OPM-Specific Clauses

1752.200-70 On-Site Working Conditions (May 2022)

(a) OPM facilities are smoking restricted workplaces. Due to the nature of the work, facilities, and requirements, contractor staff may only smoke outside in designated smoking areas.

(b) Normal operating hours are 7:00 am to 5:30 pm, Monday through Friday. Meeting task objectives within specific timeframes may require the working of extended/overtime hours. Any extended hours must be authorized in advance and certified as worked by the task Government Project Manager(s).

(c) Government personnel observe the following days as holidays:

New Year's Day	January 1 *
Birthday of Martin Luther King, Jr.	Third Monday in January
Washington's Birthday	Third Monday in February
Memorial Day	Last Monday in May
Juneteenth National Independence Day	June 19*
Independence Day	July 4*
Labor Day	First Monday in September
Columbus Day	Second Monday in October
Veterans Day	November 11
Thanksgiving Day	Fourth Thursday in November
Christmas Day	December 25*

* If the date falls on a Saturday, the Government holiday is the preceding Friday. If the date falls on a Sunday, the Government holiday is the following Monday.

(d) In addition to the days designated as holidays, the Government observes the following days:

- Any other day designated by Federal Statute
- Any other day designated by Executive Order
- Presidential Inauguration Day
- Any other day designated by the President's Proclamation

(e) It is understood and agreed between the Government and the Contractor that observance of such days by Government personnel shall not otherwise be a reason for an additional period of performance, or entitlement of compensation except as set forth within the contract. In the event the Contractor's personnel work during the holiday, they may be reimbursed by the Contractor, however, no form of holiday or other premium compensation will be reimbursed either as a direct or indirect cost, other than their normal compensation for the time worked. This provision does not preclude reimbursement for authorized overtime work if applicable to this contract.

(f) When the Federal, State, Local or other Governmental entity grants excused absence to its employees, assigned Contractor personnel may also be dismissed. The Contractor agrees to continue to provide sufficient personnel to perform critical tasks already in operation or scheduled, and must be guided by the instructions issued by the CO or COR.

(g) If Government personnel are unavailable due to furlough or any other reason, the Contractor must contact the CO or the COR to receive direction. It is the Government's decision as to whether the contract price/cost will be affected. Generally, the following situations apply:

(1) Contractor personnel who are able to continue contract performance (either on-site or at a site other than their normal workstation), must continue to work and the contract price shall not be reduced or increased.

(2) Contractor personnel who are not able to continue contract performance (e.g., support functions) may be asked to cease their work effort. This may result in a reduction to the contract price.

1752.204-70 Contractor Personnel Security Requirements (Jan 2008)

(a) The U.S. Office of Management and Budget (OMB) Memorandum M-05-24, referenced in paragraph (a) of FAR 52.204-9, Personal Identity Verification of Contractor Personnel, is available on-line at http://www.whitehouse.gov/omb/memoranda/fy2005/m05-24.pdf.

(b) The Government may require security clearances for performance of this contract. The Contractor must obtain these clearances before beginning work on the contract (OPM will not allow Contractor employees without clearance in any of its facilities). The Contractor must obtain these clearances by using the eQIP system. If satisfactory security arrangements cannot be made with the Contractor, the required services must be obtained from other sources.

(c) The level of classified access required will be indicated on DD-254 or other appropriate form incorporated into each request requiring access to classified information. Contractors are required to have background investigations for suitability if they occupy positions of trust (e.g., systems administration) even if they do NOT have access to classified information.

(d) Necessary facility and/or staff clearances must be in place prior to start of work on the contract

(e) Contractors are responsible for the security, integrity and appropriate authorized use of their systems interfacing with the Government and or used for the transaction of any and all Government business. The Government, through the Government's Contracting Officer, may require the use or modification of security and/or secure communications technologies related to Government systems access and use.

(f) The Government, at its discretion, may suspend or terminate the access and/or use of any or all Government access and systems for conducting business with any/or all Contractors when a security or other electronic access, use or misuse issue gives cause for such action. The suspension or termination may last until such time as the Government determines that the situation has been corrected or no longer exists.

1752.209-70 Contractor Performance Capabilities (July 2005)

The Contractor must be capable of performing all the tasks described in the Statement of Work. The Government shall not be liable for any costs or other involvement in the purchase, repair, maintenance or replacement of Contractor items used to implement or comply with requirements of the contract. Likewise, the Government shall in no way be held accountable by the Contractor for the Contractor's inability to perform under this Contract due to Government technology implementations and or changes.

1752.209-71 Contractor's Key Personnel (July 2005)

(a) In order to ensure a smooth and orderly start up of work, it is essential that the key personnel specified in the Contractor's proposal be available on the effective date of the contract. If these personnel are not made available at that time, the Contractor must notify the Government Contracting Officer and show cause. If the Contractor does not show cause, the Contractor may be subject to default action.

(b) The Contractor shall not of its own will remove or replace any personnel designated as "key" personnel without the written concurrence of the cognizant Contracting Officer. Prior to utilizing employees other than specified personnel, the Contractor shall notify the Government Contracting Officer and the COR. This notification must be no later than five (5) calendar days in advance of any proposed substitution and must include justification (including resume(s) of proposed substitution(s)) in sufficient detail to permit evaluation of the impact on contract performance.

(c) Substitute personnel qualifications must be equal to, or greater than, those of the personnel being substituted. If the Government Contracting Officer and the COR determine that the proposed substitute personnel is unacceptable, or that the reduction of effort would be so substantial as to impair the successful performance of the work under the contract, the Contractor may be subject to default action. If deemed necessary by the Government, substitute personnel must be given a one-(1) day orientation by Contractor personnel at no additional cost to the Government and with no change in the delivery schedule.

(d) In the event that the performance of assigned Contractor personnel or any substitute(s) is determined by the Government to be unsatisfactory at any time during the life of the Contract, the Government reserves the right to request and receive satisfactory personnel replacement within five (5) calendar days of receipt by the Contractor of written notification. Notification will include the reason for requesting replacement personnel.

(e) The Contractor-supplied personnel are employees of the Contractor and under the administrative control and supervision of the Contractor. The Contractor, through its personnel, shall perform the tasks prescribed herein. The Contractor must select, supervise, and exercise control and direction over its employees (including subcontractors) under this Contract. The Government shall not exercise any supervision or control over the Contractor in its performance of contractual services under this contract. The Contractor is accountable to the Government for the action of its personnel.

(f) The Contractor is herewith notified that employee recruiting and employee retention practices shall be monitored on a regular basis.

1752.209-72 Qualifications of Contractor's Employees (January 2017)

(a) The contracting officer or a designated representative may require the Contractor to remove any employee(s) from OPM controlled buildings or other real property should it be determined that the individual(s) is either unsuitable for security reasons or otherwise unfit to work on OPM controlled property.

(b) The Contractor shall fill out and cause all of its employees performing work on the contract work to fill out, for submission to the Government, such forms as may be necessary for security or other reasons. Upon request of the Contracting Officer, the Contractor and its employees shall be fingerprinted.

(c) Each employee of the Contractor shall be a citizen of the United States of America, or an alien who has been lawfully admitted for permanent residence as evidenced by Alien Registration Receipt Card Form I-151, or, who presents other evidence from the Immigration and Naturalization Service that employment will not affect his immigration status.

1752.209-73 Standards of Conduct (June 2006)

(a) Personnel assigned by the contractor to the performance of work under this order must be acceptable to the Government in terms of personal and professional conduct. Contractor personnel shall conform to standards of conduct as follows:

(1) No contractor employees shall solicit new business while performing work under this order.

(2) The contractor and its employees shall not discuss with unauthorized persons any information obtained in the performance of work under this order.

(b) Should the continued assignment to work under this order of any person in the contractor's organization be deemed by the Contracting Officer to conflict with the interests of the Government, that person shall be removed immediately from assignment, and the reason for removal shall be fully documented in writing by the Contracting Officer. Employment and staffing difficulties shall not be justification for failure to meet established schedules, and if such difficulties impair performance, the contractor may be subject to default.

1752.209-74 Organizational Conflicts of Interest (July 2005)

(a) The Contractor warrants that, to the best of the Contractor's knowledge and belief, there are no relevant facts or circumstances which could give rise to an organizational conflict of interest (OCI), as defined in FAR 9.5, Organizational and Consultants Conflicts of Interest, or that the Contractor has disclosed all such relevant information.

(b) The Contractor agrees that if an actual or potential OCI is discovered after award, the Contractor shall make a full disclosure in writing to the Contracting Officer. This disclosure must include a description of actions, which the Contractor has taken or proposes to take, after consultation with the Contracting Officer, to avoid, mitigate, or neutralize the actual or potential conflict.

(c) The Contracting Officer may terminate this contract for convenience, in whole or in part, if it deems such termination necessary to avoid an OCI. If the Contractor was aware of a potential OCI prior to award or discovered an actual or potential conflict after award and did not disclose or misrepresented relevant information to the Contacting Office, 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.

(d) The Contractor must include this clause in all subcontracts and in lower tier subcontracts unless a waiver is requested from, and granted by, the Contracting Officer.

(e) In the event that a requirement changes in such a way as to create a potential conflict of interest for the Contractor, the Contractor must:

(1) Notify the Contracting Officer of a potential conflict, and;

(2) Recommend to the Government an alternate approach which would avoid the potential conflict, or

(3) Present for approval a conflict of interest mitigation plan that will:

(i) Describe in detail the changed requirement that creates the potential conflict of interest; and

(ii) Outline in detail the actions to be taken by the Contractor or the Government in the performance of the task to mitigate the conflict, division of subcontractor effort, and limited access to information, or other acceptable means.

(4) The Contractor must not commence work on a changed requirement related to a potential conflict of interest until specifically notified by the Contracting Officer to proceed.

(5) If the Contracting Officer determines that it is in the best interest of the Government to proceed with work, notwithstanding a conflict of interest, a request for waiver must be submitted in accordance with FAR 9.503.

1752.209-75 Reducing Text Messaging While Driving (Oct 2009)

(a) In accordance with Section 4 of the Executive Order, "Federal Leadership on Reducing Text Messaging While Driving," dated October 1, 2009, you are hereby encouraged to:

(1) Adopt and enforce policies that ban text messaging while driving company-owned or -rented vehicles or Government-owned, -leased or –rented vehicles, or while driving privately-owned vehicles when on official Government business or when performing any work for or on behalf of the Government; and

(2) Consider new company rules and programs, and reevaluating existing programs to prohibit text messaging while driving, and conducting education, awareness, and other outreach for company employees about the safety risks associated with texting while driving. These initiatives should encourage voluntary compliance with the company's text messaging policy while off duty.

(b) For purposes of complying with the Executive Order:

(1) "Texting" or "Text Messaging" means reading from or entering data into any handheld or other electronic device, including for the purpose of SMS texting, e-mailing, instant messaging, obtaining navigational information, or engaging in any other form of electronic data retrieval or electronic data communication.

(2) "Driving" means operating a motor vehicle on an active roadway with the motor running, including while temporarily stationary because of traffic, a traffic light or stop sign, or otherwise. It does not include operating a motor vehicle with or without the motor running when one has pulled over to the side of, or off, an active roadway and has halted in a location where one can safely remain stationary.

1752.222-70 Notice of Requirement for Certification of Nonsegregated Facilities (July 2005)

By signing this offer or contract, the contractor will be deemed to have signed and agreed to the provisions of Federal Acquisition Regulations (FAR) Clause 52.222-21, Certification of Nonsegregated Facilities, incorporated by reference in this solicitation/contract. The certification provides that the bidder or offeror does not maintain or provide for its employees, facilities which are segregated on a basis of race, color, religion, or national origin, whether such facilities are segregated by directive or on a de facto basis. The certification also provides that the bidder/offeror does not and will not permit its employees to perform their services at any location under its control where segregated facilities are maintained. FAR Clause 52.222-21 must be included in all subcontracts as well.

1752.222-71 Special Requirements for Employing Special Disabled Veterans, Veterans of the Vietnam Era, and Other Eligible Veterans (July 2005)

(a) If this contract contains FAR Clause 52.222-35 (Equal Opportunity for Special Disabled Veterans, Veterans of the Vietnam Era, and Other Eligible Veterans), your company must comply with the requirements of this clause, including the listing of employment opportunities with the local office of the state employment service system.

(b) If this contract contains FAR clauses 52.222-37 (Employment Reports on Special Disabled Veterans, Veterans of the Vietnam Era, and Other Eligible Veterans) or 52.222-38 (Compliance with Veterans' Employment Reporting Requirements), you are reminded that your company must comply with the special reporting requirements described in those clauses. Your company must submit information on several aspects of its employment and hiring of special disabled and Vietnam era veterans or other veterans who served on active duty during a war or in a campaign or expedition for which a campaign badge has been authorized. You must submit this information no later than September 30 of each year, in the "Federal Contractor Veterans' Employment Report" or VETS-100 Report. The U.S. Department of Labor has established a web site for submitting this report. The address is: http://www.dol.gov/vets/vets4212.htm.

1752.224-70 Definition of Terms (Feb 2022)

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): is information the Government creates or possesses, or that an entity creates or possesses for or on behalf of the Government, that a law, regulation, or Government-wide policy requires or permits an agency to handle using safeguarding or dissemination controls. However, CUI does not include classified information or information a non-executive branch entity possesses and maintains in its own systems that did not come from, or was not created or possessed by or for, an executive branch agency or an entity acting for an agency. Law, regulation, or Government-wide policy may require or permit safeguarding or dissemination controls in three ways: Requiring or permitting agencies to control or protect the information but providing no specific controls, which makes the information CUI Basic; requiring or permitting agencies to control or protect the information and providing specific controls for doing so, which makes the information CUI Specified; or requiring or permitting agencies to control the information and specifying only some of those controls, which makes the information CUI Specified, but with CUI Basic controls where the authority does not specify.

c. Personally Identifiable Information (PII): This term refers to information 53that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual. Because there are many different types of information that can be used to distinguish or trace an individual's identity, the term PII is necessarily broad. To determine whether information is PII, the agency shall perform an assessment of the specific risk that an individual can be identified using the information with other information that is linked or linkable to the individual. In performing that assessment, it is important to recognize that information that is not PII can become PII whenever additional information becomes available – in any medium or from any source – that would make it possible to identify an individual.

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

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.

e. Information Security Incident (ISI): An occurrence that (1) actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or (2) constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies.

f. Breach: The loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where (1) a person other than an authorized user accesses or potentially accesses personally identifiable information or (2) an authorized user accesses or potentially accesses personally identifiable information for other than authorized purposes.

g.

h. Record:

(1) For the purpose of Records Management, this term refers to all books, papers, maps, photographs, machine readable materials, or other documentary materials, regardless of form or characteristics, made or received by an agency of the United States Government 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 or a contractor on the behalf of 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.

i. System of Records on individuals: This term refers to a group of any Records under the control of ant 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.

j. 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 maintenance, collection, use, and dissemination of Records.

k.

l. 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.

1752.224-71 Freedom of Information Act Requests (Sep 2009)

(a) Offerors are reminded that information furnished under this solicitation may be subject to disclosure under the Freedom of Information Act (FOIA). Therefore:

(1) All items that are confidential to business, or contain trade secrets, proprietary, or personnel information must be clearly marked in all documents submitted to the U.S. Office of Personnel Management (OPM or The Government). Marking of items will not necessarily preclude disclosure when the OPM determines disclosure is warranted by FOIA. However, if such items are not marked, all information contained within the submitted documents will be deemed to be releasable.

(2) No later than five (5) business days after award of a contract, blanket purchase agreement (BPA), or order, the Contractor must provide OPM a redacted copy of the contract/BPA/order in electronic format. This copy will be used to satisfy any requests for copies of the contract/BPA/order under the FOIA. If the Contracting Officer believes that any redacted information does not require protection from public release, the issue will be resolved in accordance with paragraph 3.104-4(d) of the Federal Acquisition Regulation.

(b) Any information made available to the Contractor by the Government must be used only for the purpose of carrying out the provisions of this contract and must not be divulged or made known in any manner to any person except as may be necessary in the performance of the contract.

(c) In performance of this contract, the Contractor assumes responsibility for protection of the confidentiality of Government records and must ensure that all work performed by its subcontractors shall be under the supervision of the Contractor or the Contractor's responsible employees.

(d) Each officer or employee of the Contractor or any of its subcontractors to whom any Government record may be made available or disclosed must be notified in writing by the Contractor that information disclosed to such officer or employee can be used only for a purpose and to the extent authorized herein, and that further disclosure of any such information, by any means, for a purpose or to an extent unauthorized herein, may subject the offender to criminal sanctions imposed by 19 U.S.C. 641. That section provides, in pertinent part, that whoever knowingly converts to their use or the use of another, or without authority, sells, conveys, or disposes of any record of the United States or whoever receives the same with intent to convert it to their use or gain, knowing it to have been converted, shall be guilty of a crime punishable by a fine of up to $10,000, or imprisoned up to ten years, or both.

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.

1752.224-74 Privacy Act (Feb 2022)

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 is required to accomplish an OPM function: 52.224-1 Privacy Act Notification (Apr 1984) and 52.224-2 Privacy Act (Apr 1984).

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

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.

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.

1752.224-77 Information Security Incidents (ISI) (Feb 2022)

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 OPM, or its designate, full access and cooperation for all activities determined by CO or COR to be required to perform inspection and forensic analysis in the event of an ISI.

(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.

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.

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.

1752.228-70 Insurance (July 2005)

(a) In accordance with FAR 52.228-5, "Insurance-Work on a Government Installation (JAN 1997)" incorporated by reference, the Contractor must secure, pay the premiums for and

keep in force until the expiration of this contract, and any renewal thereof, adequate insurance of the types and in the amounts as specified under FAR 28.3.

(b) Each policy of insurance must contain an endorsement that any cancellation or material change in the coverage adversely affecting the Government's interest must not be effective unless the insurer or the Contractor gives written notice of cancellation or change, as required by the CO. When the coverage is provided by self-insurance, the Contractor shall not change or decrease the coverage without the CO's prior approval.

(c) A certificate of each policy of insurance must be furnished to the CO within ten (10) days after notice of award certifying, among other things, that the policy contains the aforementioned endorsement. The insurance company providing the above insurance must be satisfactory to the Government. Notices of policy changes shall be furnished to the CO. The substance of this clause must be made to flow down to any subcontractors.

1752.232-71 Method of Payment (July 2005)

(a) Payments under this contract will be made either by check or by wire transfer through the Treasury Financial Communications System at the option of the Government.

(b) The Contractor must forward the following information in writing to the Contracting Officer not later than seven (7) days after receipt of notice of award:

(1) Full Name (where practicable), title, telephone number, and complete mailing address of responsible official(s):

(i) to whom check payments are to be sent, and

(ii) who may be contacted concerning the bank account information requested below.

(2) The following bank account information required to accomplish wire transfers:

(i) Name, address, and telegraphic abbreviation of the receiving financial institution.

(ii) Receiving financial institution's 9-digit American Bankers Association (ABA) identifying number for routing transfer of funds. (Provide this number only if the receiving financial institution has access to the Federal Reserve Communications System.)

(iii) Recipient's name and account number at the receiving financial institution to be credited with the funds. If the receiving financial institution does not have access to the Federal Reserve Communications System, provide the name of the correspondent financial institution through which the receiving institution receives electronic funds transfer messages. If a correspondent financial institution is specified, also provide:

(A) Address and telegraphic abbreviation of the correspondent financial institution.

(B) The correspondent financial institution's 9-digit ABA identifying number for routing transfer of funds.

(c) Any changes to the information furnished under paragraph (b) of this clause shall be furnished to the Contracting Officer in writing at least 30 days before the effective date of the change. It is the Contractor’s responsibility to furnish these changes promptly to avoid payments to erroneous addresses or bank accounts.

(d) The document furnishing the information required in paragraphs (b) and (c) must be dated and contain the signature, title, and telephone number of the Contractor official authorized to provide it, as well as the Contractor's name and contract number

1752.232-74 Providing Accelerated Payment to Small Business Subcontractors (Oct 2012)

(a) This clause implements the temporary policy provided by OMB Policy Memorandum M-12-16, Providing Prompt Payment to Small Business Subcontractors, dated July 11, 2012. (Note: OMB Policy Memorandum M-12-16 is accessible on line at: http://www.whitehouse.gov/sites/default/files/omb/memoranda/2012/m-12-16.pdf.)

(b) Upon receipt of accelerated payments from the Government, the contractor is required to pay all small business subcontractors on an accelerated timetable to the maximum extent practicable after receipt of invoice and all proper documents.

(c) Include the substance of this clause, including this paragraph (b), in all subcontracts with small business.

1752.232-75 Electronic Submission of Invoices (May 2021)

a) The Office of Personnel Management (OPM) will only accept electronic invoices submitted through the Delphi eInvoicing system.

b) Payment system registration. All persons accessing the Delphi eInvoicing web-portal shall have a unique user Delphi eInvoicing ID and be authenticated through login.gov.

1. Vendors must provide opmisupplieraccess@opm.gov the full name, valid email address, and current phone number of users who require access to the Delphi eInvoicing web-portal for invoice submission and payment tracking purposes. Each email address must be unique for each user.
2. To make changes to vendor users who will have access to the Delphi eInvoicing web-portal, the vendor must notify opmisupplieraccess@opm.gov and include the full name, valid email address, and current phone number of any new vendor users.
3. Vendors are responsible to contact the Delphi Help Desk when their firm's points of contacts will no longer be submitting invoices so they can be removed from the system. Instructions for contacting the Delphi Help Desk can be found at http://einvoice.esc.gov.
4. Designated vendor users will be notified via e-mail when the account is created. The vendor user will be provided detailed instructions for logging into their Delphi eInvoicing account.
5. Electronic authentication. Click on the following link to create a login.gov account: https://login.gov.

6. To create a login.gov account, the user will need a valid email address and a working phone number. The user will create a password and establish a secondary authentication method to keep their account secure.

c) Training on Delphi. To facilitate use of DELPHI, comprehensive user information is available at http://einvoice.esc.gov.

d) The Delphi eInvoicing system is managed by the Enterprise Services Center (ESC). In order to receive payment and in accordance with the Prompt Payment Act, all invoices and required supporting documentation must be attached in the Delphi eInvoicing web-portal and must contain the information specified in the appropriate clause in the vendor's contract, for example, FAR 52.212-4 or 52.232-25.

e) If the contract includes allowances for travel on a reimbursable basis, all invoices for charges pertaining to travel expenses must catalog a breakdown of reimbursable expenses with the appropriate receipts to substantiate the travel expenses.

1752.237-70 Non-Personal Services (July 2005)

(a) As stated in the Office of Federal Procurement Policy Letter 92-1, dated September 23, 1992, Inherently Governmental Functions, no personal services shall be performed under this contract. No Contractor employee will be directly supervised by the Government. All individual employee assignments, and daily work direction, shall be given by the applicable employee supervisor. If the Contractor believes any Government action or communication has been given that would create a personal services relationship between the Government and any Contractor employee, the Contractor must promptly notify the Contracting Officer of this communication or action.

(b) The Contractor must not perform any inherently Governmental actions under this contract. No Contractor employee shall hold him or herself out to be a Government employee, agent, or representative. No Contractor employee may state orally or in writing at any time that he or she is acting on behalf of the Government. In all communications with third parties in connection with the contract, Contractor employees must identify themselves as Contractor employees and specify the name of the company for which they work. In all communications with other Government Contractors in connection with this contract, the Contractor employee must state that they have no authority to in any way change the contract and that if the other Contractor believes this communication to be a direction to change their contract, they should notify the Contracting Officer for that contract and not carry out the direction until a clarification has been issued by the Contracting Officer.

(c) The Contractor must insure that all of its employees working on this contract are informed of the substance of this clause. Nothing in this clause limits the Government's rights in any way under any other provision of the contract, including those related to the Government's right to inspect and accept the services to be performed under this contract. The substance of this clause must be included in all subcontracts at any tier.

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.

1752.239-76 Security Assessment and Authorization (Feb 2022)

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 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. Any Cloud Service Offerings (CSO) that already are GSA FedRAMP Authorized do not require an independent 3PAO assessment, but instead OPM will leverage the security documentation of that Authorized CSO by reusing the security package from an existing federal agency.

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. However, for a CSO as highlighted in (b), the templates and documentation used by the GSA FedRAMP program will be a valid alternative submission.

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. As part of the authorization process, the Contractor may be required to support the Government in the completion of a Privacy Threshold Analysis (PTA). The completion of the PTA is triggered by the creation, use, modification, upgrade, or disposition of Contractor IT systems that will collect, store, maintain, use, and/or disseminate PII. Upon review of the PTA, the OPM Senior Agency Official for Privacy, or designee, determines whether a Privacy Impact Assessment (PIA) and or a Privacy Act System of Records Notice (SORN), or modification thereto, are required. The Contractor shall provide all support necessary to assist OPM in completing the PIA in a timely manner and shall ensure that project management plans and schedules include time for the completion of the PTA, PIA, and SORN (to the extent required) as milestones. Support in this context includes responding timely to requests for information from the Government about the collection, use, access, storage, and maintenance of PII on the Contractor's system, and providing timely review of relevant compliance documents for factual accuracy.

g. The Contractor must submit an updated SA&A package, along with the 3PAO report (unless otherwise noted for CSOs), 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. For CSOs the onsite visit and inspection will not be required if already part of the vendor's FedRAMP documentation.

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.

1752.239-77 Federal Reporting Requirements (Feb 2022)

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 also comply will any cybersecurity related Executive Orders issued from OMB. 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.

1752.239-78 Cloud Service Offerings (Feb 2022)

a. The use of Cloud Service Offerings (CSO) is divided into multiple categories; FedRAMP Authorized, FedRAMP in Process, FedRAMP Ready, or not part of the FedRAMP program. Depending upon which category the Contractor's offering uses, there will be different requirements for each.

a. FedRAMP Authorized: A designation provided to CSPs that have successfully completed the FedRAMP Authorization process with the JAB or a federal agency. FedRAMP Authorized service offerings are available for government-wide reuse.

b. FedRAMP Ready: A designation provided to Cloud Service Providers (CSPs) which indicates that a Third Party Assessment Organization (3PAO) attests to a CSO's security capabilities, and that a Readiness Assessment Report (RAR) has been reviewed and deemed acceptable by the FedRAMP PMO. FedRAMP Ready indicates a CSO has a high likelihood of successfully completing an initial FedRAMP Authorization with the Joint Authorization Board (JAB) or a federal agency.

c. FedRAMP In Process: A designation provided to CSPs that are actively working toward a FedRAMP Authorization with either the JAB or a federal agency.

d. Not Part of FedRAMP: The CIO and CISO will determine the path that such a service could be utilized. The Contractor must obtain approval from the Chief Technology Officer (CTO), through the Contracting Officer (CO) or Contracting Officer's Representative (COR), that the use of that cloud service has been authorized by the Chief Information Officer (CIO).

b. Whenever possible, the Contractor will focus upon utilizing FedRAMP Authorized cloud services as part of their offering.

c. Information stored in a CSO remains the sole property of OPM, not the Contractor or the CSO.

d. The CSO 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.

e. The CSO 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.

f. The CSO, and any subcontractor or teaming partner CSOs, 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 if not using a FedRAMP Authorized CSO. 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 CSOs Systems Security Plan, as part of the Contractor's Systems Security Plan.

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.

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.

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.

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.

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.

1752.239-85 Security Monitoring and Alerting Requirements (Feb 2022)

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
(1) OPM requires access to all security related logs associated to the IT System
(2) A secure connection to the OPM SOC is established to transport all security related logs

c. System, User, and Data Segmentation

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.

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.

1752.242-72 Security 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.

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.

1752.242-88 Contract Performance Information (July 2005)

(a) Dissemination of Contract Performance Information

The Contractor must not publish, permit to be published, or distribute for public consumption, 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. Two copies of any material proposed to be published or distributed must be submitted to the Contracting Officer for approval.

(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. Neither the Contractor nor its employees must testify on a matter related to work performed or information provided under this contract, either voluntarily or pursuant to a request, in any judicial or administrative proceeding unless approved by the Contracting Officer or required by a judge in a final court order.