

Addendum: Cybersecurity Tasks Checklist

Indicated below are the applicable cybersecurity tasks to include in IT requirements, per EPA Acquisition Guide (EPAAG) 39.1.2.

TASK	TITLE	APPLICABLE
A	Personally Identifiable Information Contract Closeout	X
B	Contractor Return of all EPA-Provided and EPA-Activity-Related Information	X
C	Verified Secure Destruction of All EPA-Provided and EPA-Activity-Related Information	X
D	Contractor Return of all EPA-Owned and Leased Computing and Information Storage Equipment	
E	Authority to Operate (ATO) Suspension or Revocation	X
F	Security Monitoring and Alerting Requirements	X
G	IT Security and Privacy Awareness Training	X-Mandatory Training
H	Specialized Information Security Training for Staff with Significant Security Responsibilities	X-RBT
I	Federal Reporting Requirements	X
J	Protecting Sensitive Information	x
K	Security Assessment and Authorization (SA&A)	X-CMA Audit
L	Contractor System Oversight/Compliance	X
M	Contractor Access to EPA IT Systems	X -WebCMS
N	Individual Notification for Personally Identifiable Information	
O	Credit Monitoring and Identity Protection	
P	Compliance with IT Security Policies	X
Q	Secure Technical Implementation	x
R	Internet Protocol Version 6 (IPv6)	
S	Cloud Service Computing	
T	Contract Performance Information and Testimony	x
U	Rehabilitation Act Section 508 Standards	X
V	Termination for Default - Failure to Report Information Security Incident	X

TASK KEY:

Requirement Type	Required Tasks
IT Hardware	A,B,C,F,G,H,I,J,K,M,P,Q,R,T,U,V
IT Software	A,F,H,I,J,K,L,M,P,Q,R,T,U,V
Green IT	A,B,C,E,F,H,I,J,K,M,P,Q,R,U,V
IT Services	A,B,C,D,E,G,H,I,J,L,M,O,P,Q,T,U,V
Data Center Services	A,B,C,E,F,G,H,I,J,K,L,M,N,O,P,Q,R,T,U,V
Cloud Computing	A,B,C,E,F,G,H,I,J,K,L,M,N,O,P,Q,R,S,T,U,V
Cyber Security Product and Services	A,B,E,F,G,H,I,J,K,L,M,O,P,Q,R,T,V

Addendum: Cybersecurity Tasks Checklist

The full text of the tasks are described, as follows:

Task A - Personally Identifiable Information Contract Closeout

(a) *Definition.* Personally Identifiable Information (PII) - as defined in OMB Memorandum M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*, PII refers to sensitive information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual.

(b) *Certification of Sanitization of EPA-provided and EPA-Activity-Related Files and Information (including but not limited to all records, files, and metadata in electronic or hardcopy format).* As part of contract closeout, the Contractor shall submit a *Certification of Sanitization of EPA-provided and EPA-Activity-Related Files and Information* to the Contracting Officer and the Contracting Officer's Representative (COR) following the template provided in Appendix G of National Institute of Standards and Technology (NIST) Special Publication 800-88, *Guidelines for Media Sanitization Revision 1*, which assesses risk associated with Personally Identifiable Information (PII) that was generated, maintained, transmitted, stored or processed by the Contractor. The Senior Agency Official for Privacy (SAOP) shall review the Certification and coordinate with the Contracting Officer and the COR.

(c) The Contractor agrees to insert in each subcontract or consultant agreement placed hereunder, provisions which shall conform substantially to the language of this requirement, including this paragraph, unless otherwise authorized by the Contracting Officer.

Task B - Contractor Return of all EPA-Provided and EPA-Activity-Related Information

(a) Within thirty (30) days (or a different time period approved by EPA) of an EPA request, or after the end of the contract performance period, the Contractor must return all originals of all EPA-provided and EPA-Activity-Related Information (including but not limited to all records, files, and metadata in electronic or hardcopy format). The Contractor must return originals obtained while conducting activities in accordance with the contract with EPA; or distributed for any purpose by the Contractor to any other related organization and/or any other component or separate business entity; or received from the Contractor by any other related organization and/or any other component or separate business entity. Contractors must return all originals so that they cannot be used for further business by Contractor.

(b) Concurrent with the return of all originals as set forth in paragraph (a), the Contractor must document to the EPA the return of all originals of all EPA-provided and EPA-Activity-Related Information (including but not limited to all records, files, and metadata in electronic or hardcopy format). The Contractor must document originals obtained while conducting activities in accordance with the contract with EPA; or distributed for any purpose by the Contractor to any other related organization and/or any other component or separate business entity; or received from the Contractor by any other related organization and/or any other component or separate business entity.

(c) The Contractor agrees to insert in each subcontract or consultant agreement placed hereunder, provisions which shall conform substantially to the language of this requirement, including this paragraph, unless otherwise authorized by the Contracting Officer.

Task C - Verified Secure Destruction of All EPA-Provided and EPA-Activity-Related Information

(a) Within 60 days after the end of the contract performance period or a time period approved by EPA, or after the contract is suspended or terminated by EPA for any reason, and after EPA has accepted and approved the Contractor's return of information, the Contractor must execute secure destruction (either by

Addendum: Cybersecurity Tasks Checklist

the Contractor or third-party firm approved in advance by EPA) of all existing active and archived originals and/or copies of all EPA-provided and EPA-activity-related files and information (including but not limited to all records, files, and metadata in electronic or hardcopy format). This information includes but is not limited to information obtained by the Contractor while conducting activities in accordance with the contract with EPA; or distributed for any purpose by the Contractor to any other related organization and/or any other component or separate business entity; or received from the Contractor by any other related organization and/or any other component or separate business entity. Destruction Methods shall be by procedures approved by EPA in advance in writing.

(b) Within 75 days after the end of the contract performance period or a time period approved by EPA, or after the contract is suspended or terminated by EPA for any reason, and after EPA has accepted and approved the Contractor's return of information, the Contractor must document to the EPA the secure destruction of all existing active and archived originals and/or copies of all EPA-provided and EPA-activity-related files and information, (including but not limited to all records, files, and metadata in electronic or hardcopy format). This information includes but is not limited to information obtained by the Contractor while conducting activities in accordance with the contract with EPA; or distributed for any purpose by the Contractor to any other related organization and/or any other component or separate business entity; or received from the Contractor by any other related organization and/or any other component or separate business entity. Destruction Methods shall be by procedures approved by EPA in advance in writing.

(c) The Contractor agrees to insert in each subcontract or consultant agreement placed hereunder, provisions which shall conform substantially to the language of this requirement, including this paragraph, unless otherwise authorized by the Contracting Officer.

Task D - Contractor Return of all EPA-Owned and Leased Computing and Information Storage Equipment

(a) Within 60 days (or a different time period approved by EPA) after the end of the contract performance period, the Contractor must return all EPA-owned and leased computing and information storage equipment to EPA.

(b) The Contractor agrees to insert in each subcontract or consultant agreement placed hereunder, provisions which shall conform substantially to the language of this requirement, including this paragraph, unless otherwise authorized by the Contracting Officer.

Task E - Authority to Operate (ATO) Suspension or Revocation

(a) *Definitions.*

(i) *Authority to Operate (ATO)* - Signed by the Agency chief information officer (CIO) or deputy CIO, ATOs are issued for all information systems that input, store, process, and/or output Government information. In order to be granted an ATO, all federal information systems must be compliant with National Institute of Standard and Technology (NIST) Special Publication (SP) 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*, and FIPS Publication 200, *Minimum Security Requirements for Federal Information and Information Systems*. Contractors whose internal information systems will process Sensitive Information incidental to Agency product or service development must meet requirements for NIST SP 800-171, *Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations*, instead of NIST SP 800-53.

Addendum: Cybersecurity Tasks Checklist

(ii) *Information Security Incident* - an occurrence that results in actual or potential jeopardy to the confidentiality, integrity, or availability of an information system or the information the system processes, stores or transmits, or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies. The Contractor must report all known Information Security Incidents if they involve Sensitive Information.

(iii) *Sensitive Information* - As defined in NIST SP 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*, Sensitive Information is any information where the loss, misuse or unauthorized access to, or modification of, could adversely affect the national interest or the conduct of federal programs, or the privacy to which individuals are entitled under 5 U.S.C. Section 552a (the Privacy Act), but that has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept classified in the interest of national defense or foreign policy. Sensitive Information is subject to stricter handling requirements than non-sensitive information because of the increased risk if the data are compromised. Some categories of Sensitive Information include Financial, Medical or Health, Legal, Strategic and Business, Human Resources, Personally Identifiable Information (PII), and Sensitive PII. These categories of information require appropriate protection as stand-alone information and may require additional protection in aggregate.

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

(c) The Contractor agrees to insert in each subcontract or consultant agreement placed hereunder, provisions which shall conform substantially to the language of this requirement, including this paragraph, unless otherwise authorized by the Contracting Officer.

Task F - Security Monitoring and Alerting Requirements

(a) All Contractor-operated systems that use or store EPA information must meet or exceed EPA policy requirements pertaining to security monitoring and alerting. All systems are subject to the requirements of existing federal law, policy, regulation and guidance (e.g., Federal Information Security Management Act of 2002). The Contractor must comply with the EPA-used Department of Homeland Security (DHS) Continuous Diagnostics and Mitigation (CDM) policy for security monitoring and alerting, which includes requirements not limited to:

(1) System and Network Visibility and Policy Enforcement at the following levels:

- (i) Edge
- (ii) Server / Host
- (iii) Workstation / Laptop / Client
- (iv) Network
- (v) Application
- (vi) Database
- (vii) Storage
- (viii) User

(2) Alerting and Monitoring

Addendum: Cybersecurity Tasks Checklist

(3) System, User, and Data Segmentation

(b) The Contractor agrees to insert in each subcontract or consultant agreement placed hereunder, provisions which shall conform substantially to the language of this requirement, including this paragraph, unless otherwise authorized by the Contracting Officer.

Task G - IT Security and Privacy Awareness Training

(a) The Contractor must ensure that all Contractor personnel complete EPA-provided mandatory security and privacy training prior to gaining access to EPA information systems. Non-compliance may result in denial of system access.

(b) The Contractor must ensure that all Contractor personnel complete security and privacy refresher training on an annual basis. EPA will provide notification and instructions to the Contractor on completing this training.

(c) The Contractor must ensure that each Contractor employee review and sign the *EPA Rules of Behavior* pertaining to appropriate use of EPA information systems prior to gaining access to EPA information systems. The Contractor must also ensure that each Contractor employee reviews these *EPA Rules of Behavior* at least annually. EPA will provide notification to the Contractor when these reviews are required.

(d) The Contractor agrees to insert in each subcontract or consultant agreement placed hereunder, provisions which shall conform substantially to the language of this requirement, including this paragraph, unless otherwise authorized by the Contracting Officer.

Task H - Specialized Information Security Training for Staff with Significant Security Responsibilities

(a) The Contractor must ensure that Contractor personnel with significant information security responsibilities complete specialized information security training based on the requirements defined in the EPA role-based training program (*program provided after Contract award*). The objective of the information security role-based training is to develop an EPA information security workforce with a common understanding of the concepts, principles, and applications of information security to ensure the confidentiality, integrity and availability of EPA's information and information systems. The Contractor is required to report training completed to ensure competencies are addressed. The Contractor must ensure employee training hours are satisfied in accordance with EPA Security and Privacy Training Standards (*provided after Contract award*). The Contracting Officer's Representative (COR) will provide additional information for specialized information security training based on the requirements in paragraph (b).

(b) The following role-based requirements are provided:

[Program office adds role-based requirements; otherwise write "none" or "not applicable"]

(c) The Contractor must ensure that all IT and Information Security personnel receive the necessary technical (for example, operating system, network, security management, and system administration) and security training to carry out their duties and maintain certifications.

(d) The Contractor agrees to insert in each subcontract or consultant agreement placed hereunder,

Addendum: Cybersecurity Tasks Checklist

provisions which shall conform substantially to the language of this requirement, including this paragraph, unless otherwise authorized by the Contracting Officer.

Task I - Federal Reporting Requirements

(a) Contractors operating information systems on behalf of EPA must comply with Federal Information Security Modernization Act (FISMA) 44 USC Section 3541 reporting requirements. Annual and quarterly data collection will be coordinated by EPA. Contractors must provide EPA with the requested information based on the timeframes provided with each request. Contractor systems must comply with monthly data feed requirements as coordinated by EPA. Reporting requirements are determined by the Office of Management and Budget (OMB), and may change for each reporting period. The Contractor will provide the EPA Contracting Officer's Representative (COR) with all information to fully satisfy FISMA reporting requirements for Contractor systems.

(b) The Contractor agrees to insert in each subcontract or consultant agreement placed hereunder, provisions which shall conform substantially to the language of this requirement, including this paragraph, unless otherwise authorized by the Contracting Officer.

Task J - Protecting Sensitive Information

(a) *Definitions.*

(1) Sensitive Information.

As defined in National Institute of Standards and Technology Special Publication (NIST SP) 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*, Sensitive Information is any information where the loss, misuse or unauthorized access to, or modification of, could adversely affect the national interest or the conduct of federal programs, or the privacy to which individuals are entitled under 5 U.S.C. Section 552a (the Privacy Act), but that has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept classified in the interest of national defense or foreign policy. Sensitive Information is subject to stricter handling requirements than non-sensitive information because of the increased risk if the data are compromised. Some categories of Sensitive Information include Financial, Medical or Health, Legal, Strategic and Business, Human Resources, Personally Identifiable Information (PII), and Sensitive PII. These categories of information require appropriate protection as stand-alone information and may require additional protection in aggregate.

(2) Personally Identifiable Information (PII).

PII, as defined in OMB Memorandum M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*, refers to sensitive information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual. The definition of PII is not anchored to any single category of information or technology. Rather, it requires a case-by-case assessment made by the EPA Privacy Officer of the specific risk that an individual can be identified. Non-PII can become PII whenever additional information that is publicly available — in any medium and from any source — is or can be combined to identify an individual. As an example, PII includes a name and an address because it uniquely identifies an individual, but alone may not constitute Sensitive PII.

(3) Sensitive PII.

Addendum: Cybersecurity Tasks Checklist

Sensitive PII refers to personally identifiable information that can be used to target, harm, or coerce an individual or entity, assume or alter an individual's or entity's identity, or alter the outcome of an individual's or entity's activities. Sensitive PII requires stricter handling than PII because of the increased risk to an individual or associates if the information is compromised. Some categories of Sensitive PII include stand-alone information, such as Social Security numbers (SSN) or biometric identifiers. Other information such as a financial account, date of birth, maiden names, citizenship status, or medical information, in conjunction with the identity of an individual (directly or indirectly inferred), are also considered Sensitive PII. In addition, the context of the information may determine whether it is sensitive, such as a list of employees with poor performance ratings or a list of employees who have filed a grievance or complaint.

(b) Authorization to Use, Store, or Share Sensitive Information.

(1) Through the Contracting Officer, the Contractor must obtain written approval by the Chief Information Officer (CIO) or designee prior to the use or storage of EPA Sensitive Information, or sharing of EPA Sensitive Information by the Contractor with any subcontractor, person, or entity other than the EPA.

(2) The Contractor shall not remove Sensitive Information from approved location(s), electronic device(s), or other storage systems, without prior approval of the CIO or designee obtained through the Contracting Officer.

(c) Information Types. Sensitive Information includes PII, which in turn includes Sensitive PII. Therefore all requirements for Sensitive Information apply to PII and Sensitive PII, and all requirements for PII apply to Sensitive PII.

(d) Information Security Incidents. An *Information Security Incident* is an occurrence that results in actual or potential jeopardy to the confidentiality, integrity, or availability of an information system or the information the system processes, stores or transmits, or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies. The Contractor must report all known Information Security Incidents if they involve Sensitive Information.

(1) Information Security Reporting Requirements.

(i) The Contractor must report all Information Security Incidents and Privacy Breaches in accordance with the requirements below, even if it is believed the Incident may be limited, small, or insignificant. An information security report shall not, by itself, be interpreted as evidence that the Contractor has failed to provide adequate information security safeguards for Sensitive Information, or has otherwise failed to meet contract requirements.

(ii) The Contractor must report via email all Information Security Incidents and Privacy Breaches to the EPA Service Helpdesk immediately, but not later than 30 minutes, after becoming aware of the Incident. The Contractor shall email the EPA Service Helpdesk at CSIRC@epa.gov, and shall also email the Contracting Officer and Contracting Officer Representative (COR). If the Contractor fails to report in 30 minutes, specific Government remedies may include termination in accordance with EPA Requirement *Termination for Default – Failure to Report Information Security Incident*.

(iii) The types of information required in an Information Security Incident and Privacy Breach reports include: Contractor name and point-of-contact (POC) information, Contract number; the

Addendum: Cybersecurity Tasks Checklist

type, amount and description of information compromised; and incident details such as location, date, method of compromise, and impact, if known.

(iv) The Contractor shall not include any Sensitive Information in the subject or body of any e-mail. To transmit Sensitive Information, the Contractor shall use Federal Information Processing Standards (FIPS) 140-2 compliant encryption modules to protect Sensitive Information in attachments to email.

(v) If applicable, the Contractor must also provide supplemental information or reports related to a previously reported incident directly to the Contracting Officer, COR and EPA Service Helpdesk at CSIRC@epa.gov. The Contractor shall include any related ticket numbers in the subject line of the email.

(2) Information Security Incident Response Requirements.

(i) All determinations related to Information Security Incidents and Privacy Breaches, including response activities, notifications to affected individuals and related services (e.g., credit monitoring and identity protection) will be made in writing by authorized EPA officials at EPA's discretion and communicated by the Contracting Officer.

(ii) The Contractor must provide full access and cooperation for all activities determined by EPA to be required to ensure an effective Incident Response, including providing all requested images, log files, and event information to facilitate rapid resolution of Information Security Incidents. The Contractor shall maintain the capabilities to: determine what sensitive information was or could have been accessed and by whom, construct a timeline of user activity, determine methods or techniques used to access the information, identify the initial attack vector, and remediate and restore the protection of information. The Contractor is required to preserve all data, records, logs and other evidence that are reasonably necessary to conduct a thorough investigation of the Information Security Incident.

(iii) The Contractor is responsible for performing Incident and Privacy Breach Response activities required by EPA, including but not limited to inspections, investigations, forensic reviews, data analyses and processing by EPA and EPA OIG personnel and others on behalf of EPA. As requested by the Contracting Officer, the Contractor may provide technical support for the Government's final determinations of responsibility activities for the Incident and/or liability activities for any additional Incident Response activities (e.g., possible restitution calculation to affected individuals).

(iv) EPA, at its sole discretion, may obtain the assistance of Federal agencies and/or third-party firms to aid in Incident Response activities.

(v) The Contractor is responsible for all costs and related resource allocations required for all subsequent Incident Response activities determined to be required by EPA.

(e) Contractor Plan for Protection of Sensitive Information. The Contractor is responsible for the proper handling and protection of Sensitive Information to prevent unauthorized disclosure. Upon contract award, the Contractor shall develop and maintain a documentation plan addressing the following minimum requirements regarding the protection and handling of Sensitive Information:

(1) Proper marking, control, storage and handling of Sensitive Information residing on electronic media, including computers and removable media, and on paper documents.

Addendum: Cybersecurity Tasks Checklist

(2) Proper control and storage of mobile technology, portable data storage devices, and communication devices.

(3) Proper use of Federal Information Processing Standards (FIPS) 140-2 compliant encryption modules to protect Sensitive Information while at rest and in transit throughout EPA, Contractor, and/or subcontractor networks, and on host and client platforms.

(4) Proper use of FIPS 140-2 compliant encryption modules to protect Sensitive Information in email attachments, including policy that passwords must not be communicated in the same email as the attachment.

(5) Information Security Incidents. The Contractor shall report to the Government any security incident involving Personally Identifiable Information (PII) of which it becomes aware.

(6) Contractor Access to EPA IT Systems. The Contractor shall configure their network to support access to government systems (e.g., configure ports and protocols for access).

(a) Requirement for Business to Government (B2G) network connectivity. The Contractor will connect to the B2G gateway via a Contractor-procured Internet Service Provider (ISP) connection, and assume all responsibilities for establishing and maintaining their connectivity to the B2G gateway. This will include acquiring and maintaining the circuit to the B2G gateway, and acquiring a FIPS-140-2 Virtual Private Network (VPN)/Firewall device compatible with the Agency's VPN device. Maintenance and repair of contractor procured VPN equipment shall be the responsibility of the Contractor.

(b) Dial-Up ISP Connections are not acceptable.

(c) The Contractor must comply with the Agency's Guidance regarding allowable ports, protocols and risk mitigation strategies (e.g. File Transfer Protocol or Telnet).

(7) IT Security and Privacy Awareness Training. The Contractor must ensure annual security education, training, and awareness programs are conducted for their employees performing under the subject contract that addresses, at a minimum, physical security, acceptable use policies, malicious content and logic, and non-standard threats such as social engineering for their employees. The Contractor must also ensure employees performing under the subject contract receive the Agency's initial and annual information security awareness training.

(8) The Contractor must not conduct default installations of "out of the box" configurations of Commercially Off the Shelf (COTS) purchased products. The contractor shall configure COTS products in accordance with EPA, NIST, Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIGs) or Center for Internet Security (CIS) standards. Standards are listed in order of precedence for use. If standards do not exist from one of these sources, the contractor shall coordinate with EPA to develop a configuration.

(f) *Subcontract flowdown.* The Contractor agrees to insert in each subcontract or consultant agreement placed hereunder, provisions which shall conform substantially to the language of this requirement, including this paragraph, unless otherwise authorized by the Contracting Officer.

Task K - Security Assessment and Authorization (SA&A)

Addendum: Cybersecurity Tasks Checklist

- (a) The Contractor is required to undergo Security Assessment and Authorization (SA&A); i.e., the process by which a federal agency examines its information technology infrastructure and develops supporting evidence necessary for security assurance accreditation, prior to using information systems to access and/or store Government information, potentially including Sensitive Information. The Contractor's facilities must also meet the security requirements for "moderate confidentiality impact" as defined by the Federal Information Processing Standards (FIPS) 199 publication *Standards for Security Categorization of Federal Information and Information Systems*.
- (b) For all information systems that will input, store, process, and/or output Government information, the contractor shall obtain an Authorization to Operate (ATO) signed by the Chief Information Officer (CIO) from the Contracting Officer (working with the Contracting Officer's Representative (COR)) before using EPA information in the system. The contractor may be able to obtain an Authorization to Test from the SIO for the office obtaining services that will allow use of EPA information in certain circumstances to facilitate system development or implementation. Before a federal information system can be granted an ATO, it must be compliant with National Institute of Standard and Technology (NIST) SP 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*, and FIPS Publication 200, *Minimum Security Requirements for Federal Information and Information Systems*. Contractors whose internal information systems will process Sensitive Information incidental to Agency product or service development must meet requirements for NIST SP 800-171, *Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations* (instead of NIST SP 800-53) in order to be granted an ATO.
- (c) FIPS 199 moderate confidentiality impact must be utilized for Contractor information technology (IT) systems and security control baseline requirements.
- (d) Prior to Agency SA&A activities, the COR must complete a Privacy Threshold Analysis (PTA) for all IT systems. Then the COR must provide the completed PTA to the EPA Privacy Officer for a determination of whether a Privacy Impact Assessment (PIA) is required. If a determination is made that a PIA is required, it will be completed by EPA in accordance with EPA PIA Template instructions.
- (e) The Contractor is responsible for preparing SA&A documentation with the use of EPA tools and security documentation templates including System Security Plan, Security Assessment Report, Contingency Plan, and Incident Response Plan. The Contractor must follow federally mandated SA&A and Risk Management Framework (RMF) processes throughout the IT system lifecycle process to ensure proper oversight by EPA. RMF modifies the traditional Certification and Accreditation process and integrates information security and risk management activities into the system development life cycle.
- (f) The Contractor must submit SA&A documentation as defined in paragraph (e) to the COR at least 60 days before the ATO expiration date.
- (g) The Contractor shall fix or mitigate system or security vulnerabilities within a time frame commensurate with the level of risk (as identified by the EPA and Contractor) they present:
- High Risk = 2 business days from vulnerability notification from contractor
 - Moderate Risk = 7 business days from vulnerability notification from contractor
 - Low Risk = 30 business days from vulnerability notification from contractor
- (h) The Contractor agrees to insert in each subcontract or consultant agreement placed hereunder, provisions which shall conform substantially to the language of this requirement, including this paragraph, unless otherwise authorized by the Contracting Officer.

Addendum: Cybersecurity Tasks Checklist

Task L - Contractor System Oversight/Compliance

(a) Pursuant to National Institute of Standards and Technology Special Publication (NIST SP) 800-53 Rev 4, the EPA and GAO have the authority to conduct site reviews for compliance validation and will conduct security reviews on a periodic and event-driven basis for the life of the contract. Full cooperation by the Contractor is required for audits and forensics.

(b) The Contractor shall provide EPA access to the Contractor's facilities, installations, operations, documentation, databases, information technology (IT) systems and devices, and personnel used in performance of the contract, regardless of the location. The Contractor shall provide access to the extent required, in EPA's judgment, to conduct an inspection, evaluation, investigation or audit, including vulnerability testing to safeguard against threats and hazards to the integrity, availability and confidentiality of agency data or to the function of information technology systems operated on behalf of agency, and to preserve evidence of information security incidents. This information shall be available to the EPA upon request.

(c) All Contractor systems used in the performance of the contract must comply with Information Security Continuous Monitoring (ISCM) and Reporting as identified in OMB Memorandum M-14-03, *Enhancing the Security of Federal Information and Information Systems*. In addition, EPA reserves the right to perform ISCM and IT security scanning of Contractor systems with tools and infrastructure of EPA's choosing.

(d) All Contractor systems used in the performance of the contract must perform monthly vulnerability scanning as defined by EPA IT and Security Policy, and the Contractor must provide scanning reports to the Contracting Officer, who will forward them to the EPA CIO or designee on a monthly basis.

(e) All Contractor systems used in the performance of the contract must participate in the implementation of automated security controls testing mechanisms and provide automated test results in Security Compliant Automation Protocol (SCAP) compliant data to the Contracting Officer, who will forward to the EPA CIO or designee on a monthly basis.

(f) The Contractor agrees to insert in each subcontract or consultant agreement placed hereunder, provisions which shall conform substantially to the language of this requirement, including this paragraph, unless otherwise authorized by the Contracting Officer.

Task M - Contractor Access to EPA IT Systems

(a) Immediately following contract award, the Contractor shall provide to the Contracting Officer's Representative (COR) a complete list of Contractor employee names that require access to EPA information systems.

(b) The Contractor shall provide a Contractor employee change report by the fifth day of each month after contract award to the COR. The report shall contain the listing of all Contractor employees who separated or were hired under the contract in the past 60 days. This report shall be submitted even if no separations or hires have occurred during this period. Failure to submit a Contractor employee change report may, at the Government's discretion, result in the suspension of all network accounts associated with this contract. The format for this report will be provided by the COR.

(c) (1) The Contractor shall require each of its employees who will need system access for six months or less to utilize a Personal Identity Verification-Interoperable (PIV-I) card or equivalent, as determined by EPA, in order to access EPA information technology (IT) systems and Sensitive Information. The

Addendum: Cybersecurity Tasks Checklist

Contractor shall ensure that its employees will not share accounts to access EPA IT systems and Sensitive Information.

(2) The Contractor shall require each of its employees who will need system access for more than six months to utilize an HSPD-12 compliant Personal Identity Verification (PIV) card, such as the EPA EPASS card, in order to access EPA IT systems and Sensitive Information. The Contractor shall ensure that its employees complete a federal government-initiated background investigation as part of the PIV issuance process. The Contractor shall ensure that its employees will not share accounts to access EPA IT systems and Sensitive Information.

(d) EPA, at its discretion, may suspend or terminate Contractor access to any systems, information/data, and/or facilities when an Information Security Incident or other electronic access violation, use or misuse issue warrants such action. The suspension or termination shall last until EPA determines that the situation has been corrected or no longer exists. Upon request by EPA, the Contractor shall immediately return all EPA information/data, as well as any media type that houses or stores Government information.

(e) The Contractor shall notify the COR at least five days prior to a Contractor employee being removed from a contract (notification shall be at least 15 days for key personnel in accordance with requirement 1552.237-72, *Key Personnel*). For unplanned terminations or removals of Contractor employees from the Contractor organization that occur with less than five days notice, the Contractor shall notify the COR immediately. The Contractor shall ensure that HSPD-12/PIV cards issued to a Contractor's employee shall be returned to the COR prior to the employee's departure.

(f) The Contractor agrees to insert in each subcontract or consultant agreement placed hereunder, provisions which shall conform substantially to the language of this requirement, including this paragraph, unless otherwise authorized by the Contracting Officer.

Task N - Individual Notification for Personally Identifiable Information

(a) Definitions.

(1) *Information Security Incident* is an occurrence that results in actual or potential jeopardy to the confidentiality, integrity, or availability of an information system or the information the system processes, stores or transmits, or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.

(2) *Personally Identifiable Information (PII)*, as defined in OMB Memorandum M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*, refers to sensitive information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual. The definition of PII is not anchored to any single category of information or technology. Rather, it requires a case-by-case assessment made by the EPA Privacy Officer of the specific risk that an individual can be identified. Non-PII can become PII whenever additional information that is publicly available — in any medium and from any source — is or can be combined to identify an individual. As an example, PII includes a name and an address because it uniquely identifies an individual, but alone may not constitute Sensitive PII.

(3) *Sensitive PII* refers to personally identifiable information that can be used to target, harm, or coerce an individual or entity, assume or alter an individual's or entity's identity, or alter the outcome of an individual's or entity's activities. Sensitive PII requires stricter handling than PII because of the increased risk to an individual or associates if the information is compromised. Some categories of

Addendum: Cybersecurity Tasks Checklist

Sensitive PII include stand-alone information, such as Social Security numbers (SSN) or biometric identifiers. Other information such as a financial account, date of birth, maiden names, citizenship status, or medical information, in conjunction with the identity of an individual (directly or indirectly inferred), are also considered Sensitive PII. In addition, the context of the information may determine whether it is sensitive, such as a list of employees with poor performance ratings or a list of employees who have filed a grievance or complaint.

(b) The Contractor shall have in place procedures and the capability to notify any individual whose Personally Identifiable Information (PII) resided in the Contractor information technology (IT) system at the time of an Information Security Incident not later than five business days after being directed by the Contracting Officer to notify individuals, unless otherwise approved by the Contracting Officer. The procedures must be approved by the EPA prior to use. The method and content of any notification by the Contractor shall be coordinated with, and subject to prior written approval, by the Contracting Officer in consultation with authorized EPA officials at EPA's discretion. The Contractor shall not proceed with notification unless the Contracting Officer has determined in writing that notification is appropriate.

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

- (1) A brief description of the incident;
- (2) A description of the types of PII and Sensitive PII involved;
- (3) A statement as to whether the PII or Sensitive PII was encrypted or protected by other means;
- (4) Steps individuals may take to protect themselves;
- (5) What the Contractor and/or the Government are doing to investigate the incident, to mitigate the incident, and to protect against any future incidents; and
- (6) Information identifying who individuals may contact for additional information, including Contractor name and point of contact (POC) and contract number.

(d) The Contractor agrees to insert in each subcontract or consultant agreement placed hereunder, provisions which shall conform substantially to the language of this requirement, including this paragraph, unless otherwise authorized by the Contracting Officer.

Task O - Credit Monitoring and Identity Protection

(a) Definitions.

(1) *Information Security Incident* is an occurrence that results in actual or potential jeopardy to the confidentiality, integrity, or availability of an information system or the information the system processes, stores or transmits, or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.

(2) *Personally Identifiable Information (PII)*, as defined in OMB Memorandum M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*, refers to sensitive information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual. The definition of PII is not anchored to any single category of information or technology. Rather, it requires a case-by-case assessment made by the EPA Privacy Officer of the specific risk that an individual can be identified. Non-PII can become PII whenever additional information that is publicly available — in any medium and from any source — is or can be

Addendum: Cybersecurity Tasks Checklist

combined to identify an individual. As an example, PII includes a name and an address because it uniquely identifies an individual, but alone may not constitute Sensitive PII.

(3) *Sensitive PII* refers to personally identifiable information that can be used to target, harm, or coerce an individual or entity, assume or alter an individual's or entity's identity, or alter the outcome of an individual's or entity's activities. Sensitive PII requires stricter handling than PII because of the increased risk to an individual or associates if the information is compromised. Some categories of Sensitive PII include stand-alone information, such as Social Security numbers (SSN) or biometric identifiers. Other information such as a financial account, date of birth, maiden names, citizenship status, or medical information, in conjunction with the identity of an individual (directly or indirectly inferred), are also considered Sensitive PII. In addition, the context of the information may determine whether it is sensitive, such as a list of employees with poor performance ratings or a list of employees who have filed a grievance or complaint.

(b) *Credit Monitoring Requirements.* In the event that an Information Security Incident involves PII or Sensitive PII, the Contractor may be required to do the following tasks as directed by the Contracting Officer:

(1) Provide notification to affected individuals as described in the "Individual Notification for Personally Identifiable Information" requirement;

(2) Provide credit monitoring and identity protection services to individuals whose data was under the control of the Contractor or resided in the Contractor information technology (IT) system at the time of the Information Security Incident for a period beginning the date of the Incident and extending not less than 18 months from the date the individual is notified; and/or

(3) Use a dedicated call center; or establish one if necessary and as authorized in writing by the Contracting Officer. Call center services provided by the Contractor shall include:

(i) A dedicated telephone number for affected individuals to contact customer service within a fixed time period as determined by the Contracting Officer;

(ii) Information necessary for affected individuals to access credit reports and credit scores;

(iii) Weekly reports submitted to the Contracting Officer's Representative (COR) on call center volume, issue escalation (i.e., those calls that cannot be handled by call center staff and must be resolved by call center management or EPA, as appropriate), and other key metrics;

(iv) Escalation of calls that cannot be handled by call center staff to call center management or EPA for resolution, as appropriate;

(v) Preparation of customized frequently-asked-questions-and-answers (FAQs), in consultation as applicable with other parties like subject matter experts and CORs, and that must be approved in advance in writing by the Contracting Officer; and

(vi) Information for affected individuals to contact customer service representatives and fraud resolution representatives for credit monitoring and identity protection assistance.

(c) *Credit monitoring and identity protection services.* At a minimum, the Contractor shall provide the following credit monitoring and identity protection services:

Addendum: Cybersecurity Tasks Checklist

- (1) Triple credit bureau monitoring with Equifax, Experian and Transunion;
- (2) Daily customer service;
- (3) Alerts provided to the individual for changes in credit posture and fraud; and/or
- (4) Assistance to the individual with enrollment in the services and the use of fraud alerts.

(d) The Contractor agrees to insert in each subcontract or consultant agreement placed hereunder, provisions which shall conform substantially to the language of this requirement, including this paragraph, unless otherwise authorized by the Contracting Officer.

Task P - Compliance with IT Security Policies

(a) Information systems and system services provided to EPA by the Contractor must comply with current EPA information technology (IT), IT security, physical and personnel security and privacy policies and guidance, and EPA Acquisition Regulation 1552.211-79, *Compliance with EPA Policies for Information Resources Management*.

(b) Contractors are also required to comply with current Federal regulations and guidance found in the Federal Information Security Modernization Act (FISMA) of 2014, Privacy Act of 1974, E-Government Act of 2002, Federal Information Processing Standards (FIPS), the 500- and SP500- and 800-Series Special Publications (SP), Office of Management and Budget (OMB) memoranda and other relevant Federal laws and regulations that are applicable to EPA.

(c) The Contractor agrees to insert in each subcontract or consultant agreement placed hereunder, provisions which shall conform substantially to the language of this requirement, including this paragraph, unless otherwise authorized by the Contracting Officer.

Task Q - Secure Technical Implementation

(a) The Contractor shall use applications that are fully functional and operate correctly as intended on systems using the United States Government Configuration Baseline (USGCB).

(b) The Contractor's standard installation, operation, maintenance, updates, and/or patching of software must not alter the configuration settings from the approved USGCB configuration.

(c) Contractor applications designed for normal/regular, i.e., non-privileged end users must run in the standard user context without elevated system administration privileges.

(d) The Contractor shall apply due diligence at all times to ensure that Federal Information Processing Standard (FIPS) 199 "moderate confidentiality impact" security is always in place to protect EPA systems and information.

(e) The Contractor agrees to insert in each subcontract or consultant agreement placed hereunder, provisions which shall conform substantially to the language of this requirement, including this paragraph, unless otherwise authorized by the Contracting Officer.

Task R - Internet Protocol Version 6 (IPv6)

Addendum: Cybersecurity Tasks Checklist

- (a) In accordance with EPA technical standards, all system hardware, software, firmware, and/or networked component or service (voice, video, or data) utilized, developed, procured, acquired or delivered in support and/or performance of this contract shall be capable of transmitting, receiving, processing, forwarding, and/or storing digital information across system boundaries utilizing system packets that are formatted in accordance with commercial standards of Internet Protocol version 6 (IPv6) as set forth in the USGv6 Profile (NIST Special Publication 500-267) and corresponding declarations of conformance defined in the USGv6 Test Program. In addition, devices and systems shall maintain interoperability with IPv4 products.
- (b) Any IP product or system utilized, developed, acquired, produced or delivered must interoperate with both IPv6 and IPv4 systems and products, in an equivalent or better way than current IPv4 capabilities with regard to functionality, performance, management and security; and have available contractor/vendor IPv6 technical support for development and implementation and fielded product management.
- (c) As IPv6 evolves, the Contractor shall upgrade or provide an appropriate migration path for each item developed, delivered or utilized, at no additional cost to the Government. The Contractor shall retrofit all non-IPv6 capable equipment, as defined above, which is fielded under this contract with IPv6 capable equipment, at no additional cost to the Government.
- (d) The Contractor shall provide technical support for both IPv4 and IPv6.
- (e) All Contractor-provided system or software must be able to operate on networks supporting IPv4, IPv6, or one supporting both.
- (f) Any product whose non-compliance is discovered and made known to the Contractor within one year after acceptance shall be upgraded, modified, or replaced to bring it into compliance, at no additional cost to the Government.
- (g) EPA reserves the right to require the Contractor's products to be tested within an EPA or third-party test facility to demonstrate contract compliance.
- (h) In accordance with FAR 11.002(g), this acquisition must comply with the National Institute of Standards and Technology (NIST) US Government (USG) v6 Profile and IPv6 Test Program. The Contractor shall fund and provide resources necessary to support these testing requirements, and it will not be paid for as a direct cost under the subject contract.
- (i) The Contractor agrees to insert in each subcontract or consultant agreement placed hereunder, provisions which shall conform substantially to the language of this requirement, including this paragraph, unless otherwise authorized by the Contracting Officer.

Task S - Cloud Service Computing

- (a) The Contractor handling EPA information or operating information systems on behalf of EPA must protect EPA information and information systems against unauthorized access, use, disclosure, disruption, modification, or destruction per the Federal Information Security Modernization Act (FISMA) and EPA policy.
- (b) EPA information stored in a cloud environment remains the property of EPA, and not the Contractor or cloud service provider (CSP). The Contractor may also be the CSP. EPA retains ownership of the information and any media type that stores Government information.

Addendum: Cybersecurity Tasks Checklist

(c) In the event the Contractor is the CSP or can control the CSP through a subcontracting or other business relationship then the following requirements will apply:

(1) The CSP does not have rights to use the EPA information for any purposes other than those explicitly stated in the contract or applicable “Rights in Data” contract requirements.

(2) The CSP must protect EPA information from all unauthorized access.

(3) The CSP must allow EPA access to EPA information including data schemas, metadata, and other associated data artifacts that are required to ensure EPA can fully and appropriately retrieve EPA information from the cloud environment that can be stored, read, and processed.

(4) The CSP must have been evaluated by a Third Party Assessment Organization (3PAO) certified under the Federal Risk and Authorization Management Program (FedRAMP). The Contractor must provide the most current, and any subsequent, Security Assessment Reports to the Contracting Officer’s Representative (COR) for consideration by the Information Security Officer (ISO) as part of the Contractor’s overall Systems Security Plan.

(5) The Contractor must require the CSP to follow cloud computing contract best practices identified in “Creating Effective Cloud Computing Contracts for the Federal Government” produced by the Federal Chief Information Officer (CIO) Council and Federal Chief Acquisition Officers Council.

(d) The Contractor agrees to insert in each subcontract or consultant agreement placed hereunder, provisions which shall conform substantially to the language of this requirement, including this paragraph, unless otherwise authorized by the Contracting Officer.

Task T - Contract Performance Information and Testimony

(a) *Dissemination of Contract Performance Information.* The Contractor must not publish, permit to be published, or distribute to the public, any information, oral or written, concerning the results or conclusions made pursuant to the performance of this contract, without the prior written consent of the Contracting Officer. A copy of any material proposed to be published or distributed must be submitted to the Contracting Officer for written approval prior to publication.

(b) *Contractor Testimony.* All requests for the testimony of the Contractor or its employees, and any intention to testify as an expert witness relating to: (a) any work required by, and or performed under, this contract; or (b) any information provided by any party to assist the Contractor in the performance of this contract, must be immediately reported to the Contracting Officer.

(c) *Subcontract flowdown.* The Contractor agrees to insert in each subcontract or consultant agreement placed hereunder, provisions which shall conform substantially to the language of this requirement, including this paragraph, unless otherwise authorized by the Contracting Officer.

Task U - Rehabilitation Act Section 508 Standards

(a) All electronic and information technology (EIT) procured through this contract must meet the applicable accessibility standards at 36 CFR 1194, unless a FAR 39.204 exception to this requirement exists. 36 CFR 1194 implements Section 508 of the Rehabilitation Act of 1973, as amended, and is viewable at <http://www.access-board.gov/sec508/508standards.htm>.

Addendum: Cybersecurity Tasks Checklist

(b) The following standards are determined to be applicable to this contract:

- (1) 1194.21. Software applications and operating systems
- (2) 1194.22. Web-based intranet and Internet information and applications
- (3) 1194.23 Telecommunications products
- (4) 1194.24 Video and multimedia products
- (5) 1194.25 Self-contained, closed products
- (6) 1194.26 Desktop and portable computers
- (7) 1194.31 Functional performance criteria
- (8) 1194.41 Information, documentation, and support

(c) EPA is required by Section 508 of the Rehabilitation Act of 1973, as amended (29 U.S.C. 794d), to offer access to electronic and information technology for disabled individuals within its employment, and for disabled members of the public seeking information and services. This access must be comparable to that which is offered to similar individuals who do not have disabilities. Standards for complying with this law and any future updates are prescribed by the Architectural and Transportation Barriers Compliance Board ("The Access Board").

(d) Contractor deliverable(s) must comply with these standards.

(e) The final work product must include documentation that demonstrates or provides assurance that the deliverable conforms to the Section 508 Standards promulgated by the Access Board.

(f) In the event of a dispute between the Contractor and EPA, EPA's assessment of the Section 508 compliance will control and the Contractor will make any additional changes needed to conform with EPA's assessment, at no additional charge to EPA.

(g) The Contractor agrees to insert in each subcontract or consultant agreement placed hereunder, provisions which shall conform substantially to the language of this requirement, including this paragraph, unless otherwise authorized by the Contracting Officer.

Task V - Termination for Default - Failure to Report Information Security Incident

(a) *Definition.* *Information Security Incident* is an occurrence that results in actual or potential jeopardy to the confidentiality, integrity, or availability of an information system or the information the system processes, stores or transmits, or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.

(b) If the Contractor was aware of an Information Security Incident and did not disclose it in accordance with the requirements specified in this contract or misrepresented relevant information to the Contracting Officer, the Government may terminate the contract for default, debar the Contractor from Government contracting, or pursue such other remedies as may be permitted by law or this contract.

(c) The Contractor agrees to insert in each subcontract or consultant agreement placed hereunder, provisions which shall conform substantially to the language of this requirement, including this paragraph, unless otherwise authorized by the Contracting Officer.