STATEMENT OF WORK

Cloud Hosting, System Administration, and Website Support and Development for the Institute of Education Sciences

I. BACKGROUND

The Institute of Education Sciences (IES) of the U.S. Department of Education currently maintains a virtual data center hosted in Amazon Web Services (AWS). The virtual data center consists of approximately 60 virtual servers, most of which are a version of Windows Server. The primary function of the data center is to host survey collection and dissemination websites in support of IES' mission. This includes web servers, database servers, a vast array of websites and data driven web applications, a system management and web development environment, terminal servers housing analytical and statistical software, and other system support servers. Support for all aspects of IES' web operations, including system administration, website administration and development, and user, staff and developer support, is provided by a team within IES which is comprised of government and contractor staff.

II. SCOPE OF WORK

The objective of this Statement of Work is to acquire the services of a Contractor to provide:

- Access to Amazon Web Services, Infrastructure-as-a-Service (IaaS),
- System support staff
- Website administration and development staff
- System, security, and analytical software.

Contract Type

The contract type for this task order is hybrid, with firm fixed price and cost reimbursement tasks.

Task 1	Cost Reimbursement
Task 2	Firm Fixed Price
Task 3	Firm Fixed Price
Task 4	Cost Reimbursement

III. REQUIREMENTS

Task 1. *Amazon Web Services (AWS)/IaaS Solution*

The Contractor shall provide a cost-effective infrastructure hosted in AWS that meets Federal IT security requirements and utilizes industry standards and best practices that meet or exceed the following criteria.

The Contractor shall:

a. Assume AWS account ownership from incumbent contractor, including gaining full control of all IES owned system resources and accounts hosted in AWS that comprise the IES Data Center. This is expected to take no longer than 4 weeks.

b. Provide AWS cloud services that are currently utilized in the IES Data Center, as well as providing the ability to expand AWS services as usage demands change over time.

c. Provide access to AWS cloud services that meets or exceeds Federal Information Security Management Act (FISMA) requirements for information systems categorized as FIPS-199 defined Moderate and complies with the Federal Risk and Authorization Management Process (FedRAMP) requirements.

d. Provide a solution that shall be physically located in the continental United States, and be in a facility capable of being certified and accredited to host U.S. Government systems.

e. Provide physical colocation space (Equinix SV5, San Jose, CA) to house MTIPS security equipment and cross-connect AWS Direct Connect and MTIPS provider circuits.

f. Provide a robust, fault tolerant infrastructure that allows for high availability of 99.9%, and a one (1) hour recovery time after failure.

g. Provide technical documentation required for certification and accreditation.

Period of Performance

• **Base Year:**	Mar 1, 2020 – Feb, 28, 2021
• **Option Year 1:**	Mar 1, 2021 – Feb 28, 2022
• **Option Year 2:**	Mar 1, 2022 – Feb 28, 2023
• **Option Year 3:**	Mar 1, 2023 – Feb 29, 2024
• **Option Year 4:**	Mar 1, 2024 – Feb 28, 2025

Task 2. *System Operations Support*

The Contractor shall provide system operations support staff, able to perform their work off-site. Support staff shall have experience working with systems in a federal owned data center and demonstrate an understanding through past performance of government IT mandates, regulations, and best practices. Support staff shall have demonstrated experience with and have strong understanding of privacy and data integrity concerns of federal statistical agencies.

The contractor shall:

a. Transition custody of all IES owned software licensing agreements and AWS accounts including all IES hosting assets from the incumbent.

b. Manage all aspects of the IES virtual data center hosted in Amazon Web Services (AWS), which includes:

   - Managing virtual private network, including VPCs, subnets, ACLs, security groups, route tables, IP address allocation, Direct Connect, and DNS.

   - Provisioning and maintaining virtual servers, including server resource allocation, storage, and network resources.

   - Performing disaster recovery and incident response activities, including server backups and drive snapshots, AWS Cloud Trail monitoring, system redundancy, and monitoring the AWS FedRamp package for FISMA compliance monthly.

   - Managing and routinely auditing security and access policies to all AWS resources, including IAM user accounts, groups, and policies, and certificate and key management.

c. Manage all IES servers by providing technical expertise in Microsoft Windows Server, Microsoft SQL Server, and Microsoft Internet Information Services (IIS). Operations support will manage the production and development infrastructure, restore infrastructure operational capabilities during disaster recovery efforts, and perform daily backups.

d. Perform system maintenance, including system and application patching, McAfee ePO management (anti-virus and HIPS), log management, vulnerability scans and remediation, Active Directory management, storage maintenance. To minimize impact on users and program activities, it may be necessary to perform some maintenance activities outside of core business hours (7:30 AM – 5:30 PM EST).

e. Manage all IES websites, databases, and support IES web developers. This includes, but not limited to, website troubleshooting, database maintenance, application and file migration, share access, and user account management.

f. Provide staffing that has experience with and have strong understanding of privacy concerns of federal statistical agencies in respect to sensitive data.

g. Act as technical point of contact for IES hosted systems and related issues for IES Government and contractor staff.

h. Provide an annual review of all FISMA documentation, (e.g. System Security Plan, Disaster Recovery Plan, and Configuration Management Plan)

i. Maintain IES Data Center system information and Plan of Action and Milestones (POA&M) in the Department of Justice Cyber Security Assessment and Management (CSAM) system.

j. Perform annual tests of the Disaster Recovery Plan, Contingency Plan, and Incident Response Plan.

k. Support the following software and applications:

   - Microsoft Windows Server

- Microsoft SQL Server
- Microsoft ASP, ASP.NET, .NET Core
- Linux
- F5 BigIP (LTM, APM, AFM)
- Nagios Log Server
- Microsoft Team Foundation Server
- Microsoft Active Directory
- Microsoft Sharepoint
- AWS Management Console Resources (VPC, EC2, S3, Route 53, Direct Connect, Cloud Watch, Cloud Front, API Gateway, IAM, and SNS)
- Tenable Nessus
- McAfee ePO
- Apache SOLR
- Solarwinds Serv-U
- PA Server Monitor
- Redgate (SQL Compare, SQL Data Compare, SQL Backup)
- ArcGIS
- Tableau
- Windows Server Update Services (WSUS)

Period of Performance

Base Year:	Mar 1, 2020 – Feb, 28, 2021
Option Year 1:	Mar 1, 2021 – Feb 28, 2022
Option Year 2:	Mar 1, 2022 – Feb 28, 2023
Option Year 3:	Mar 1, 2023 – Feb 29, 2024
Option Year 4:	Mar 1, 2024 – Feb 28, 2025

Task 3. *Website Administration and Development*

The Contractor shall provide website administration and development staff, able to perform their work off-site. The contractor shall provide support, administration, and improvements for IES' dissemination and survey collection websites; ensure that the websites IES hosts comply with standards, agency and federal regulations, and industry best practices; take the lead in developing and maintaining the web development standards that ensure the quality of products disseminated on the websites; consult and advise on technical issues and standards implementation related to the websites; improve website architecture to provide higher quality services; and develop and maintain applications to improve workflow and provide better service to the public and other federal agencies.

The contractor shall:

a. Review all new and existing web content for standards compliance, updating technical standards to align with changing industry standards, federal laws, and agency policies, proving technical support to staff and contractors, answer user submitted questions, publish new content to the website, convert print publications to web format, develop new data dissemination tools as well as update and improve existing tools, and improve overall website architecture and design.

b. Review new and existing content to ensure that the products released on the websites, and the websites themselves, meet federal regulations (including but not limited to Section 508 of the Rehabilitation Act http://www.access-board.gov/508.htm), industry standards and best practices, and IES style and technical standards. In addition to meeting standards, the contractor shall test new web applications for performance, usability, and functionality.

c. Continually monitor the request system for new submissions, review new requests to ensure they are correctly formatted and categorized, and establish priority of each request based on time of release or severity if the request is to correct an issue on a live website.

d. Provide technical support to staff and contracts on all matters related to the IES websites, including providing assistance with meeting standards, developing templates and tutorials related to web publishing, answering technical questions about website and server infrastructure and system limitations, providing web analytics support, and assisting the server operations team with application issues and technical guidance.

e. Respond to user questions related to the websites in a timely manner or refer questions to appropriate IES staff members based on subject matter of the question and the area or expertise of the staff.

f. Continually update IES' web development standards with new specifications and remove obsolete standards to be current and align with industry, agency and federal standards.

g. Convert publications specifically selected by IES staff into a suitable web format. Some of the publications include, but are not limited to, Condition of Education (http://nces.ed.gov/programs/coe/), Digest of Education Statistics (http://nces.ed.gov/programs/digest/), and Projections of Education Statistics (http://nces.ed.gov/programs/projections/). This process entails creating html and image files that meet NCES standards, converting tables into accessible html tables, creating navigation based off of publication table of contents, and creating and optimizing graphics.

h. Continually update IES' websites with content provided by IES staff to ensure that the websites stay current with the latest information. Examples of updated content includes, but is not limited to: updating and adding new conferences and trainings, updating the publication release calendar, posting new What's New, Highlights, and Data Snapshots items to the homepage, adding and removing IES staff listings, publishing new Stat Chats, posting Commissioner's Remarks and press releases, processing publication requests, and updating site navigation and site map. The contractor shall also send "Newsflash" emails upon request, which occur on average 5 times a week. The Newsflash content and designated audience will be provided by IES staff.

i. Update the content on the various survey and program area sections and create new survey and program areas sections as needed.

j. Monitor user search patterns and create new keywords, key matches, and filters to return better search results and help users find website content.

k. Publish new content provided by NCES and other Forum participants to the Childstats.gov website, including updating and creating new HTML and image files.

l. Maintain and update websites for IES (http://ies.ed.gov) This work includes, but is not limited to, posting new publications and content to IES websites, adding new grants/funding information, updating the grants database with detailed grants and grant program descriptions, principal investigators, and other details, posting webinars, and publishing the IES bi-monthly newsletter. The Regional Educational Laboratory Program (REL) website (http://ies.ed.gov/ncee/edlabs/) has additional needs including adding new publications and projects to the REL project database and maintaining the information on the various labs.

m. Update dissemination tools to use the most recently available data and improve those search tools by adding new features requested by NCES program staff. The tools to be updated include, but are not limited to: College Navigator (http://nces.ed.gov/collegenavigator/), and Search for Schools and Colleges (http://nces.ed.gov/globallocator/).

n. Manage and update the ERIC.ED.GOV website, including importing new records, adding application features and new data fields, and maintaining data import tools.

o. Update and improve existing tools on the IES Members Site such as the request management system, web publication system, calendar and conference tools, Newsflash system, and create new website management and workflow improvement tools as needed.

p. Maintain the Review Tracking System (RTS) application on the IES intranet site to improve the performance and to facilitate electronic publication tracking of IES publications and data products, as directed by the RTS task leader.

q. Update and improve the common website framework that allows for a standard look and menu elements, and ease development and management, including adding new features, regularly updating graphical elements and styles, and improving standards compliance and performance.

r. Provide all deliverables in electronic formats and provide all computer programming source files and code used in the creation of deliverables.

Period of Performance

- **Base Year:** Nov 1, 2020 – Feb, 28, 2021
- **Option Year 1:** Mar 1, 2021 – Feb 28, 2022
- **Option Year 2:** Mar 1, 2022 – Feb 28, 2023
- **Option Year 3:** Mar 1, 2023 – Feb 29, 2024
- **Option Year 4:** Mar 1, 2024 – Feb 28, 2024

Task 4. *Software Licenses*

The Contractor shall provide system and software licenses allowing for additional functionality in support of IES' cloud hosted systems. The software and software licensing to be purchased through this task order are as follows:

Product	QTY
BIG-IP Virtual Edition Best Bundle (v. 12.1.x - 18.x) - license - 1 Gbps	2
PA Server Monitor Pro 1 Year Support	1
Shutterstock subscription renewal (1 year subscription)	1
Stat/Transfer 25 User Site License - Academic (annual lease)	1
McAfee Associate MFE Endpoint Protection 1YR GL P+ 51-100U (EPSYFM-AA-CA)	75
Stata/MP4 network maintenance for 501306217520; 7–user network license	1
Serv-U MFT 1 year upgrade protection	1
SAS Analytics Pro for a Virtual Machine with 4 processor cores, Windows 64 bit. Annual Maintenance for Site 671625. (SAS-CORES-APRO-4M)	1
SAS/ETS & SAS/IML for a Virtual Machine with 4 processor cores, Windows 64 bit. Annual Maintenance for Site 671625. (SAS-CORES-OTHER-4M)	2
SAS/Access to ODBC & SAS/Access to PCFF for a Virtual Machine with 4 processor cores, Windows 64 bit. Annual Maintenance for Site 671625. (SAS-CORES-ACCESS-4M)	2
FileUp Standard Edition - Annual Maintenance	1
SUDAAN Release 11.0.1 - Annual License	1
NESSUS PROFESSIONAL ONPREM-ANNUAL SUB (RENEW) LICSEU#-003360824, INSTITUTE OF EDUCATIO, SERV-NES-R	1
IBM SPSS AMOS CONCURRENT USER ANNUAL SW SUBSCRIPTION & SUPPORT RENEWAL (E09QRLL)	5
IBM SPSS ADVANCED STATISTICS CONCURRENT USER ANNUAL SW SUBSCRIPTION & SUPPORT RENEWAL (E09PULL)	5
IBM SPSS STATISTICS BASE CONCURRENT USER ANNUAL SW SUBSCRIPTION & SUPPORT RENEWAL (E09PWLL)	5
IBM SPSS COMPLEX SAMPLES CONCURRENT USER ANNUAL SW SUBSCRIPTION & SUPPORT RENEWAL (E09PNLL)	5
IBM SPSS CUSTOM TABLES CONCURRENT USER ANNUAL SW SUBSCRIPTION & SUPPORT RENEWAL (E09PYLL)	5
IBM SPSS MISSING VALUES CONCURRENT USER ANNUAL SW SUBSCRIPTION & SUPPORT RENEWAL (E09Q3LL)	5
IBM SPSS REGRESSION CONCURRENT USER ANNUAL SW SUBSCRIPTION & SUPPORT RENEWAL (E09PJLL)	5
Microsoft Azure DevOps Server - license & software assurance – Server (125-00214)	1
Microsoft Azure DevOps Server - license & software assurance – User CAL (126-00371)	10
Nagios Log Server – 2 server instances	1

Period of Performance

- **Base Year:** Mar 1, 2020 – Feb, 28, 2021
- **Option Year 1:** Mar 1, 2021 – Feb 28, 2022
- **Option Year 2:** Mar 1, 2022 – Feb 28, 2023
- **Option Year 3:** Mar 1, 2023 – Feb 29, 2024
- **Option Year 4:** Mar 1, 2024 – Feb 28, 2025

IV. SCHEDULE DELIVERABLES

Activity	Deliverable	Estimated Due Date
	Base Year	
Task 1	Availability of Base Virtualized Hosting Environment	Within two weeks from award date
Task 2	Support personnel assigned to support systems	Within two weeks from award date
Task 3	Website staff assigned to support website	Within two weeks from start of period of performance
Task 4	System license or software	Within two weeks of request for license

V. INVOICING

The contractor shall submit **monthly reports** on or before the 10th of each month. The monthly reports are to be submitted via lectronic transmission. The monthly report shall be submitted to the COR, appointed Task Leader, and Contract Specialist.

The report shall include the following:

a) The progress on each task and activity relative to the schedule and a discussion of discrepancies;

b) Accomplishments associated with each task and activity for the month;

c) Problems that have been resolved or are in need of resolution;

d) A discussion of the work to be performed during the next monthly reporting period;

e) Brief description of the work performed by each subcontractor during the month;

f) Detailed breakdown of cloud hosting spending;

g) Funding expended by major category, including staff, travel, consultant, subcontractors, and other costs, including obligated costs of subcontractors; and

h) Expected future technical and budgetary problems and proposed solutions to these.

VI. CONFIDENTIALITY, SECURITY, IT & OTHER REQUIREMENTS

Staffing

The contractor shall provide in writing at least two (2) weeks advanced notice for replacement of staff proposed. This notice shall be provided to the Task Leader, COR and Contracting Officer (CO) and shall include justification (including proposed substitutions) in sufficient detail to permit evaluation of the impact on the program. All resumes of proposed replacement staff must be provided and approved by the COR and Task Leader before replacing any individual on this project.

Security Clearance

The work to be performed on this contract has been classified at the OPM risk level of "High Risk. Potential for exceptionally serious impact to the public's trust; position duties and responsibilities are especially critical to the agency or a program mission." The contractor shall provide staff capable of achieving a 6c Public Trust Clearance.

Confidentiality of Individuals and Institutions

IES assures participating individuals and institutions that any data collected conforms to the IES standards for protecting the privacy of individuals as required by Section 183 of the Education Sciences Reform Act of 2002 (P.L. 107-279):

> ". . . all collection, maintenance, use, and wide dissemination of data by the Institute, including each office, board, committee, and Center of the Institute, shall conform with the requirements of section 552A of Title 5, United States Code [which protects the confidentiality rights of individual respondents with regard to the data collected, reported, and published under this title]." (Section 183)

Under the Education Sciences Reform Act of 2002 (ESRA 2002), all individually identifiable information about students, their families, and their schools shall remain confidential. To this end, this law requires that no person may:

- Use any individually identifiable information furnished under the provisions of this section for any purpose other than statistical purposes for which it is supplied, except in the case of terrorism;
- Make any publication whereby the data furnished by any particular person under this section can be identified; or
- Permit anyone other than the individuals authorized by the Commissioner to examine individual reports.

Further, individually identifiable information is immune from legal process, and shall not, without the consent of the individual concerned, be admitted as evidence or used for any purpose in any action, suit, or other judicial or administrative proceeding, except in the case of terrorism. Employees, including temporary employees, or other persons who have sworn to observe the limitations imposed by this law, who knowingly publish or communicate any individually identifiable information will be subject to fines of up to $250,000 or up to 5 years in prison, or both (Class E felony).

Protection and Security of Data

The confidentiality of individually identifiable information contained in project documents, data, and other information supplied by the Institute of Education Sciences, U.S. Department of Education (the Department) or information acquired in the course of performance under this contract where the information was furnished under the provisions of Section 183 of the Education Sciences Reform Act of 2002 is a material aspect of the contract and must be maintained, secured, and protected from disclosure as provided in Section 183. The Privacy Act of 1974 (5 U.S.C. 552a) also applies.

The contractor shall enforce strict procedures for assuring confidentiality. These procedures shall apply to all phases of the project and should include but not be limited to: information used to locate study respondents, data collection in the field, coding and editing phases of data prior to machine processing, safeguarding response documents, and maintenance of any respondent follow-up information. Contractor shall physically separate the identifying data required for any follow-up from data required for research purposes.

The contractor shall be familiar with and comply with:

1) The Privacy Act of 1974 (5 U.S.C. 552a), https://www.justice.gov/opcl/privacy-act-1974
2) Confidentiality Information Protection and Statistical Efficiency Act (CIPSEA) of 2002 (P.L. 107-347, Title V, Subtitle A, “Confidential Information Protection”), http://www.gpo.gov/fdsys/pkg/STATUTE-116/pdf/STATUTE-116-Pg2899.pdf
3) Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. 1232g; 34 CFR Part 99), https://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html
4) The Freedom of Information Act (5 U.S.C. 552), https://www.foia.gov/ n
5) Part C of the Education Sciences Reform Act of 2002 (P.L. 107-279), https://www.congress.gov/107/plaws/publ279/PLAW-107publ279.pdf,
6) Part E, Section 183 of the Education Sciences Reform Act of 2002 (P.L. 107-279), https://www2.ed.gov/policy/rschstat/leg/PL107-279.pdf,
7) No Child Left Behind Act (20 U.S.C. 70), https://www2.ed.gov/policy/elsec/leg/esea02/index.html,
8) USA Patriot Act of 2001 (P.L. 107-56), https://www.congress.gov/bill/107th-congress/house-bill/3162,
9) Office of Management and Budget (OMB) Federal Statistical Confidentiality Order of 1997, https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/federal_register/FR1997/conf-order.pdf,

10) OMB Guidance of 7/12/2006 on the Reporting of Incidents Involving Personally Identifiable Information (M-06-19), http://www.whitehouse.gov/OMB/memoranda/fy2006/mo6-19.pdf,
11) OMB Guidance of 5/22/2006 on Safeguarding Personally Identifiable Information (M-06-15), http://www/whitehouse.gov/omb/memoranda/fy2006/m-06-15.pdf,
12) Federal Information Security Management Act (FISMA) of 2002 (P.L. 107-347, Title III),

The contractor shall maintain the confidentiality of all documents, data, and other information supplied by IES/ED or acquired in the course of performance of this contract, except for any documents or other information specifically designated as non-confidential by IES/ED. The contractor shall take such measures as are necessary to maintain the required security and protection of confidential information (see section Data Security Plan). The contractor shall be prepared to develop compliance procedures in cooperation with the COR concurrently with the development of the study design.

IT Security and Policies

The contractor shall:

- Complete/update the appropriate level of Security Accreditation (SA) documentation per NIST Risk Management Framework guidance, security controls testing, interagency security agreements (ISAs), and risk assessments in support of government issuance of security assessment and authorization to operate (ATO) decisions

- Ensure that systems/products/applications have the ability to facilitate single-sign-on capabilities and required support for HSPD 12 Personal Identity Verification (PIV) enablement and integration

- Include the capability for network traffic that flows between externally hosted systems and networks, to/from Department systems and networks, to be routed through one of the Department’s Trusted Internet Connections (TIC) gateways as part of the solution configuration. Implement controls to ensuring all possible traffic, including mobile and cloud, goes through a TIC. Implement connections between Department systems and networks with externally hosted systems that are in compliance with the requirements of the Trusted Internet Connections (TIC) initiative

- Architect contractor hosting environments to use security isolation and network segmentation principles in order to ensure that the environments are properly protected against an unauthorized access and threat from adversaries who may strive to move laterally across internal Department or contractor hosted systems and network segments.

- Provide an automated capability and process to scan and assess all systems and assets, and associated logs for malicious indicators of compromise (IOCs) identified by the Department regarding priority threat-actor Techniques, Tactics, and Procedures (TTPs); the contractor is required to have the capability to scan for indicators of compromise within 24 hours of receipt of the indicators provided by the Department of Education from the Department of Homeland Security

- Implement and maintain capabilities and processes to support the timely detection of, reporting, and rapid response and recovery to cyber incidents in accordance with timelines and requirements specified in Federal guidance and Department cybersecurity incident reporting policy guidance

- In support of cybersecurity performance measure reporting, the contractor shall implement and maintain an automated software asset management/inventory and hardware asset inventory capability (e.g. scans/device discovery processes) at the enterprise-level.

- Implement capabilities to rapidly deploy emergency security patches and implement specific security control enhancements as directed by the Department of Homeland Security to all Federal Departments via mechanisms such as the DHS Cybersecurity Coordination, Assessment, and Response (C-CAR) action items, and DHS Binding Operational Directives (BODs).

- Implement capabilities and processes to patch all critical vulnerabilities identified to the Department of Education by DHS immediately or, at a minimum, within 30 days of patch release.

- Ensure robust physical and cybersecurity protections are in place for all of the Department's high value assets (HVAs). The identification of HVAs by the Department will be an ongoing activity due to the dynamic nature of cybersecurity risks.

- Implement remote access solutions that only use multi-factor authentication solutions and that prohibit the use of split tunneling and/or dual-connected remote hosts where the connecting device has two active connections.

- Implement remote access solutions that scan for malware before allowing full connections and that time out after 30 minutes (or less) of inactivity and require re-authentication to re-establish a session

- Implement capabilities for all incoming email traffic to pass through anti-phishing and anti-spam filtration at the outermost border mail agent or server

- Implement capabilities for all incoming email traffic to be analyzed using sender authentication protocols (e.g., DKIM, DMARC, VBR, SPF, iprev)

- Implement capabilities that ensure that incoming email traffic is analyzed using a reputation filter (to perform threat assessment of sender)

- Implement capabilities that ensure that incoming email traffic is analyzed for detection of clickable URLs, embedded content, and attachments; and incoming email traffic is first analyzed for suspicious or potentially nefarious attachments and opened in a sandboxed environment or detonation chamber

- Implement capabilities for all outbound communications traffic to be checked at the external boundaries to detect encrypted exfiltration of information (i.e. capability to decrypt/interrogate and re-encrypt)

- Implement effective network segmentation design and security solutions to limit potential threats from adversaries attempting lateral movement across systems on the Department's (or contractor's networks), and also to better protect and securely isolate the Department's HVAs

- Implement and maintain Information Security Continuous Monitoring (ISCM) and Continuous Diagnostics and Mitigation (CDM) capabilities for all IT assets to be subject to an automated inventory, configuration, and vulnerability management capability, with real time reporting

- Implement and maintain strong authentication capabilities requiring the technical enforcement of all users being required to use a Personal Identity Verification (PIV) card to authenticate to the network, (with exceptions for a very limited set of users specifically approved by the Department)

- Develop and maintain (or update existing) System Security Plans (SSP) and security controls assessment (SCA) test plans for the network general support system (GSS), and infrastructure systems

- Provide support to creating the security assessment and authorization (or accreditation) (SA&A) packages and documentation in accordance with the Risk Management Framework guidance and processes specified by NIST and Department guidance

- Implement security configurations on all IT assets and systems using DISA STIGs and other industry recognized best practices or guidance

- Perform security configuration management to include configuring all Windows based systems with the latest United States Government Configuration Baseline (USGCB) security settings available from the NIST website

- Support annual or emergent security audits and security scans that may be performed by the Office of Inspector General (OIG), the General Accountability Office (GAO), or the Department of Homeland Security (DHS)

- The contractor shall provide availability and accessibility to the Department, to the OIG, and to any third party vendors designated by the Department to: 1) Review audit findings; 2) Determine if corrective actions were properly implemented and the associated audit findings were properly closed; 3) Support cybersecurity incident analysis and forensics activities

- Produce scheduled Monthly/Quarterly/Annual security performance measure reports that align to the Department's cybersecurity performance measure reporting requirements specified by OMB for FISMA, the President's cybersecurity Cross Agency Priority (CAP) goals and targets, and CyberScope reporting. Security performance measure reports shall use the format and template specified in the Annual CIO FISMA metrics specified by OMB and DHS.

- Provide for the encryption for PII, CUI, Data at Rest and data in transit, Encryption solutions applied must be FIPS 140-2 validated.

- Document and track contractor personnel cyber training based on roles

- Develop, maintain, and publish a listing of Contractor-provided security controls, hybrid security controls, and "customer"-provided security controls, in support of systems security assessments and authorizations, and the issuance of authority to operate (ATO) decisions by the Department

- Provide security audit support (e.g. A-123), including scheduled and event-driven audits

- Capture and provide forensic disk images to support security incident analysis, malware analysis, or other investigative requirements (such as specific requests from the OIG or law enforcement)

- Provide support for threat monitoring and analysis, incident response, vulnerability management, risk management, continuous monitoring and reporting and other traditional security operations center activities

- Provide and maintain multi-factor authentication solutions utilizing the Personal Identity Verification (PIV) card (or a Department- approved Level of Authentication -4 solution); and utilize FIPS 140-2 approved encryption for all remote access requirements

- Provide robust encryption capabilities to include services such as digitally signed and encrypted email, and default encryption for sensitive information held by the Department. Solutions should be available to enable encryption of as much data at rest and data in transit as possible.

- Identify, perform, track, and report vulnerability and security weakness remediation and mitigation activities through the Department's Plan of Action and Milestones process (POA&M) in accordance with Departmental information security policy

- Establish, maintain, and execute standard configuration management processes for all cybersecurity software and hardware

- Implement and maintain a Privileged Account Management Solution to improve the identity and access management of user accounts, while also meeting Department targets to tightly control and limit the number of users with elevated privileges

- Implement and maintain tightened processes for managing privileged user accounts, to include implementation of capabilities to limit functions that can be performed when using privileged accounts; limit the duration that privileged users can be logged in; limit the privileged functions that can be performed using remote access; prohibit Internet access when privileged users are performing systems administrations tasks; and ensure that privileged user activities are logged and regularly reviewed

- Document and maintain system security boundaries, system configuration details, and network diagrams, in support of security assessment and authorization to operate (ATO) processes

- Develop and implement processes for revising system security documentation on a scheduled and event-driven basis

- Provide support for maintaining system security documentation in support of FISMA reporting requirements and security compliance status in the Department's Cyber Security Assessment and Management (CSAM) system

- Develop and submit system security documentation, risk assessments, security controls testing reports, and any required privacy impact analysis (PIA) to the Department in support of the Risk Management Framework processes and ATO decisions for IT environment components

- Develop corrective/remediation plans of action and milestones (POAMs) and strategies to address security audit and assessment findings, and other reports of system security weaknesses or non-compliance

- Develop and maintain a system security architecture; the contractor's solution shall include effective network segmentation design and solutions to limit lateral movement across systems on the Department's networks, and also better protect the Department's HVAs
- Utilize PIV or other approved Level of Assurance 4, as defined in NIST SP 800-63-2 Electronic Authentication Guidelines, compliant Identity and Access Control mechanisms for network/domain administrative enterprise access.
- Maintain near real-time security monitoring and intrusion detection capabilities to enable the contractor and the Department to know the security risk posture of the network at any given time;
- Configure all Windows based systems with the latest United States Government Configuration Baseline (USGCB) security settings available from the NIST website
- Utilize multi-factor authentication, including integration and compliance with HSPD-12 PIV requirements, for all remote access solutions for the Department's sensitive information systems
- Provide a multi-tier disaster recovery capability that provides the infrastructure and process to meet the recovery requirements of all of its High Value Assets (HVAs), and applications (Mission-Critical, Decision Support, Other)
- Provide IT Disaster Recovery Planning and Management capabilities and support
    - Define business risk and risk assessment
    - Develop disaster recovery strategies
    - Develop disaster recovery plans
    - Develop IT system contingency plans
    - Conduct disaster recovery exercises, training and awareness
- Provide Disaster Recovery Operational Services, including Contractor support to the Department in the planning, preparation, implementation, and documentation of a Disaster Recovery Program that includes the capabilities described below:

The contractor, and all sub-contractors, shall comply with the Department of Education's IT security policy requirements, and other applicable procedures and guidance. The contractor, and all sub-contractors, shall develop and implement management, operational and technical security controls to assure required levels of protection for information systems. The contractor, and all sub-contractors, shall further comply with all applicable Federal IT security requirements including, but not limited to, the Federal Information Security Modernization Act (FISMA) of 2014, Office of Management and Budget (OMB) Circular A-130, Homeland Security Presidential Directives (HSPD), including HSPD-12, Personal Identity Verification (PIV) Enablement and Integration, and single sign-on, the most recent National Institute of Standards and Technology (NIST) special publications, standards and guidance, and the Federal Risk and Authorization Management Program (FedRAMP) requirements and guidance.

These security requirements include, but are not limited to, the successful Security Assessment and Authorization (SA&A) of the system (includes commercially owned and operated systems managed by the commercial vendor and its sub-contractors, supporting Department programs, contracts, and projects);

obtaining a full Authority to Operate (ATO) before being granted operational status; performance of annual self-assessments of security controls; annual Contingency Plan testing; performance of periodic vulnerability scans; updating all information system security documentation as changes occur; and other continuous monitoring activities, which may include, mapping, penetration and other intrusive scanning. Full and unfettered access for any of the Department's third party Managed Security Services Provider (MSSP) or Cyber-operations prevention testers, or vulnerability scanners, or auditors must be granted to access all computers and networks used for this system. Additionally, when there is a significant change to the system's security posture, the system (Federal and commercial prime- and sub- contractors included) must have a new SA&A, with all required activities to obtain a new ATO, signed by the Authorizing Official (AO).

System security controls shall be designed and implemented consistent with the current, finalized version of the NIST SP 800-53, 'Recommended Security Controls for Federal Information Systems and Organizations.' All NIST SP 800-53 controls must be tested / assessed no less than every 3 years, according to federal and Department policy. The risk impact level of the system will be determined via the completion of the Department's inventory form and shall meet the accurate depiction of security categorization as outlined in Federal Information Publishing Standards (FIPS) 199, 'Standards for Security Categorization of Federal Information and Information Systems.'

System security documentation shall be developed to record and support the implementation of the security controls for the system. This documentation shall be maintained for the life of the system. The contractor, and all sub-contractors, shall review and update the system security documentation at least annually and after significant changes to the system, to ensure the relevance and accurate depiction of the implemented system controls and to reflect changes to the system and its environment of operation. Security documentation must be developed in accordance with the NIST 800 series and Department of Education policy and guidance.

The contractor, and all sub-contractors, shall allow Department employees (or Department designated third party contractors) access to the hosting facility to conduct SA&A activities to include control reviews in accordance with the current, finalized version of the NIST SP 800-53, and the current, finalized version of the NIST SP 800-53A. The contractor, and all sub-contractors, shall be available for interviews and demonstrations of security control compliance to support the SA process and continuous monitoring of system security. In addition, if the system is rated as 'Moderate' or 'High' for FIPS 199 risk impact, vulnerability scanning and penetration testing shall be performed on the hosting facility and application as part of the SA&A process. Appropriate access agreements will be reviewed and signed before any scanning or testing occurs.

Identified deficiencies between required security controls within the current, finalized version of the NIST SP 800-53 and the contractor's, and all sub-contractor's implementation, as documented in the Risk Assessment Report, System Security Plan (SSP) and Security Assessment Report (SAR), shall be tracked for mitigation through the development of a Plan of Action and Milestones (POA&M) in accordance with Department policy. Depending on the severity of the deficiencies, the Department may require remediation before an ATO is issued.

The contactor shall provide cybersecurity strategies, infrastructure hosting environments, and solutions that comply with the requirements of the Federal Information Security Modernization Act (FISMA), Department cybersecurity policy guidance, and guidance contained in the NIST Special Publications series such as NIST Special Publication 800-53 and other NIST Special Publications. The contractor shall provide solutions that support the Department's efforts to implement and maintain effective protection activities such as reducing the attack surface and complexity of IT infrastructure; minimizing the use of administrative privileges; utilizing strong authentication credentials; safeguarding data at rest and in-transit; training personnel; ensuring repeatable processes and procedures; adopting innovative and modern technology; ensuring strict domain separation of critical/sensitive information and information systems; implementing network segmentation architectures to better protect and isolate the Department's high value assets and most sensitive information and data; and ensuring a current inventory of hardware and software components. The contractor shall include actions and initiatives to implement the NIST Cybersecurity Framework that emphasizes and measures capabilities to "Identify, Protect, Detect, Respond, and Recover," and ensure that all applicable Service Level Agreements (SLA)s are adhered to, complied with, and satisfied.

All awarded contracts shall ensure that:

1. Their IT product/system is monitored during all hours of operations using entrusted detective/preventive systems;
2. Their IT product/system has current antiviral products installed and operational;
3. Their IT product/system is scanned on a reoccurring basis;
4. Vulnerabilities are remediated in a timely manner on their IT product/system; and
5. Access/view for cyber security situational awareness on their IT product/system is made available to the Department CIRC (cyber incident response capability).
6. All applicable Service Level Agreements (SLA)s are adhered to, complied with, and satisfied.

Internet Protocol version 6 (IPv6)

For IPv6, the contractor shall provide COTS solutions that are IPv6 capable. An IPv6 capable system or product shall be capable of receiving, processing, transmitting and forwarding IPv6 packets and/or interfacing with other systems and protocols in a manner similar to that of IPv4. Specific criteria to be deemed IPv6 capable are:

- An IPv6 capable system that meets the IPv6 base requirements defined by the USGv6 Profile (http://www.antd.nist.gov/usgv6/profile.html).
- Systems being developed, procured or acquired shall maintain interoperability with IPv4 systems/capabilities.
- Systems shall implement IPv4/IPv6 dual-stack and shall also be built to determine which protocol layer to use depending on the destination host it is attempting to communicate with or establish a socket with. If either protocol is possible, systems shall employ IPv6.
- The contractor shall provide IPv6 technical support for system development, implementation and management.

Per OMB-M-17-12, Preparing for and Responding to a Breach of Personally Identifiable Information, the following requirements statements should be added to all SOWs/SOOs/PWSs/BPAs/MOUs/IAAs/MOUs/ISAs that include the management of Personally Identifiable Information (PII) and / or Sensitive Personally Identifiable Information (SPII):

- The contractor shall cooperate with and exchange information with agency officials, as determined necessary by the agency, in order to effectively report and manage a suspected or confirmed breach.
- The contractor and subcontractors (at any tier) shall properly encrypt PII in accordance with OMB Circular A-130 and other applicable policies and to comply with any agency-specific policies for protecting PII;
- The contractor shall complete regular Department training for contractors and subcontractors (at any tier) on how to identify and report a breach;
- The contractor and subcontractors (at any tier) shall report a suspected or confirmed breach in any medium or form, including paper, oral, and electronic, as soon as possible and without unreasonable delay, consistent with the agency's incident management policy and US-CERT notification guidelines;
- The contractor and subcontractors (at any tier) shall maintain capabilities to determine what Federal information was or could have been accessed and by whom, construct a timeline of user activity, determine methods and techniques used to access Federal information, and identify the initial attack vector;
- The contractor shall allow for an inspection, investigation, forensic analysis, and any other action necessary to ensure compliance with this Federal and Department PII Breach Response policies (such as OMB-M-17-12), the Department’s breach response plan, and to assist with responding to a breach;
- The contractor shall identify roles and responsibilities, in accordance with Federal and Department PII Breach Response policies (such as OMB-M-17-12), and the agency's breach response plan; and,
- The contractor shall be aware that a report of a breach shall not, by itself, be interpreted as evidence that the contractor or its subcontractor (at any tier) failed to provide adequate safeguards for PII.

Reporting of Data Security Breaches

If there is a suspected or known breach/disclosure of PII due to lost, theft, intercepted transfer, or other, the contractor must ensure that this breach is reported to the agency as soon as the contractor has knowledge of it. Per Office of Management and Budget Memorandum M-17-12, Federal agencies have a requirement to report breaches of PII security to the United States Computer Emergency Response Team (US-CERT).” The (PO) must notify the department within 30 minutes of discovering the incident (and the agency should not distinguish between suspected or confirmed breaches). The data security plan must be written to reflect this requirement, and the contractor must provide sufficient notification and documentation of the suspected loss, as it is understood at the time of notification to the agency for this requirement to be met. Follow-up reports of the final status of loss events will also be prepared by the contractor within a reasonable period of time as advised by the COR.

FOR E-MAIL:

In accord with BOD-18-01:

- Email Security: Agencies must configure all internet-facing mail servers to offer STARTTLS, and all second-level agency domains to have valid SPF/DMARC records. Additionally, agencies must ensure Secure Sockets Layer (SSL) v2 and SSLv3 are disabled on mail servers, and 3DES and RC4 ciphers are disabled on mail servers:
  - Within one year after issuance of this directive, issued 10-16-2017 (so, due by 10-16-2018), agencies will be required to set a DMARC policy of "reject" for all second-level domains and mail-sending hosts.
  - In accord with OMB Memorandums M-17-06, and M-15-13, and M-08-23, M-10-23, and with Binding Operational Directive (BOD) BOD-18-01, and with the NIST SP 800-52 and with the NIST SP 800-44, all e-mail applications must have SMTP enabled.

FOR NON-PUBLIC-FACING WEBSITES:

- Implement capabilities for all inbound network traffic to pass through a web content filter, which provides anti-phishing, anti-malware, and blocking of malicious websites (e.g., fake software updates, fake antivirus offers, and phishing offers)
- In accord with OMB Memorandums M-17-06, and M-15-13, and M-08-23, M-10-23, and with Binding Operational Directive (BOD) BOD-18-01, and with the NIST SP 800-52 and with the NIST SP 800-44, all Federal websites and web services must be accessible through a secure connection (HTTPS only, with HSTS), and e-mail applications must have SMTP enabled. The use of HTTPS is encouraged on intranets, but not explicitly required.
- In accord with BOD-18-01: In accord with OMB Memorandum M-08-23, in order to ensure Domain Name System Security (DNSSEC), all federal websites must be hosted on a *.gov location.

FOR PUBLIC-FACING WEBSITES:

- Implement controls to ensure that all publicly accessible externally hosted Department websites and web services only provide service through a secure connection, (such as the Hypertext Transfer Protocol Secure (HTTPS)).
- Implement controls to ensure that all publicly accessible Department websites and web services only provide service through a secure connection, (such as the Hypertext Transfer Protocol Secure (HTTPS))

In accord with BOD-18-01:

- Web Security: Agencies must ensure all publicly accessible Federal websites and web services provide service through a secure connection (HTTPS-only, with HSTS); SSLv2 and SSLv3 are disabled on web servers, and DES and RC4 ciphers are disabled on web servers; and must provide a list to DHS of agency second-level domains that can be HSTS preloaded, for which HTTPS will be enforced for all subdomains.
- If an official public-facing website will be developed, modified, or maintained, then, in accord with OMB Memorandum M-17-06, each agency must use only an approved .gov or .mil domain for its official public-facing websites. The requirement to use only approved government domains does not apply in circumstances where the agency is a user or a customer of a third-party website or service that resides on a non-governmental domain.

OMB-17-06 Policies and Requirements for Public Websites

- For requirements involving web applications, web servers, and web services, the contractor shall follow the policies, principles, standards, and guidelines on information security and privacy, in accordance with FISMA, and implement security and privacy requirements as set forth in OMB Circular A-130 and National Institute of Standards and Technology (NIST) Special Publication 800-44, Guidelines on Securing Public Web Servers.
- The public expects Federal Government websites to be secure and their interactions with those websites to be private. The contractor shall comply with requirements specified in OMB Memorandum M-15-13, Policy to Require Secure Connections across Federal Websites and Web Services, that requires that all publicly accessible Federal websites and web services only provide service through a secure connection (HTTPS with HSTS).
- The contractor shall use only an approved .gov or .mil domain for official public-facing websites. The requirement to use only approved government domains does not apply in circumstances where the Department is a user or a customer of a third-party website or service that resides on a non-governmental domain. Department use of third-party websites and applications must comply with all relevant privacy protection requirements and a careful analysis of privacy implications as specified in OMB Memorandum M-10-23, Guidance for Agency Use of Third-Party Websites.
- The contractor shall ensure compliance with Federal requirements to maintain public/external facing servers and services to use native IPv6. All procurements of networked information technology shall comply with Federal Acquisition Regulation (FAR) requirements for use of the U.S. Government IPv6 Profile and Test Program for the completeness and quality of their IPv6 capabilities

FOR CLOUD SOLUTIONS:

- Implement controls to ensure that all publicly accessible externally hosted Department websites and web services only provide service through a secure connection, (such as the Hypertext Transfer Protocol Secure (HTTPS)).
- Only utilize FedRAMP approved cloud solutions. FedRAMP is mandatory for federal agency cloud deployments and service models at the low and moderate risk impact levels.
- If a cloud solution will be used, then an ED-issued, FedRAMP-Compliant Authorization To Operate (ATO) is a Federal and a Departmental requirement, and one must be obtained.

FOR CYBEROPERATIONS, PENETRATION TESTING, VULNERABILITY SCANNING, INTRUSION DETECTION, AND INCIDENT RESPONSE FUNCTIONS:

- Implement scanning capabilities that assess for vulnerabilities using only Security Content Automation Protocol (SCAP) validated products
- Perform penetration and regular vulnerability testing and scanning of systems, IT devices, and websites. Vulnerability scanning shall be conducted at least monthly, with reports provided to the Department.
- Maintain the tools and capabilities to support asset discovery, to include passive network monitoring, active network monitoring, and automated network mapping
- Maintain tools and capabilities to support behavior monitoring, to include NetFlow analysis and network traffic capture, which captures the Transmission Control Protocol/Internet Protocol (TCP/IP) stream, allowing for replay of activity to determine what happened during a breach or incident
- Maintain tools and capabilities for intrusion prevention, to include host intrusion prevention systems (HIPS) and network intrusion prevention systems (NIPS)

- Maintain a firewall system designed to prevent unauthorized access to or from any contractor systems and network
- Maintain tool and capabilities to perform Security Incident/Event Management and Analysis, to include centralized logging, log correlation, and a Security Information and Event Management (SIEM) solution that provides centralized monitoring of security incidents; network behavior analytics to provide behavior-based detection to help protect against zero-day attacks; and a quarantine/sandbox environment that will isolate and analyze live traffic and/or suspected malware
- Maintain tools and capabilities to perform vulnerability and risk management and analysis to include threat intelligence threat hunt capabilities, sharing platforms, risk management or trouble ticketing system, anti-malware and anti-phishing services
- Maintain tools and capabilities to provide security situational awareness and visibility throughout the enterprise; this includes capabilities for full packet capture that collects detailed network information at the gateway and makes capture data available to analysts; endpoint incident response that enables searches all endpoints for Indicators of Compromise (IOCs) in a rapid fashion; and encrypted traffic inspection
- If working as a SOC contractor or subcontractor, will provide a Daily Morning Report, 7 days per week, that summarizes the noteworthy daily security activities. Examples include activities such as the daily count of security incidents detected (viruses, malware, etc. . .), email traffic analysis for spam and phishing attempts, vulnerability scan results and progress in closing open weaknesses from scan results. The contractor is encouraged to propose a world class daily security morning report format, with the most noteworthy performance measures, to include any graphic displays, and charts to enhance reporting
- Provide and maintain automated means of discovering, monitoring, and protecting sensitive data to ensure protection of data in motion, at rest, and in use
- Provide and maintain an automated means of preventing unauthorized users and computing devices from accessing contractor hosted environments, including access via remote access, wired and wireless technologies
- Provide and maintain externally facing web application firewall capabilities providing inbound and outbound traffic filtering
- Provide and maintain an Out of Band network device management solution
- Administer, operate, maintain, configure and tune cybersecurity software and hardware
- Provide full government visibility of continuous monitoring tool configurations and output on a real-time basis as well as historical data/logs
- Maintain the capability to perform periodic penetration testing, and also support for external agency red team testing, penetration testing, cyber hygiene web site vulnerability scanning tests and vulnerability assessments that the Department may need to conduct

FOR GOVERNMENT FURNISHED EQUIPMENT (GFE):

- Implement capabilities to ensure that GFE endpoints are covered by an intrusion prevention system, and by an antivirus (AV) solution using file reputation services, checking files against cloud-hosted, continuously updated malware information
- Implement capabilities to ensure that GFE endpoints are covered by an anti-exploitation tool (e.g., Microsoft's Enhanced Mitigation Experience Toolkit (EMET) or similar)
- Implement capabilities to ensure that GFE endpoints are protected by a browser-based (e.g., Microsoft SmartScreen Filter, Microsoft Phishing Filter, etc.) or enterprise-based tool to block known phishing websites and IP addresses

Managing Controlled Unclassified Information (CUI) Requirements

Applicability

The contractor shall be responsible for handling sensitive and/or Controlled Unclassified Information (CUI) that is collected, stored, transmitted, or destroyed for the purposes of this contract in accordance with any applicable laws, regulations and government wide Policies (LRGWP) to include EO 13556, 32 CFR 2002 Part 2, The Department of Education Directive and NIST-800-171B when approved. These requirements apply to the Contractor, its subcontractors and teaming partners, and employees (hereafter referred to collectively as "Contractor"). These requirements are applicable to all Department information and data, regardless of medium, maintained by the Contractor for the performance of this contract.

Authorization to Handle CUI

No person may have access to CUI unless that person has a valid need for such access in connection with the accomplishment of a lawful and authorized US Government mission. The Authorized holder is an individual, agency, organization, or group of users that is permitted to designate or handle CUI, in accordance with 32 CFR Part 2002. The authorized holder who designates the CUI must make recipients aware of the information's CUI status in accordance with 32 CFR Part 2002.

Safeguarding

The contractor shall be responsible for safeguarding any CUI that is collected for the purposes of this contract. The Contractor shall ensure that the appropriate personnel, administrative, technical, and physical safeguards are established to ensure the security and confidentiality of this information, data, audio, video, documentary material, records and/or equipment is properly protected. The Contractor shall abide by and follow all LRGWP as it pertains to safeguarding of CUI. All electronically stored CUI shall be encrypted at rest and in motion as defined in the SOW. Contractors must take reasonable precautions to guard against unauthorized disclosure of CUI. Contractors must include the following measures among the reasonable precautions:

- Establish controlled environments in which to protect CUI from unauthorized access or disclosure and make use of those controlled environments;
- Reasonably ensure that unauthorized individuals cannot access or observe CUI, or overhear conversations discussing CUI;
- Keep CUI under the authorized holder's direct control or protect it with at least one physical barrier, and reasonably ensure that the authorized holder or the physical barrier protects the CUI from unauthorized access or observation when outside a controlled environment; and
- Protect the confidentiality of CUI that The Department or authorized holders process, store, or transmit on Federal information systems in accordance with the applicable security requirements and controls established in FIPS PUB 199, FIPS PUB 200, and NIST SP 800-53, (incorporated by reference, see § 2002.2), and paragraph (g) of Section 2002.14
- All Contractors must safeguard CUI using one of the following types of standards:
  - CUI Basic is the default set of standards authorized holders must apply to all CUI.

  - CUI Specified must be safeguarded in accordance with the requirements indicated in the NARA CUI Registry for the designated CUI Category.

- Safeguarding Information systems that process, store, or transmit CUI Basic, in accordance with FIPS PUB 199 (incorporated by reference, see § 2002.2), is categorized at no less than the moderate confidentiality impact level.

- Contractors must also apply the appropriate security requirements and controls from FIPS PUB 200 and NIST SP 800-53 to CUI in accordance with any risk-based tailoring decisions.

Physical Environments

CUI must be stored or handled in controlled environments that prevent or detect unauthorized access. Controlled environment and office spaces should include storing CUI in sealed envelopes, providing electronic locks and cabinets, locked doors, overhead bins and drawers.

Protecting Physical Equipment/Media that contains CUI

All electronic devices, storage media – i.e. video, audio, photographic images must be protected in accordance to the regulations defined in the NARA CUI Registry and mandatory CUI

Training.

Protecting CUI when shipping or mailing.

When sending CUI, authorized holders:

- May use the United States Postal Service or any commercial delivery service when they need to transport or deliver CUI to another entity;

- Should use in-transit automated tracking and accountability tools when they send CUI;

- May use interoffice or interagency mail systems to transport CUI; and

- Must mark packages that contain CUI according to marking requirements contained in this part and in guidance published by the CUI EA. See § 2002.20 for more guidance on marking requirements.

Reproducing CUI

When reproducing CUI documents on equipment such as printers, copiers, scanners, or fax machines, ensure that the equipment does not retain data or the agency must otherwise sanitize it in accordance with NIST SP 800-53 (incorporated by reference, see § 2002.2).

Transporting

The Contractor shall not remove material from Government facilities or systems, or facilities or systems operated or maintained on the Government's behalf, without the express written permission of the Head of the Contracting Activity. When traveling, contractors should ideally store material and equipment containing CUI in a locked vehicle, or in the trunk of a vehicle (weather conditions permitting) and out of plain sight.

Decontrolling

No contractor may decontrol CUI without approval by the CO/COR through the designated owner. Once the approval has been granted, the contractor may remove CUI markings. Decontrolling does not mean that the information can be released to the public.

Destroying and Deleting CUI

When destroying and deleting CUI, including in electronic form, contractors must do so in a manner that makes it unreadable, indecipherable, and irrecoverable. Contractor must comply with the process - Return of data section documented in this SOW.

Marking

All CUI documents must be protected according to LRGWP as defined in 32 CFR 2002, Part 2, ED Directive and NIST 800-171B (when published). The Contractor will adhere to the procedures for marking CUI as outlined in the NARA CUI Registry. Authorized holders of CUI will be held accountable for knowing and following the marking procedures as defined in the NARA CUI Registry.

Training

The Contractor shall ensure that initial mandatory Handling Sensitive Information training is completed before handling sensitive and CUI. The contractor will complete Functional CUI Training when appropriate and complete annual thereafter. The Contractor shall not allow any employee access to a system of records, or permit any employee to create, collect, use, process, store, maintain, disseminate, disclose, dispose or otherwise handle CUI, or to design, develop, maintain, or operate a system of records unless the employee has completed training, as required by this clause. The Contractor shall maintain and, upon request, provide documentation of completion of privacy training to the Contracting Officer.

Retention of Authorizing Documentation

The Contractor must maintain a current and complete file of all documentation authorizing handling of CUI during the period of performance of the contract, unless otherwise instructed by the Contracting Officer. Documentation will be made accessible during inspections or upon written request by the CO or the COR.

Transmitting

Upon completion of the contract, all CUI information, data, documentary material, records and/or equipment shall be returned to Department control or the Contractor must hold it until otherwise directed.

Self-Inspection

Contractors will be required to perform an annual self-inspection to demonstrate compliance to the CUI program. Self-Inspection Program Requirements include:

- Evaluate adherence to the principles and requirements of the ED Directive (#)
- Safeguarding

- Security Violations
- Education and Training

Compliance with Information Protection Requirements

The Chief Information Officer (CIO) or the Office of Inspector General (OIG), through the CO or COR, reserves the right to verify compliance with information security requirements established by this contract. Verification may include, but is not limited to, onsite or offsite inspections, audits, documentation reviews, process observation, network and IT system scanning. The Contractor will fully comply with all Department-initiated inspections as permissible by law.

Information Security Incidents (ISI)

Contractors must immediately report any and all suspected security incidents, breaches, and events involving Department information to the Department's Computer Incident Response Center (EDCIRC) and the Department's Security Operations Center (EDSOC); EDCIRC@ED.GOV; EDSOC voice: 202-243-6550. The EDSOC is available 24 hours per day, 365 days per year. Contractors must report any and all ISI involving information technology (IT) systems and CUI immediately upon becoming aware of the ISI but no later than 60 minutes after becoming aware of the ISI, regardless of day or time; regardless of internal investigation, evaluation, or confirmation of procedures or activities; and regardless of whether the ISI is suspected, known, or determined to involve IT systems operated in support of this contract.

Misuse of CUI / Incident Response and Access to Contractor Information Technology (IT) Systems

During the period of performance of the contract and throughout any contract close-out period, the Contractor must provide the Department, or its designate, with immediate access to all IT systems used by the Contractor to support the performance of the contract for the purpose of inspection and forensic analysis in the event of an ISI. The Contractor shall immediately notify the appropriate CO upon discovery of any inadvertent or unauthorized disclosures of information, data, documentary materials, records or equipment that is CUI. Disclosure of CUI is limited to authorized personnel with a lawful need-to-know.

IT Accessibility Requirements

Section 508 of the Rehabilitation Act, as amended by the Workforce Investment Act of 1998 (P.L. 105-220) requires that when Federal agencies develop, procure, maintain, or use information and communication technology (ICT), it shall be accessible to people with disabilities. Federal employees and members of the public who have disabilities must have access to, and use of, information and data that is comparable to people without disabilities. Products, platforms and services delivered as part of this work statement that are ICT, or contain ICT, must conform to the Revised 508 Standards, which are located at 36 C.F.R. § 1194.1 & Apps. A, C & D, and available at https://www.access-board.gov/guidelines-and-standards/communications-and-it/about-the-ict-refresh/final-rule/text-of-the-standards-and-guidelines.

Applicable Functional Performance Criteria: All functional performance criteria apply when using an alternative design or technology that achieves substantially equivalent or greater accessibility and usability by individuals with disabilities, than would be provided by conformance to one or more of the requirements in Chapters 4-6 of the Revised 508 Standards, or when Chapters 4-6 do not address one or more functions of ICT.

Applicable requirements for software features and components: All WCAG Level AA Success Criteria, 502 Interoperability with Assistive Technology, 503 Application Applicable requirements for hardware features and components: All requirements apply Applicable support services and documentation: All requirements apply.

Instructions: 1. Provide an Accessibility Conformance Report (ACR) for each commercially available Information and Communication Technology (ICT) item offered through this contract. Create the ACR using the Voluntary Product Accessibility Template Version 2.1 or later, located at https://www.itic.org/policy/accessibility/vpat. Complete each ACR in accordance with the instructions provided in the VPAT template. Each ACR must address the applicable Section 508 requirements referenced in the Work Statement. Each ACR shall state exactly how the ICT meets the applicable standards in the remarks/explanations column, or through additional narrative. All "Not Applicable" (N/A) responses must be explained in the remarks/explanations column or through additional narrative. Address each standard individually and with specificity, and clarify whether conformance is achieved throughout the entire ICT Item (for example - user functionality, administrator functionality, and reporting), or only in limited areas of the ICT Item. Provide a description of the evaluation methods used to support Section 508 conformance claims. The agency reserves the right, prior to making an award decision, to perform testing on some or all of the Offeror's proposed ICT items to validate Section 508 conformance claims made in the ACR. 2. Describe your approach to incorporating universal design principles to ensure ICT products or services are designed to support disabled users. 3. Describe plans for features that do not fully conform to the Section 508 Standards. 4. Describe "typical" user scenarios and tasks, including individuals with disabilities, to ensure fair and accurate accessibility testing of the ICT product or service being offered. Instructions: Insert the following language into the Acceptance Criteria section of the solicitation.

Acceptance Criteria: Prior to acceptance, the government reserves the right to perform testing on required ICT items to validate the offeror's Section 508 conformance claims. If the government determines that Section 508 conformance claims provided by the offeror represent a higher level of conformance than what is actually provided to the agency, the government shall, at its option, require the offeror to remediate the item to align with the offeror's original Section 508 conformance claims prior to acceptance.

ICT Accessibility Requirements Statement per the Revised Section 508 of the Rehabilitation Act Data Services or Information Retrieval Systems Electronic Content

Technical Criteria: E205.1 General -

- Electronic content shall comply with E205.
- E205.2 Public Facing -
- Electronic content that is public facing shall conform to the accessibility requirements specified in E205.4.
- 602 Support Documentation -

- 603 Support Services -
- 302 Functional Performance Criteria -
- Software

Technical Criteria: E207.1 General -

- Where components of ICT are software and transmit information or have a user interface, such components shall conform to E207 and the requirements in Chapter 5
- E207.2 WCAG Conformance -
- User interface components, as well as the content of platforms and applications, shall conform to Level A and Level AA Success Criteria and Conformance Requirements in WCAG 2.0 (incorporated by reference, see 702.10.1).

E207.2.1 Word Substitution -

- When Applying WCAG to Non-Web Software For non-Web software, wherever the term "Web
- page" or "page" appears in WCAG 2.0 Level A and AA Success Criteria and Conformance Requirements, the term "software" shall be substituted for the terms "Web page" and "page". In addition, in Success Criterion in 1.4.2, the phrase "in software" shall be substituted for the phrase "on a Web page."

E207.3 Complete Process for Non-Web Software: Where non-Web software requires multiple steps to accomplish an activity, all software related to the activity to be accomplished shall conform to WCAG 2.0 as specified in E207.2.

Exceptions: E501.1 Scope: Where Web applications do not have access to platform accessibility services and do not include components that have access to platform accessibility services, they shall not be required to conform to 502 or 503 provided that they conform to Level A and Level AA Success Criteria and Conformance Requirements in WCAG 2.0 (incorporated by reference, see 702.10.1).

Functional Performance Criteria:

- 301.1 Scope - The requirements of Chapter 3 shall apply to ICT where required by 508 Chapter 2 (Scoping Requirements), 255 Chapter 2 (Scoping Requirements), and where otherwise referenced in any other chapter of the Revised 508 Standards or Revised 255 Guidelines.
- 302.1 Without Vision - Where a visual mode of operation is provided, ICT shall provide at least one mode of operation that does not require user vision.
- 302.2 With Limited Vision - Where a visual mode of operation is provided, ICT shall provide at least one mode of operation that enables users to make use of limited vision.
- 302.3 Without Perception of Color - Where a visual mode of operation is provided, ICT shall provide at least one visual mode of operation that does not require user perception of color.

- 302.4 Without Hearing - Where an audible mode of operation is provided, ICT shall provide at least one mode of operation that does not require user hearing.
- 302.5 With Limited Hearing - Where an audible mode of operation is provided, ICT shall provide at least one mode of operation that enables users to make use of limited hearing.
- 302.6 Without Speech - Where speech is used for input, control, or operation, ICT shall provide at least one mode of operation that does not require user speech.
- 302.7 With Limited Manipulation - Where a manual mode of operation is provided, ICT shall provide at least one mode of operation that does not require fine motor control or simultaneous manual operations.
- 302.8 With Limited Reach and Strength - Where a manual mode of operation is provided, ICT shall provide at least one mode of operation that is operable with limited reach and limited strength.
- 302.9 With Limited Language, Cognitive, and Learning Abilities - ICT shall provide features making its use by individuals with limited cognitive, language, and learning abilities simpler and easier. END

Records Management Obligations

A. Applicability

This clause applies to all Contractors whose employees create, work with, or otherwise handle Federal records, as defined in Section B, regardless of the medium in which the record exists.

B. Definitions

"Federal record" as defined in 44 U.S.C. § 3301, includes all recorded information, regardless of form or characteristics, made or received by a Federal agency under Federal law or in connection with the transaction of public business and preserved or appropriate for preservation by that agency or its legitimate successor as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of the United States Government or because of the informational value of data in them.

The term Federal record: includes Department of Education (DoED) records. does not include personal materials. applies to records created, received, or maintained by Contractors pursuant to their DoED contract. may include deliverables and documentation associated with deliverables.

C. Requirements

Contractor shall comply with all applicable records management laws and regulations, as well as National Archives and Records Administration (NARA) records policies, including but not limited to the Federal Records Act (44 U.S.C. chs. 21, 29, 31, 33), NARA regulations at 36 CFR Chapter XII Subchapter B, and those policies associated with the safeguarding of records covered by the Privacy Act of 1974 (5 U.S.C. 552a). These policies include the preservation of all records, regardless of form or characteristics, mode of transmission, or state of completion.

In accordance with 36 CFR 1222.32, all data created for Government use and delivered to, or falling under the legal control of, the Government are Federal records subject to the provisions of 44 U.S.C. chapters 21, 29, 31, and 33, the Freedom of Information Act (FOIA) (5 U.S.C. 552), as amended, and the Privacy Act of 1974 (5 U.S.C. 552a), as amended and must be managed and scheduled for disposition only as permitted by statute or regulation.

In accordance with 36 CFR 1222.32, Contractor shall maintain all records created for Government use or created in the course of performing the contract and/or delivered to, or under the legal control of the Government and must be managed in accordance with Federal law. Electronic records and associated metadata must be accompanied by sufficient technical documentation to permit understanding and use of the records and data, which should address at minimum the following according to 36 CFR 1236.10:

The following types of records management controls are needed to ensure that Federal records in electronic information systems can provide adequate and proper documentation of agency business for as long as the information is needed. Agencies must incorporate controls into the electronic information system or integrate them into a recordkeeping system that is external to the information system itself (see § 1236.20 of this part).

(a) Reliability: Controls to ensure a full and accurate representation of the transactions, activities or facts to which they attest and can be depended upon in the course of subsequent transactions or activities.

(b) Authenticity: Controls to protect against unauthorized addition, deletion, alteration, use, and concealment.

(c) Integrity: Controls, such as audit trails, to ensure records are complete and unaltered.

(d) Usability: Mechanisms to ensure records can be located, retrieved, presented, and interpreted.

(e) Content: Mechanisms to preserve the information contained within the record itself that was produced by the creator of the record;

(f) Context: Mechanisms to implement cross-references to related records that show the organizational, functional, and operational circumstances about the record, which will vary depending upon the business, legal, and regulatory requirements of the business activity; and

(g) Structure: controls to ensure the maintenance of the physical and logical format of the records and the relationships between the data elements.

DoED and its contractors are responsible for preventing the alienation or unauthorized destruction of records, including all forms of mutilation. Records may not be removed from the legal custody of DoED or destroyed except for in accordance with the provisions of the agency records schedules and with the written concurrence of the Head of the Contracting Activity. Willful and unlawful destruction, damage or alienation of Federal records is subject to the fines and penalties imposed by 18 U.S.C. 2701. In the event of any unlawful or accidental removal, defacing, alteration, or destruction of records, Contractor must report to DoED. The agency must report promptly to NARA in accordance with 36 CFR 1230.

The Contractor shall immediately notify the appropriate Contracting Officer upon discovery of any inadvertent or unauthorized disclosures of information, data, documentary materials, records or equipment. Disclosure of non-public information is limited to authorized personnel with a need-to-know as described in the Statement of Work (SOW). The Contractor shall ensure that the appropriate personnel, administrative, technical, and physical safeguards are established to ensure the security and confidentiality of this information, data, documentary material, records and/or equipment is properly protected. The Contractor shall not remove material from Government facilities or systems, or facilities or systems operated or maintained on the Government's behalf, without the express written permission of the Head of the Contracting Activity. When information, data, documentary material, records and/or equipment is no longer required, it shall be returned to DoED control or the Contractor must hold it until otherwise directed. Items returned to the Government shall be hand-carried, mailed, emailed, or securely electronically transmitted to the Contracting Officer or address prescribed in the SOW. Destruction of records is EXPRESSLY PROHIBITED unless in accordance with Paragraph (4).

The Contractor is required to obtain the Contracting Officer's approval prior to engaging in any contractual relationship (sub-contractor) in support of this contract requiring the disclosure of information, documentary material and/or records generated under, or relating to, contracts. The Contractor (and any sub-contractor) is required to abide by Government and DoED guidance for protecting sensitive, proprietary information, classified, and controlled unclassified information.

The Contractor shall only use Government IT equipment for purposes specifically tied to or authorized by the contract and in accordance with DoED policy.

The Contractor shall not create or maintain any records containing any non-public DoED information that are not specifically tied to or authorized by the contract.

The Contractor shall not retain, use, sell, or disseminate copies of any deliverable that contains information covered by the Privacy Act of 1974 or that which is generally protected from public disclosure by an exemption to the Freedom of Information Act.

The DoED owns the rights to all data and records produced as part of this contract. All deliverables under the contract are the property of the U.S. Government for which DoED shall have unlimited rights to use, dispose of, or disclose such data contained therein as it determines to be in the public interest. Any Contractor rights in the data or deliverables must be identified as required by FAR 52.227-11 through FAR 52.227-20.

Training. All Contractor employees assigned to this contract who create, work with or otherwise handle records are required to take DoED-provided records management training. The Contractor is responsible for confirming training has been completed according to agency policies, including initial training and any annual or refresher training.

[Note: To the extent an agency requires contractors to complete records management training, the agency must provide the training to the contractor.]

D. Flowdown of requirements to subcontractors

The Contractor shall incorporate the substance of this clause, its terms, and requirements including this paragraph, in all subcontracts under this SOW, and require written subcontractor acknowledgment of same.

Violation by a subcontractor of any provision set forth in this clause will be attributed to the Contractor.