INFORMATION TECHNOLOGY

CONTRACT CLAUSES

December 28, 2015

Contents

Introduction

This document has been prepared to detail the Information Technology (IT) requirements for contracts awarded by the Office of Personnel Management (OPM). These clauses have been developed with the entirety of the IT community in mind, including, and most prominently, the IT Security and Privacy communities.

The OPM Chief Information Officer (CIO) has compiled these IT requirements and formed them into clauses. Additionally, Appendix A provides guidance to Contracting personnel on the appropriate use of these clauses in various types of contracts that involve IT. Appendix B provides a list of deliverables associated with each clause, as applicable.

Information Technology Contract Clauses

1752.224-70 Definition of Terms (Dec 2015)

The following definitions apply to this contract:

a. Information: This term is synonymous with the term Data. Both terms refer to single or multiple instances of any recorded or communicated fact or opinion being stored or transferred in any digital or analog format or medium.

b. Controlled Unclassified Information (CUI): This term refers to that sub-category of Information where the loss, misuse, or unauthorized access or modification could adversely affect the national interest or the conduct of federal programs, or the privacy to which individuals are entitled under 5 USC Section 552a (the Privacy Act) 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.

c. Personally Identifiable Information (PII): This term refers to that sub-category of CUI 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.

d. Information System: This term refers to a system composed of people and equipment that processes or interprets Information.

e. Information Technology (IT) System: This term refers to that sub-category of Information System composed of hardware, software, data, and networks that processes or interprets Information.

f. Information Security Incident (ISI): This term refers to any event that includes the known, potential, or suspected exposure, loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or unauthorized access of any Contractor or Government Information or Information Systems**.**

g. Record:

(1) For the purpose of Records Management, this term refers to all recorded Information, regardless of form or characteristics, made or received by a Federal agency under Federal law or in connection with the transactions 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 US Government or because of the informational value of the data in them.

(2) For the purpose of the Privacy Act, this term refers to any item, collection, or grouping of Information about an individual that is maintained by an agency,

including, but not limited to, education, financial transactions, medical history, or criminal or employment history, and that contains the person's name, or the identifying number, symbol, or other identifier assigned to the individual, such as a fingerprint, voiceprint, or a photograph.

h. System of Records on individuals: This term refers to a group of any Records from which Information is retrieved by the name of the individual or by some identifying number, symbol, or other identifier assigned to the individual.

i. Operation of a System of Records: This term refers to the performance of any of the activities associated with maintaining the System of Records, including the collection, use, and dissemination of Records.

j. Privileged User: This term refers to a user that is assigned an organization-defined privileged role that allows that individual to perform certain security-relevant functions that ordinary users are not authorized to perform. These privileged roles include, but are not limited to, IT system development, key management, account management, network and system administration, database administration, and web administration.

(End of Clause)

1752.224-72 Access to Contractor Information Technology (IT) Systems (Dec 2015)

During the period of performance of the contract and throughout any contract close-out period, the Contractor must provide OPM, or its designate, with immediate access to all IT systems used by the Contractor to support the performance of the contract for the purpose of inspection and forensic analysis in the event of an Information Security Incident (ISI).

(End of Clause)

1752.224-73 Protecting Information (Dec 2015)

a. Applicability

(1) This clause applies to the Contractor, its subcontractors and teaming partners, and employees (hereafter referred to collectively as "Contractor").

(2) These requirements are applicable to all Information, regardless of medium, maintained by the Contractor for the performance of this contract.

(3) These requirements are in addition to all applicable requirements established by the Privacy Act of 1974 (5 U.S.C. 552a); and to all other requirements established by various Federal statutes, mandates, and Executive Orders for the management and security of Information and Information Systems. The following additional requirements should not be construed to alter or diminish civil and/or criminal liabilities provided under the Privacy Act or any other applicable Federal statutes.

b. Authorization to Handle Controlled Unclassified Information (CUI)

(1) Prior to receiving, collecting, transmitting, storing, using, accessing, sharing, or removing CUI from any approved locations; the Contractor must receive approval in writing from the Chief Information Officer (CIO) through the Contracting Officer (CO) or Contracting Officer's Representative (COR).

(2) If the Contractor should begin to receive, collect, transmit, store, use, access, or share CUI without appropriate approval, it should be reported as an Information Security Incident (ISI).

(3) Prior to removing CUI from any approved location, electronic device, removable media, or storage container, approval must be received in writing from the CO or COR.

c. Authorization to Use Information Technology (IT) Systems

(1) Prior to designing, developing, operating, accessing, or using an IT system that will store or process Information other than general information necessary to manage the contract (such as billing), the Contractor must receive approval in writing from the CIO through the CO or COR.

(2) The time required to obtain approval may be lengthy, and the Contractor should identify this requirement as soon as possible.

(3) If the Contractor should begin to operate, access, or use an IT system without appropriate approval, it must be reported as an ISI.

d. Retention of Authorizing Documentation

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

(End of Clause)

1752.224-74 Privacy Act (Dec 2015)

The following Federal Acquisition Regulation (FAR) clauses apply as prescribed within FAR 24.104 for solicitations and contracts, when the design, development, or operation of a system of records on individuals is required to accomplish an OPM function.

Additionally, in instances where the Contractor is required to access a system of records on individuals to accomplish an OPM function, the contractor is subject to the Privacy Act, Privacy Act Notification, and applicable agency regulations.

52.224-1 Privacy Act Notification

PRIVACY ACT NOTIFICATION (APR 1984)

The Contractor will be required to design, develop, or operate a system of records on individuals, to accomplish an agency function subject to the Privacy Act of 1974, Public Law 93-579, December 31, 1974 (5 U.S.C. 552a) and applicable agency regulations. Violation of the Act may involve the imposition of criminal penalties.

(End of clause)

52.224-2 Privacy Act

PRIVACY ACT (APR 1984)

(a) The Contractor agrees to—

(1) Comply with the Privacy Act of 1974 (the Act) and the agency rules and regulations issued under the Act in the design, development, or operation of any system of records on individuals to accomplish an agency function when the contract specifically identifies—

(i) The systems of records; and

(ii) The design, development, or operation work that the contractor is to perform;

(2) Include the Privacy Act notification contained in this contract in every solicitation and resulting subcontract and in every subcontract awarded without a solicitation, when the work statement in the proposed subcontract requires the redesign, development, or operation of a system of records on individuals that is subject to the Act; and

(3) Include this clause, including this paragraph (3), in all subcontracts awarded under this contract which requires the design, development, or operation of such a system of records.

(b) In the event of violations of the Act, a civil action may be brought against the agency involved when the violation concerns the design, development, or operation of a system of records on individuals to accomplish an agency function, and criminal penalties may be imposed upon the officers or employees of the agency when the violation concerns the operation of a system of records on individuals to accomplish an agency function. For purposes of the Act, when the contract is for the operation of a system of records on individuals to accomplish an agency function, the Contractor is considered to be an employee of the agency.

(c)(1) “Operation of a system of records,” as used in this clause, means performance of any of the activities associated with maintaining the system of records, including the collection, use, and dissemination of records.

(2) “Record,” as used in this clause, means any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, education, financial transactions, medical history, and criminal or employment history and that contains the person’s name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a fingerprint or voiceprint or a photograph.

(3) “System of records on individuals,” as used in this clause, means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual.

(End of clause)

(End of Clause)

1752.224-75 Information Protection Policies and Procedures (Dec 2015)

The Contractor must ensure its policies and procedures address compliance with all information protection requirements of this contract. The policies and procedures must address the following:

a. Proper identification, marking, control, storage, transmission, use, and handling of Controlled Unclassified Information (CUI), regardless of medium.
b. Proper control, storage, and protection of mobile devices, portable data storage devices, and communication devices containing CUI.
c. Proper use of FIPS 140-2 compliant encryption, redaction, and masking methods to protect CUI while at rest and in transit throughout contractor networks, and on host and client platforms.
d. Proper use of FIPS 140-2 compliant encryption methods to protect CUI transmitted in email attachments, including policy that passwords must not be communicated in the same email as the attachment.
e. Roles and responsibilities and proper actions to be taken during Information Security Incidents (ISIs).
f. Proper procedures for obtaining authorized access to information technology (IT) systems.
g. General IT security and protection training for all employees.
h. Specialized IT security and protection training for IT security staff.
i. Information Systems policy compliance requirements and procedures.

This is not an all-inclusive list and may include additional requirements which the contractor shall address during performance.

(End of Clause)

1752.224-76 Compliance with Information Protection Requirements (Dec 2015)

The Chief Information Officer, through the Contracting Officer or Contracting Officer's Representative, reserves the right to verify compliance with information security requirements established by this contract. Verification may include, but is not limited to, onsite or offsite inspections, documentation reviews, process observation, network and IT system scanning. The Contractor will fully comply with all OPM-initiated inspections as permissible by law.

(End of Clause)

1752.224-77 Information Security Incidents (ISI) (Dec 2015)

a. ISI Reporting Activities

(1) Contractors must report any and all ISI involving OPM Information to the OPM Security Monitoring Center (SMC) at CyberSolutions@opm.gov, 844-377-6109. The SMC is available 24 hours per day, 365 days per year.

(2) Contractors must report any and all ISI involving information technology (IT) systems and Controlled Unclassified Information (CUI) immediately upon becoming aware of the ISI but no later than 30 minutes after becoming aware of the ISI, regardless of day or time; regardless of internal investigation, evaluation, or confirmation of procedures or activities; and regardless of whether the ISI is suspected, known, or determined to involve IT systems operated in support of this contract.

(3) Contractors reporting an ISI to the SMC by email or phone must copy the Contracting Officer (CO) or Contracting Officer's Representative (COR) if possible; but if not, must notify the CO or COR immediately after reporting to the SMC.

(4) When reporting an ISI to the SMC by email:

(a) Do not include any CUI in the subject or body of any email;

(b) Use FIPS 140-2 compliant encryption methods to protect CUI to be included as an email attachment, and do not include passwords in the same email as the encrypted attachment; and

(c) Provide any supplementary information or reports related to a previously reported incident directly to the OPM SMC with the following text in the subject line of the email: "Supplementary Information / Report related to previously reported incident # [insert number]."

b. ISI Review and Response Activities

(1) The Contractor must provide full access and cooperation for all activities determined by CO or COR to be required to ensure an effective review and response to protect OPM's Information and Information Systems operated in support of this contract.

(2) The Contractor must promptly respond to all requests by the CO or COR for ISI and system-related information, including but not limited to disk images, log files, event information, and any other information determined by OPM to be required for a rapid but comprehensive technical and forensic review.

(3) OPM, at its sole discretion, may obtain the assistance of Federal agencies and/or third party firms to aid in ISI Review and Response activities.

c. ISI Determination Activities

(1) The Contractor must not make any determinations related to an ISI associated with Information Systems or Information maintained by the Contractor in support of the activities authorized by this contract, including determinations related to notification of affected individuals and/or Federal agencies (except reporting criminal activity to Law Enforcement Organizations) and offering of services, such as credit monitoring.

(2) The Contractor must not conduct any internal ISI-related review or response activities that could modify or eliminate any existing technical configuration or information or forensic technical evidence existing at the time of the ISI without approval from the OPM Chief Information Officer (CIO) through the CO or COR.

(3) All determinations related to an ISI associated with Information Systems or Information maintained by the Contractor in support of the activities authorized by this contract will be made only by the OPM CIO through the CO or COR.

(4) The Contractor must report criminal activity to Law Enforcement Organizations upon becoming aware of such activity.

(End of Clause)

1752.224-78 Information Security Inspections (Dec 2015)

a. The Contractor must permit and cooperate with any mutually agreed upon pre-scheduled onsite or offsite information security inspections, such as:

(1) Before initiation of the performance period;
(2) As periodically scheduled for contract oversight and compliance purposes;
(3) As determined by the OPM Chief Information Officer (CIO) through the Contracting Officer (CO) or Contracting Officer's Representative (COR) to be required for evaluation of or in response to any reported Information Security Incident (ISI); or
(4) As determined by the OPM CIO through the CO or COR to be required to address any risk of non-compliance with the requirements of this contract.

b. OPM will provide the Contractor with a Post-Inspection Report, which will state findings and specify the Contractor's requirement for remediating findings to maintain compliance with this contract.

c. The Contractor must provide a formal response to the OPM Post-Inspection Report within fifteen (15) days of receipt of the report for critical/high risk findings and within thirty (30 days for all other findings.

(End of Clause)

1752.224-79 Suspension of Contract for Security Concerns (Dec 2015)

If at any time during Contract performance it is determined that the Contractor is not in full compliance with the security requirements of this Contract, the Government may immediately suspend performance under this Contract and require the immediate return of all Controlled Unclassified Information (CUI) materials and information to the Government at full Contractor expense. Any work suspension resulting from a security lapse will not be subject to equitable adjustment; all costs incurred will be borne by the Contractor.

(End of Clause)

1752.239-70 Internet Protocol Version 6 (IPV6) Compliance (Dec 2015)

All information technology (IT) functionality, capabilities, and features must be supported and operational in both a dual-stack IPv4/IPv6 environment and an IPv6 only environment. Furthermore, all management, user interfaces, configuration options, reports, and other administrative capabilities that support IPv4 functionality will support comparable IPv6 functionality. The Contractor is required to certify that its products have been tested to meet the requirements for both a dual-stack IPv4/IPv6 and IPv6 only environment. The Contracting Officer (CO) or Contracting Officer's Representative (COR) reserves the right to require the Contractor's products to be tested within an OPM or third party test facility to show compliance with this requirement. All costs and resource allocations required for this third party service must be the sole responsibility of the Contractor. Compliance certification shall be provided in writing to the CO or COR.

(End of Clause)

1752.239-72 Access to OPM Information Technology (IT) Systems (Dec 2015)

a. The Contractor must provide to the distribution list "System Access Control" (systemaccesscontrol@opm.gov) an initial and complete list of employee names that require access to OPM IT systems. This list will be provided at least five (5) days prior to required access.

b. The Contractor must send a staffing change report by the fifth day of each month after contract award to the Contracting Officer (CO), Contracting Officer's Representative (COR), and systemaccesscontrol@opm.gov. The report must contain the listing of all staff members who separated or were hired under this contract in the past 60 days. This form must be submitted even if no separations or hires have occurred during this period. Failure to submit a 'Contractor Staffing Change Report' each month may, at the Government's discretion, result in the suspension of all accounts associated with this contract.

c. Each contractor employee is required to utilize a Personal Identity Verification (PIV) card to access OPM IT systems and Controlled Unclassified Information (CUI), in accordance with the National Institutes of Standards and Technology (NIST) Federal Information Processing Standard (FIPS) 201. Using shared accounts to access OPM IT systems and CUI is strictly prohibited. OPM will disable accounts, and access to OPM IT systems will be revoked and denied if contractor employees share accounts. Users of the IT systems will be subject to periodic auditing to ensure compliance with OPM policies.

d. OPM, at its discretion, may suspend or terminate the access to any IT systems and/or facilities when an Information Security Incident (ISI) or other electronic access violation, use or misuse issue gives cause for such action. The suspension or termination may last until such time as the CO or COR determines that the situation has been corrected or no longer exists.

e. Upon request of the CO or COR, the Contractor must immediately return all Government Information, as well as any media type that houses or stores Government Information, regardless of potential violations of other contracts the contractor may have in place, including, but not limited to, data stored on recovery media, tape backups, and images.

f. The CO, COR and the OPM Helpdesk (helpdesk@opm.gov or 202-606-4927) must be notified at least five (5) days prior to a contractor employee being removed from a contract. For unplanned terminations or removals of contractor employees from the contractor organization, the CO, COR and OPM Helpdesk must be notified immediately. OPM PIV cards issued to Contractor employees must be returned to the COR within two (2) days of departure of a Contractor employee.

(End of Clause)

1752.239-73 Section 508 Standards (Dec 2015)

a. All information technology (IT) procured through this contract must meet the applicable accessibility standards at 36 CFR 1194, unless an OPM 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.

b. The following standards have been 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. OPM is required by Section 508 of the Rehabilitation Act of 1973, as amended (29 U.S.C. 794d), to offer access to IT 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 are prescribed by the Architectural and Transportation Barriers Compliance Board ("The Access Board").

d. The final work product must include documentation that the deliverable conforms to the Section 508 Standards promulgated by the US Access Board.

e. OPM's assessment of the Section 508 compliance will control. In the event that additional changes are needed to conform with OPM's assessment, the Contractor shall make these changes at no additional charge to OPM.

(End of Clause)

1752.239-75 Information System Security Requirements (Dec 2015)

a. The activities required by this contract necessitate the Contractor's access to Government Information, including Controlled Unclassified Information (CUI). Contractors are required to comply with current Federal regulations and guidance found in the Federal Information Security Modernization Act (FISMA); Privacy Act of 1974; E-Government Act of 2002, Section 208; National Institute of Standards and Technology (NIST); Federal Information Processing Standards (FIPS); Office of Management and Budget (OMB) memorandums; and other relevant Federal laws and regulations with which OPM must comply.

b. The Contractor shall comply with implementation of required security controls for protection of the Government Information based on the sensitivity of the data within the system as outlined by Federal regulatory requirements, including but not limited to, Health Insurance Portability and Accountability Act (HIPAA), IRS 1075 for federal tax information, Executive Order 13556 for Controlled Unclassified Information (CUI) and any additional regulatory requirements.

c. The Contractor shall implement and maintain an Information security program that is compliant with FISMA, NIST Special Publications, OMB guidelines, OPM security policies, and other applicable laws, throughout the performance of this contract.

d. The Contractor facilities and IT systems shall meet the security requirements for the same impact level or greater as defined by the FIPS 199 as required for the protection of Government Information. The OPM Chief Information Officer, through the Contracting Officer or Contracting Officer's Representative shall provide written approval of the FIPS 199 security categorization.

(End of Clause)

1752.239-76 Security Assessment and Authorization (SA&A) (Dec 2015)

a. This contract requires the Contractor to develop, deploy, and/or use information technology (IT) systems to access and/or store Government Information, including Controlled Unclassified Information (CUI).

b. All IT systems that input, store, process, and/or output Government Information must be provided an Authority to Operate (ATO) signed by the Contractor Chief Information Officer (CIO) or higher level executive prior to operation of the IT system. The Contractor must complete the SA&A process independently of OPM, including the selection and funding of an approved Federal Risk and Authorization Management Program (FEDRAMP) Third-Party Assessor Organization (3PAO) to validate the security and privacy controls in place for the systems and the overall accuracy of SA&A packages.

c. The Contractor must submit to the OPM Chief Information Officer (CIO), through the Contracting Officer (CO) or Contracting Officer's Representative (COR) the signed SA&A package, along with the security assessment report and supporting documentation such as system and configuration scans from the 3PAO at least sixty (60) days prior to operation of the IT system for review and authorization by the OPM Authorizing Officials (AOs), through the CO or COR. Should the AOs not consider the signed package to meet OPM SA&A requirements for any reason, the AOs retain the right to not issue an ATO for the system. Should the AOs consider it possible for the Contractor to improve the compliance of the A&A package, the CO or COR may provide general or detailed information to the Contractor for possible modification to the package to improve compliance and resubmission to the CO or COR after modification. The CO or COR reserves the right to limit the number of re-submissions of a modified package before a final determination that a resubmitted package will not receive an ATO and no further resubmissions will be accepted. This may be grounds for contract termination. The OPM CIO is the final authority on the compliance of a submitted package with OPM SA&A requirements.

d. The Contractor Security Assessment and Authorization (SA&A) SA&A documentation package must be developed with the use of OPM Security Assessment and Authorization (SA&A) documentation templates in accordance with the OPM Security Assessment and Authorization policy based on the most current NIST Risk Management Framework (RMF), as adapted for Contractor IT systems supporting OPM. Templates are available for all required security documentation including, but not limited to, the System Security Plan, the Security Assessment Plan, the Security Assessment Report, Contingency Plan and Incident Response Plan. The SA&A process must be followed throughout the IT system lifecycle process to ensure proper oversight by OPM.

e. The IT systems must meet the security requirements for the same impact level or greater as defined by the Federal Information Process Standard (FIPS) 199 for the Information being accessed. The OPM CIO, through the CO or COR, must provide written approval of the FIPS 199 security categorization.

f. The Contractor shall complete a Privacy Threshold Analysis (PTA) for all systems as a requirement for an ATO. Based on the PTA, the OPM Chief Privacy Officer will determine whether a Privacy Impact Assessment (PIA) is required to be completed by the Contractor as part of the SA&A package.

g. The Contractor must submit an updated SA&A package, along with the 3PAO report, and supporting documentation to the CO or COR at least 90 days before the expiration of an existing ATO for security review and verification of security controls. Security reviews may include onsite visits that involve physical or logical inspection of the Contractor environment and IT systems.

h. The Contractor must ensure a plan of action and milestones (POA&M) is generated for each security finding and is remediated within a time frame commensurate with the level of risk, as follows, or as otherwise negotiated and approved in writing by the OPM CIO, through the CO or COR:

(1) High Risk = 30 days;
(2) Moderate Risk = 90 days; and
(3) Low Risk = 120 days.

(End of Clause)

1752.239-77 Federal Reporting Requirements (Dec 2015)

The Contractor must comply with both OPM IT Security policies and OPM's continuous monitoring reporting requirements as required by the Federal Information Security Modernization Act (FISMA). The Contractor must provide OPM with the requested information within the timeframes provided for each request. Failure to do so may result in the loss of OPM's authorization to receive and process sensitive information or operate an IT system containing sensitive information. Reporting requirements may change each reporting period.

(End of Clause)

1752.239-78 Cloud Computing (Dec 2015)

a. Prior to using any commercial Cloud Service Provider (CSP), the Contractor shall obtain approval from the Chief Information Officer (CIO), through the Contracting Officer (CO) or Contracting Officer's Representative (COR).

b. Information stored in a cloud environment remains the sole property of OPM, not the Contractor or the CSP.

c. The CSP must provide all the protections levied on the Contractor, and must be held accountable for all other requirements for IT systems and CUI, unless waived in writing by the OPM CIO, through the CO or COR.

d. The CSP must allow the OPM CIO, through the CO or COR, access to OPM Information including data schemas, meta data, and other associated data artifacts that are required to ensure OPM can fully and appropriately retrieve OPM Information from the CSP.

e. The CSP, and any subcontractor or teaming partner CSPs, must be evaluated by a Federal Risk and Authorization Management Program (FEDRAMP) Third Party Assessment Organization (3PAO). The contractor is responsible for the selection and funding of the 3PAO. The most current, and any subsequent, security assessment reports must be made available to the CIO, through the CO or COR, for consideration, including the CSP's Systems Security Plan, as part of the Contractor's Systems Security Plan.

(End of Clause)

1752.239-80 Information Technology (IT) Security and Privacy Awareness Training (Dec 2015)

a. The Contractor must ensure that all Contractor employees complete OPM-provided mandatory security and privacy training prior to gaining access to OPM IT systems and periodically thereafter based on OPM policy requirements. OPM will provide notification and instructions for completing this training. Non-compliance shall result in revocation of system access.

b. With written permission and justification from the Chief Information Officer, through the Contracting Officer or Contracting Officer's Representative, in lieu of the OPM-provided training, the Contractor may provide its own continuous training and awareness for Contract employees. All costs and resource allocations required must be the sole responsibility of the Contractor. Evidence of training for contractor employees shall be provided to OPM upon request.

(End of Clause)

1752.239-81 Specialized IT Security Awareness Training (Dec 2015)

a. Contractor personnel performing work related to IT security are required to complete specialized IT security training based on the role-based requirements listed below every fiscal year within the contract period of performance. The Contractor must certify to the Contracting Officer or Contracting Officer's Representative (COR) that IT security personnel have completed the requisite training hours satisfying the below training requirements.

IT Security Roles/Functions	Minimum Hours Required for Specialized Training
• Contractor System Manager\Owner	5
• Information Security Specialist • Information System Security Officer (ISSO)	20
• Privacy Officer	5
• System Administrator • Network Administrator • Database Administrator • Service Desk Personnel/Helpdesk • Programmer/Developer	10
• Other IT Personnel with security responsibilities	2

b. The Information System Security Officer (ISSO) and Information Security Specialists must be a Certified Information Systems Security Professional **(**CISSP**)** within 6 months of contract award and maintain certification throughout the period of performance, which will serve to fulfill the requirement for specialized training.

(End of Clause)

1752.239-82 HSPD-12 Compliance (Dec 2015)

a. All Contactor employees must consent to screening and sign an access agreement prior to being authorized access to Government IT systems or Controlled Unclassified Information (CUI); and rescreening according to change in position risk designation or other requirements according to HSPD-12 requirements.

b. The Contracting Officer (CO) or Contracting Officer's Representative (COR) approval is required prior to contractor personnel accessing OPM IT systems and CUI.

c. Procurements for services and products involving facility or system access control must be in accordance with HSPD-12 policy and other applicable Federal regulations.

d. All IT systems must enforce the use of Personal Identity Verification (PIV) credentials, in accordance with the National Institute of Standards and Technology (NIST) Federal Information Processing Standards (FIPS) 201. Development and test IT systems may be approved to use alternate 2-factor authentication, such as tokens, with the written approval of the OPM Chief Information Officer, through the CO or COR, prior to implementation.

(End of Clause)

1752.239-83 Secure Technical Implementation (Dec 2015)

a. The Contractor must certify applications are fully functional and operate correctly as intended on systems using the Federal Desktop Core Configuration (FDCC)\United States Government Configuration Baseline (USGCB).

b. The standard installation, operation, maintenance, updates, and/or patching of software must not alter the configuration settings from the approved FDCC\USGCB configuration.

c. Applications designed for normal end users must run in the standard user context without elevated system administration privileges.

d. The Contractor must apply due diligence at all times to ensure that the required level of security is always in place to protect OPM systems and information, such as using Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIG). The Contracting Officer or Contracting Officer's Representative (COR) reserves the right to verify compliance.

(End of Clause)

1752.239-84 Data Protection Requirements (Dec 2015)

a. Controlled Unclassified Information (CUI) shall be encrypted in transit and at rest using Federal Information Process Standard (FIPS) 140 and validated by the Cryptographic Module Validation Program (CMVP).

b. The Contractor must provide the validation certificate number to the Contracting Officer or Contracting Officer's Representative (COR) for verification. This shall occur prior to award and upon any changes to the cryptographic module. This shall only occur for the cryptographic modules.

c. The Contractor shall redact or mask all CUI that is not essential to users, including privileged users.

(End of Clause)

1752.239-85 Security Monitoring and Alerting Requirements (Dec 2015)

All contractor-operated systems that use or store OPM Information must meet or exceed OPM IT Security policy requirements pertaining to security monitoring and alerting. The minimum requirements are listed further below:

a. System and Network Visibility and Policy Enforcement at the following levels:

(1) Edge
(2) Server / Host
(3) Workstation / Laptop / Client
(4) Network
(5) Application
(6) Database
(7) Storage
(8) User

b. Alerting and Monitoring

c. System, User, and Data Segmentation

(End of Clause)

1752.239-86 Contractor Information Technology (IT) System Oversight / Compliance (Dec 2015)

a. The Contractor must support OPM in its efforts to assess and monitor the IT systems and infrastructure used in support of the performance of this contract. The Contractor must provide logical and physical access to the Contractor's facilities, installations, technical capabilities, operations, documentation, records, devices, applications and databases used in performance of the contract, regardless of location, upon Agency request. The Contractor will be expected to perform automated scans and continuous monitoring activities which may include, but will not limited be to, authenticated and unauthenticated scans of networks, operating systems, applications, and databases and provide the results of the scans to the Contracting Officer's Representative (COR), or allow the COR to run the scans directly.

b. All Contractor systems must participate in the OPM Information Security Continuous Monitoring (ISCM) program utilizing the OPM Information Security Continuous Monitoring Plan for security control monitoring and must submit to the COR, the report on security control monitoring as required following the OPM Information Security Continuous Monitoring Reporting template as defined in the OPM IT Security Policy.

c. All Contractor systems must perform vulnerability scanning as defined by OPM IT Security continuous monitoring program and will provide requested vulnerability scanning reports to the COR in accordance with OPM's continuous monitoring program plan.

d. All Contractor systems 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 COR in accordance with OPM's continuous monitoring program.

(End of Clause)

1752.242-71 Return of OPM and OPM-Activity-Related Information (Dec 2015)

a. Within thirty (30) days after the end of the contract performance period or after the contract is suspended or terminated by the Contracting Officer, unless otherwise instructed by the Contracting Officer, the Contractor must return all original OPM-provided and OPM-Activity-Related Information, such as records, files, and metadata in electronic or hardcopy format, including but not limited to the following:

(1) provided by OPM;
(2) obtained by the Contractor while conducting activities in accordance with the contract with OPM;
(3) distributed for any purpose by the Contractor to any other related organization and/or any other component or separate business entity; or
(4) received from the Contractor by any other related organization and/or any other component or separate business entity.

b. Within forty-five (45) days after the end of the contract performance period or after the contract is suspended or terminated by the Contracting Officer, unless otherwise instructed by the Contracting Officer, the Contractor must provide the Contracting Officer and COR with an associated Certification of Verified Return of all original OPM and OPM-Activity-Related Information, such as records, files, and metadata in electronic or hardcopy format, including but not limited to the following:

(1) provided by OPM;
(2) obtained by the Contractor while conducting activities in accordance with the contract with OPM;
(3) distributed for any purpose by the Contractor to any other related organization and/or any other component or separate business entity; or
(4) received from the Contractor by any other related organization and/or any other component or separate business entity.

(End of Clause)

1752.242-72 Secure Destruction of All OPM and OPM-Activity-Related Information (Dec 2015)

a. Within sixty (60) days after the end of the contract performance period or after the contract is suspended or terminated by the Contracting Officer, BUT ONLY after the Contracting Officer (CO) or Contracting Officer's Representative (COR) has accepted and approved the Contractor's compliance with the Certification of Verified Return, the Contractor must execute secure destruction of all copies of all OPM and OPM-activity-related files and information (including but not limited to all records, files, and metadata in electronic or hardcopy format) not returned to OPM and held in possession by the Contractor, by procedures approved by the CO or COR in advance and in accordance with applicable OPM IT Security Policy Requirements, including but not limited to the following:

(1) provided by OPM;
(2) obtained by the Contractor while conducting activities in accordance with the contract;
(3) distributed for any purpose by the Contractor to any other related organization and/or any other component or separate business entity; or
(4) received from the Contractor by any other related organization and/or any other component or separate business entity.

b. Within seventy-five (75) days after the end of the contract performance period or after the contract is suspended or terminated by the CO, BUT ONLY after the CO or COR has accepted and approved the Contractor's compliance with the Certification of Verified Return, the Contractor must provide the CO or COR with Certification of Secure Destruction of all existing active and archived originals and/or copies of all OPM and OPM-activity-related files and information, (including but not limited to all records, files, and metadata in electronic or hardcopy format); by procedures approved by OPM in advance and in accordance with applicable OPM IT Security Policy Requirements; including but not limited to the following:

(1) provided by OPM;
(2) obtained by the Contractor while conducting activities in accordance with the contract;
(3) distributed for any purpose by the Contractor to any other related organization and/or any other component or separate business entity; or
(4) received from the Contractor by any other related organization and/or any other component or separate business entity.

(End of Clause)

1752.242-73 Mandatory Requirement for Contractor Return of all OPM-Owned and Leased Computing and Information Storage Equipment (Dec 2015)

a. Within sixty (60) days after the end of the contract performance period or after the contract is suspended or terminated by the Contracting Officer, or within a time period approved by the Contracting Officer or Contracting Officer's Representative (COR), the Contractor must return all OPM-owned and leased computing and information storage equipment.

b. Within seventy-five (75) days after the end of the contract performance period or after the contract is suspended or terminated by the Contracting Officer, the Contractor must provide OPM with Certified Verification of Return of all OPM-Owned and Leased Computing and Information Storage Equipment.

(End of Clause)

APPENDIX A: Information Technology Contract Clause Usage Guidance

The table below provides guidance on using the IT contract clauses in specific situations. There are five basic contracting situations that require the use of IT contract clauses. Each is discussed below.

All OPM Contracts: These clauses ensure the Contractor understands it is NOT authorized to perform IT work, use IT systems (other than for administrative purposes, such as billing), or use CUI, unless expressly permitted. They also require the Contractor reports any unauthorized use of IT or access to CUI as an ISI.

Contracts that Use CUI: These clauses authorize a Contractor to handle CUI. Unless other clauses are included which cover IT systems, the CUI must be in paper form only. The clauses for these contracts ensure the protection of CUI and require the Contractor to report any loss of CUI as an ISI.

Contracts that Use Contractor IT Systems: These clauses authorize the Contractor to use its own IT systems to perform the work required by the contract where the type of information to be processed using the IT systems is more significant than general administrative information, such as billing. These clauses ensure the Contractor's IT systems meet the Government's requirements for protection of Government Information.

Contracts that Use Government IT Systems: These clauses authorize the Contractor to use Government IT systems to perform the work required by the contract. They ensure the Contractor understands its responsibilities for accessing Government IT systems.

Contracts that Design or Develop IT Systems: These clauses authorize the Contractor to design, develop, and deliver IT systems to the Government, including software and hardware deliverables. They ensure these deliverables meet Government requirements for IT systems, including technical specifications and operational requirements.

Contract Clause	Contract Clause Title	All OPM Contracts	Contracts that Use CUI	Contracts that Use Contractor IT Systems	Contracts that Use Government IT Systems	Contracts that Design or Develop IT Systems
1752.224-70	Definition of Terms (Dec 2015)	X				
1752.224-73	Protecting Information (Dec 2015)	X				
1752.224-72	Access to Contractor Information Technology (IT) Systems (Dec 2015)			X		
1752.224-74	Privacy Act (Dec 2015)		X	X	X	X
1752.224-75	Information Protection Policies and Procedures (Dec 2015)		X	X	X	X
1752.224-76	Compliance with Information Protection Requirements (Dec 2015)		X	X	X	X
1752.224-77	Information Security Incidents (ISI) (Dec 2015)	X				
1752.224-78	Information Security Inspections (Dec 2015)	X				
1752.224-79	Suspension of Contract for Security Concerns	X				
1752.239-70	Internet Protocol Version 6 (IPV6) Compliance (Dec 2015)					X
1752.239-72	Access to OPM Information Technology (IT) Systems (Dec 2015)				X	X
1752.239-73	Section 508 Standards (Dec 2015)					X

Contract Clause	Contract Clause Title	All OPM Contracts	Contracts that Use CUI	Contracts that Use Contractor IT Systems	Contracts that Use Government IT Systems	Contracts that Design or Develop IT Systems
1752.239-75	Information System Security Requirements (Dec 2015)			**X**	**X**	
1752.239-76	Security Assessment and Authorization (SA&A) (Dec 2015)			**X**		**X**
1752.239-77	Federal Reporting Requirements (Dec 2015)			**X**	**X**	
1752.239-78	Cloud Computing (Dec 2015)			**X**		**X**
1752.239-80	Information Technology (IT) Security and Privacy Awareness Training (Dec 2015)		**X**	**X**	**X**	**X**
1752.239-81	Specialized IT Security Awareness Training (Dec 2015)			**X**	**X**	**X**
1752.239-82	HSPD-12 Compliance (Dec 2015)		**X**	**X**	**X**	**X**
1752.239-83	Secure Technical Implementation (Dec 2015)			**X**	**X**	**X**
1752.239-84	Data Protection Requirements (Dec 2015)		**X**	**X**	**X**	**X**
1752.239-85	Security Monitoring and Alerting Requirements (Dec 2015)			**X**		**X**
1752.239-86	Contractor Information Technology (IT) System Oversight / Compliance (Dec 2015)			**X**	**X**	**X**
1752.242-71	Return of OPM and OPM-Activity-Related Information (Dec 2015)	**X**				
1752.242-72	Secure Destruction of All OPM and OPM-Activity-Related Information (Dec 2015)	**X**				
1752.242-73	Mandatory Requirement for Contractor Return of all OPM-Owned and Leased Computing and Information Storage Equipment (Dec 2015)		**X**	**X**	**X**	**X**

APPENDIX B: Information Technology Contract Clause Deliverables

The below Deliverables Table shall be incorporated into the master deliverable table of the contract as applicable.

Deliverables associated with each contract clause are identified in the table below.

Contract Clause	Contract Clause Title	Deliverable(s)
1752.224-70	Definition of Terms (Dec 2015)	None
1752.224-72	Access to Contractor Information Technology (IT) Systems (Dec 2015)	None
1752.224-73	Protecting Information (Dec 2015)	None
1752.224-74	Privacy Act (Dec 2015)	None
1752.224-75	Information Protection Policies and Procedures (Dec 2015)	None
1752.224-76	Documentation of Compliance with Information Protection Requirements (Dec 2015)	None
1752.224-77	Information Security Incidents (ISI) (Dec 2015)	The Contractor must report all security incidents to the SMC immediately upon becoming aware of the ISI but no later than thirty (30) minutes after becoming aware of the ISI.
1752.224-78	Information Security Inspections (Dec 2015)	The Contractor must provide a formal response to the OPM Post-Inspection Report within fifteen (15) days of receipt of the report for critical/high risk findings and within thirty (30days for all other findings.
1752.224-79	Suspension of Contract for Security Concerns	None
1752.239-70	Internet Protocol Version 6 (IPV6) Compliance (Dec 2015)	The Contractor must certify that its products have been tested to meet the requirements for both a dual-stack IPV4/IPV6 and IPV6 only environment.
1752.239-72	Access to OPM Information Technology (IT) Systems (Dec 2015)	The Contractor must provide an initial and complete list of employee names that require access to OPM IT systems five (5) days prior to required access. The Contractor must send a staffing change report by the fifth day of each month after contract award. The COR and OPM Helpdesk must be notified at least five (5) days prior to Contractor employee being removed from the contract. For unplanned terminations or removals, the COR and OPM Helpdesk must be notified immediately.
1752.239-73	Section 508 Standards (Dec 2015)	The Contractor must document that the deliverable conforms to the Section 508 Standards.

Contract Clause	Contract Clause Title	Deliverable(s)
1752.239-75	Information System Security Requirements (Dec 2015)	The Contractor must complete a FIPS 199 for approval by the OPM CIO.
1752.239-76	Security Assessment and Authorization (SA&A) (Dec 2015)	The Contractor must complete a FIPS 199 for approval by the OPM CIO. The Contractor must complete a PTA (and PIA if determined applicable by the Chief Privacy Officer). The Contractor must submit to OPM a signed A&A package approved by the Contractor Chief Information Officer (CIO) or higher level executive, along with the report and supporting documentation such as system and configuration scans from the FEDRAMP 3PAO at least 60 days prior to the operation of the IT system or 90 days prior to the expiration of the existing ATO. The Contractor must submit a POA&M for each security finding.
1752.239-77	Federal Reporting Requirements (September 2014)	The Contractor must provide OPM with FISMA and OPM continuous monitoring information.
1752.239-78	Cloud Computing (Dec 2015)	The Cloud Service Provider (CSP) must make available the most current, and any subsequent, security assessment reports, including the System Security Plan.
1752.239-80	Information Technology (IT) Security and Privacy Awareness Training (Dec 2015)	None
1752.239-81	Specialized IT Security Awareness Training (Dec 2015)	The Contractor must certify that IT security personnel have completed the requisite training. The Contractor must provide proof of a CISSP for the ISSO and Information Security Specialists within 6 months of contract award.
1752.239-82	HSPD-12 Compliance (Dec 2015)	All Contractor employees must sign an access agreement.
1752.239-83	Secure Technical Implementation (Dec 2015)	The Contractor must certify applications are fully functional and operate as intended on systems using the Federal Desktop Core Configuration (FDCC) / US Government Configuration Baseline (USGCB).
1752.239-84	Data Protection Requirements (Dec 2015)	The Contractor must provide the validation certificate number for FIPS 140 as validated by the Cryptographic Module Validation Program (CMVP).
1752.239-85	Security Monitoring and Alerting Requirements (Dec	None

Contract Clause	Contract Clause Title	Deliverable(s)
	2015)	
1752.239-86	Contractor Information Technology (IT) System Oversight / Compliance (Dec 2015)	All Contractor systems must perform vulnerability scanning as defined by OPM IT Security Policy and provide scanning reports to the OPM CIO (or designate). All Contractor systems 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 OPM CIO (or designate).
1752.242-71	Return of OPM and OPM-Activity-Related Information (Dec 2015)	Within forty-five (45) days after the end of the contract performance period of after the contract is terminated, the Contractor must provide OPM with an associated Certification of Verified Return of all original (and at least one duplicate copy of those information types specified by OPM) OPM and OPM-Activity-Related Information.
1752.242-72	Secure Destruction of All OPM and OPM-Activity-Related Information (Dec 2015)	Within seventy-five (75) days after the end of the contract performance period or after the contract is terminated, the Contractor must provide OPM with Certification of Secure Destruction of all existing active and archived originals and/or copies of all OPM and OPM-activity-related files and information.
1752.242-73	Mandatory Requirement for Contractor Return of all OPM-Owned and Leased Computing and Information Storage Equipment (Dec 2015)	Within seventy-five (75) days after the end of the contract performance period or after the contract is terminated, the Contractor must provide OPM with Certification of Verified Return of all OPM-Owned and Leased Computing and Information Storage Equipment.

899

900