Department Information Security and Privacy Requirements

May 4th, 2023

U.S. Department of Education (ED)
Office of the Chief Information Officer (OCIO)
Information Assurance Services (IAS)

Revision History

The table below identifies all changes that have been incorporated into this document.

Table 1: Revision History

Version	Date	Summary of Changes
1.0	11/18/2019	Initial draft
2.0	09/29/2020	Added Sections 2.33 through 2.39 and updated Federal & ED cybersecurity requirements.
2.1	09/23/2021	Updated Section 2.39, and IPv6 section (2.5); added Sections 2.41 and 2.42. Note: The Revision History short description content box for V. 2.1 erroneously stated that paragraphs 2.40 and 2.41 were inserted. However, v. 2.1 actually inserted paragraphs 2.41 and 2.42, while paragraph 2.40 was omitted due to administrative error. Paragraph 2.40 will remain as "Reserved." V. 2.3 corrects the short description content box for V. 2.1 to reflect the actual update that occurred (i.e., paragraph 2.40 was not inserted).
2.2	02/24/2022	Removed references to legacy standards from section 2.8 and added "Phishing resistant" to 2.18 item k.
2.3	05/04/2023	Retitled the document. Updated acronyms and formatting throughout. Updated Sections 1.2a-b, 2.1c, 2.2c, 2.3, 2.8a-b, 2.8e-f, 2.10b, 2.10d, 2.12a, 2.12 j, 2.12y, 2.15, 2.16b, 2.18a, 2.18c, 2.18e, 2.18 h-i, 2.18k, 2.18s-t, 2.18w-x, 2.18bb, 2.18gg, 2.18ii, 2.18oo, 2.18ss, 2.18uu(Reserved), 2.18vv, 2.18zz(ii), 2.18zz(v), 2.21a, 2.21g, 2.21j(i), 2.21j(v-vi), 2.24a-b, 2.24e(iii-viii), 2.25a(ii), 2.27e, 2.29a, 2.32e, 2.34, 2.35, 2.36, 2.39, and 2.42, 2.42a-c, 2.42f, 2.43, and 2.44.

Contents

1 INTRODUCTION

1.1 Purpose

This document establishes the security and privacy requirements for all Department of Education (ED) information technology (IT) procurements. In doing so, it supersedes any prior documentation establishing such requirements.

1.2 Applicability

The requirements established in this document apply to all Department of Education contractors. The requirements established herein apply to the entire contract or order (hereafter referred to as a "contract"), or any portion thereof and includes either or both of the following:

a. **Access (Physical or Logical) to Government Information**: Physical and Logical Access refers to when contractor personnel are expected to have (1) routine physical access to an ED-controlled facility; (2) logical access to an ED-controlled information system; (3) access to government information, whether in an ED-controlled information system or in hard copy; or (4) any combination of circumstances (1) through (3) as per Office of Management and Budget (OMB) M-05-24, Implementation of Homeland Security Presidential Directive (HSPD) 12 – Policy for a Common Identification Standard for Federal Employees and Contractors.

   If a PIV card is required, per "Contractor Vetting Security Requirements," the Contractor personnel (including remote personnel) shall be responsible for obtaining and maintaining required Department credentials, to include PIV cards, Unless a PIV exception is authorized by Enterprise Technology Services (ETS).

b. **Use or Operation of Information Technology Supporting the ED Mission**: A Contractor/employee will use or operate a federal system and information technology containing information that supports the ED mission. In addition to the Federal Acquisition Regulation (FAR) Subpart 2.1 definition of "information technology" (IT), the term as used in this section includes computers, ancillary equipment (including imaging peripherals, input, output, and storage devices necessary for security and surveillance), peripheral equipment designed to be controlled by the central processing unit of a computer, software, firmware and similar procedures, services (including support services), and related resources.

2 REQUIREMENTS

2.1 Safeguarding Information and Information Systems

In accordance with the Federal Information Processing Standards Publication (FIPS) 199, *Standards for Security Categorization of Federal Information and Information Systems*, the Contractor shall:

a. Protect Government information and information systems to ensure:

   i. Confidentiality, which means preserving authorized restrictions on access and disclosure, based on the security terms found in this contract, including means for protecting personal privacy and proprietary information.

   ii. Integrity, which means guarding against improper information modification or destruction, and ensuring information non-repudiation and authenticity.

   iii. Availability, which means ensuring timely and reliable access to and use of information.

b. Provide security for any Contractor systems, and information contained therein, connected to an ED network or operated by the Contractor on behalf of ED regardless of location. In addition, if new or unanticipated threats or hazards are discovered by either the agency or Contractor, or if existing safeguards have ceased to function, the discoverer shall immediately, **within sixty (60) minutes or less**, bring the situation to the attention of the other party.

c. Adopt and implement policies, procedures, controls, and standards required by the ED Information Security Program to ensure the confidentiality, integrity, and availability of government information and government information systems for which the Contractor is responsible under this contract or to which the Contractor may otherwise have access under this contract. Obtain the ED Information Security Program security requirements, outlined in the Departmental / Cybersecurity Policy (ACSD-OCIO-004/OCIO 3-112), and its subordinate Cybersecurity Standards documents.

d. Comply with the Privacy Act requirements and with the Federal Information Security Modernization Act (FISMA) and with the OMB Memorandum M-17-12, *Preparing for and Responding to a Breach of Personally Identifiable Information*, and with the Family Educational Rights and Privacy Act (FERPA).

   Per OMB Circular A-130, Personally Identifiable Information (PII) is “information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual.” Examples of PII include, but are not limited to the following: social security number, date and place of birth, mother’s maiden name, biometric records, etc.

Sensitive PII is PII that if released improperly could result in harm, embarrassment, inconvenience, or unfairness to the individual whose name or identity is linked to the information.

Context shall be accounted for to determine whether PII is sensitive. Some PII is always sensitive, and some is only sensitive when it is used in a particular context. For example, a list of people subscribing to a government newsletter is generally not sensitive PII; a list of people receiving treatment for substance abuse would always be considered sensitive PII.

The list below is not exhaustive. Context shall be accounted for in order to determine whether PII is sensitive. The following types of information are always considered sensitive:

- Social Security Numbers (including using just the last 4 digits of the SSN)
- Date of birth
- Mother's maiden name
- Biometric identifiers (e.g., fingerprint, iris scan, voice print)
- Personal financial information, credit card and purchase card account numbers
- Citizenship and immigration status
- Criminal history
- Computer access passwords and security questions
- Medical records

2.2 Safeguarding Controlled Unclassified Information (CUI)

CUI is defined as "information that laws, regulations, or Government-wide policies require to have safeguarding or dissemination controls, excluding classified information." The Contractor shall comply with Executive Order 13556*, Controlled Unclassified Information, (implemented at 32 CFR,* part 2002*)* and Department Directive, OCIO: 3-113, *Controlled Unclassified Information Program* when handling CUI. 32 CFR 2002.4(aa) as implemented the term "*handling"* refers to "…any use of CUI, including but not limited to marking, safeguarding, transporting, disseminating, re- using, and disposing of the information." 81 Fed. Reg. 63323. All sensitive information that has been identified as CUI by a regulation or statute, handled by this solicitation/contract, shall be:

a. Marked appropriately
b. Disclosed to authorized personnel on a "Need-To-Know" basis
c. Protected in accordance with the Departmental / Cybersecurity Policy (ACSD-OCIO-004/OCIO 3-112) and its subordinate Cybersecurity Standards documents, the finalized version of NIST Special Publication (SP) 800-53, *Security and Privacy Controls for Federal Information*

Systems and Organizations applicable baseline, if handled by a Contractor system operated on behalf of the agency, or NIST SP 800-171, *Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations* if handled by internal Contractor system

d. Returned to ED control, destroyed when no longer needed, or held until otherwise directed. Destruction of information and/or data shall be accomplished in accordance with NIST SP 800-88, *Guidelines for Media Sanitization*

2.3 Safeguarding Sensitive Information

For security purposes, information is or may be sensitive because it requires security to protect its confidentiality, integrity, and/or availability. The Contractor shall protect all government information that is or may be sensitive in accordance with FISMA by securing it with a FIPS 140-2 or FIPS 140-3 validated solution.

2.4 Confidentiality, Integrity, Availability, and Nondisclosure of Information

Any information provided to the Contractor by ED or collected by the Contractor on behalf of ED shall be used only for the purpose of carrying out the provisions of this contract and shall not be disclosed or made known in any manner to any persons except as may be necessary in the performance of the contract.

The Contractor assumes responsibility for protection of the confidentiality, integrity, and availability of Government records and shall ensure that all work performed by its employees and subcontractors shall be under the supervision of the Contractor. Each Contractor employee or any of its subcontractors at any level to whom any ED records may be made available or disclosed shall be notified in writing by the Contractor that information disclosed to such employee or subcontractor can be used only for that purpose and to the extent authorized herein.

The confidentiality, integrity, and availability of such information shall be protected in accordance with ED policies and instructions. Unauthorized disclosure of information will be subject to the ED sanction policies and/or governed by the following laws and regulations:

- 18 U.S.C. 641 (Criminal Code: Public Money, Property or Records)
- 18 U.S.C. 1905 (Criminal Code: Disclosure of Confidential Information)
- 44 U.S.C. Chapter 35, Subchapter I (Paperwork Reduction Act)
- 18 U.S.C. 1030 The Computer Fraud and Abuse Act (CFAA)
- 44 U.S.C. 3301 Definition of Records.

2.5 Internet Protocol Version 6 (IPv6)

Any system hardware, software, firmware, or networked component (voice, video, or data) developed, procured, or acquired in support or performance of this contract shall be capable of transmitting, receiving, processing, forwarding, and storing digital information across system boundaries utilizing system packets that are formatted in accordance with commercial standards of Internet protocol (IP) version 6 (IPv6) as set forth in Internet Engineering Task Force (IETF) Request for Comments (RFC) 2460 and associated IPv6-related IETF RFC standards.

In addition, this system shall maintain interoperability with IPv4 systems and provide at least the same level of performance and reliability capabilities of IPv4 products. Specifically, any new IP product or system developed, acquired, or produced must:

1. Interoperate with both IPv6 and IPv4 systems and products
2. Have available Contractor/vendor IPv6 technical support for development and implementation and fielded product management

2.6 Government Websites

All new and existing government websites shall be securely configured with Hypertext Transfer Protocol Secure (HTTPS) using the most recent version of Transport Layer Security (TLS). In addition, HTTPS shall enable HTTP Strict Transport Security (HSTS) to instruct compliant browsers to assume HTTPS at all times to reduce the number of insecure redirects and protect against attacks that attempt to downgrade connections to plain HTTP.

2.7 Public-Facing Websites

The Contractor shall implement controls to ensure that all publicly accessible Department websites and web services only provide service through a secure connection, (such as the HTTPS).

In accordance with Department of Homeland Security (DHS), Cybersecurity and Infrastructure Agency (CISA) Binding Operational Directive (BOD) 18-01: *Enhance E-Mail and Web Security*, any web services provided for or on behalf of ED shall 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 shall provide a list to ED to provide to DHS of agency second-level domains that can be HSTS preloaded, for which HTTPS will be enforced for all sub-domains.

If an official public-facing website will be developed, modified, or maintained, then, in accordance with OMB Memorandum M-08-23, *Securing the Federal Government's Domain Name System Infrastructure* and OMB Memorandum M-17-06, *Policies and Requirements for Public Websites*, the Contractor shall use only an approved ed.gov domain.

In accordance with OMB-M-17-06, 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 current, final version of NIST SP 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 use of third-party websites and applications shall 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*.

2.8 Encryption

The Contractor shall:

a. Comply with Executive Order (EO) 14028, *Improving the Nation's Cybersecurity* (May 12, 2021), Section 3(d)(iii) requirements for encrypting data at rest and data in transit, OMB M-22-09, *Zero Trust Strategy*, and ED Information Technology (IT) System and Communications Protection (SC) Standard to prevent unauthorized access to government information.

b. Encrypt all Federal data and information in motion (i.e., email, network connections, etc.) and at rest (i.e., servers, storage devices, mobile devices, backup media, etc.) with FIPS 140-2 or FIPS 140-3 validated encryption solution.

c. Secure all devices (i.e.: desktops, laptops, mobile devices, etc.) that store and process federally owned or federally managed information and ensure devices meet ED and IAS-specific encryption standard requirements.

d. Maintain a complete and current inventory of all laptop computers, desktop computers, and other mobile devices and portable media that store or process sensitive government information (including PII).

e. Verify that the encryption solutions in use have been validated under the Cryptographic Module Validation Program to confirm compliance with FIPS 140-2 or FIPS 140-3. The Contractor shall provide a written copy of the validation documentation to the COR when required by the Program Office.

f. Use the Key Management system on the ED personal identification verification (PIV) card or establish and use a key recovery mechanism to ensure the ability for authorized personnel to encrypt/decrypt information and recover encryption keys. Encryption keys shall be provided to the COR, or to IAS, or to the ED Security

Operations Center (EDSOC), or to the Project Manager or Program Manager, upon request and at the conclusion of the contract.

2.9 Privacy Threshold Analysis (PTA)/Privacy Impact Assessment (PIA)

The Contractor shall assist the ED Senior Agency Official for Privacy (SAOP) or designee with conducting a PTA for the information system and/or information handled under this contract to determine whether a full PIA needs to be completed.

If the results of the PTA show that a full PIA is needed, the Contractor shall assist the ED SAOP or designee with completing a PIA for the system or information within the timeframe required by the Program Office after completion of the PTA and in accordance with ED policy and OMB M-03-22, *Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*.

The Contractor shall assist the SAOP or designee in reviewing the PIA at least annually throughout the system development lifecycle (SDLC)/information lifecycle, or when determined by the agency that a review is required based on a major change to the system, or when new types of PII are collected that introduces new or increased privacy risks, whichever comes first.

2.10 Training

a. **Mandatory Training for All Contractor Staff -** All contractor/employees assigned to work on this contract shall complete the applicable ED Cybersecurity and Privacy Awareness training (provided upon contract award) before performing any work under this contract (this training is available to new contractors, even if they do not have a PIV card). Thereafter, the employees shall complete the ED Cybersecurity and Privacy Awareness training at least *annually*, during the life of this contract. All provided training shall be compliant with ED training policies.

b. **Role-based Training (RBT) –** The Contractor shall identify and document all employees and contractors in positions with significant security responsibilities (SSR), map their job function to the designated work role and specialty area in accordance with the current version of NIST SP 800-181, *Workforce Framework for Cybersecurity (NICE Framework)*, apply the corresponding Office of Personnel Management (OPM) Cybersecurity Work Role Code, and communicate the resulting mapping monthly to the COR to support RBT and FISMA reporting. Note: Individuals are considered to have SSR if their work roles or positions could, upon execution, have the potential to adversely impact the security posture of one or more ED systems and/or the Department. Elevated privileges are roles or permissions that provide a higher level of access than a standard user; also referred to as privileged users. Examples of positions with elevated privileges include system administrators, application administrators, user administrators, etc.

   All contractors with SSR must complete role-based training annually in accordance with ED policy, regardless of the work roles or position assigned.

c. **Training Records -** The Contractor shall maintain training records for all its employees working under this contract in accordance with ED policy. A copy of the training records shall be provided to the CO and/or COR within thirty (30) days after contract award and annually thereafter, or upon request.

d. To enhance its training program and satisfy NIST security controls for awareness training, the Department conducts practical exercises simulating actual cyber-attacks, including phishing. These exercises simulate actual cyber attacks and phishing. The contractor's employees will be required to pass practical exercises periodically conducted by the Department. Failing an exercise may result in the contractor's employees being required to take and pass the Department's phishing awareness training course two weeks after training is assigned, or risk losing network access until completed. Repeated failure to successfully complete exercises may result in revocation of network access for the remainder of the fiscal year.

2.11 Rules of Behavior

a. The Contractor shall ensure that all employees performing on the contract comply with the applicable ED Rules of Behavior and any specific rules provided by the Program Office.

b. All contractor employees performing on the contract shall read and adhere to the Rules of Behavior before accessing Department data or other information, systems, and/or networks that store/process government information, initially at the beginning of the contract and at least annually thereafter, which may be done as part of annual ED Cybersecurity and Privacy Awareness training.

c. Employees, contractors, and anyone assigned to a contract shall sign Rules of Behavior (RoB). Signed copies of RoB shall be kept on file by the Contractor's program manager.

2.12 Incident Response

- The Contractor shall respond to all alerts/Indicators of Compromise (IOCs) provided by either the EDSOC, the Information System Security Manager (ISSM), the Mission/Business Owner (MBO), the Information System Owner (ISO), the Information System Security Officer (ISSO), the Project Manager, the Program Manager, the CO, the COR, the SAOP (or designee), or the CISO (or designee) **within 24 hours**, whether the response is positive or negative.
- FISMA defines an incident as "an occurrence that (1) actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or (2) constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies."

- A privacy breach is a type of incident and is defined by FISMA as the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where (1) a person other than an authorized user accesses or potentially accesses personally identifiable information or (2) an authorized user accesses or potentially accesses personally identifiable information for any other-than-authorized purpose.

In the event of a suspected or confirmed incident or breach, the Contractor shall:

a. Protect all sensitive information, including any PII created, stored, or transmitted in the performance of this contract to avoid a secondary sensitive information incident with FIPS 140-2 or FIPS 140-3 validated encryption.

b. NOT notify affected individuals unless so instructed by the contracting officer or designated representative. If instructed by the contracting officer or representative, the Contractor shall send ED and Program Office approved notifications to affected individuals within the timeframe established by the Program Office.

c. Report all suspected and confirmed information security and privacy incidents and breaches to the EDSOC, at EDSOC@ed.gov, and to the COR, including incidents involving PII, in any medium or form, including paper, oral, or electronic, as soon as possible and without unreasonable delay, within no more than sixty (60) minutes, and consistent with the applicable ED policy and procedures, NIST standards and guidelines, as well as with United States Computer Emergency Readiness Team (US-CERT) notification guidelines. The types of information required in an incident report shall include at a minimum: company and point of contact information, contract information, impact classifications/threat vector, and the type of information compromised.

d. Cooperate and exchange any information, as determined by the agency, necessary to effectively manage or mitigate a suspected or confirmed breach.

e. NOT include any sensitive information in the subject or body of any reporting e-mail.

f. Encrypt sensitive information in attachments to email, media, etc.

g. Comply with OMB M-17-12, *Preparing for and Responding to a Breach of Personally Identifiable Information*, and with the ED incident response policies when handling PII breaches.

h. Provide full access and cooperate on all activities as determined by the United States Government, including ED, any involved law enforcement or Department of Defense (DoD) agencies, such as DHS CISA, the Federal

Bureau of Investigation (FBI), the Central Intelligence Agency (CIA), the National Security Agency (NSA), the Defense Information Systems Agency (DISA), or the Office of Personnel Management (OPM) etc., to ensure an effective incident response, including providing all requested images, log files, and event information to facilitate rapid resolution of sensitive information incidents. This may involve disconnecting the system processing, storing, or transmitting the sensitive information from the Internet or other networks or applying additional security controls. This may also involve physical access to contractor facilities during a breach/incident investigation.

i. Implement scanning capabilities that assess for vulnerabilities using only Security Content Automation Protocol (SCAP) validated products.

j. Perform penetration ("Moderate" and "High" impact and HVA systems) and regular vulnerability testing and scanning of systems, IT devices, and websites. Scanning shall be conducted with reports provided to the Department. The Contractor shall ensure authenticated Web Application and Data Base Application scans are conducted monthly (or as needed to be more frequent). In addition, authenticated Operating System (OS) scans are conducted at a minimum on a weekly basis. Once the Information System is integrated with the Continuous Diagnostics and Mitigation (CDM) program, vulnerability information for all IT assets within the scope of the awarded contract shall be updated at minimum every 72 hours.

k. Maintain the tools and capabilities to support asset discovery, to include passive network monitoring, active network monitoring, and automated network mapping.

l. 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.

m. Maintain tools and capabilities for intrusion prevention, to include host intrusion prevention systems (HIPS) and network intrusion prevention systems (NIPS).

n. Maintain a firewall system designed to prevent unauthorized access to or from any contractor systems and network.

o. 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.

p. 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.

q. 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 IOCs in a rapid fashion; and encrypted traffic inspection.

r. If working as a SOC contractor, provide a Daily Morning Report, seven (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.

s. Provide and maintain automated means of discovering, monitoring, and protecting sensitive data to ensure protection of data in motion, at rest, and in use.

t. 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.

u. Provide and maintain externally facing web application firewall capabilities providing inbound and outbound traffic filtering.

v. Provide and maintain an Out of Band network device management solution.

w. Administer, operate, maintain, configure, and tune cybersecurity software and hardware.

x. Provide full government visibility of continuous monitoring tool configurations and output on a real-time basis as well as historical data/logs.

y. Maintain the capability to perform periodic penetration testing, and 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. The Department's Security Assessment and Authorization (CA) Standard, requires penetration testing of High Value Assets and systems with a “High” or “Moderate” FIPS 199 impact rating.

2.13 Contract Initiation and Expiration

The Contractor shall comply with the following contract initiation and expiration requirements:

a. **System Documentation**. Contractors shall follow and adhere to current, final version of NIST SP 800-37, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy* at a minimum, for system development and provide system documentation at designated intervals (specifically, at the expiration of the contract) within the SDLC that require artifact review and approval.

b. **Sanitization of Government Files and Information**. As part of contract closeout and at expiration of the contract, the Contractor shall provide all required documentation, as specified by the Program Office**,** to the CO and/or COR to certify that, at the government’s direction, all electronic and paper records are appropriately disposed of and all devices and media are sanitized in accordance with NIST SP 800-88, *Guidelines for Media Sanitization*.

c. **Notification**. The Contractor shall notify the CO and/or COR and system ISSO within five (5) calendar days (or as otherwise specified by the Program Office) when an employee stops working under this contract, or immediately upon an employee’s termination or vacancy if prior-to-departure notice is not possible.

d. **Contractor Responsibilities Upon Physical Completion of the Contract** The Contractor shall return all government information and IT resources (i.e., government information in nongovernment-owned systems, media, and backup systems) acquired during the term of this contract to the CO and/or COR. Additionally, the Contractor shall provide a certification that all government information has been properly sanitized and purged from contractor-owned systems, including backup systems and media used during contract performance, in accordance with ED and Program Office policies.

   Further, the Contractor shall perform and document the actions identified in the Department’s Contractor Employee Separation Checklist when an employee terminates work under this contract within five (5) calendar days (or as otherwise specified by the Program Office) of the employee’s exit from the contract. All documentation shall be made available to the CO and/or COR upon request.

2.14 Records Management and Retention

The Contractor shall maintain all information in accordance with Executive Order

13556 -- *Controlled Unclassified Information*, National Archives and Records Administration (NARA) records retention policies and schedules and ED and policies and shall not dispose of any records unless authorized by ED.

In the event that the Contractor accidentally disposes of or destroys a record without proper authorization, it shall be documented and reported as an incident in accordance with ED policies. Per OM: 6103, *Records and Information Management Program,* records include 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. (44 USC 3101, Definition of Records).

2.15 Government-Furnished Equipment (GFE)

When the contractor configures, manages, and maintains GFE on behalf of the Department, the Contractor shall:

a. Enforce the Department approved image and baseline configurations. GFE laptops, smart phones, tablets should include the capability for and support mobile device management.

b. Comply with Office of Management and Budget (OMB) M-23-13 by removing all existing installations of TikTok and preventing any further installation. TikTok is defined as the social networking service TikTok or any successor application or service of TikTok developed or provided by ByteDance Limited or an entity owned by ByteDance Limited.

c. Prohibit internet traffic to the social networking service TikTok.

d. Coordinate with the assigned Contracting Officer Representative to request an exception from the Department CISO when the use of TikTok is required under contract to support law enforcement activities, national security interests and activities, and security research.

2.16 Non-Public Facing Websites

The Contractor shall:

a. 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).

b. In accordance with OMB Memorandums M-22-09, M-17-06, M-15-13, M-08- 23, and M-10-23, DHS BOD 18-01, and with NIST SP 800-52 and NIST SP 800-44, all Federal websites and web services shall be accessible through a secure connection (HTTPS only, with HSTS), and e-mail applications shall have SMTP enabled. The use of HTTPS is encouraged on intranets, but not explicitly required.

c. In accordance with BOD 18-01: In accordance with OMB Memorandum M-08-23, to ensure Domain Name System Security (DNSSEC), all Department websites must use an ed.gov domain. All websites that disseminate and/or do business on the Department's behalf must adhere to this OMB Memorandum.

2.17 E-mail Security

The Contractor shall:

a. Configure all internet-facing mail servers to offer STARTTLS, and all second-level agency domains to have valid SPF/DMARC records. Additionally, the Contractor shall ensure Secure Sockets Layer (SSL) v2 and SSLv3 are disabled on mail servers, and 3DES and RC4 ciphers are disabled on mail servers.
b. Ensure that the requirement is met to set a DMARC policy of "reject" for all second-level domains and mail-sending hosts.
c. Enable SMTP for all e-mail applications, in accordance with OMB Memoranda M-17-06, M-15-13, M-08-23, M-10-23; DHS BOD 18-01; and NIST SP 800-52 and SP 800-44.
d. Abide by Department guidelines concerning auto-forwarding of Department email to non-Department accounts by not configuring Department email accounts to auto-forward to non-ED.gov email addresses as this is explicitly prohibited unless specifically authorized through the Department Risk Acceptance process.

2.18 Departmental IT Security Checkpoints

The Contractor shall:

a. Complete/update the appropriate level of Security Accreditation (SA) documentation per NIST Risk Management Framework guidance and the Department's IT System Planning (PL) Standard, security controls testing, interagency security agreements (ISAs), and risk assessments in support of government issuance of security assessment and authorization to operate (ATO) decisions.

b. 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.

c. Include the capability for network traffic that flows between externally hosted systems and networks, to/from Department systems and networks, to be Trusted Internet Connection (TIC) compliant 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 comply with the requirements of the Trusted Internet Connections (TIC) 3.0 initiative.

d. Architect contractor hosting environments to use security isolation and network segmentation principles 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.

e. 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 IOCs within 24 hours of receipt of the indicators provided by the Department of Education from DHS.

f. 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.

g. 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.

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

i. Implement capabilities and processes to patch all critical vulnerabilities identified to the Department of Education by DHS immediately or in accordance with DHS Emergency Directives and BODs.

j. Ensure robust physical and cybersecurity protections are in place for all 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.

k. Implement remote access solutions that only use either PIV or phishing resistant 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. "Phishing resistant" refers to authentication processes designed to detect and prevent disclosure of authentication secrets and outputs to a website or application masquerading as a legitimate system.

l. Implement remote access solutions that scan for malware before allowing full connections and that time out in accordance with Department Standard and require re-authentication to re-establish a session.

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

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

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

p. 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.

q. 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).

r. 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 to better protect and securely isolate the Department’s HVAs.

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

t. Implement and maintain strong authentication capabilities requiring the technical enforcement of all users being required to use a PIV card to authenticate to the network, (with exceptions for a very limited set of users specifically approved by the Department) or use a federated Identity Provider (IdP) that supports phishing-resistant multi-factor authentication.

u. 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.

v. 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.

w. Implement security configurations on all IT assets and systems using the most updated DISA STIG, with Security Engineering and Architecture

Branch (SEA) authorized deviations as needed.

x. Use the following configuration standards, in the order of precedence shown, when a DISA STIG is not available for a product or system:

- NIST standards and baselines
- Other US Government standards
- Cybersecurity industry best practices, benchmarks, and guidelines (i.e., Center for Internet Security, or CIS)
- Vendor checklists and baselines

y. 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 DHS.

z. 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.

aa. 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.

bb. Provide for the encryption for PII, CUI, Data at Rest, and Data in Transit. Encryption solutions applied shall be FIPS 140-2 or FIPS 140-3 validated.

cc. Document and track contractor personnel cyber training based on roles Develop, maintain, and publish a listing of Contractor-provided security controls, hybrid security controls, contractor common controls, and "customer"-provided security controls, in support of systems security assessments and authorizations, and the issuance of ATO decisions by the Department.

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

ee. 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).

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

gg. Provide and maintain multi-factor authentication solutions utilizing the Personal Identity Verification (PIV) card; derived PIV PKI credentials (NIST AAL2, also phishing resistant); FIDO2/WebAuthN credentials, a federated IdP that supports phishing resistant options (e.g., GSA's Login.gov or commercial options) or an equivalent phishing resistant multifactor authentication solution rated NIST AAL3; and utilize FIPS 140-2 or FIPS 140-3 approved encryption for all remote access requirements.

hh. 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.

ii. 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 and standards as well as supporting POA&M Standard Operating Procedures.

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

kk. 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.

ll. 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.

mm. Document and maintain system security boundaries, system configuration details, and network diagrams, in support of security assessment and ATO processes.

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

oo. Provide support for maintaining system security documentation in support of FISMA reporting requirements and security compliance status in the Department's Governance, Risk and Compliance tool (GRC), currently Cyber Security Assessment and Management (CSAM) system.

pp. 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.

qq. Develop corrective/remediation POA&Ms and strategies to address security audit and assessment findings, and other reports of system security weaknesses or non-compliance.

rr. 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 better protect the Department's HVAs.

ss. Utilize PIV or other approved Level of Assurance 3, as defined in Executive Order 14028, OMB M-22-09, NIST SP 800-63-3 Electronic Authentication Guidelines, and compliant Identity and Access Control mechanisms for network/domain administrative enterprise access.

tt. 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.

uu. Reserved.

vv. Utilize multi-factor authentication, including integration and compliance with HSPD-12 PIV and OMB M-22-09 requirements, for all remote access solutions for the Department's sensitive information systems. Establish a process for ongoing remediation of vulnerabilities that CISA identifies, through inclusion in the CISA-managed catalog of known exploited vulnerabilities (BOD 22-01) and remediate each vulnerability according to the timelines set forth in the CISA-managed vulnerability catalog. These default timelines may be adjusted in the case of grave risk to the Federal Enterprise.

ww. Provide a multi-tier disaster recovery capability that provides the infrastructure and process to meet the recovery requirements of all its HVAs, and applications (Mission-Critical, Decision Support, Other).

xx. Provide IT Disaster Recovery Planning and Management capabilities and support.

yy. Define business risk and risk assessment to Develop disaster recovery strategies to Develop disaster recovery plans to Develop IT system contingency plans to Conduct disaster recovery exercises, training, and awareness.

zz. 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:

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

ii. 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 subcontractors, and commercial systems that are connected to commercial or other systems that need to meet ED requirements supporting Department programs, contracts, and projects); obtaining a full ATO before being granted operational status; performance of annual self-assessments of security controls; annual Contingency Plan, Incident Response Plan, Disaster Recovery Plan testing in accordance with the Department's IT Planning (PL) Standard; performance of periodic vulnerability scans and remediation as required by the Department's IT System Risk Assessment (RA) Standard; 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, including those retained or hired by the OIG, or vulnerability scanners, or auditors shall 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 shall 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 most, recent finalized version of the NIST SP 800-53, *Security and Privacy Controls for Information Systems and Organizations*. All NIST SP 800-53 controls shall be tested / assessed no less than every 3 years, according to federal and Department policy and upon entry into the Department's Ongoing Security Authorization (OSA) program, in accordance with the current OSA schedule. 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 FIPS 199, Standards for Security Categorization of Federal Information and Information Systems.

iii. 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 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 shall be developed in accordance with the NIST 800 series and Department of Education policy and guidance.

iv. The Contractor 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.

v. The Contractor 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 a High Value Asset or rated as 'Moderate' or 'High' for FIPS 199 risk impact, authenticated vulnerability scanning, or otherwise authorized through rules of engagement (RoE) scans and penetration testing or other means or exemption(s) vulnerability scanning, and penetration testing shall be performed on the hosting facility and application as part of the SA&A process. Systems rated as "Moderate" or "High" for FIPS risk impact or identified as a High Value Asset are also subject to penetration testing. Appropriate access agreements and rules of engagement will be reviewed and signed before any scanning or testing occurs.

vi. Identified deficiencies between required security controls within the current, finalized version of the NIST SP 800-53 and the contractor's, and all subcontractor'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 POA&M in accordance with Department policy.

Depending on the severity of the deficiencies, the Department may require remediation before an ATO is issued.

vii. The Contractor shall provide cybersecurity strategies, infrastructure hosting environments, and solutions that comply with the requirements of FISMA, Department and OMB cybersecurity policy guidance, and guidance contained in the NIST Special Publications series such as NIST SP 800-53 and other NIST Special Publications.

viii. 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.

ix. 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 (SLAs) are adhered to, complied with, and satisfied.

In conducting its security testing the Government intends to follow NIST SP 800-115, *Technical Guide to Information Security Testing and Assessment* and other appropriate testing, and assessment standards as may be designated by the CIO or designee at time of contract award.

2.19 Health Care Records and Data

For acquisitions involving personal health care records or personal health care data (such as background investigation or clearance application health data): In accordance with the Health Insurance Portability and Accountability Act (HIPAA), the Contractor shall adhere to the HIPAA requirements, and to all SPII requirements and procedures regarding all electronic storage, safekeeping, warehousing, transmission, modification, archival of, disposition of, destruction of, and distribution of electronic health care records, and preserve and protect the correct ethical and legal confidentiality, integrity, and availability of all such records. Please refer to https://www.hhs.gov/hipaa/for-professionals/index.html.

2.20 Privacy Act Requirements

If performance of this contract has been determined to involve the design, development, or operation of a system of records on individuals, the Contractor shall comply with the Privacy Act of 1974, and complete all Department of Education Privacy Impact Assessment requirements as requested by the contracting officer representative.

For contracts subject to the Privacy Act of 1974, the Contractor shall support a system of records in accordance with any Privacy Impact Assessments (PIAs) required and generated by any Privacy Threshold Analyses (PTAs), and any applicable System or Record Notices (SORNs), in conjunction with the judgment of the SAOP, and NARA-approved records schedule(s) and protection requirements for federal agencies to manage their electronic records in accordance with 36 CFR § 1236.20 & 1236.22 (ref. a), including but not limited to maintenance of links between records and metadata, and categorization of records to manage retention and disposal, either through transfer of permanent records to NARA or deletion of temporary records in accordance with NARA- approved retention schedules.

2.21 Security Requirements for Government-Owned/Contractor-Operated (GOCO) and Contractor-Owned/Contractor-Operated (COCO) Information Systems

The Contractor shall comply with the following:

a. **Federal Policies**

The Contractor shall comply with applicable federal laws, regulations, NIST guidance, DHS Emergency and Binding Operational Directives and policies that include, but are not limited to, Department of Education cybersecurity policies and standards documents, FISMA (44 U.S.C. 101); NIST SP 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*; OMB Circular A-130, *Managing Information as a Strategic Resource*; and other applicable federal laws, regulations, NIST guidance, and Departmental policies.

b. **Security Assessment and Authorization (SA&A)**

A valid ATO certifies that the Contractor's information system meets the contract's requirements to protect the agency data. If the system under this contract does not have a valid ATO, the Contractor shall work with the agency and supply the deliverables required to complete the ATO within the specified timeline(s) by the Program Office. The Contractor shall conduct the SA&A requirements in accordance with Department of Education cybersecurity policies, and ED's Cybersecurity Standards documents and NIST SP 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach* (latest revision).

Program Office acceptance of the ATO does not alleviate the Contractor's responsibility to ensure the system security and privacy controls are implemented and operating effectively.

c. **SA&A Package Deliverables**

The Contractor shall provide a SA&A package within the timeline, process and format specified by the Program Office to the CO and/or COR. Any additional SA&A deliverables that are required, if any, are detailed within the contract's statement of work/performance work statement.

d. **System Security Plans (SSP)**

The due date for the SSP is identified in the contract's statement of work/performance work statement. The SSP shall comply with the NIST SP 800-18, *Guide for Developing Security Plans for Federal Information Systems*, the FIPS 200, *Recommended Security Controls for Federal Information Systems*, and NIST SP 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations* applicable baseline requirements, and other applicable NIST guidance as well as ED and Program Office policies and other guidance.

The SSP shall be consistent with and detail the approach to IT security contained in the contractor's offer that resulted in the award of this contract. The SSP shall provide an overview of the system environment and security requirements to protect the information system as well as describe all applicable security controls in place or planned for meeting those requirements. It should provide a structured process for planning adequate, cost-effective security protection for a system. The Contractor shall update the SSP at least annually thereafter. Per the NIST SP 800-137, *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations*, "…FISMA… further emphasized the importance of continuously monitoring information system security by requiring agencies to conduct assessments of security controls at a frequency appropriate to risk, but no less than annually."

e. **Security Assessment Plan/Report (SAP/SAR)**

The due date is specified in the contract's statement of work/performance work statement. The appropriate security assessment will be conducted by the Program Office. It will be consistent with NIST SP 800-53A, NIST SP 800-30, and ED and Program Office policies. The assessor will document the assessment results in the SAR.

Thereafter, the Contractor, in coordination with the Program Office shall conduct and/or assist in the assessment of the security controls, in the timeline specified, and update the SAR at least annually. Per NIST SP 800-137, "…FISMA… further emphasized the importance of continuously monitoring information system security by requiring agencies to conduct assessments of security controls at a frequency appropriate to risk, but no less than annually."

f. **Independent Assessments**

The Contractor 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 Security Authorization package, and report on technical, operational, and management level deficiencies as outlined in NIST SP 800-53. The Contractor shall address all “high” deficiencies, and any other deficiency requiring contractor mitigation as identified by the Program Office, before submitting the package to the Government for acceptance. All remaining deficiencies shall be documented in a system POA&M.

g. **POA&Ms**

POA&Ms are due as specified in the contract. All POA&Ms shall be documented consistent with the Department’s IT System Security Assessment and Authorization (CA) Standard. All high-risk weaknesses shall be mitigated within the timeframe specified by the Program Office and all medium weaknesses shall be mitigated within the number of days specified by the Program Office from the date the weaknesses are formally identified and documented. The Program Office will determine the risk rating of vulnerabilities.

Identified risks stemming from deficiencies related to the security control baseline implementation, assessment, continuous monitoring, vulnerability scanning, and other security reviews and sources, as documented in the SAR, shall be documented and tracked by the Contractor for mitigation in the POA&M document. Depending on the severity of the risks, the Program Office may require designated POA&M weaknesses to be remediated before an ATO is issued. Thereafter, the POA&M shall be updated at least quarterly, or as specified by the Program Office.

h. **Contingency Plans and Contingency Plan Testing**

Contingency Plan due dates as specified in the contract. The Contingency Plan shall be developed in accordance with NIST SP 800-34, *Contingency Planning Guide for Federal Information Sy*stems, and be consistent with ED and Program Office policies. Upon acceptance by the System Owner, the Contractor, in coordination with the System Owner, shall test the Contingency Plan and prepare a Contingency Plan Test Report that includes the test results, lessons learned and any action items that need to be addressed. Thereafter, the Contractor shall update and test the Contingency Plan at least annually. Per the NIST SP 800-137, *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations*, “…FISMA… further emphasized the importance of continuously monitoring information system security by requiring agencies to conduct assessments of security controls at a frequency appropriate to risk, but no less than annually.

i. **E-Authentication Questionnaire**

The contractor shall collaborate with government personnel to ensure that an E-Authentication Threshold Analysis (E-auth TA) is completed to determine if a full E-Authentication Risk Assessment (E-auth RA) is necessary. System documentation developed for a system using E-auth TA/E-auth RA methods shall follow OMB 04-04 and current, final version of NIST SP 800-63, *Electronic*

Authentication Guidelines. Based on the level of assurance determined by the E-Auth, the Contractor shall ensure appropriate authentication to the system, including remote authentication, is in-place in accordance with the assurance level determined by the E- Auth (when required) in accordance with ED policies, OMB 22-09, and Executive Order 14028.

j. **Information Security Continuous Monitoring**

Upon the Government issuance of an ATO, the contractor-owned/operated systems that input, store, process, output, and/or transmit government information, shall meet or exceed the information security continuous monitoring (ISCM) requirements in accordance with FISMA and NIST SP 800-137, *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations*, and the ED Departmental Cybersecurity Policy, and its subordinate Policy Framework Instructions / Standards documents, based on NIST *Framework for Improving Critical Infrastructure Cybersecurity*. The following are the minimum requirements for ISCM the Contractor shall perform:

i. **Annual Assessment/Penetration Testing** - Assess the system security and privacy controls (or ensure an assessment of the controls is conducted) at least annually to determine the implemented security and privacy controls are operating as intended and producing the desired results (for systems identified as FIPS “High” impact rated or High Value Assets, this may involve penetration testing conducted by the agency or independent third-party.) In addition, review all relevant SA&A documentation (SSP, POA&M, Contingency Plan, etc.) and provide updates by Program Office specified due date.

ii. **Asset Management** - Using any available Security Content Automation Protocol (SCAP)-compliant automated tools for active/passive scans, provide an inventory of all information technology (IT) assets for hardware and software, (computers, servers, routers, databases, operating systems, etc.) that are processing ED-owned information/data. It is anticipated that this inventory information will be maintained as current. IT asset inventory information shall include IP address, machine name, operating system level, security patch level, and SCAP- compliant format information. The Contractor shall maintain a capability to provide an inventory of 100% of its IT assets using SCAP- compliant automated tools.

iii. **Configuration Management -** Use available SCAP-compliant automated tools, per the NIST IR 7511, *Security Content Automation Protocol (SCAP) Version 1.2*, Validation Program Test Requirements, as amended, Revision 4, for authenticated scans to provide visibility into the security configuration compliance status of all IT assets, (computers, servers, routers, databases, operating systems, application, etc.) that store and process government information. Compliance will be measured using IT assets and standard ED and government configuration baselines at least monthly, or more frequently if required by Department policy. The Contractor shall maintain a capability to provide security configuration compliance information for 100% of its IT assets using SCAP-compliant automated tools.

iv. **Vulnerability Management -** Use SCAP-compliant automated tools for authenticated scans to scan information system(s) and detect any security vulnerabilities in all assets (computers, servers, routers, Web applications, databases, operating systems, etc.) that store and process government information. Contractor shall actively manage system vulnerabilities using automated tools and technologies where practicable and in accordance with ED policy & Federal Directives. Automated tools shall be compliant with NIST-specified SCAP standards for vulnerability identification and management. The Contractor shall maintain a capability to provide security vulnerability scanning information for 100% of IT assets using SCAP- compliant automated tools and report to the agency at least weekly or more frequent as required by Department Policy.

v. **Patching and Vulnerability Remediation -** The Contractor shall install software/product vendor released security patches and remediate in systems processing government information in an expedited manner, within Federal Directives and Department specified timeframes within the IT System Risk Assessment Standard. NOTE: Many patches are applied in immediate response to a detection of a specific threat and/or a specific vulnerability. In the absence of such a detection, available patches shall be applied at least annually, unless contra-indicated due to any other more important factor(s) determined in a risk assessment.

vi. **Secure Coding -** Follow secure coding best practice requirements, as directed by US-CERT specified standards and the Open Web Application Security Project (OWASP), that will limit system software vulnerability exploits.

vii. **Boundary Protection -** The Contractor shall ensure that government information, other than unrestricted information, being transmitted from federal government entities to external entities is routed through a Trusted Internet Connection (TIC).

viii. **Open Security Controls Assessment Language (OSCAL) Overlays** - develop and maintain OCSAL overlays expressed in Extensible Markup Language (XML), JavaScript Object Notation (JSON), and YAML Markup Language (YAML) formats which provide machine-readable representations of control catalogs, control baselines, system security plans, and assessment plans and results.

2.22 Government Access for Security Assessment

The Contractor shall afford the Government access to the contractor’s facilities, installations, operations, documentation, information systems, and personnel used in performance of this contract to the extent required to carry out a program of security assessment (to include vulnerability testing), investigation, and audit to safeguard against threats and hazards to the confidentiality, integrity, and availability of federal data or to the protection of information systems operated on behalf of ED, including but are not limited to:

aa. At any tier handling or accessing information, consent to and allow the Government, or an independent third party working at the Government’s direction, without notice at any time during a weekday during regular business hours contractor local time, to access contractor installations, facilities, infrastructure, data centers, equipment (including but not limited to all servers, computing devices, and portable media), operations, documentation (whether in electronic, paper, or other forms), databases, and personnel which are used in performance of the contract.

The Government includes but is not limited to the U.S. Department of Justice, U.S. Government Accountability Office, and the ED Office of the Inspector General (OIG). The purpose of the access is to facilitate performance inspections and reviews, security and compliance audits, and law enforcement investigations. For security audits, the audit may include but not be limited to such items as buffer overflows, open ports, unnecessary services, lack of user input filtering, cross site scripting vulnerabilities, Structured Query Language (SQL) injection vulnerabilities, and any other known vulnerabilities.

bb. At any tier handling or accessing protected information, fully cooperate with all audits, inspections, investigations, forensic analysis, or other reviews or requirements needed to carry out requirements presented in applicable law or policy. Beyond providing access, full cooperation also includes, but is not limited to, disclosure to investigators of information sufficient to identify the nature and extent of any criminal or fraudulent activity and the individuals responsible for that activity. It includes timely and complete production of requested data, metadata, information, and records relevant to any inspection, audit, investigation, or review, and making employees of the Contractor available for interview by inspectors, auditors, and investigators upon request. Full cooperation also includes allowing the Government to make reproductions or copies of information and equipment, including, if necessary, collecting a machine or system image capture.

cc. Logically segregate, and/or otherwise identify, distinguish, and appropriately safeguard Government protected information and metadata on the handling of Government protected information from other information. Logical commingling of information is prohibited. Inspectors, auditors, and investigators will not be precluded from having access to the sought information if sought information is commingled with other information.

dd. Cooperate with inspections, audits, investigations, and reviews.

2.23 End of Life Compliance

The Contractor shall use Commercial off the Shelf (COTS) software or other software that is supported by the manufacturer. In addition, the COTS/other software need to be within one major version of the current version; deviation from this requirement will only be allowed via the ED waiver process (approved by ED CISO). The Contractor shall retire and/or upgrade all software/systems that have reached end-of-life in accordance with ED Lifecycle Management (LCM) Framework, OCIO: 1-106. Under no circumstances will the Department allow contractors to utilize unsupported COTS applications or systems or programs or utilities without a specific written exception, signed and authorized by the CIO.

2.24 Desktops, Laptops, and Other Computing Devices

The Contractor shall ensure that all IT equipment (e.g., laptops, desktops, servers, routers, mobile devices, peripheral devices, etc.) used to process information on behalf of ED are deployed and operated in accordance with approved security configurations and meet the following minimum requirements:

ee. Encrypt equipment and information stored and/or processed by such equipment in accordance with ED and FIPS 140-2 or FIPS 140-3 encryption standards.

ff. Establish and document configuration settings for components employed within desktops, laptops and other information systems which reflect the most restrictive mode consistent with operational requirements using the most updated DISA STIG, with Security Engineering and Architecture Branch (SEA) authorized deviations as needed; use the following configuration standards, in the order of precedence shown, when a DISA STIG is not available for a product or system:

   i. NIST standards and baselines

   ii. Other US Government standards

   iii. Cybersecurity industry best practices, benchmarks, and guidelines (i.e., Center for Internet Security, or CIS)

   iv. Vendor checklists and baselines

gg. Maintain the latest operating system patch release and anti-virus software definitions.

hh. Validate the configuration settings after hardware and software installation, operation, maintenance, update, and patching and ensure changes in hardware and software do not alter the approved configuration settings.

ii. Automate configuration settings and configuration management in accordance with ED security policies, including but not limited to:

  i. Configuring its systems to allow for periodic ED vulnerability and security configuration assessment scanning.

  ii. Using Security Content Automation Protocol (SCAP)-validated tools to scan its systems at least monthly and report the results of these scans to the CO and/or COR, Project Officer, and any other applicable designated POC.

  iii. Perform automated asset discovery every 7 days. While many methods and technologies can be used to accomplish this task, this discovery must cover the entire Internet Protocol space used by the Contractor to support the Department.

  iv. Initiate vulnerability enumeration across all discovered assets, including all discovered nomadic/roaming devices (e.g., laptops), every 7 days. The Department understands that in some instances achieving full vulnerability discovery on the entire contractor space may not complete in 14 days. Enumeration processes should still be initiated at regular intervals to ensure all systems within the enterprise are scanned on a regular cadence within this window.

  v. All vulnerability enumeration performed on managed endpoints (e.g., servers, workstations, desktops, laptops) and managed network devices (e.g., routers, switches, firewalls) must be conducted with privileged credentials (for the purpose of this directive, both network-based credentialed scans and client- or agent-based vulnerability detection methods are viewed as meeting this requirement).

  vi. All vulnerability detection signatures used must be updated at an interval no greater than 24 hours from the last vendor-released signature update.

  vii. Contractors must perform the same type of vulnerability enumeration on mobile devices (e.g., iOS and Android) and other devices that reside outside of agency on-premises networks.

  viii. All alternative asset discovery and vulnerability enumeration methods (e.g., for systems with specialized equipment or those unable to utilize privileged credentials) must be approved by the Department.

2.25 FedRAMP Privacy and Security Requirements

The Contractor shall be responsible for the following privacy and security requirements:

a. **FedRAMP-Compliant ATO**

If a cloud solution will be used, then an ED-issued, FedRAMP- Compliant ATO is a Federal and a Departmental requirement, and one shall be obtained. Comply with FedRAMP Security Assessment and Authorization (SA&A) requirements and ensure the information system/service under this contract has a valid FedRAMP compliant (approved) ATO in accordance with FIPS Publication 199 defined security categorization. FedRAMP-compliance does not simply mean that a FedRAMP-compliant ATO has been issued. Rather it means only that a FedRAMP-compliant ATO has been issued for a particular cloud service provider/product.

Options for ATO Issuance

i. ED can leverage FedRAMP-compliant assessments that have already been completed by other agencies; or The FedRAMP PMO can make its own risk/ATO decisions for any affected ED applications.

ii. The value proposition offered by FedRAMP is that Agencies themselves do not have to individually sponsor Cloud Service Providers (CSPs) through FedRAMP for individual acquisitions/requirements. It is important to note that CSPs wishing to do business with the federal government can initiate the FEDRAMP compliance ATO on their own. For their part, Agencies need to ensure that they identify the requirement (via SOWs, PWSs, etc.,) for compliance when acquiring new services or when there is an opportunity to update existing agreements.

iii. In the case of a CSP where there is not yet a FedRAMP-compliant ATO, the program office would have to provide the following until such a time as the FEDRAMP-compliant ATO is obtained:

iv. Plan for obtaining a FedRAMP compliant ATO; and

v. ED ATO decision for each affected system; and Risk acceptance until: the FedRAMP-compliant assessment has been completed; and a FedRAMP-compliant ATO has been obtained; and the assessment results are available for consideration by ED; and an ED ATO decision for each affected ED system has been obtained.

vi. In accepting the risk, the program office shall be required to evaluate and document what the risk is based on ED's business requirements/objectives (e.g., what are we using the CSP for, what ED data is stored, processed, transmitted by the CSP, etc.?).

Contractor Responsibilities:

i. If a FedRAMP compliant ATO has not been granted, the Contractor shall submit a plan to obtain a FedRAMP compliant ATO by the date, and in the format, instructed by the Program Office. In addition, the Contractor shall also accomplish the following:

ii. Implement applicable FedRAMP baseline controls commensurate with the agency-defined security categorization and the applicable FedRAMP security control baseline (www.FedRAMP.gov). The ED Departmental Handbook on Information Assurance/Cybersecurity Policy (ACSD-OCIO-004/OCIO 3-112), and its subordinate Cybersecurity Standards documents, further define the baseline policies as well as roles and responsibilities. The Contractor shall also implement a set of additional controls identified by the agency when applicable.

iii. A security control assessment shall be conducted by a FedRAMP third-party assessment organization (3PAO) for the initial ATO and annually thereafter or whenever there is a significant change to the system's security posture in accordance with the FedRAMP Continuous Monitoring Plan.

iv. The Department has a responsibility to assess CSP environments and control implementations against the Department's requirements to ensure that sufficient controls are implemented so that the confidentiality, integrity, and availability of the Department's information and information systems hosted in the CSP environment is assured in a manner that incorporates review of all the documentation relied on for issuance of an ATO. The FedRAMP provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud services. Although a cloud service provider may have been granted an ATO by the FedRAMP Project Management Office (PMO) or another Federal agency, the Department must also grant an ATO for any cloud services used by the Department. An AO can leverage ATO documentation from the FedRAMP PMO or other federal agency, to support an authorization decision, but it is not a substitute for an explicit authorization decision by an AO within the Department. All FedRAMP authorization packages are required to be reviewed and approved by the Department's Chief Information Security Officer (CISO) prior to connecting the system to the Department's network.

b. **Data Jurisdiction**

The Contractor shall store all information within the security authorization boundary, data at rest or data backup, within the Continental United States (CONUS).

c. **Service Level Agreements**

The Contractor shall understand the terms of the service agreements that define the legal relationships between cloud customers and cloud providers and work with Program Office to develop and maintain an SLA.

d. **Interconnection Agreements/Memorandum of Agreements**

The Contractor shall establish and maintain Interconnection Agreements and or Memoranda of Agreement/Understanding in accordance with ED policies.

2.26 Protection of Information in a Cloud Environment

a. If contractor personnel must remove any information from the primary work area, they shall protect it to the same extent they would the proprietary data and/or company trade secrets and in accordance with ED policies.

b. ED will retain unrestricted rights to all federally owned and/or federally managed data and/or metadata that ED either owns or manages that is handled under this contract. Specifically, ED retains ownership of any user created/loaded data and applications collected, maintained, used, or operated on behalf of ED and hosted on contractor’s infrastructure, as well as maintains the right to request full copies of these at any time. If requested, data shall be available to ED within ***one (1) business day*** from request date or within the timeframe specified otherwise. In addition, the data shall be provided at no additional cost to ED.

c. The Contractor shall ensure that the facilities that house the network infrastructure are physically and logically secure in accordance with FedRAMP requirements and ED policies.

d. The disposition of all ED data shall be at the written direction of ED. This may include documents returned to ED control; destroyed; or held as specified until otherwise directed. Items returned to the Government shall be hand carried or sent by certified mail to the COR.

e. If the system involves the design, development, or operation of a system of records on individuals, the Contractor shall comply with the Privacy Act requirements.

2.27 Security Assessment and Authorization

f. The Contractor shall comply with ED and FedRAMP requirements as mandated by federal laws, regulations, and ED policies, including making available any documentation, physical access, and logical access needed to support the SA&A requirement. The level of effort for the SA&A is based on the system’s FIPS 199 security categorization and ED security policies.

g. In addition to the FedRAMP-compliant ATO, the Contractor shall complete and maintain an agency SA&A package to obtain agency ATO prior to system deployment/service implementation. Any additional ATO requirements are specified in the contract’s statement of work/performance work statement. The agency ATO shall be approved by the Program Office authorizing official (AO) prior to implementation of system and/or service being acquired.

h. CSP systems categorized as FIPS 199 high or moderate shall leverage a FedRAMP accredited third-party assessment organization (3PAO). CSP systems categorized as FIPS 199 low impact may leverage a non-accredited, independent assessor.

i. For all acquired cloud services, the contract's statement of work/performance work statement specifies whether Department or FedRAMP required processes and templates will be utilized. The SA&A package shall contain the required documentation. Following the initial ATO, the Contractor shall review and maintain the ATO in accordance with ED policies.

j. ED reserves the right to perform penetration testing (pen testing) on all systems operated on behalf of ED, and to the right to have access to, at any point in time, to all systems and all data on all systems operated on behalf of ED. This is crucial for ED to be able to provide relevant data to law enforcement and/or to incident responders, in a timely manner, when time is critical, and of the essence. If ED exercises this right, the Contractor shall allow ED employees (and/or designated third parties) to conduct Security Assessment activities to include control reviews in accordance with ED requirements. Review activities include, but are not limited to, scanning operating systems, web applications, wireless scanning; network device scanning to include routers, switches, and firewall, and IDS/IPS; scanning databases and other applicable systems, including general support structure, that support the processing, transportation, storage, or security of Government information for vulnerabilities.

k. The Contractor shall identify any gaps between required FedRAMP Security Control Baseline/Continuous Monitoring controls and the Contractor's implementation status as documented in the Security Assessment Report and related Continuous Monitoring artifacts. In addition, all gaps shall be documented and tracked by the Contractor for mitigation in a POA&M document. Depending on the severity of the risks, ED may require remediation at the contractor's expense before ED issues an ATO.

l. The Contractor shall mitigate security risks for which they are responsible, including those identified during SA&A and continuous monitoring activities. All vulnerabilities and other risk findings shall be remediated by the prescribed timelines from discovery: (1) critical vulnerabilities no later than **thirty (30)** days and (2) high, medium, and low vulnerabilities no later than **sixty (60)** days [or shorter timeline as specified in the contract's Performance Work Statement. If a specific vulnerability or other risk finding cannot be mitigated within the prescribed timelines above, they shall be added to the designated POA&M and mitigated within the newly designated timelines specified by the Program Office.

ED will determine the risk rating of vulnerabilities using FedRAMP baselines, and as a part of that process, shall also identify, and account for, and incorporate any and all identifiable risks based on venue and jurisdiction issues that are tied to, and dependent upon, the laws and circumstances tied to national, international, and geographic boundaries that convey with the physical location(s) where data, infrastructure, systems, software, and platforms literally reside, in a cloud environment.

m. Revocation of a Cloud Service: ED and/or the Program Office has the right to act in response to the CSP's lack of compliance and/or increased level of risk. In the event the CSP fails to meet ED and FedRAMP security and privacy requirements and/or there is an incident involving sensitive information, ED and/or the Program Office] may suspend or revoke an existing agency ATO (either in part or in whole) and/or cease operations. If an ATO is suspended or revoked in accordance with this provision, the CO and/or COR may direct the CSP to take additional security measures to secure sensitive information. These measures may include restricting access to sensitive information on the Contractor information 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.

2.28 Reporting and Continuous Monitoring

Following the initial ATOs, the Contractor shall perform the minimum ongoing continuous monitoring activities specified below, submit required deliverables by the specified due dates, and meet with the system/service owner and other relevant stakeholders to discuss the ongoing continuous monitoring activities, findings, and other relevant matters. The CSP shall work with the agency to schedule ongoing continuous monitoring activities. [Program Office include meetings/deliverables timelines as applicable/necessary]

a. At a minimum, the Contractor shall provide the following artifacts/deliverables monthly, in the format prescribed by the Program Office: Operating system, database, Web application, and network vulnerability scan results.

b. Updated POA&Ms; Any updated authorization package documentation as required by the annual attestation/assessment/review or as requested by the Program Office System Owner or AO.

c. Any configuration changes to the system and/or system components or CSP's cloud environment, that may impact ED/ [Program Office]'s security posture. Changes to the configuration of the system, its components, or environment that may impact the security posture of the system under this contract shall be approved by the agency.

2.29 Configuration Baseline

n. The Contractor shall certify that applications are fully functional and operate correctly as intended on systems using the most updated DISA Security Technical Implementation Guides (STIGs), with Security Engineering and Architecture Branch (SEA) authorized deviations, as needed. The Contractor shall use the following configuration standards, in the order of precedence shown, when a DISA STIG is not available for a product or system:

- NIST standards and baselines
- Other US Government standards
- Cybersecurity industry best practices, benchmarks, and guidelines (i.e., Center for Internet Security, or CIS)
- Vendor checklists and baselines

The standard installation, operation, maintenance, updates, and/or patching of software shall not alter the configuration settings from the approved ED/Program Office configuration baseline.

o. The Contractor shall use Security Content Automation Protocol (SCAP) validated tools with configuration baseline scanner capability to certify their products operate correctly with ED and NIST defined configurations and do not alter these settings.

2.30 Media Transport

p. The Contractor shall be accountable and document all activities associated with the transport of government information, devices, and media transported outside controlled areas and/or facilities. These include information stored on digital and non-digital media (e.g., CD- ROM, tapes, etc.), mobile/portable devices (e.g., USB flash drives, external hard drives, and SD cards).

q. All information, devices and media shall be encrypted with ED-approved encryption mechanisms to protect the confidentiality, integrity, and availability of all government information transported outside of controlled facilities.

2.31 Card Readers

The Contractor shall include FIPS 201-compliant smart card readers (referred to as LACS Transparent Readers) with the purchase of servers, printers, desktops, and laptops.

2.32 Other Requirements

r. The Contractor shall follow secure coding best practice requirements, as directed by the US-CERT specified standards and OWASP that will limit system software vulnerability exploits.

s. The Contractor shall ensure IT applications designed and developed for end users (including mobile applications and software licenses) run in the standard user context without requiring elevated administrative privileges.

t. The Contractor shall ensure that computer software developed on behalf of ED or tailored from an open-source product, is fully functional and operates correctly on systems configured in accordance with government policy and federal configuration standards. The Contractor shall test applicable products and versions with all relevant and current updates and patches updated prior to installing in the ED environment. No sensitive data shall be used during software testing.

u. The Contractor shall protect information that is deemed sensitive from unauthorized disclosure to persons, organizations or subcontractors who do not have a need to know the information. Information which, either alone or when compared with other reasonably available information, is deemed sensitive or proprietary by ED shall be protected as instructed in accordance with the magnitude of the loss or harm that could result from inadvertent or deliberate disclosure, alteration, or destruction of the data.

v. The contractor shall employ secure software development environments in accordance with the Secure Software Development Framework (SSDF) and processes specified by NIST to reduce the number of vulnerabilities in released software, reduce the potential impact of the exploitation of undetected or unaddressed vulnerabilities, and address the root causes of vulnerabilities to prevent recurrences.

2.33 Binding Operation Directives

The Contractor shall ensure that information system or services provided to the Department of Education adhere to all applicable DHS CISA Security cybersecurity BODs and Emergency Directives requirements (https://cyber.dhs.gov/directives/).

2.34 Continuous Monitoring / Ongoing Security Assessment & Authorization

Following the issuance of an ATO, contractors shall support continuous monitoring activities to identify and remediate risks while monitoring changing conditions which could potentially affect the ability to conduct core missions and business functions. Contractors shall address and remediate POA&M action items and track completion dates as required by the Department ISSM. POA&Ms shall be managed and maintained in the Department's GRC tool, currently CSAM. Contractors shall review open POA&Ms regularly to determine which items require additional attention or resources and report to the AO of any action item completion date not met. Systems which have been evaluated by the Office of the Chief Information Officer (OCIO) as having sufficient combined manual and automated system-level continuous monitoring in place and adhere to the control assessment schedules and delivery of control artifacts.

2.35 Identity, Credential, and Access Management (ICAM) and PIV

Systems

The Contractor shall conduct a risk assessment for Identity Assurance Level (IAL) and Authentication Assurance Level (AAL) as defined in the latest version of the NIST Special Publication 800-63 "Digital Identity Guidelines" and will also conduct a Federation Assurance Level (FAL) assessment if accepting credentials from federal, state, or non-government organizations. The Contractor shall ensure that the Information System leverages the department approved enterprise ICAM Access Management solution using modern SAML, OIDC protocols for authentication throughout the full contract period of performance.

The Contractor must provide a System for Cross-Domain Identity Management (SCIM) interface for the Information System or provide an implementation plan to enable and support a SCIM interface for their Information System throughout the full contract period of performance.

2.36 Zero Trust Architecture/Zero Trust Network

The Contractor shall ensure the Information System or Service adheres to applicable Zero Trust Architecture (ZTA) and Zero Trust Network (ZTN) requirements as documented in OMB Memo M-22-09, *Federal Zero Trust Strategy*, NIST SP 800-207, *Zero Trust Architecture* and the version of the Department of Education Zero Trust Architecture current throughout full contract period of performance.

The Contractor shall ensure that any ED infrastructure (on premises, cloud, off-premises, etc., for which Zero Trust is employed shall always comply with the Section 889(a)(1)(B) of the John S. McCain National Defense Authorization Act (NDAA) prohibition, which prohibits agencies from procuring or obtaining equipment or services that use covered telecommunications equipment or services as a substantial or essential component or critical technology. (FAR 52.204-25).

2.37 Department of Education Cyber Data Lake (EDCDL)

A data lake is a centralized repository allowing all structured, unstructured, and hybrid data at any scale. The Contractor shall ensure that the systems and services delivered under the contact shall integrate with EDCDL in accordance with applicable Department's standards and guidelines. The Contractor shall ensure that all data required for collection and retention in accordance with the applicable Department policies and standards is sent and ingested by the EDCDL, including but not limiting to: CDM data feeds, security events logs, systems and security configuration information. The Contractor shall ensure that all unstructured, structured, and hybrid data routed into, and potentially, out of the EDCDL, shall always comply with the Section 889(a)(1)(B) of the John S. McCain National Defense Authorization Act (NDAA) prohibition, which prohibits agencies from procuring or obtaining equipment or services that use covered telecommunications equipment or services as a substantial or essential component or critical technology. (FAR 52.204-25).

2.38 Trusted Internet Connections

The Contractor shall ensure that government information, other than unrestricted information, being transmitted from federal government entities to external entities using cloud services is inspected by Trusted Internet Connection (TIC) processes as documented in TIC 3.0 guidance documentation established by the DHS CISA. This is in accordance with the Office of Management and Budget (OMB) Memorandum 19-26: *Update to the TIC Initiative*. TIC 3.0 expands on the original initiative to drive security standards and leverage advances in technology to secure a wide spectrum of Department network architectures.

The Contractor shall route all external connections through a TIC and 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. The Contractor shall implement controls to ensuring all traffic, including mobile and cloud, goes through approved traditional TIC gateways or TIC 3.0 security architecture and capabilities. The Contractor shall implement connections between Department systems and networks with externally hosted systems that comply with the requirements of the Trusted Internet Connections (TIC) initiative.

2.39 Transition to National Institute of Standards and Technology Special Publication 800-53, Rev. 5 from Rev. 4 – Security and Privacy Controls for Information Systems and Organizations

The Contractor shall adhere to the current, final version of NIST SP 800-53, Rev. 5, *Security and Privacy Controls for Information System and Organizations.* For contracts awarded on or after October 1, 2021, the contractor shall be compliant with NIST 800-53 Rev 5 at date of award. For contracts awarded prior to October 1, 2021, the contractor shall take action to comply with NIST SP 800-53, Rev 5 on or before January 31, 2022. The Contractor shall comply with all Rev. 4 to 5 migration actions and timeframes required by Department policy or CISO memo.

2.40 Reserved

2.41 Use of Unauthorized External Email Systems

The Contractor shall not use unauthorized external information systems (such as corporate or personal email or online storage accounts), equipment, or services to conduct any ED business.

2.42 Office of Management and Budget (OMB) and Executive Order Compliance (EO 14028)

The Contractor shall ensure that information system or services provided to the Department of Education adhere to requirements contained within Executive Order (EO), *Improving the Nation's Cybersecurity* (EO 14028 released May 12, 2021) and comply with all OMB memorandums issued to implement EO 14028 requirements.

a. The Contractor shall employ a robust Endpoint Detection and Response (EDR) solution, as defined in OMB M-22-01, *Improving Detection of Cybersecurity Vulnerabilities and Incidents on Federal Government Systems through Endpoint Detection and Response,* to improve the Contractor's and the Department's ability to detect and respond to increasingly sophisticated threat activity.

b. In accordance with OMB M-21-31, *Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents,* the Contractor shall collect and preserve data, information, and reporting relevant to cybersecurity event prevention, detection, response, and investigation on all information systems over which they have control, including systems operated on behalf of government. The Contractor shall share such data, information, and reporting, as they relate to cyber incidents or potential incidents relevant to the Department of Education.

c. The Contractor shall provide a list of all critical software over which they have control, including systems operated on behalf of the Government to comply with OMB M-21-30, *Protecting Critical Software Through Enhanced Security Measures.* NIST defines critical software as any software that has, or has direct software dependencies upon, one or more components with at least one of these attributes:

    i. is designed to run with elevated privilege or manage privileges

    ii. has direct or privileged access to networking or computing resources

    iii. is designed to control access to data or operational technology

    iv. performs a function critical to trust

    v. operates outside of normal trust boundaries with privileged access

    The definition of critical software applies to software of all forms (e.g., standalone software, software integral to specific devices or hardware components, cloud-based software) that is purchased for, or deployed in, information systems and used for operational purposes.

d. The Contractor shall report all cybersecurity incidents involving a software product or service provided to the Department or involving a support system for a software product or service provided.

e. The Contractor shall collaborate with the Department in their investigations of and responses to incidents or potential incidents on Federal Information Systems, including by implementing technical capabilities, such as monitoring networks for threats and shall share cyber threat and incident information with the Department, doing so, where possible, in industry-recognized formats for incident response and remediation.

f. All information and communications technology (ICT) service providers entering contracts with government shall within 60 minutes, report to government when they discover a cyber incident involving a software product or service provided to ED or involving a support system for a software product or service provided to ED.

All Contractors that produce software, also referred to as software producers, as well as contractors who procure software for use at the Department, must comply with OMB M-22-18 requirements.

2.43 Restriction on Performance Location

Except where otherwise specified in the contract, contract performance (including remote access) is required to be within the United States and its territories. In emergency (personal emergencies are not justification for authorization), exigent circumstances, or crisis, necessitating contract performance in a foreign country, prior authorization by the Contracting Officer, with CISO approval, is required to:

- Take Government Furnished Equipment to the foreign country
- Access ED Information Technology (IT) systems from a foreign country
- Access contractor systems operated with ED data from a foreign country; and
- Interface with ED systems from a foreign country.

2.44 Compliance with Title 15 of the Code of Federal Regulations Part 7

The regulations issued by the Department of Commerce under Executive Order 13873 require contractors to comply with certain restrictions on the acquisition, importation, transfer, or use of information and communications technology or services (ICTS) originating foreign adversaries that pose national security risks. *See* 15 C.F.R. § 7, “Securing the Information and Communications Technology and Services (ICTS) Supply Chain”. Contractors shall be solely responsible for bearing any costs associated with compliance with these regulations and shall certify that they have conducted due diligence to ensure that any ICTS they use in connection with this contract comply with the Commerce regulations.

For purposes of Executive Order 13873 and its implementing regulations, the Secretary of Commerce has stated that the following constitute foreign adversaries:

- The People’s Republic of China including the Hong Kong Special Administrative Region (China)
- Republic of Cuba (Cuba)
- Islamic Republic of Iran (Iran)
- Democratic People’s Republic of Korea (North Korea)
- Russian Federation (Russia)
- Venezuelan politician Nicolas Maduro (Maduro Regime)

Contractors are strongly discouraged from using any ICTS that has been designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary. The Department of Commerce has the authority to identify, review, shape, and prohibit any covered transaction involving a federal agency, which may impose significant transaction costs on contractors.

Failure to comply with the Commerce regulations may result in termination of the contract, liability for damages, and other legal or administrative penalties. Contractors shall promptly notify the agency of any changes in their use of ICTS that may affect compliance with the Commerce regulations.