obligation for this award is shown in box 17(i).		[redacted]	[redacted]	0.00	
	TOTAL CARRIED FORWARD TO 1ST PAGE (ITEM 17(H))	▷			$0.00	

TICS II

HSSCCG-17-J-00003

List of Attachments

Attch No.	Title	
1	Statement of Work	15
2	Task Order Clauses	6
3	Security Requirements	19
4	Capitalized Property, Plant and Equipment (PP&E) Assets IUS	2

STATEMENT OF WORK

Transformation Integration and Configuration Services (TICS) II

1. AGENCY MISSION AND GOALS

U.S. Citizenship and Immigration Services (USCIS) oversees lawful immigration to the United States. USCIS secures America's promise as a nation of immigrants by providing accurate and useful information to our customers, granting immigration and citizenship benefits, promoting an awareness and understanding of citizenship, and ensuring the integrity of our immigration system.

2. BACKGROUND

Enforcing and administering United States immigration laws through USCIS business Transformation is a priority goal of the Department of Homeland Security (DHS). In its current state, USCIS relies largely on the movement of paper to deliver immigration benefits and services. In the near future, USCIS will utilize a paperless electronic immigration system that will transform nearly all of the agency's processes.

The challenges facing USCIS today are numerous. It has become evident that traditional testing techniques do not fully identify software defects. USCIS OIT has adopted Agile testing techniques and continuous integration, instead of traditional testing techniques, to address the agency's need for efficient, comprehensive testing and integration.

Transformation Integration and Configuration Services (TICS II) will provide continuous development, maintenance and enhancement of various automated tools by providing self-service platforms and tools so the developers can perform continuous IT code integration and configuration management services in direct support of USCIS Agency and Transformation goals. USCIS intends to adopt a standard Continuous Integration(CI)/Continuous Delivery(CD) pipeline that includes automated build and compile processes, automation of unit testing and smoke testing, and ultimately promotes the solution to automated acceptance testing and production readiness within these self service capabilities for the developers. USCIS considers it critical that the software is integrated early and frequently. TICS II will identify integration challenges in the early stages of a project. Ensuring early integration of functional modules or components is critical for transparency of the development process and its progress.

2.1 Technical Landscape

Open Source solutions and platform agnostic software will be employed wherever possible to create the possibility of more easily deploying solutions on standard DHS private cloud infrastructure, or on secure public cloud as a Service (aaS) offerings, such as Amazon Web Services (AWS). ELIS is conducting continuous integration in AWS, which will act as a model for future agile development teams at USCIS and within DHS.

USCIS has implemented a CI/CD environment in the AWS environment for development, integration and testing. Production builds will be published in this environment using Microservices and infrastructure as services.

The USCIS technical landscape is shifting from a costly, proprietary, COTS-based framework to a wide adoption of open source offerings. The current ELIS development architecture has demonstrated success with a stack of predominately open source dev/test tools that are currently under consideration for standardization across development teams at USCIS.

The tools currently used for the continuous integration environment are identified in *Table 1: Continuous Integration Tool Suite.* These tools have been identified by the Architecture and Design Services (ADS) team as part of the Candidate Architecture for Continuous Integration. The TICS II contractor will have the opportunity to propose changes to the tool suite if sufficient justification is presented. The program office must request approval for all non-approved hardware and software to be added to the DHS approved products list before it is used in the DHS environment. The contractor will assist the program office in completing the necessary forms to add all required hardware and software to the Enterprise Architecture (EA) Technical Reference Model (TRM).

Table 1: Continuous Integration Tool Suite

Technology	Description/Purpose
CHEF	Deployment scripting
CLOUDWATCH	A web service that provides real-time monitoring to Amazon's EC2 customers on their resource utilization such as CPU, disk and network.
CLOUDTRAIL	A web service that records AWS API calls made on your account and delivers log files to your Amazon S3 bucket.
Cucumber	It runs automated acceptance tests written in a behavior-driven development (BDD) style
Docker	Building Microservices - Package the application into a standardized unit for software development
ECS	EC2 Container Service (ECS) is a highly scalable, high performance container management service
EC2	Amazon Elastic Compute Cloud (EC2), a commercial web service for hosting computer applications. These are our server’s platform
Github Enterprise	Distributed version control
Gradle	Open source build automation tool
Jenkins	Open source continuous integration server
Junit	Unit testing
JIRA	Defect tracking
Nexus	Software Repository Manager
Maven	Open source build repository

RHEL	Red Hat Enterprise Linux (or RHEL) is a commercially supported derivative of the Fedora operating system, tailored to meet the requirements of enterprise customers
RDS	A distributed relational database service by Amazon Web Services
Sonar Nexus	Open source repository manager
Selenium	Browser testing in Firefox
Serenity	Serenity is an open source library that helps you write higher quality autoty is an open source library that helps you write higher quality automated acceptance tests faster.

Table 2: Current Dev/Test Tool Suite

The development suite to be used by the development teams includes:

Name	Manufacturer	Function
Activiti	Activiti.org	Workflow and Business Process Management (BPM) Platform
Adobe LiveCycle Server	Adobe	PDF generation
ActiveMQ	Apache Software Foundation	Open Source Message Broker (MMS)
Bower		A package manager for web components that contain HTML, CSS, JavaScript, etc.
Chef	Chef.io	Used to streamline the task of configuring and maintaining a company's servers
Eclipse	eclipse.org	Open Source IDE for software development
Firefox	Mozilla.org	A free and open-source web browser developed by the Mozilla Foundation and its subsidiary, the Mozilla Corporation.
Gradle	Gradle.org	Open source build automation/orchestration tool
Gulp		task runners / build systems
Grunt-cli		task runners / build systems
Jenkins	jenkins.org	An open source continuous integration tool written in Java.
Java	Oracle	A general-purpose computer programming language that is concurrent, class-based, object-oriented, and specifically designed to have as few implementation dependencies as possible.
jasmine-reporters		Reporter classes for the jasmine test framework
Karma		Test runner for Javascript
karma-junit-reporter		Used to produce test result with schema acceptable in sonar
karma-ng-html2js-preprocessor		Preprocessors in Karma allow you to do some work with your files before they get served to the browser

Name	Manufacturer	Function
karma-jasmine		A Karma plugin - adapter for Jasmine testing framework
karma-cli		The Karma command line interface
Liquidbase	Apache Software Foundation	An open source database-independent library for tracking, managing and applying database schema changes.
Logrotate	Redhat	An automated process used in system administration in which dated log files are archived
Mysql	Oracle	An open-source relational database management system (RDBMS).
Nodejs		Unit testing
Nodepkg		Open source to automatically install missing dependencies and save them into your package.json
Npm		JavaScript developers to share and reuse code, and it makes it easy to update the code that you're sharing
PostgreSQL	PostgreSQL	General purpose and object-relational database management system
promised-io		Promise-based IO for JavaScript
Promise		Replacement for asynchronous use of callbacks
protractor		Protractor is an end-to-end test framework
sonareQubeRunner	SonarSource S.A	Allows for the execution of source code analyzes on the fly.
SonarQube	SonarSource S.A	An open source platform for continuous inspection of code quality.
Tomcat	Apache Software Foundation	Application server from the Apache Software Foundation that executes Java servlets and renders Web pages that include Java Server Page coding
Tortoisegit		Windows Graphical User Interface to Git, used to execute Git commands from a windows explorer.
Winscp		A tool that uses a File Transfer protocol to transfer files between different file systems.

3. SCOPE

In conjunction with TICS II, USCIS will establish an ecosystem with multiple agile development teams working concurrently to develop releases with the Electronic Immigration System (ELIS) capability and/or refactored capability based on the new architecture using agile methodologies, and designed and coded to the new standards. These development teams will be the centerpiece of this effort. The TICS II contractors shall provide a platform for self-service tools to enable development teams to quickly build, integrate, test and release their own software. Further, the TICS II team(s) shall support, maintain and enhance the common infrastructure software and monitoring software to enable development teams to be more productive.

Services in support of TICS II shall be provided by teams of experts with demonstrated experience with the tools and technologies described in section *2.1 Technical Landscape*. The ELIS architecture is evolving, and the tools and technologies identified thus far may change during the task order period of performance.

Having multiple contractor development teams working in parallel requires a strong integration function that can pull the disparate work products into a coherent, operational baseline to establish a continuous delivery environment. Using open source platforms and tools wherever possible, the contractor shall provide a platform for services and tools to establish, standardize and execute a repeatable, automated build process and environment to enable frequent integration, testing, monitoring, infrastructure cluster management and database management. The Contractor shall build automated tools for the developers community on their laptops so the developers can develop code, debug and promote it to various environments, enforce API contracts on how to interact, set up/maintain a CI/CD environment and assist in continuous delivery of the software.

The contractor shall ensure that software is maintained in a releasable state, rapid feedback is provided to development teams when issues arise and acceptance criteria is maintained by providing several automated tools and paths using Docker solutions and CI/CD pipelines to support production. Providing a platform of standards and automated services for Configuration and integration will be an essential component of USCIS' strategy for rapid software development and continuous integration. Configuration and integration standards and operating procedures will be required, as will services, for the configuration management and integration support.

The goal of TICS II is to improve the quality of software, decrease the time it takes to release, enhance monitoring/logging/alerting of running systems and provide tools to the development teams to promote small chunks of code to all the environments on an on demand basis and with zero downtime. To be successful, the contractor must minimize the risk of defects in the code base, detect bugs early, detect production problems early, and make debugging easier and faster. This can be accomplished through the incorporation of continuous integration practices such as continuous and automated testing and proactively improves the overall ELIS architecture. It must reduce human error during deployment, and create visibility into the software's health attributes, such as complexity. The contractor must reduce repetitive and ad hoc activities across projects to accelerate time to deployment, such as code compilation, database integration, testing, inspection, deployment and feedback. By building automated tools for the development community, this task order should empower the development teams to build and promote bug free code to various cloud environments, and ultimately to production, with zero downtime.

TICS II tools and practices must scale to several independent services. As opposed to designing and maintaining one monolithic pipeline, the contractor must help development teams with automated tools to create and maintain continuous delivery solutions that support multiple interdependent Microservices that can be deployed and tested independently.

Most importantly, the contractor will be successful if USCIS systems can be readily built and released to production with minimal effort, minimal downtime, and a minimal number of bugs.

4. TASKS

The contractor shall work closely with the government, which will provide leadership and direction. The contractor's responsibilities will be to empower development teams to release their own code through automated tools that support integration, testing, promotion, and proactive logging/monitoring/alerting. The contractor shall further build, maintain and enhance tools to enable the developers community to promote code quality and unit testing, and capture best practices such as zero-downtime deployment and seamless database refactoring.

The contractor's responsibilities will be to provide automated tools to empower the development teams to integrate ELIS code through automated practices received from development teams, prepare it for testing, and promote code between testing, staging, and production environments. The promoted software code will be baselined with version control methodology and maintained under configuration management as a configuration item.

4.1 DevOps Team(s)

The contractor shall provide DevOps team(s) (two teams with one optional team) to provide the required services as detailed in this SOW. Each team shall be comprised of ten full time equivalents (FTEs), and each team must consist of the same labor mix. At least three of the ten FTEs on each team must have AWS certification.

The contractor shall provide the proper skill mix and level of personnel resources to deliver USCIS professional information technology CI/CD support throughout the deployment pipeline for enterprise-level web and database applications. This includes support for version control, automated builds, automated testing, continuous integration, code review tools, configuration management, system monitoring/logging/alerting, setting up automated tools on developers laptops, database refactoring, overseeing changes in CI/CD pipelines, building automated tools for the development teams and TICS II teams, database configuration and management support, infrastructure cluster management and integration test functions. The deployment pipeline will test the fitness of the application builds and improve USCIS confidence as they move to increasingly production-like environments. This allows USCIS to eliminate unfit release functionalities early in the process and communicate root causes of the failure to development teams as quickly as possible

4.2 Tools Activities

- The contractor shall be responsible for providing various automated tools to the development community to promote small chunks of code to all the environments on an on demand basis with zero downtime
- The contractor shall use and customize a standardized dev/test and CI (Continuous Integration) suite, with the expectation that the dev/test architecture will evolve. If the tools are insufficient, the contractor shall evaluate and bring in new tools, as well as write custom code to fill the gaps and improve ELIS capabilities.
- The contractor shall use and customize standard logging/monitoring/alerting tools that will assist development teams in quickly finding and addressing issues in running systems.
- The contractor shall evaluate the current technical architecture of their Virtual Machines (VM) for the continuous integration environments and make necessary proactive improvements to reduce cost and improve overall efficiency.

- The contractor shall be responsible for setup and administration of the development and test environments using the AWS VM servers and workstations they are assigned.

4.3 Implementation Activities

- The contractor shall be responsible for empowering various development teams by creating new tools to help manage, monitor, and promote quality code to various development/testing environments.
- The contractor shall enable development teams to achieve self-managed platform for CI/CD capabilities in support of the agile methodology as specified by USCIS OIT, with an understanding that processes will be continuously improved in collaboration with the TICS and development teams. The contractor shall be responsible for monitoring, modifying and setting up new CI/CD pipelines as necessary, and for overseeing changes in the pipelines.
- The contractor shall be responsible for monitoring and managing alert services for the health of the entire cloud architecture, including, but not limited to, CI/CD pipelines, database, application tier, external interfaces, etc.
- The contractor shall build insight engineering platforms for providing real-time operational insights to development teams.
- The contractor shall be responsible for proactively monitoring and enhancing the existing AWS architecture.
- The CI/CD services shall focus on creating automated tools and platforms for the technical integration of the development teams’ output and the tasks associated with coordinating and communicating the CI/CD services and associated workflow, processes, and findings.
- The contractor shall be responsible for overseeing and maintaining overall cluster management software (currently Amazon ECS), and improving and upgrading it as new capabilities become available.
- The contractor shall promote and support “server-less” code management tools, such as Amazon Lambda, that can further reduce overhead and maintenance.
- The contractor shall be responsible for performing database management expert duties such as, but not limited to, maintain the overall integrity and quality of the database, backward compatible database changes, regular improvements and patching of the servers, database optimization, database cluster management, ability to work with various teams to provide technical assistance and troubleshoot and resolve any issues related to database, ability to capture and generate reports for any DHS audits and secure database by developing policies, procedures, and controls.
- The contractor shall be responsible for the administration of USCIS CI/CD processes to enable the early detection of bugs and increase the quality of code and the overall quality of the software. The contractor is responsible for ensuring the integration of test scripts developed by development teams and independent testers into the build process.
- The contractor shall enable automation of various forms of testing through a robust CI/CD implementation. The contractor shall institute testing best practices (e.g. idempotent tests, high test coverage) and enforce them via automated means wherever possible.

- The contractor will manage infrastructure and enable automated tools for the test teams to perform all automated testing as part of the agency's CI/CD implementation and daily build/smoke test of projects.
- The contractor shall provide the tools to allow the continuous integration of the development teams' software output, which may be up to multiple times per day, resulting from mid-sprint builds, sprint completions, releases and break/fixes, new requirements, and emergency releases.
- The contractor shall provide the monitoring ability and tools for various development teams to resolve conflicts resulting from merge and/or build failures.
- The contractor shall work closely with both development teams and their testers and the USCIS OIT Independent Validation & Verification (IV&V) teams throughout the deployment pipeline to integrate and automate test scripts as part of the build process.
- The contractor shall ensure that the automatic build and deployment process works effectively across all environments, including the production environment, staging, and dev/test enclaves.
- The contractor shall confer with test and development teams to troubleshoot issues during the build process in the various environments. This is especially crucial in the production environment.
- The contractor shall manage their Code Management (CM) and integration efforts in accordance with their stated methodologies.
- The contractor will ensure that the infrastructure environments support continuous integration and delivery of functional code at the discretion of USCIS and sustain the future multiple inter-dependent Microservices demand. Code delivery, testing and deployment preparation shall be a collaborative and continuous effort.
- The contractor shall propose a methodology for integrating with the development teams.
- The contractor shall provide tools and platforms to allow team-managed deployments to various environments, including but not limited to, performance testing, pre-production (also known as staging) and production.

4.4 Administrative Activities

- The contractor shall be located at the onsite Government facility; close coordination and communication with the development teams is required, especially with regard to communicating standards and practices, and providing feedback about unsuccessful builds and test results.
- The contractor shall develop and implement an approach for coordinating with multiple development teams across the Washington D.C. region and the Government at its locations in downtown Washington, D.C.
- The contractor shall provide points of contact for all systems being developed that are part of USCIS' continuous integration environment. This POC shall be responsible for ensuring the development team aligns their process with those developed by the TICS team for CI/CD.

5. KEY PERSONNEL

The contractor shall identify key personnel and provide statements of qualifications for these individuals. The contractor shall identify key personnel that shall be the **management lead** and the **technical lead** for the task order as a whole. The contractor may allocate these key personnel across the various development teams as the contractor deems necessary. The management lead *shall not* be a member of any of the development teams. The technical lead *shall* be one of the ten FTEs on a development team.

At a minimum, the Management Lead shall meet the education and/or experience requirements of a Level II labor category as defined in the EAGLE II contract. The Technical Lead shall meet the minimum education and/or experience requirements listed below-

- Master's Degree
- Certified AWS Solutions Architect – Professional
- 10 or more years Enterprise IT experience

The management lead shall ensure that all work on this contract complies with contract terms and conditions and shall have access to contractor corporate senior leadership when necessary. The contractor's management lead shall be the primary interface with the USCIS Contracting Officer's Representative (COR) and Contracting Officer (CO) and shall attend status meetings and ad hoc meetings with stakeholders as required, accompanied by the technical lead when necessary. The management lead shall be responsible for managing risks, and the cost, schedule, and scope of tasks. The technical lead shall be responsible for successfully delivering a CI/CD environment and associated standards and processes that meet the stated business needs in accordance with the SOW.

In accordance with HSAR Clause 3052.215-70 Key Personnel or Facilities, prior to removing, replacing, or diverting any of the key personnel, the contractor shall notify the CO via the COR reasonably in advance (not less than 30 days), and shall submit written justification (including proposed substitutions) in sufficient detail to permit evaluation of the impact on this task order. The contractor shall make no diversions in key personnel without the prior written consent of the CO.

6. TRANSITION SUPPORT

6.1 Transition-In

As this is a re-compete contract for USCIS, a comprehensive transition plan will be provided by the incumbent contractor. The incoming contractor shall review, provide feedback or concerns, and ultimately come to an agreement and sign the transition plan provided by the incumbent. There will be a 60-day "transition-in" period to transfer the responsibilities from the incumbent contractor to the new contractor.

6.2 Transition-Out

At the completion of performance of this task order, the contractor shall fully support the transition of the work that is turned over to another entity, either government or a successor. The contractor shall assist with transition planning and shall comply with the transition milestones and schedule.

To ensure the necessary continuity of services and to maintain the required level of support, USCIS may retain services of the incumbent contractor for some or all of the transition period, as required.

The contractor shall be responsible for the transition of all technical activities identified in this task order. As part of the transition, the contractor shall be responsible for:

- Inventory and orderly transfer of all GFP, to include hardware, software, and licenses, Contractor Acquired Government Property, and Government Furnished Information (GFI)
- Transfer of documentation currently in process
- Transfer of all software code in process
- Certification that all non-public DHS information has been purged from any contractor-owned system
- Exchange of accounts to access software and hosted infrastructure components
- Participation in knowledge transfer activities in accordance with the transition plan (as described below)
- Participate in transition of management team

Transition planning generally begins 120 days before the transition deadline. If the government provides a Transition Plan template, the contractor shall complete it as assigned; otherwise the contractor shall submit a Transition Plan at the direction of the government. The Transition Plan shall:

- Document the strategic approach
- Identify equipment, hardware, software, documents and other artifacts that are included in the transition
- Establish milestones and schedules
- Establish activities
- Identify transition risks and risk mitigation
- Define roles and responsibilities
- Define transition approval authorities and lines of communication
- Define appropriate labor mix to perform CI/CD activities
- Define a knowledge transfer approach
- Define a property inventory and transition approach
- Create bi-party or tri-party agreements
- Provide checklists

7. DELIVERABLES

The contractor shall submit electronic copies of document deliverables that are indicated in the table below to the CO and COR (and others as may be specified by the CO and/or COR) via e-mail in the format specified. All document deliverables shall be made by close of business (COB) 4:30pm local time Monday through Friday, unless stated otherwise.

All deliverables submitted in electronic format shall be free of any known computer virus or defects. If a virus or defect is found, the deliverable will not be accepted. The replacement file shall be provided within two (2) business days after notification of the presence of a virus.

Each document deliverable shall be accompanied by a cover letter from the contractor on Company letterhead. Multiple deliverables may be delivered with a single cover letter describing the contents of the complete package.

7.1 Task Order Management Artifacts

The contractor shall provide standard that support task order management, as described below:

- Status Briefings

  As required by the COR, the contractor shall attend meetings with the COR and/or other USCIS stakeholders in order to review work accomplished, work in progress, plans for future work, transition plans and status, and issues pertinent to the performance of work tasks that require USCIS attention.

7.2 Deliverables Schedule

The deliverables that apply to this task order, and that the contractor shall provide are outlined in *Table 3: Deliverables Schedule.*

Table 3: Deliverables Schedule

Section References	Item / Description	Frequency of Delivery	Acceptable Formats
2.1	CI Environment Design Documents and install guides for the tools listed in the SOW such as, but not limited to: Jenkins Install Guide; JIRA Install Guide; SonarQube Install Guide; Nexus Install Guide; Git Install Guide; Chef Install Guide, etc.	Iteratively updated to reflect current Environment Design and install guides	Electronic format within that can be accessible by the development and OIT community.
4.3	Standard Operating Procedures (SOPs) as needed. Such as, but not limited to - Code Check in and Check-out SOP; Check-in SOP; code merger/branching SOP; Jenkins Job Deployment SOP; Code Deployment SOPs (testing, staging, production), emergency code branching SOP, etc.	As needed and iteratively updated to improve processing quality	Electronic format within that can be accessible by the development and OIT community.
4.3	Code Library Specifications and configurations	As needed and iteratively updated to improve processing quality	Electronic format within that can be accessible by the development and OIT community.

Section References	Item / Description	Frequency of Delivery	Acceptable Formats
4.3	Jenkins Jobs, Microservices pipelines, auto scaling environments scripts; any automated chef scripts/jobs	As needed and iteratively update the existing ones	Appropriate job file format, word.
6.2	Transition-Out Plan	Based on mutual agreement	MS Word
Security Attachment 3	IT Security Plan	30 days after contract award	updated annually MS Word
Security Attachment 3	IT Security Accreditation – Written Proof along with: Final Security Plan; Risk Assessment; Security T&E; DR Plan and COOP (Per HSAR clause 3052.204-70)	Within 6 months after contract award as required	MS Word
5.0	Monthly Reports and Status Briefings – including presentations, database extractions, meeting reports, burn down charts, etc.	Weekly, Monthly, and as directed by the COR	MS Word, Excel, Visio, JIRA, or PowerPoint
5.0	Status Briefings, such as presentations, database extractions, meeting reports, burndown charts, etc.	As directed by the product owner and/or PM, COR	MS Word, Excel, Visio, or PowerPoint
4.1	Confirmation of AWS Certification for at least three FTEs per development team	Annually	Email to COR
	Separation Notification – The CO and COR must be notified of each contract employee termination / resignation (the COR will then notify the Office of Security and Integrity (OSI) Personnel Security Division (PSD) to coordinate the exit clearance forms).	Within 5 days of each occurrence	Email to COR & CO

All deliverables listed above and any other data required to be delivered during the performance of the task order are to be delivered with unlimited rights as per FAR 52.227-17.

7.3 Inspection and Acceptance

Various government stakeholders will inspect contractor services and deliverables. The CO will provide official notification of rejection of deliverables. Inspection and acceptance of deliverables will use the following procedures:

- The government will provide written acceptance, comments, and/or change requests, if any, within fifteen (15) business days of receipt of task order deliverables.

- If government acceptance, comments, and/or change requests are not provided to the contractor within 15 business days after delivery of a deliverable, the contractor must check with the government prior to assuming government acceptance.
- Upon receipt of the government comments, the contractor shall, within three (3) business days, rectify the situation and re-submit the contract deliverable(s) if it is not a “draft” deliverable. If it is a “draft” deliverable, the contractor shall rectify the situation before the next scheduled submission of this deliverable.

8. TASK ORDER ADMINISTRATION DATA

8.1 Place of Performance

The principal place of performance shall be at the onsite Government building co-located with development teams at 20 Massachusetts Avenue NW, Washington DC. If additional teams are required, the government shall provide the necessary space at a government facility. Meetings generally take place at USCIS offices in the Washington, DC Metropolitan Area including, but not limited to, 20 Massachusetts Avenue, NW and 111 Massachusetts Avenue NW, Washington DC.

8.2 Hours of Operation

Normal duty hours for the Government are from 8:00am to 5:00pm (Eastern Standard Time), Monday through Friday. The contractor will have access to the facility during these hours.

At times, based on the needs of the mission, the Government will require service outside of the normal duty hours including evenings, holidays and weekends upon COR direction, and given an advanced notice if possible. The outside of normal duty hours’ support is expected for outages, deployment support, interface issues and releases (estimated to be about 30 total hours per month). USCIS Government employees must be present during such instances. The contractor shall be available during this time period.

8.3 Government Furnished Property (GFP)

Laptops and phones will be issued and used in performing work on this contract. No personal or company owned storage devices, (thumb drives, DVDs, or CDs) shall be used with the GFP. After GFP laptops are provided, the contractor shall use only the government provided e-mail system and the DHS network for electronic communications with the task order’s government stakeholders. A webinar account, such as AT&T Connect, will be provided to the contractor to facilitate virtual demos and other meetings with stakeholders at various physical locations.

Equipment / Government Property	Date / Event Indicate when the GFP will be furnished	Date / Event Indicate when the GFP will be returned	Unit	Unit Acquisition Cost	Quantity	Serial Number(s)	Manufacture & Model Number	"As-Is"
MacBook Pro computer with power cord, docking station and desk lock	After EOD	Upon Departure	EA	$3000.00	Up to 31	TBD	Standard USCIS approved manufacturer	TBD
Phone	After EOD	Upon Departure	EA	TBD	TBD	TBD	Standard USCIS approved manufacturer	TBD

The property may not be used for any non-task order purpose. The Contractor bears full responsibility for any and all loss of this property, whether accidental or purposeful, at full replacement value.

9. HLS EA COMPLIANCE LANGUAGE:

DHS Enterprise Architecture Compliance
All solutions and services shall meet DHS Enterprise Architecture policies, standards, and procedures. Specifically, the contractor shall comply with the following HLS EA requirements:

- All developed solutions and requirements shall be compliant with the HLS EA.
- All IT hardware and software shall be compliant with the HLS EA Technical Reference Model (TRM) Standards and Products Profile.
- Description information for all data assets, information exchanges and data standards, whether adopted or developed, shall be submitted to the Enterprise Data Management Office (EDMO) for review, approval and insertion into the DHS Data Reference Model and Enterprise Architecture Information Repository.
- Development of data assets, information exchanges and data standards will comply with the DHS Data Management Policy MD 103-01 and all data-related artifacts will be developed and validated according to DHS data management architectural guidelines.
- Applicability of Internet Protocol Version 6 (IPv6) to DHS-related components (networks, infrastructure, and applications) specific to individual acquisitions shall be in accordance with the DHS Enterprise Architecture (per OMB Memorandum M-05-22, August 2, 2005) regardless of whether the acquisition is

for modification, upgrade, or replacement. All EA-related component acquisitions shall be IPv6 compliant as defined in the U.S. Government Version 6 (USGv6) Profile National Institute of Standards and Technology (NIST) Special Publication 500-267) and the corresponding declarations of conformance defined in the USGv6 Test Program.

Task Order Clauses

Federal Acquisition Regulation (FAR) clauses incorporated by reference

52.209-10 **Prohibition on Contracting With Inverted Domestic Corporations** (Nov 2015)

52.227-17 **Rights in Data—Special Works** (DEC 2007)

52.217-8 **Option to Extend Services** (Nov 1999)

fill-in: **30 days before the task order expires**

52.232-39 **Unenforceability of Unauthorized Obligations** (Jun 2013)

52.237-3 **Continuity of Serves** (Jan 1991)

Federal Acquisition Regulation (FAR) clauses incorporated in full text

52.252-4 **Alterations in Contract** (Apr 1984)

Portions of this contract are altered as follows:

Use of the word "contract" is understood to mean "task order" wherever such application is appropriate. Use of the word "solicitation" is understood to mean "fair opportunity notice" wherever such application is appropriate.

52.203-99 **Prohibition On Contracting With Entities That Require Certain** (Jul 2016)

Internal Confidentiality Agreements (DEVIATION)

(a) The contractor shall not require its employees or subcontractors seeking to report fraud, waste, or abuse to sign or comply with internal confidentiality agreements or statements prohibiting or otherwise restricting such employees or subcontractors from lawfully reporting waste, fraud, or abuse related to the execution of a Government contract to a designated investigative or law enforcement representative of a Federal department or agency authorized to receive such information (e.g., agency Office of the Inspector General).

(b) The contractor shall notify current employees and subcontractors that prohibitions and restrictions of any internal confidentiality agreements covered by this clause, to the extent that such prohibitions and restrictions are inconsistent with the prohibitions of this clause, are no longer in effect.

(c) The prohibition in paragraph (a) of this clause does not contravene requirements applicable to Standard Form 312 (Classified Information Nondisclosure Agreement), Form 4414 (Sensitive Compartmented Information Nondisclosure Agreement), or any other form issued by a Federal department or agency governing the nondisclosure of classified information.

(d) In accordance with Section 743 of Division E, Title VII, of the Consolidated and Further Continuing Appropriations Act, 2015, (Pub. L. 113-235) use of funds appropriated (or otherwise made available) under that or any other Act may be prohibited, if the Government determines that the contractor is not in compliance with the provisions of this clause.

(e) The contractor shall include the substance of this clause, including this paragraph (f), in subcontracts under such contracts.

(f) The Government may seek any available remedies in the event the contractor fails to comply with the provisions of this clause.

52.217-9 **Option to Extend the Term of the Contract** (Mar 2000)

(a) The Government may extend the term of this contract by written notice to the contractor within **15 days before the task order expires**; provided that the Government gives the contractor a preliminary written notice of its intent to extend at least **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 contract 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 **24 months**.

Other Task Order Requirements

ADDITIONAL INVOICING INSTRUCTIONS

(a) In accordance with FAR Part 32.905, all invoices submitted to USCIS for payment shall include the following:

(1) Name and address of the contractor.

(2) Invoice date and invoice number.

(3) Contract number or other authorization for supplies delivered or services performed (including order number and contract line item number).

(4) Description, quantity, unit of measure, period of performance, unit price, and extended price of supplies delivered or services performed.

(5) Shipping and payment terms.

(6) Name and address of contractor official to whom payment is to be sent.

(7) Name (where practicable), title, phone number, and mailing address of person to notify in the event of a defective invoice.

(8) Taxpayer Identification Number (TIN).

(b) Invoices not meeting these requirements will be rejected and not paid until a corrected invoice meeting the requirements is received.

(c) USCIS' preferred method for invoice submission is electronically. Invoices shall be submitted in Adobe pdf format with each pdf file containing only one invoice. The pdf files shall be submitted electronically to **USCISInvoice.Consolidation@ice.dhs.gov** with each email conforming to a size limit of 500 KB.

(d) If a paper invoice is submitted, mail the invoice to:

**USCIS Invoice Consolidation
PO Box 1000
Williston, VT 05495
(802) 288-7600**

PERFORMANCE REPORTING

The Government intends to record and maintain contractor performance information for this task order in accordance with FAR Subpart 42.15. The contractor is encouraged to enroll at www.cpars.gov so it can participate in this process.

HSAR CLAUSES INCORPORATED

The following HSAR clauses of the parent EAGLE II Contract apply:

Clause	**EAGLE II Section**
HSAR clause 3052.204-71	I.4.2

Special Clause – Safeguarding of Sensitive Information (MAR 2015)	H.40
Special Clause – Information Technology Security and Privacy Training (MAR 2015)	H.41

POSTING OF ORDER IN FOIA READING ROOM

(a) The Government intends to post the order resulting from this notice to a public FOIA reading room.

(b) Within 30 days of award, the contractor shall submit a redacted copy of the executed contract (or order) (including all attachments) suitable for public posting under the provisions of the Freedom of Information Act (FOIA). The contractor shall submit the documents to the USCIS FOIA Office by email at **foiaerr.nrc@uscis.dhs.gov** with a courtesy copy to the contracting officer.

(c) The USCIS FOIA Office will notify the contractor of any disagreements with the contractor's redactions before public posting of the contract or order in a public FOIA reading room.

KEY PERSONNEL

For the purposes of the contract clause at HSAR 3052.215-70, Key Personnel or Facilities, the Key Personnel are listed in Section 5 in the Statement of Work (SOW). All personnel submitted by a contractor to fill a key person billet shall meet required standards per Section 5 of the SOW.

The Key Personnel under this Task Order are:

[redacted]

NOTICE TO PROCEED (NTP)

(a) Performance of the work requires unescorted access to Government facilities or automated systems, and/or access to sensitive but unclassified information. The Attachment titled Security Requirements applies.

(b) The contractor is responsible for submitting packages from employees who will receive favorable entry-on-duty (EOD) decisions and suitability determinations, and for submitting them in a timely manner. A Government decision not to grant a favorable EOD decision or suitability determination, or to later withdraw or terminate such decision or termination, shall not excuse the contractor from performance of obligations under this task order.

(c) The contractor may submit background investigation packages immediately following task order award.

(d) This task order does not provide for direct payment to the contractor for EOD efforts. Work for which direct payment is not provided is a subsidiary obligation of the contractor.

(e) The Government intends the Transition-In CLIN to begin **60 days** after task order award (allowing 60 days for the EOD period).

(f) The Government intends for full performance to begin **120 days** after task order award (the 60 day transition period will occur prior to full performance beginning). The contracting officer will issue a notice to proceed (NTP) at least one day before full performance is to begin.

CONSENT TO SUBCONTRACT

For the purposes of the contract clause at FAR 52.244-2, Subcontracts, the fill-in for paragraph (d) is "ALL."

EXPECTATION OF CONTRACTOR PERSONNEL

The Government expects competent, productive, qualified IT professionals to be assigned to the DevOps Team. The Contracting Officer may, by written notice to the contractor, require the contractor to remove any employee that is not found to be competent, productive, or qualified IT professional.

FINAL PAYMENT

As a condition precedent to final payment, 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 shall be completed. A release of claims will be forwarded to the contractor at the end of each performance period for contractor completion as soon thereafter as practicable.

INFORMATION TECHNOLOGY SECURITY AND PRIVACY TRAINING (MAR 2015)

(a) *Applicability*. This clause applies to the Contractor, its subcontractors, and Contractor employees (hereafter referred to collectively as "Contractor"). The Contractor shall insert the substance of this clause in all subcontracts.

(b) *Security Training Requirements*.

(1) All users of Federal information systems are required by Title 5, Code of Federal Regulations, Part 930.301, Subpart C, as amended, to be exposed to security awareness materials annually or whenever system security changes occur, or when the user's responsibilities change. The Department of Homeland Security (DHS) requires that Contractor employees take an annual Information Technology Security Awareness Training course before accessing sensitive information under the contract. Unless otherwise specified, the training shall be completed within thirty (30) days of contract award and be completed on an annual basis thereafter not later than October 31st of each year. Any new Contractor employees assigned to the contract shall complete the training before accessing sensitive information under the contract. The training is accessible at http://www.dhs.gov/dhs-security-and-training-requirements-contractors. The Contractor shall maintain copies of training certificates for all Contractor and subcontractor employees as a record of compliance. Unless otherwise specified, initial training certificates for each Contractor and subcontractor employee shall be provided to the Contracting Officer's Representative (COR) not later than thirty (30) days after contract award. Subsequent training certificates to satisfy the annual training requirement shall be submitted to the COR via e-mail notification not later than October 31st of each year. The e-mail notification shall state the required training has been completed for all Contractor and subcontractor employees.

(2) The DHS Rules of Behavior apply to every DHS employee, Contractor and subcontractor that will have access to DHS systems and sensitive information. The DHS Rules of Behavior shall be signed before accessing DHS systems and sensitive information. The DHS Rules of Behavior is a document that informs users of their responsibilities when accessing DHS systems and holds users accountable for actions taken while accessing DHS systems and using DHS Information Technology resources capable of inputting, storing, processing, outputting, and/or transmitting sensitive information. The DHS Rules of Behavior is accessible at http://www.dhs.gov/dhs-security-and-training-requirements-contractors. Unless otherwise specified, the DHS Rules of Behavior shall be signed within thirty (30) days of contract award. Any new Contractor employees assigned to the contract shall also sign the DHS Rules of Behavior before accessing DHS systems and sensitive information. The Contractor shall maintain signed copies of the DHS Rules of Behavior for all Contractor and subcontractor employees as a record of compliance. Unless otherwise specified, the Contractor shall e-mail copies of the signed DHS Rules of Behavior to the COR not later than thirty (30) days after contract award for each employee. The DHS Rules of Behavior will be reviewed annually and the COR will provide notification when a review is required.

(c) *Privacy Training Requirements.* All Contractor and subcontractor employees that will have access to Personally Identifiable Information (PII) and/or Sensitive PII (SPII) are required to take *Privacy at DHS: Protecting Personal Information* before accessing PII and/or SPII. The training is accessible at http://www.dhs.gov/dhs-security-and-training-requirements-contractors. Training shall be completed within thirty (30) days of contract award and be completed on an annual basis thereafter not later than October 31st of each year. Any new Contractor employees assigned to the contract shall also complete the training before accessing PII and/or SPII. The Contractor shall maintain copies of training certificates for all Contractor and subcontractor employees as a record of compliance. Initial training certificates for each Contractor and subcontractor employee shall be provided to the COR not later than thirty (30) days after contract award. Subsequent training certificates to satisfy the annual training requirement shall be submitted to the COR via e-mail notification not later than October 31st of each year. The e-mail notification shall state the required training has been completed for all Contractor and subcontractor employees.

(End of clause)

SAFEGUARDING OF SENSITIVE INFORMATION (MAR 2015)

(a) *Applicability*. This clause applies to the Contractor, its subcontractors, and Contractor employees (hereafter referred to collectively as "Contractor"). The Contractor shall insert the substance of this clause in all subcontracts.

(b) *Definitions*. As used in this clause—

"Personally Identifiable Information (PII)" means information that can be used to distinguish or trace an individual's identity, such as name, social security number, or biometric records, either alone, or when combined with other personal or identifying information that is linked or linkable to a specific individual, such as date and place of birth, or mother's maiden name. The definition of PII is not anchored to any single category of information or technology. Rather, it requires a case-by-case assessment of the specific risk that an individual can be identified. In performing this assessment, it is important for an agency to recognize that non-personally identifiable information can become personally identifiable information whenever additional information is made publicly available—in any medium and from any source—that, combined with other available information, could be used to identify an individual.

PII is a subset of sensitive information. Examples of PII include, but are not limited to: name, date of birth, mailing address, telephone number, Social Security number (SSN), email address, zip code, account numbers, certificate/license numbers, vehicle identifiers including license plates, uniform resource locators (URLs), static Internet protocol addresses, biometric identifiers such as fingerprint, voiceprint, iris scan, photographic facial images, or any other unique identifying number or characteristic, and any information where it is reasonably foreseeable that the information will be linked with other information to identify the individual.

"Sensitive Information" is defined in HSAR clause 3052.204-71, Contractor Employee Access, as any information, which if lost, misused, disclosed, or, without authorization is accessed, or modified, could adversely affect the national or homeland security interest, the conduct of Federal programs, or the privacy to which individuals are entitled under section 552a of Title 5, United States Code (the Privacy Act), 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, homeland security or foreign policy. This definition includes the following categories of information:

(1) Protected Critical Infrastructure Information (PCII) as set out in the Critical Infrastructure Information Act of 2002 (Title II, Subtitle B, of the Homeland Security Act, Public Law 107-296, 196 Stat. 2135), as amended, the implementing regulations thereto (Title 6, Code of Federal Regulations, Part 29) as amended, the applicable PCII Procedures Manual, as amended, and any supplementary guidance officially communicated by an authorized official of the Department of Homeland Security (including the PCII Program Manager or his/her designee);

(2) Sensitive Security Information (SSI), as defined in Title 49, Code of Federal Regulations, Part 1520, as amended, "Policies and Procedures of Safeguarding and Control of SSI," as amended, and any supplementary guidance officially communicated by an authorized official of

the Department of Homeland Security (including the Assistant Secretary for the Transportation Security Administration or his/her designee);

(3) Information designated as “For Official Use Only,” which is unclassified information of a sensitive nature and the unauthorized disclosure of which could adversely impact a person’s privacy or welfare, the conduct of Federal programs, or other programs or operations essential to the national or homeland security interest; and

(4) Any information that is designated “sensitive” or subject to other controls, safeguards or protections in accordance with subsequently adopted homeland security information handling procedures.

“Sensitive Information Incident” is an incident that includes the known, potential, or suspected exposure, loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or unauthorized access or attempted access of any Government system, Contractor system, or sensitive information.

“Sensitive Personally Identifiable Information (SPII)” is a subset of PII, which if lost, compromised or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. Some forms of PII are sensitive as stand-alone elements. Examples of such PII include: Social Security numbers (SSN), driver’s license or state identification number, Alien Registration Numbers (A-number), financial account number, and biometric identifiers such as fingerprint, voiceprint, or iris scan. Additional examples include any groupings of information that contain an individual’s name or other unique identifier plus one or more of the following elements:

(1) Truncated SSN (such as last 4 digits)
(2) Date of birth (month, day, and year)
(3) Citizenship or immigration status
(4) Ethnic or religious affiliation
(5) Sexual orientation
(6) Criminal History
(7) Medical Information
(8) System authentication information such as mother’s maiden name, account passwords or personal identification numbers (PIN)

Other PII may be “sensitive” depending on its context, such as a list of employees and their performance ratings or an unlisted home address or phone number. In contrast, a business card or public telephone directory of agency employees contains PII but is not sensitive.

(c) *Authorities.* The Contractor shall follow all current versions of Government policies and guidance accessible at http://www.dhs.gov/dhs-security-and-training-requirements-contractors, or available upon request from the Contracting Officer, including but not limited to:

(1) DHS Management Directive 11042.1 Safeguarding Sensitive But Unclassified (for Official Use Only) Information

(2) DHS Sensitive Systems Policy Directive 4300A
(3) DHS 4300A Sensitive Systems Handbook and Attachments
(4) DHS Security Authorization Process Guide
(5) DHS Handbook for Safeguarding Sensitive Personally Identifiable Information
(6) DHS Instruction Handbook 121-01-007 Department of Homeland Security Personnel Suitability and Security Program
(7) DHS Information Security Performance Plan (current fiscal year)
(8) DHS Privacy Incident Handling Guidance
(9) Federal Information Processing Standard (FIPS) 140-2 Security Requirements for Cryptographic Modules accessible at http://csrc.nist.gov/groups/STM/cmvp/standards.html
(10) National Institute of Standards and Technology (NIST) Special Publication 800-53 Security and Privacy Controls for Federal Information Systems and Organizations accessible at http://csrc.nist.gov/publications/PubsSPs.html
(11) NIST Special Publication 800-88 Guidelines for Media Sanitization accessible at http://csrc.nist.gov/publications/PubsSPs.html

(d) *Handling of Sensitive Information.* Contractor compliance with this clause, as well as the policies and procedures described below, is required.

(1) Department of Homeland Security (DHS) policies and procedures on Contractor personnel security requirements are set forth in various Management Directives (MDs), Directives, and Instructions. *MD 11042.1, Safeguarding Sensitive But Unclassified (For Official Use Only) Information* describes how Contractors must handle sensitive but unclassified information. DHS uses the term "FOR OFFICIAL USE ONLY" to identify sensitive but unclassified information that is not otherwise categorized by statute or regulation. Examples of sensitive information that are categorized by statute or regulation are PCII, SSI, etc. The *DHS Sensitive Systems Policy Directive 4300A* and the *DHS 4300A Sensitive Systems Handbook* provide the policies and procedures on security for Information Technology (IT) resources. The *DHS Handbook for Safeguarding Sensitive Personally Identifiable Information* provides guidelines to help safeguard SPII in both paper and electronic form. *DHS Instruction Handbook 121-01-007 Department of Homeland Security Personnel Suitability and Security Program* establishes procedures, program responsibilities, minimum standards, and reporting protocols for the DHS Personnel Suitability and Security Program.

(2) The Contractor shall not use or redistribute any sensitive information processed, stored, and/or transmitted by the Contractor except as specified in the contract.

(3) All Contractor employees with access to sensitive information shall execute *DHS Form 11000-6, Department of Homeland Security Non-Disclosure Agreement (NDA),* as a condition of access to such information. The Contractor shall maintain signed copies of the NDA for all employees as a record of compliance. The Contractor shall provide copies of the signed NDA to the Contracting Officer's Representative (COR) no later than two (2) days after execution of the form.

(4) The Contractor's invoicing, billing, and other recordkeeping systems maintained to support financial or other administrative functions shall not maintain SPII. It is acceptable to maintain in

these systems the names, titles and contact information for the COR or other Government personnel associated with the administration of the contract, as needed.

(e) *Authority to Operate*. The Contractor shall not input, store, process, output, and/or transmit sensitive information within a Contractor IT system without an Authority to Operate (ATO) signed by the Headquarters or Component CIO, or designee, in consultation with the Headquarters or Component Privacy Officer. Unless otherwise specified in the ATO letter, the ATO is valid for three (3) years. The Contractor shall adhere to current Government policies, procedures, and guidance for the Security Authorization (SA) process as defined below.

(1) Complete the Security Authorization process. The SA process shall proceed according to the *DHS Sensitive Systems Policy Directive 4300A* (Version 11.0, April 30, 2014), or any successor publication, *DHS 4300A Sensitive Systems Handbook* (Version 9.1, July 24, 2012), or any successor publication, and the *Security Authorization Process Guide* including templates.

(i) Security Authorization Process Documentation. SA documentation shall be developed using the Government provided Requirements Traceability Matrix and Government security documentation templates. SA documentation consists of the following: Security Plan, Contingency Plan, Contingency Plan Test Results, Configuration Management Plan, Security Assessment Plan, Security Assessment Report, and Authorization to Operate Letter. Additional documents that may be required include a Plan(s) of Action and Milestones and Interconnection Security Agreement(s). During the development of SA documentation, the Contractor shall submit a signed SA package, validated by an independent third party, to the COR for acceptance by the Headquarters or Component CIO, or designee, at least thirty (30) days prior to the date of operation of the IT system. The Government is the final authority on the compliance of the SA package and may limit the number of resubmissions of a modified SA package. Once the ATO has been accepted by the Headquarters or Component CIO, or designee, the Contracting Officer shall incorporate the ATO into the contract as a compliance document. The Government's acceptance of the ATO does not alleviate the Contractor's responsibility to ensure the IT system controls are implemented and operating effectively.

(ii) Independent Assessment. Contractors shall have an independent third party validate the security and privacy controls in place for the system(s). The independent third party shall review and analyze the SA package, and report on technical, operational, and management level deficiencies as outlined in *NIST Special Publication 800-53 Security and Privacy Controls for Federal Information Systems and Organizations*. The Contractor shall address all deficiencies before submitting the SA package to the Government for acceptance.

(iii) Support the completion of the Privacy Threshold Analysis (PTA) as needed. As part of the SA process, the Contractor may be required to support the Government in the completion of the PTA. The requirement to complete a PTA is triggered by the creation, use, modification, upgrade, or disposition of a Contractor IT system that will store, maintain and use PII, and must be renewed at least every three (3) years. Upon review of the PTA, the DHS Privacy Office determines whether a Privacy Impact Assessment (PIA) and/or Privacy Act System of Records Notice (SORN), or modifications thereto, are required. The Contractor shall provide all support necessary to assist the Department in completing the PIA in a timely manner and shall ensure that project management plans and schedules include time for the completion of the PTA, PIA, and SORN (to the extent required) as milestones. Support in this context includes responding timely to requests for information from the Government about the use, access, storage, and maintenance of PII on the Contractor's system, and providing timely review of relevant compliance documents for factual accuracy. Information on the DHS privacy compliance process, including PTAs, PIAs, and SORNs, is accessible at http://www.dhs.gov/privacy-compliance.

(2) *Renewal of ATO.* Unless otherwise specified in the ATO letter, the ATO shall be renewed every three (3) years. The Contractor is required to update its SA package as part of the ATO renewal process. The Contractor shall update its SA package by one of the following methods: (1) Updating the SA documentation in the DHS automated information assurance tool for acceptance by the Headquarters or Component CIO, or designee, at least 90 days before the ATO expiration date for review and verification of security controls; or (2) Submitting an updated SA package directly to the COR for approval by the Headquarters or Component CIO, or designee, at least 90 days before the ATO expiration date for review and verification of security controls. The 90 day review process is independent of the system production date and therefore it is important that the Contractor build the review into project schedules. The reviews may include onsite visits that involve physical or logical inspection of the Contractor environment to ensure controls are in place.

(3) *Security Review.* The Government may elect to conduct random periodic reviews to ensure that the security requirements contained in this contract are being implemented and enforced. The Contractor shall afford DHS, the Office of the Inspector General, and other Government organizations access to the Contractor's facilities, installations, operations, documentation, databases and personnel used in the performance of this contract. The Contractor shall, through the Contracting Officer and COR, contact the Headquarters or Component CIO, or designee, to coordinate and participate in review and inspection activity by Government organizations external to the DHS. Access shall be provided, to the extent necessary as determined by the Government, for the Government to carry out a program of inspection, investigation, and audit to safeguard against threats and hazards to the integrity, availability and confidentiality of Government data or the function of computer systems used in performance of this contract and to preserve evidence of computer crime.

(4) *Continuous Monitoring.* All Contractor-operated systems that input, store, process, output, and/or transmit sensitive information shall meet or exceed the continuous monitoring requirements identified in the *Fiscal Year 2014 DHS Information Security Performance Plan,* or successor publication. The plan is updated on an annual basis. The Contractor shall also store monthly continuous monitoring data at its location for a period not less than one year from the date the data is created. The data shall be encrypted in accordance with *FIPS 140-2 Security Requirements for Cryptographic Modules* and shall not be stored on systems that are shared with other commercial or Government entities. The Government may elect to perform continuous monitoring and IT security scanning of Contractor systems from Government tools and infrastructure.

(5) *Revocation of ATO.* In the event of a sensitive information incident, the Government may suspend or revoke an existing ATO (either in part or in whole). If an ATO is suspended or revoked in accordance with this provision, the Contracting Officer may direct the Contractor to take additional security measures to secure sensitive information. These measures may include restricting access to sensitive information on the Contractor IT system under this contract. Restricting access may include disconnecting the system processing, storing, or transmitting the sensitive information from the Internet or other networks or applying additional security controls.

(6) *Federal Reporting Requirements.* Contractors operating information systems on behalf of the Government or operating systems containing sensitive information shall comply with Federal reporting requirements. Annual and quarterly data collection will be coordinated by the Government. Contractors shall provide the COR with requested information within three (3) business days of receipt of the request. Reporting requirements are determined by the Government and are defined in the *Fiscal Year 2014 DHS Information Security Performance Plan*, or successor publication. The Contractor shall provide the Government with all information to fully satisfy Federal reporting requirements for Contractor systems.

(f) *Sensitive Information Incident Reporting Requirements.*

(1) All known or suspected sensitive information incidents shall be reported to the Headquarters or Component Security Operations Center (SOC) within one hour of discovery in accordance with *4300A Sensitive Systems Handbook Incident Response and Reporting* requirements. When notifying the Headquarters or Component SOC, the Contractor shall also notify the Contracting Officer, COR, Headquarters or Component Privacy Officer, and US-CERT using the contact information identified in the contract. If the incident is reported by phone or the Contracting Officer's email address is not immediately available, the Contractor shall contact the Contracting Officer immediately after reporting the incident to the Headquarters or Component SOC. The Contractor shall not include any sensitive information in the subject or body of any e-mail. To transmit sensitive information, the Contractor shall use *FIPS 140-2 Security Requirements for Cryptographic Modules* compliant encryption methods to protect sensitive information in attachments to email. Passwords shall not be communicated in the same email as the attachment. A sensitive information incident shall not, by itself, be interpreted as evidence that the Contractor has failed to provide adequate information security safeguards for sensitive information, or has otherwise failed to meet the requirements of the contract.

(2) If a sensitive information incident involves PII or SPII, in addition to the reporting requirements in *4300A Sensitive Systems Handbook Incident Response and Reporting*, Contractors shall also provide as many of the following data elements that are available at the time the incident is reported, with any remaining data elements provided within 24 hours of submission of the initial incident report:

(i) Data Universal Numbering System (DUNS);
(ii) Contract numbers affected unless all contracts by the company are affected;
(iii) Facility CAGE code if the location of the event is different than the prime contractor location;

(iv) Point of contact (POC) if different than the POC recorded in the System for Award Management (address, position, telephone, email);
(v) Contracting Officer POC (address, telephone, email);
(vi) Contract clearance level;
(vii) Name of subcontractor and CAGE code if this was an incident on a subcontractor network;
(viii) Government programs, platforms or systems involved;
(ix) Location(s) of incident;
(x) Date and time the incident was discovered;
(xi) Server names where sensitive information resided at the time of the incident, both at the Contractor and subcontractor level;
(xii) Description of the Government PII and/or SPII contained within the system;
(xiii) Number of people potentially affected and the estimate or actual number of records exposed and/or contained within the system; and
(xiv) Any additional information relevant to the incident.

(g) *Sensitive Information Incident Response Requirements.*

(1) All determinations related to sensitive information incidents, including response activities, notifications to affected individuals and/or Federal agencies, and related services (e.g., credit monitoring) will be made in writing by the Contracting Officer in consultation with the Headquarters or Component CIO and Headquarters or Component Privacy Officer.

(2) The Contractor shall provide full access and cooperation for all activities determined by the Government to be required to ensure an effective incident response, including providing all requested images, log files, and event information to facilitate rapid resolution of sensitive information incidents.

(3) Incident response activities determined to be required by the Government may include, but are not limited to, the following:

(i) Inspections,
(ii) Investigations,
(iii) Forensic reviews, and
(iv) Data analyses and processing.

(4) The Government, at its sole discretion, may obtain the assistance from other Federal agencies and/or third-party firms to aid in incident response activities.

(h) *Additional PII and/or SPII Notification Requirements*.

(1) The Contractor shall have in place procedures and the capability to notify any individual whose PII resided in the Contractor IT system at the time of the sensitive information incident not later than 5 business days after being directed to notify individuals, unless otherwise approved by the Contracting Officer. The method and content of any notification by the Contractor shall be coordinated with, and subject to prior written approval by the Contracting

Officer, in consultation with the Headquarters or Component Privacy Officer, utilizing the *DHS Privacy Incident Handling Guidance*. The Contractor shall not proceed with notification unless the Contracting Officer, in consultation with the Headquarters or Component Privacy Officer, has determined in writing that notification is appropriate.

(2) Subject to Government analysis of the incident and the terms of its instructions to the Contractor regarding any resulting notification, the notification method may consist of letters to affected individuals sent by first class mail, electronic means, or general public notice, as approved by the Government. Notification may require the Contractor's use of address verification and/or address location services. At a minimum, the notification shall include:

(i) A brief description of the incident;
(ii) A description of the types of PII and SPII involved;
(iii) A statement as to whether the PII or SPII was encrypted or protected by other means;
(iv) Steps individuals may take to protect themselves;
(v) What the Contractor and/or the Government are doing to investigate the incident, to mitigate the incident, and to protect against any future incidents; and
(vi) Information identifying who individuals may contact for additional information.

(i) *Credit Monitoring Requirements*. In the event that a sensitive information incident involves PII or SPII, the Contractor may be required to, as directed by the Contracting Officer:

(1) Provide notification to affected individuals as described above; and/or

(2) Provide credit monitoring services to individuals whose data was under the control of the Contractor or resided in the Contractor IT system at the time of the sensitive information incident for a period beginning the date of the incident and extending not less than 18 months from the date the individual is notified. Credit monitoring services shall be provided from a company with which the Contractor has no affiliation. At a minimum, credit monitoring services shall include:

(i) Triple credit bureau monitoring;
(ii) Daily customer service;
(iii) Alerts provided to the individual for changes and fraud; and
(iv) Assistance to the individual with enrollment in the services and the use of fraud alerts; and/or

(3) Establish a dedicated call center. Call center services shall include:

(i) A dedicated telephone number to contact customer service within a fixed period;
(ii) Information necessary for registrants/enrollees to access credit reports and credit scores;
(iii) Weekly reports on call center volume, issue escalation (i.e., those calls that cannot be handled by call center staff and must be resolved by call center management or DHS, as appropriate), and other key metrics;

(iv) Escalation of calls that cannot be handled by call center staff to call center management or DHS, as appropriate;
(v) Customized FAQs, approved in writing by the Contracting Officer in coordination with the Headquarters or Component Chief Privacy Officer; and
(vi) Information for registrants to contact customer service representatives and fraud resolution representatives for credit monitoring assistance.

(j) *Certification of Sanitization of Government and Government-Activity-Related Files and Information.* As part of contract closeout, the Contractor shall submit the certification to the COR and the Contracting Officer following the template provided in *NIST Special Publication 800-88 Guidelines for Media Sanitization*.

(End of clause)

U.S. Citizenship and Immigration Services
Office of Security and Integrity – Personnel Security Division

SECURITY REQUIREMENTS

GENERAL

U.S. Citizenship and Immigration Services (USCIS) has determined that performance of this contract requires that the Contractor, subcontractor(s), vendor(s), etc. (herein known as Contractor), requires access to sensitive but unclassified information, and that the Contractor will adhere to the following.

SUITABILITY DETERMINATION

USCIS shall have and exercise full control over granting, denying, withholding or terminating access of unescorted Contractor employees to government facilities and/or access of Contractor employees to sensitive but unclassified information based upon the results of a background investigation. USCIS may, as it deems appropriate, authorize and make a favorable entry on duty (EOD) decision based on preliminary security 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 as a result thereof. The granting of a favorable EOD decision or a full employment suitability determination shall in no way prevent, preclude, or bar the withdrawal or termination of any such access by USCIS, at any time during the term of the contract. No Contractor employee shall be allowed unescorted access to a Government facility without a favorable EOD decision or suitability determination by the Office of Security & Integrity Personnel Security Division (OSI PSD).

BACKGROUND INVESTIGATIONS

Contractor employees (to include applicants, temporaries, part-time and replacement employees) under the contract, needing access to sensitive but unclassified information shall undergo a position sensitivity analysis based on the duties each individual will perform on the contract as outlined in the Position Designation Determination (PDD) for Contractor Personnel. The results of the position sensitivity analysis shall identify the appropriate background investigation to be conducted. All background investigations will be processed through OSI PSD.

To the extent the Position Designation Determination form reveals that the Contractor will not require access to sensitive but unclassified information or access to USCIS IT systems, OSI PSD may determine that preliminary security screening and or a complete background investigation is not required for performance on this contract.

Completed packages must be submitted to OSI PSD for prospective Contractor employees no less than 30 days before the starting date of the contract or 30 days prior to EOD of any employees, whether a replacement, addition, subcontractor employee, or vendor. The Contractor shall follow guidelines for package submission as set forth by OSI PSD. A complete package will include the following forms, in conjunction with security questionnaire submission of the SF-85P, “Security Questionnaire for Public Trust Positions” via e-QIP:

1. DHS Form 11000-6, “Conditional Access to Sensitive But Unclassified Information Non-Disclosure Agreement”

2. FD Form 258, “Fingerprint Card” **(2 copies)**

3. Form DHS 11000-9, “Disclosure and Authorization Pertaining to Consumer Reports Pursuant to the Fair Credit Reporting Act”

4. Position Designation Determination for Contract Personnel Form

5. Foreign National Relatives or Associates Statement

6. OF 306, Declaration for Federal Employment (approved use for Federal Contract Employment)

7. ER-856, “Contract Employee Code Sheet”

EMPLOYMENT ELIGIBILITY

Be advised that unless an applicant requiring access to sensitive but unclassified information has resided in the U.S. for three of the past five years, OSI PSD may not be able to complete a satisfactory background investigation. In such cases, USCIS retains the right to deem an applicant as ineligible due to insufficient background information.

Only U.S. citizens are eligible for employment on contracts requiring access to Department of Homeland Security (DHS) Information Technology (IT) systems or involvement in the development, operation, management, or maintenance of DHS IT systems, unless a waiver has been granted by the Director of USCIS, or designee, with the concurrence of both the DHS Chief Security Officer and the Chief Information Officer or their designees. In instances where non-IT requirements contained in the contract can be met by using Legal Permanent Residents, those requirements shall be clearly described.

The Contractor must agree that each employee working on this contract will have a Social Security Card issued by the Social Security Administration.

CONTINUED ELIGIBILITY

If a prospective employee is found to be ineligible for access to USCIS facilities or information, the Contracting Officer’s Representative (COR) will advise the Contractor that the employee shall not continue to work or to be assigned to work under the contract.

In accordance with USCIS policy, contractors are required to undergo a periodic reinvestigation every five years. Security documents will be submitted to OSI PSD within ten business days following notification of a contractor’s reinvestigation requirement.

In support of the overall USCIS mission, Contractor employees are required to complete one-time or annual DHS/USCIS mandatory trainings. The Contractor shall certify annually, but no later than

December 31st each year, that required trainings have been completed. The certification of the completion of the trainings by all contractors shall be provided to both the COR and Contracting Officer.

- **USCIS Security Awareness Training** (required within 30 days of entry on duty for new contractors, and annually thereafter)
- **USCIS Integrity Training** (Annually)
- **DHS Continuity of Operations Awareness Training** (one-time training for contractors identified as providing an essential service)
- **USCIS Office Safety Training** (one-time training for contractors working within USCIS facilities; contractor companies may substitute their own training)
- **USCIS Fire Prevention and Safety Training** (one-time training for contractors working within USCIS facilities; contractor companies may substitute their own training)

USCIS reserves the right and prerogative to deny and/or restrict the facility and information access of any Contractor employee whose actions are in conflict with the standards of conduct or whom USCIS determines to present a risk of compromising sensitive but unclassified information and/or classified information.

Contract employees will report any adverse information concerning their personal conduct to OSI PSD. The report shall include the contractor's name along with the adverse information being reported. Required reportable adverse information includes, but is not limited to, criminal charges and or arrests, negative change in financial circumstances, and any additional information that requires admission on the SF-85P security questionnaire.

In accordance with Homeland Security Presidential Directive-12 (HSPD-12) http://www.dhs.gov/homeland-security-presidential-directive-12 contractor employees who require access to United States Citizenship and Immigration Services (USCIS) facilities and/or utilize USCIS Information Technology (IT) systems, must be issued and maintain a Personal Identity Verification (PIV) card throughout the period of performance on their contract. Government-owned contractor-operated facilities are considered USCIS facilities.

After the Office of Security & Integrity, Personnel Security Division has notified the Contracting Officer's Representative that a favorable entry on duty (EOD) determination has been rendered, contractor employees will need to obtain a PIV card.

For new EODs, contractor employees have [*10 business days unless a different number is inserted*] from their EOD date to comply with HSPD-12. For existing EODs, contractor employees have [*10 business days unless a different number of days is inserted*] from the date this clause is incorporated into the contract to comply with HSPD-12.

Contractor employees who do not have a PIV card must schedule an appointment to have one issued. To schedule an appointment:
http://ecn.uscis.dhs.gov/team/mgmt/Offices/osi/FSD/HSPD12/PIV/default.aspx
Contractors who are unable to access the hyperlink above shall contact the Contracting Officer's Representative (COR) for assistance.

Contractor employees who do not have a PIV card will need to be escorted at all times by a government employee while at a USCIS facility and will not be allowed access to USCIS IT systems.

A contractor employee required to have a PIV card shall:

- Properly display the PIV card above the waist and below the neck with the photo facing out so that it is visible at all times while in a USCIS facility
- Keep their PIV card current
- Properly store the PIV card while not in use to prevent against loss or theft http://ecn.uscis.dhs.gov/team/mgmt/Offices/osi/FSD/HSPD12/SIR/default.aspx

OSI PSD must be notified of all terminations/ resignations within five days of occurrence. The Contractor will return any expired USCIS issued identification cards and HSPD-12 card, or those of terminated employees to the COR. If an identification card or HSPD-12 card is not available to be returned, a report must be submitted to the COR, referencing the card number, name of individual to whom issued, the last known location and disposition of the card.

SECURITY MANAGEMENT

The Contractor shall appoint a senior official to act as the Corporate Security Officer. The individual will interface with OSI through the COR on all security matters, to include physical, personnel, and protection of all Government information and data accessed by the Contractor.

The COR and OSI shall have the right to inspect the procedures, methods, and facilities utilized by the Contractor in complying with the security requirements under this contract. Should the COR determine that the Contractor is not complying with the security requirements of this contract the Contractor will be informed in writing by the Contracting Officer of the proper action to be taken in order to effect compliance with such requirements.

The Contractor shall be responsible for all damage or injuries resulting from the acts or omissions of their employees and/or any subcontractor(s) and their employees to include financial responsibility.

SECURITY PROGRAM BACKGROUND

The DHS has established a department wide IT security program based on the following Executive Orders (EO), public laws, and national policy:

- Public Law 107-296, Homeland Security Act of 2002.
- Federal Information Security Management Act (FISMA) of 2002, November 25, 2002.
- Public Law 104-106, Clinger-Cohen Act of 1996 [formerly, Information Technology Management Reform Act (ITMRA)], February 10, 1996.
- Privacy Act of 1974, As Amended. 5 United States Code (U.S.C.) 552a, Public Law 93-579, Washington, D.C., July 14, 1987.
- Executive Order 12829, *National Industrial Security Program*, January 6, 1993.
- Executive Order 12958, *Classified National Security Information*, as amended.
- Executive Order 12968, *Access to Classified Information,* August 2, 1995.
- Executive Order 13231, *Critical Infrastructure Protection in the Information Age*, October 16, 2001
- National Industrial Security Program Operating Manual (NISPOM), February 2001.
- DHS *Sensitive Systems Policy Publication 4300A* v2.1, July 26, 2004

- DHS *National Security Systems Policy Publication 4300B* v2.1, July 26, 2004
- Homeland Security Presidential Directive 7, *Critical Infrastructure Identification, Prioritization, and Protection*, December 17, 2003.
- Office of Management and Budget (OMB) Circular A-130, *Management of Federal*
- *Information Resources*.
- National Security Directive (NSD) 42, *National Policy for the Security of National Security Telecommunications and Information Systems* (U), July 5, 1990, CONFIDENTIAL.
- 5 Code of Federal Regulations (CFR) §2635, Office of Government Ethics, *Standards of Ethical Conduct for Employees of the Executive Branch*.
- DHS SCG OS-002 (IT), National Security IT Systems Certification & Accreditation, March 2004.
- Department of State 12 Foreign Affairs Manual (FAM) 600, *Information Security*
- *Technology*, June 22, 2000.
- Department of State 12 FAM 500, *Information Security*, October 1, 1999.
- Executive Order 12472, *Assignment of National Security and Emergency Preparedness Telecommunications Functions*, dated April 3, 1984.
- Presidential Decision Directive 67, *Enduring Constitutional Government and Continuity of Government Operations*, dated October 21, 1998.
- FEMA Federal Preparedness Circular 65, *Federal Executive Branch Continuity of Operations (COOP)*, dated July 26, 1999.
- FEMA Federal Preparedness Circular 66, *Test, Training and Exercise (TT&E) for Continuity of Operations (COOP)*, dated April 30, 2001.
- FEMA Federal Preparedness Circular 67, *Acquisition of Alternate Facilities for Continuity of Operations*, dated April 30, 2001.
- Title 36 Code of Federal Regulations 1236, Management of Vital Records, revised as of July 1, 2000.
- National Institute of Standards and Technology (NIST) Special Publications for computer security and FISMA compliance.

GENERAL

Due to the sensitive nature of USCIS information, the contractor is required to develop and maintain a comprehensive Computer and Telecommunications Security Program to address the integrity, confidentiality, and availability of sensitive but unclassified (SBU) information during collection, storage, transmission, and disposal. The contractor's security program shall adhere to the requirements set forth in the DHS Management Directive 4300 IT Systems Security Pub Volume 1 Part A and DHS Management Directive 4300 IT Systems Security Pub Volume I Part B. This shall include conformance with the DHS Sensitive Systems Handbook, DHS Management Directive 11042 Safeguarding Sensitive but Unclassified (For Official Use Only) Information and other DHS or USCIS guidelines and directives regarding information security requirements. The contractor shall establish a working relationship with the USCIS IT Security Office, headed by the Information Systems Security Program Manager (ISSM).

IT SYSTEMS SECURITY

In accordance with DHS Management Directive 4300.1 "Information Technology Systems Security", USCIS Contractors shall ensure that all employees with access to USCIS IT Systems are in compliance with the requirement of this Management Directive. Specifically, all contractor

employees with access to USCIS IT Systems meet the requirement for successfully completing the annual "Computer Security Awareness Training (CSAT)." All contractor employees are required to complete the training within 60-days from the date of entry on duty (EOD) and are required to complete the training yearly thereafter.
CSAT can be accessed at the following: http://otcd.uscis.dhs.gov/EDvantage.Default.asp or via remote access from a CD which can be obtained by contacting uscisitsecurity@dhs.gov.

IT SECURITY IN THE SYSTEMS DEVELOPMENT LIFE CYCLE (SDLC)

The USCIS SDLC Manual documents all system activities required for the development, operation, and disposition of IT security systems. Required systems analysis, deliverables, and security activities are identified in the SDLC manual by lifecycle phase. The contractor shall assist the appropriate USCIS ISSO with development and completion of all SDLC activities and deliverables contained in the SDLC. The SDLC is supplemented with information from DHS and USCIS Policies and procedures as well as the National Institute of Standards Special Procedures related to computer security and FISMA compliance. These activities include development of the following documents:

- *Sensitive System Security Plan (SSSP)*: This is the primary reference that describes system sensitivity, criticality, security controls, policies, and procedures. The SSSP shall be based upon the completion of the DHS FIPS 199 workbook to categorize the system of application and completion of the RMS Questionnaire. The SSSP shall be completed as part of the System or Release Definition Process in the SDLC and shall not be waived or tailored.
- *Privacy Impact Assessment (PIA) and System of Records Notification (SORN).* For each new development activity, each incremental system update, or system recertification, a PIA and SORN shall be evaluated. If the system (or modification) triggers a PIA the contractor shall support the development of PIA and SORN as required. The Privacy Act of 1974 requires the PIA and shall be part of the SDLC process performed at either System or Release Definition.
- *Contingency Plan (CP)*: This plan describes the steps to be taken to ensure that an automated system or facility can be recovered from service disruptions in the event of emergencies and/or disasters. The Contractor shall support annual contingency plan testing and shall provide a Contingency Plan Test Results Report.
- *Security Test and Evaluation (ST&E)*: This document evaluates each security control and countermeasure to verify operation in the manner intended. Test parameters are established based on results of the RA. An ST&E shall be conducted for each Major Application and each General Support System as part of the certification process. The Contractor shall support this process.
- *Risk Assessment (RA):* This document identifies threats and vulnerabilities, assesses the impacts of the threats, evaluates in-place countermeasures, and identifies additional countermeasures necessary to ensure an acceptable level of security. The RA shall be completed after completing the NIST 800-53 evaluation, Contingency Plan Testing, and the ST&E. Identified weakness shall be documented in a Plan of Action and Milestone (POA&M) in the USCIS Trusted Agent FISMA (TAF) tool. Each POA&M entry shall identify the cost of mitigating the weakness and the schedule for mitigating the weakness, as well as a POC for the mitigation efforts.
- *Certification and Accreditation (C&A)**:*** This program establishes the extent to which a particular design and implementation of an automated system and the facilities housing that system meet a specified set of security requirements, based on the RA of security features

and other technical requirements (certification), and the management authorization and approval of a system to process sensitive but unclassified information (accreditation). As appropriate the Contractor shall be granted access to the USCIS TAF and Risk Management System (RMS) tools to support C&A and its annual assessment requirements. Annual assessment activities shall include completion of the NIST 800-26 Self-Assessment in TAF, annual review of user accounts, and annual review of the FIPS categorization. C&A status shall be reviewed for each incremental system update and a new full C&A process completed when a major system revision is anticipated.

SECURITY ASSURANCES

DHS Management Directives 4300 requires compliance with standards set forth by NIST, for evaluating computer systems used for processing SBU information. The Contractor shall ensure that requirements are allocated in the functional requirements and system design documents to security requirements are based on the DHS policy, NIST standards and applicable legislation and regulatory requirements. Systems shall offer the following visible security features:

- *User Identification and Authentication (I&A)* – I&A is the process of telling a system the identity of a subject (for example, a user) (*I*) and providing that the subject is who it claims to be (*A*). Systems shall be designed so that the identity of each user shall be established prior to authorizing system access, each system user shall have his/her own user ID and password, and each user is authenticated before access is permitted. All system and database administrative users shall have strong authentication, with passwords that shall conform to established DHS standards. All USCIS Identification and Authentication shall be done using the Password Issuance Control System (PICS) or its successor. Under no circumstances will Identification and Authentication be performed by other than the USCIS standard system in use at the time of a systems development.
- *Discretionary Access Control (DAC)* – DAC is a DHS access policy that restricts access to system objects (for example, files, directories, devices) based on the identity of the users and/or groups to which they belong. All system files shall be protected by a secondary access control measure.
- *Object Reuse* – Object Reuse is the reassignment to a subject (for example, user) of a medium that previously contained an object (for example, file). Systems that use memory to temporarily store user I&A information and any other SBU information shall be cleared before reallocation.
- *Audit* – DHS systems shall provide facilities for transaction auditing, which is the examination of a set of chronological records that provide evidence of system and user activity. Evidence of active review of audit logs shall be provided to the USCIS IT Security Office on a monthly basis, identifying all security findings including failed log in attempts, attempts to access restricted information, and password change activity.
- *Banner Pages* – DHS systems shall provide appropriate security banners at start up identifying the system or application as being a Government asset and subject to government laws and regulations. This requirement does not apply to public facing internet pages, but shall apply to intranet applications.

DATA SECURITY

SBU systems shall be protected from unauthorized access, modification, and denial of service. The Contractor shall ensure that all aspects of data security requirements (i.e., confidentiality, integrity, and availability) are included in the functional requirements and system design, and ensure that they meet the minimum requirements as set forth in the DHS Sensitive Systems Handbook and USCIS policies and procedures. These requirements include:

- *Integrity* – The computer systems used for processing SBU shall have data integrity controls to ensure that data is not modified (intentionally or unintentionally) or repudiated by either the sender or the receiver of the information. A risk analysis and vulnerability assessment shall be performed to determine what type of data integrity controls (e.g., cyclical redundancy checks, message authentication codes, security hash functions, and digital signatures, etc.) shall be used.
- *Confidentiality* – Controls shall be included to ensure that SBU information collected, stored, and transmitted by the system is protected against compromise. A risk analysis and vulnerability assessment shall be performed to determine if threats to the SBU exist. If it exists, data encryption shall be used to mitigate such threats.
- *Availability* – Controls shall be included to ensure that the system is continuously working and all services are fully available within a timeframe commensurate with the availability needs of the user community and the criticality of the information processed.
- *Data Labeling*. – The contractor shall ensure that documents and media are labeled consistent with the DHS *Sensitive Systems Handbook.*

Capitalized Property, Plant and Equipment (PP&E) Assets Internal Use Software (IUS)

1. Background

The United States Citizenship and Immigration Services Management Directive No. 128-001, USCIS/Office of Information Technology has an ongoing requirement to report Internal Use Software (IUS) costs for the programs under their purview and assignment. This report is a monthly mandatory requirement, and must include all software releases with a cumulative cost of $500K or greater; bulk purchases of $1 Million, and a useful life of 2 years or more.

2. Requirement

Reporting: All applicable charges for application releases and/or development charges are tracked and reported; documented by each applicable release so that an OIT determination can be made if the asset meets IUS criteria. USCIS has determined that the best method for identifying IUS candidates is through monthly collection of contractor cost data for all releases in development, and will capitalize the cost of an IUS project if it is classified as a G-PP&E asset and meets the required criteria.

Definition: IUS is software that is purchased from commercial off-the-shelf (COTS) vendors or ready to use with little or no changes. Internal developed software is developed by employees of USCIS, including new software and existing or purchased software that is modified with or without a contractor's assistance. Contractor-developed software is used to design, program, install, and implement, including new software and the modification of existing or purchased software and related systems, solely to meet the entity's internal or operational needs.

Invoicing and Reporting: The contractor shall identify, capture, log, track and report the costs of IUS associated with each specific release. IUS Software is typically release centric and includes the application and operating system programs, procedures, rules, and any associated documentation pertaining to the operation of a computer system or program.

The contractor shall, after OIT's determination on whether or not the release meets the capitalization criteria, support OIT's reporting of costs incurred for the project or release, as required. The contractor shall provide the nature and cost of work completed within the relevant period. Costs considered part of IUS activities include systems administration, systems engineering, and program management. The Contractor shall provide the total cost, itemized by release and include the total sum of all applicable IUS activities. At the contractor's discretion, this information may be submitted, either as an attachment or as an itemized line item within the monthly invoices, as outlined in *Table 2: Deliverables Schedule*. For information purposes, the following activities within the development lifecycle have been identified as IUS reportable costs by the USCIS Management Directive No. 128-001:

1) Design: System Design: Design System, Update System Test Plan, Update Security Test Plan, Update Project Plan, Update Business Case, Conduct Critical Design Review and Issue Memo.

2) Programming/Construction: Establish Development Environment, Create or Modify Programs, Conduct Unit & Integration Testing, Develop Operator's Manual, Update

Project Plan, Update Business Case, Migration Turnover/Test Readiness Review, Prepare Turnover Package, Develop Test Plans, Migration Turnover/Issue Test Readiness Memo

3) Testing
    a. Acceptance Testing: Develop Security Test Report, Issue Security Certification, Develop System Documentation, Conduct User Acceptance Testing, Update Project Plan, Update Business Case, Conduct Production Readiness Review, Develop Implementation Plan, Issue Production Readiness Review Memo.
    b. Coding
    c. Installation to hardware
    d. Testing, including parallel processing phase
4) Implementation Activities: Implementation/Transition: Security Accreditation (initial system accreditation only), Issue Implementation Notice, Parallel Operations, Update Project Plans, Update Business Case, Conduct Operational Readiness Review, Issue Operational Readiness Memo.
5) In addition, these cost shall contain, if not already itemized in the attachment (PER) or the invoice, the following additional costs information: Full cost (i.e., direct and indirect costs) relating to software development phase; Travel expenses by employees/contractor directly associated with developing software; Documentation Manuals; COTS purchases.

DevOps Team(s) Eagle II Labor Categories and Levels

[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]

[redacted]

			Base Period						
Item	CLIN Type	Description	QTY Unit		Base Period x = 0	Qty Unit		First Option x = 1	Second Option x = 2
				Monthly Price	$ [redacted]				
0001	FFP	[redacted]	[redacted]	Total Amt	$ [redacted]				
				Monthly Price	$ [redacted]		Monthly Price	$ [redacted]	$ [redacted]
x002	FFP	[redacted]	[redacted]	Total Amt	$ [redacted]	[redacted]	Total Amt	$ [redacted]	$ [redacted]
				Monthly Price	$ [redacted]		Monthly Price	$ [redacted]	$ [redacted]
x003	FFP	[redacted]	[redacted]	Total Amt	$ [redacted]	[redacted]	Total Amt	$ [redacted]	$ [redacted]
				Monthly Price	$ [redacted]		Monthly Price	$ [redacted]	$ [redacted]
0004	FFP	[redacted]	[redacted]	Total Amt	$ [redacted]	[redacted]	Total Amt	$ [redacted]	$ [redacted]
				Monthly Price	$ [redacted]		Monthly Price	$ [redacted]	$ [redacted]
0005	FFP	[redacted]	[redacted]	Total Amt	$ [redacted]	[redacted]	Total Amt	$ [redacted]	$ [redacted]
				Total Base	**$** [redacted]		**Total Option**	**$** [redacted]	**$** [redacted]
									$ [redacted]
w/o Options					$ [redacted]				$ [redacted]