ATF 18

Requirements for Access to Law Enforcement Sensitive Information (Jul 2019)

(a) Duplication or disclosure of the data and other information to which the Contractor will have access as a result of this contract is prohibited. It is understood that throughout performance of this contract the Contractor will have access to confidential and sensitive data, which is either the sole property of the Government or is the sole property of other than the contracting parties. The Contractor and its subcontractor(s) *(if any)* agree to maintain the confidentiality of all data to which access may be gained throughout the contract performance, whether title thereto vests in the Government or otherwise. The Contractor and its subcontractor(s) *(if any)* agree to not disclose said data, any interpretations and/or translations thereof, or data derivative, to unauthorized parties in contravention of these provisions, without the prior written approval of the Contracting Officer or the party in which title thereto is wholly vested. Subcontractors are subject to the same stipulations and may be held responsible for any violations of confidentiality.

(b) The Contractor agrees that each Contractor employee, prior to and as a pre-condition for employment relating to the subject matter of this manual, will be required to execute a Nondisclosure Agreement as provided. The Contractor shall provide the Contracting Officer with the original copy of this form signed by each employee prior to the employee's start date on the contract.

(c) The details of any and all safeguards that the Contractor may design or develop under this contract shall become and shall remain the property of the Government and shall not be published or disclosed in any manner without the expressed written consent of the Government.

(d) The details of any and all safeguards that may be revealed to the Contractor by the Government in the course of performing under this contract shall not be published or disclosed in any manner without the expressed written consent of the Government.

(e) The Government shall be afforded full, free, and uninhibited access to all facilities, installations, technical capabilities, operations, documentation, records, and databases for the purpose of carrying out a program of inspection to ensure continued efficiency and efficacy of safeguards against threats and hazards to data security, integrity, and confidentiality.

(f) If new or unanticipated threats or hazards are discovered by either the Government or the Contractor, or if existing safeguards have ceased to function, the discoverer shall immediately bring the situation to the attention of the other party. Mutual agreement shall then be reached on changes or corrections to existing safeguards or institution of new safeguards, with final determination or appropriateness being made by the Government. The Government's liability is limited to an equitable adjustment of cost for such changes or corrections, and the Government shall not be liable for claims of loss of business, damage to reputation, or damages of any other kind arising from discovery of new or unanticipated threats or hazards, or any public or private disclosure thereof.

(End of Clause)

ATF 22
Confidentiality of Information and Disclosure (Apr 2008)

The Contractor agrees, in the performance of this contract, to keep all information contained in source documents or other media furnished by the Government in the strictest confidence. The Contractor also agrees not to publish or otherwise divulge such information in whole or in part, in any manner or form, nor to authorize or permit others to do so, taking such reasonable measures as are necessary to restrict access to such information while in the Contractor s possession, to those employees needing such information to perform the work provided herein, e.g., on a need to know basis. There shall be no dissemination or publication, except within and between the Contractor and any subcontractors, of information developed under this contract or contained in the reports to be furnished pursuant to this contract without prior written approval from the Contracting Officer. No news release (including photographs and films, public announcements, denial or confirmation of same) on any part of the subject matter of this contract or any phase of any program hereunder shall be made without the prior written approval of the Contracting Officer. The Contractor is prohibited from releasing to any source, other than the sponsoring activity, any interim, draft and final reports or information pertaining to services performed under this contract until report approval or official review has been obtained. Furthermore, the Contractor shall insure that the cover of all interim, draft and final reports contain the following statement: "The view, opinions, and/or findings contained in this report are those of the author(s) and should not be construed as an official Government position, policy or decision, unless so designated by other documentation."

The Contractor agrees to immediately notify in writing the Contracting Officer named herein, in the event that the Contractor determines or has reason to suspect a breach of this requirement. The Contractor agrees to insert the substance of this clause in any consultant agreement or subcontract hereunder.

(a) Confidential information, as used in this clause, means: (1) information or data of a personal nature proprietary about an individual; (2) information or data submitted by or pertaining to an institution or organization; or (3) information or data pertaining to a law enforcement investigation or operation.

(b) In addition to the definitions in (a) (1), (2), and (3) above, confidential information includes information which might require special consideration with regard to the timing of its disclosure, such as draft budget and strategic plans, studies or research, audits, etc.

(c) The Contracting Officer and the Contractor may, by mutual consent, identify elsewhere in this contract specific information and/or categories of information which the Government will furnish to the Contractor or that the Contractor is expected to generate which is confidential. Similarly, the Contracting Officer and the Contractor may, by mutual consent, identify such confidential information from time to time during the performance of the contract. Failure to agree will be settled pursuant to the Disputes clause.

(d) If it is established that information to be utilized under this contract is subject to the Privacy Act, the Contractor will follow the rules and procedures of the disclosure set forth in the Privacy Act of 1974, 5 U.S.C. 552a, and implementing regulations and policies, with respect to systems of records determined to be subject to the Privacy Act.

(e) Confidential information, as defined in (a)(1) and (2) above, shall not be disclosed without the prior written consent of the individual, institution, or organization. Confidential information, as defined in (a)(3) shall not be disclosed without the prior written consent of the Bureau of Alcohol, Tobacco, Firearms & Explosives (ATF).

(f) Whenever the Contractor is uncertain with regard to the proper handling of material under the contract, or if the material in question is subject to the Privacy Act or is confidential information subject to the provisions of this clause, the Contractor shall obtain a written determination from the Contracting Officer prior to any release, disclosure, dissemination, or publication.

(g) The provisions of paragraph (e) of this clause shall not apply when the information is subject to conflicting or overlapping provisions in other Federal, State, or local laws.

(End of Clause)

ATF 13
Incorporation of Vendor Terms and Conditions (Jul 2007)

Incorporation of Commercial Terms and Conditions:

(a) The following terms and conditions, included in the vendor's standard commercial terms and conditions, do not apply to this order: Any terms and conditions inconsistent with the Government's terms and conditions and Statement of Work.

_____

(b) Any inconsistency or conflict between any of the vendor's remaining standard commercial terms and conditions and the Government's terms and conditions incorporated in this order shall be resolved by giving precedence to the Government's terms and conditions.

(End of Clause)

ATF 04
Background Investigation Requirements (May 2010)

Personnel Security Requirements:

The Contractor shall be responsible for ensuring that all Contractor employees assigned hereunder undergo a background investigation or other applicable personnel security procedures to determine their suitability for access to ATF information, information technology systems, and/or facilities. For the purpose of this contract, the term background investigation will be utilized to also reference other personnel security procedures that may be applied in lieu of a full background investigation.

The background investigation will be conducted by or under the auspices of the Personnel Security Branch, Office of Professional Responsibility and Security Operations, Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF). It is the responsibility of the Contractor to provide the necessary personnel suitability and security package in a timely manner, through the assigned Contracting Officer's Representative (COR), to ATF's Personnel Security Branch (PSB) so that a background investigation can be conducted.

The Contractor shall screen and review each potential Contractor employee and ensure that each potential Contractor employee to be assigned to this contract possess a personal history that is in compliance with Department of Justice (DOJ) and ATF agency specific qualifications and will permit each employee to successfully pass a background investigation conducted by the ATF. The Contractor shall not submit a personnel suitability and security package to the COR until the Contractor has screened the following aspects of each potential Contractor employee's personal history:

(a) Criminal conduct
(b) Financial responsibility
(c) Drug use
(d) Employment history
(e) Employment eligibility
(f) Selective Service registration, if applicable

(g) U.S. Residency
(h) Country of citizenship

During the Contractor's review of each potential Contractor employee's personal history, the Contractor is required to review each potential Contractor employee's personnel suitability and security package to ensure the forms are fully complete, signed, and dated.

Prior to submitting a personnel suitability and security package, the Contractor shall utilize E-Verify to verify the employment eligibility of all Contractor employees, regardless of citizenship status. The Contractor will not submit a personnel suitability and security package when employment eligibility cannot be verified. The Contractor can register for E-Verify on-line at https://www.vis-dhs.com/employerregistration/. This website provides instructions for completing a Memorandum of Understanding required for official registration. Contractors requesting additional information about theprogram can visit the E-Verify website at www.dhs.gov/E-Verify or call the E-Verify program office at 1- 888-464-4218.

The Contractor must submit a copy of a tentative employment offer with the personnel suitability and security package when it is submitted on a potential Contractor employee. The Contractor is hereby advised that a background investigation may take 60 days or more to complete, depending on the complexity of the background investigation. The Contractor is encouraged to fill all positions with employees who have recently been the subject of a Federal background investigation.

At the conclusion of the background investigation, the Personnel Security Branch will make a favorable or unfavorable determination and advise the COR and the Contracting Officer (CO). The CO or COR are responsible for advising the Contractor of ATF's determination.

Contractor employees are not authorized to access ATF proprietary information, information technology systems, and/or facilities, until a favorable determination has been made by the Personnel Security Branch in accordance with agency specific qualifications, DOJ policy, Federal suitability, and/or adjudicative guidelines.

All background investigations will be adjudicated applying the suitability standards under 5 CFR, part 731, as well as the following DOJ policy and ATF agency specific qualifications:

(a) DOJ Residency Requirement. Immediately prior to gaining access to ATF information, information technology systems, and/or facilities the PSB staff ensures all Contractor employees have:

(1) Resided in the United States for three out of the last five years; and/or

(2) Worked for the United States in a foreign country in a Federal or military capacity for three out of the last five years; and/or

(3) Been a dependent of a Federal or military employee in a foreign country for three out of the last five years.

(b) Allied Nations List. Contractor employees that only require access to ATF facilities must be United States citizens or foreign nationals legally permitted to reside in the United States. Their

country of citizenship must be listed on the Allied Nations list published by the Department of State, Office of the Assistant Legal Advisor for Treaty Affairs. Since countries on this list are subject to change, refer to the following website for current information: http://www.state.gov/s/l/treaty/collectivedefense/.

(c) Drug Policy. ATF Drug Policy for ATF Applicants, is applied. The PSB ensures that ATF Contractor employees are compliant with the policy prior to authorizing access to ATF information, information technology systems, and/or facilities.

(d) Selective Service. PSB will verify that all laws of the Selective Service are adhered to.

(e) Financial Responsibilities. The PSB ensures compliance with DOJ guidance surrounding financial obligations.

(1) Public Trust Positions - All financial obligations imposed by law must be favorably resolved through proof of payment and/or participation in a payment plan. For all other debt-related issues a risk management decision may be made in lieu of requiring payment or a payment plan. (Depending upon the position and debt history, PSB may require proof of payment and/or participation in a payment plan for financial delinquencies that are not imposed by law).

(2) National Security Positions – All delinquent financial obligations, even those not imposed by law, must be favorably resolved through proof of payment, and/or participation in a payment plan, or otherwise resolved.

(f) Foreign Nationals Accessing Information Technology Systems. DOJ Order 2640.2F Information Technology Security, states non-U.S. citizens shall not be authorized to access or assist in the development, operation, management or maintenance of Department IT systems.

(g) Homeland Security Presidential Directive 12. The PSB will conduct Personal Identity Verification to confirm the identity of the Contractor employee. Contractor employees must personally present two forms of identification in original form prior to accessing ATF information, information technology systems, and/or facilities. At least one document must be a valid State or Federal government-issued picture ID.

In the event a contract employee is found to be non-compliant with the agency specific qualifications, PSB will notify the COR and the CO. The request for investigation will be terminated and the Contractor may be requested to submit another name and complete personnel suitability and security package. Additional agency specific qualifications may be implemented without notice to the Contractor.

Denial or Disapproval of Access to ATF Information, Information Technology Systems, and/or Facilities:

In the event that a Contractor employee is denied or disapproved for access to ATF information, information technology systems, and/or facilities due to issues found during the background investigation, the Personnel Security Branch will notify the COR and the CO. The Contractor may be requested to submit another name and complete personnel suitability and security package.

Freedom of Information Act Requests:

Once a determination has been made by the PSB, a Contractor employee may receive a copy of his/her background investigative file by submitting a written Freedom of Information Act request. The request must be addressed to the Disclosure Division, Bureau of Alcohol, Tobacco, Firearms and Explosives, 99 New York Avenue, NE, Suite 1E-400, Washington, DC 20226. It is the responsibility of the Contractor employee to assume all monetary liabilities associated with such request.

Police Check Inquiries:

In those instances where the Contractor believes that its employees will not need unescorted access to ATF facilities, or access to any ATF proprietary information, data or information technology systems, the Contractor shall notify the COR. The COR will then apprise ATF's PSB of the Contractor's initial determination, citing the reasons thereof. The PSB, in consultation with the COR or CO, will make the final determination as to whether or not the Contractor employee will need to undergo a background investigation. The nature and specific degree of background investigation will be determined by the PSB, depending upon the nature and degree of risk associated with the contract position. When ATF's PSB determines that the Contractor will require escorted access to ATF facilities, and/or ATF construction sites, or will only be provided with access to ATF non-sensitive information, the Contractor employee must undergo a criminal history check. The Physical Security Programs Branch or the respective field division/office is responsible for conducting the criminal history check and making the favorable or unfavorable determination.

Access to Classified National Security Information:

In the event the Contractor employee requires access to classified National Security Information (NSI), in order to fulfill contractual requirements, the COR or CO must contact the PSB. The PSB will assess the requirements and make a determination if access to NSI is required at the Confidential, Secret, or Top Secret level (which may or may not include access to Sensitive Compartmented Information. If the PSB determines that access to NSI is required, the contract must be modified to incorporate the requirements of the National Industrial Security Program (NISP). The PSB will provide additional personnel security language to the CO and coordinate all additional personnel security requirements of the NISP with the COR.

(End of Clause)

ATF 14
Electronic Invoicing (Oct 2008)

The Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF) encourages Contractors to invoice electronically. Invoicing electronically saves time, money, and physical storage space for both the Government and the Contractor.

Each invoice must be a proper invoice in accordance with Federal Acquisition Regulations (FAR) 32.905(b). The Contractor may submit a combined invoice with each ATF contract/order number. The invoice must clearly identify the specific Contract Line Item (CLIN) or item number for which the Contractor is seeking payment under the contract/order. If the invoice covers multiple CLINs or item numbers, the invoice must clearly identify specific amounts and activity applicable to each.

Electronic invoices must be submitted to the ATF COR/POC named in Section G of this contract and Financial Management Division (FMD), FinanceBranch@ATF.gov. Electronic invoices will serve as the official original copy. The e-mail subject line must contain the name of the ATF COR/POC named in Section G of this contract (i.e., John Doe Contract Invoice Oct 08). ATF will return to the vendor any invoices that do not contain the correct subject line information.

Contractors who are unable to submit electronic invoices may mail their invoices to the COR/POC named in Section G of this contract and FMD address provided below:

Bureau of Alcohol, Tobacco, Firearms & Explosives
Attn: Finance Branch EXPEDITE CONTRACTINVOICE
99 New York Avenue, N.E.
Mail Drop 4S-288
Washington, D.C. 20226

(End of Clause)

ATF 12

Non-Us Citizens Prohibited From Access to DOJ Information Technology Systems (May 2007)

The Department of Justice does not permit the use of Non-U.S. citizens in the performance of this contract or commitment for any position that involves access to or development of any DOJ Information Technology (IT) system. By signing the contract or commitment document, the Contractor agrees to this restriction.

In those instances where other non-IT requirements contained in the contract or commitment can be met by using Non-U.S. citizens, those requirements shall be clearly described.

Financial Responsibility: Contractor employees who have delinquent unpaid debt may be required to provide proof of payment and/or proof of participation in a payment plan. If this documentation cannot be provided, the Contractor employee's background investigation may be terminated and/or access to ATF facilities, proprietary information and data, including automated information systems, without being offered an opportunity to mitigate the information.

A Contractor employee who is in direct violation of a policy established by DOJ or ATF may be denied access to ATF facilities, proprietary information, and data, including automated information systems, without being offered an opportunity to mitigate the information.

(End of Clause)

Security of Department Information and Systems (April 2015)

I. Applicability to Contractors and Subcontractors

This clause applies to all contractors and subcontractors, including cloud service providers ("CSPs"), and personnel of contractors, subcontractors, and CSPs (hereinafter collectively, "Contractor") that may access, collect, store, process, maintain, use, share, retrieve, disseminate, transmit, or dispose of DOJ Information. It establishes and implements specific DOJ requirements applicable to this Contract. The requirements established herein are in addition to those required by the Federal Acquisition Regulation ("FAR"), including FAR 11.002(g) and 52.239-1, the Privacy Act of 1974, and any other applicable laws, mandates, Procurement Guidance Documents, and Executive Orders pertaining to the development and operation of Information Systems and the protection of Government Information. This clause does not alter or diminish any existing rights, obligation or liability under any other civil and/or criminal law, rule, regulation or mandate.

II. General Definitions

The following general definitions apply to this clause. Specific definitions also apply as set forth in other paragraphs.

A. **Information** means any communication or representation of knowledge such as facts, data, or opinions, in any form or medium, including textual, numerical, graphic, cartographic, narrative, or audiovisual. Information includes information in an electronic format that allows it

be stored, retrieved or transmitted, also referred to as "data," and "personally identifiable information" ("PII"), regardless of form.

B. **Personally Identifiable Information (or PII)** means any information about an individual maintained by an agency, including, but not limited to, information related to education, financial transactions, medical history, and criminal or employment history and information, which can be used to distinguish or trace an individual's identity, such as his or her name, social security number, date and place of birth, mother's maiden name, biometric records, etc., including any other personal information which is linked or linkable to an individual.

C. **DOJ Information** means any Information that is owned, produced, controlled, protected by, or otherwise within the custody or responsibility of the DOJ, including, without limitation, Information related to DOJ programs or personnel. It includes, without limitation, Information (1) provided by or generated for the DOJ, (2) managed or acquired by Contractor for the DOJ in connection with the performance of the contract, and/or (3) acquired in order to perform the contract.

D. **Information System** means any resources, or set of resources organized for accessing, collecting, storing, processing, maintaining, using, sharing, retrieving, disseminating, transmitting, or disposing of (hereinafter collectively, "processing, storing, or transmitting") Information.

E. **Covered Information System** means any information system used for, involved with, or allowing, the processing, storing, or transmitting of DOJ Information.

III. Confidentiality and Non-disclosure of DOJ Information

A. Preliminary and final deliverables and all associated working papers and material generated by Contractor containing DOJ Information are the property of the U.S. Government and must be submitted to the Contracting Officer ("CO") or the CO's Representative ("COR") at the conclusion of the contract. The U.S. Government has unlimited data rights to all such deliverables and associated working papers and materials in accordance with FAR 52.227-14.

B. All documents produced in the performance of this contract containing DOJ Information are the property of the U.S. Government and Contractor shall neither reproduce nor release to any third-party at any time, including during or at expiration or termination of the contract without the prior written permission of the CO.

C. Any DOJ information made available to Contractor under this contract shall be used only for the purpose of performance of this contract and shall not be divulged or made known in any manner to any persons except as may be necessary in the performance of this contract. In performance of this contract, Contractor assumes responsibility for the protection of the confidentiality of any and all DOJ Information processed, stored, or transmitted by the Contractor. When requested by the CO (typically no more than annually), Contractor shall provide a report to the CO identifying, to the best of Contractor's knowledge and belief, the type, amount, and level of sensitivity of the DOJ Information processed, stored, or transmitted under the Contract, including an estimate of the number of individuals for whom PII has been processed, stored or transmitted under the Contract and whether such information includes social security numbers (in whole or in part).

IV. Compliance with Information Technology Security Policies, Procedures and Requirements

A. For all Covered Information Systems, Contractor shall comply with all security requirements, including but not limited to the regulations and guidance found in the Federal Information Security Management Act of 2014 ("FISMA"), Privacy Act of 1974, E-Government Act of 2002, National Institute of Standards and Technology ("NIST") Special Publications ("SP"), including NIST SP 800-37, 800-53, and 800-60 Volumes I and II, Federal Information Processing Standards ("FIPS") Publications 140-2, 199, and 200, OMB Memoranda, Federal Risk and Authorization Management Program ("FedRAMP"), DOJ IT Security Standards, including DOJ Order 2640.2, as amended. These requirements include but are not limited to:

1. Limiting access to DOJ Information and Covered Information Systems to authorized users and to transactions and functions that authorized users are permitted to exercise;

2. Providing security awareness training including, but not limited to, recognizing and reporting potential indicators of insider threats to users and managers of DOJ Information and Covered Information Systems;

3. Creating, protecting, and retaining Covered Information System audit records, reports, and supporting documentation to enable reviewing, monitoring, analysis, investigation, reconstruction, and reporting of unlawful, unauthorized, or inappropriate activity related to such Covered Information Systems and/or DOJ Information;

4. Maintaining authorizations to operate any Covered Information System;

5. Performing continuous monitoring on all Covered Information Systems;

6. Establishing and maintaining baseline configurations and inventories of Covered Information Systems, including hardware, software, firmware, and documentation, throughout the Information System Development Lifecycle, and establishing and enforcing security configuration settings for IT products employed in Information Systems;

7. Ensuring appropriate contingency planning has been performed, including DOJ Information and Covered Information System backups;

8. Identifying Covered Information System users, processes acting on behalf of users, or devices, and authenticating and verifying the identities of such users, processes, or devices, using multifactor authentication or HSPD-12 compliant authentication methods where required;

9. Establishing an operational incident handling capability for Covered Information Systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities, and tracking, documenting, and reporting incidents to appropriate officials and authorities within Contractor's organization and the DOJ;

10. Performing periodic and timely maintenance on Covered Information Systems, and providing effective controls on tools, techniques, mechanisms, and personnel used to

conduct such maintenance;

11. [Reserved]

12. Protecting Covered Information System media containing DOJ Information, including paper, digital and electronic media; limiting access to DOJ Information to authorized users; and sanitizing or destroying Covered Information System media containing DOJ Information before disposal, release or reuse of such media;

13. Limiting physical access to Covered Information Systems, equipment, and physical facilities housing such Covered Information Systems to authorized U.S. citizens unless a waiver has been granted by the Contracting Officer ("CO"), and protecting the physical facilities and support infrastructure for such Information Systems;

14. Screening individuals prior to authorizing access to Covered Information Systems to ensure compliance with DOJ Security standards;

15. Assessing the risk to DOJ Information in Covered Information Systems periodically, including scanning for vulnerabilities and remediating such vulnerabilities in accordance with DOJ policy and ensuring the timely removal of assets no longer supported by the Contractor;

16. Assessing the security controls of Covered Information Systems periodically to determine if the controls are effective in their application, developing and implementing plans of action designed to correct deficiencies and eliminate or reduce vulnerabilities in such Information Systems, and monitoring security controls on an ongoing basis to ensure the continued effectiveness of the controls;

17. Monitoring, controlling, and protecting information transmitted or received by Covered Information Systems at the external boundaries and key internal boundaries of such Information Systems, and employing architectural designs, software development techniques, and systems engineering principles that promote effective security; and

18. Identifying, reporting, and correcting Covered Information System security flaws in a timely manner, providing protection from malicious code at appropriate locations, monitoring security alerts and advisories and taking appropriate action in response.

B. Contractor shall not process, store, or transmit DOJ Information using a Covered Information System without first obtaining an Authority to Operate ("ATO") for each Covered Information System. The ATO shall be signed by the Authorizing Official for the DOJ component responsible for maintaining the security, confidentiality, integrity, and availability of the DOJ Information under this contract. The DOJ standards and requirements for obtaining an ATO may be found at DOJ Order 2640.2, as amended. (For Cloud Computing Systems, see Section V, below.)

C. Contractor shall ensure that no Non-U.S. citizen accesses or assists in the development, operation, management, or maintenance of any DOJ Information System, unless a waiver has been granted by the by the DOJ Component Head (or his or her designee) responsible for the DOJ Information System, the DOJ Chief Information Officer, and the DOJ Security Officer.

D. When requested by the DOJ CO or COR, or other DOJ official as described below, in

connection with DOJ's efforts to ensure compliance with security requirements and to maintain and safeguard against threats and hazards to the security, confidentiality, integrity, and availability of DOJ Information, Contractor shall provide DOJ, including the Office of Inspector General ("OIG") and Federal law enforcement components, (1) access to any and all information and records, including electronic information, regarding a Covered Information System, and (2) physical access to Contractor's facilities, installations, systems, operations, documents, records, and databases. Such access may include independent validation testing of controls, system penetration testing, and FISMA data reviews by DOJ or agents acting on behalf of DOJ, and such access shall be provided within 72 hours of the request. Additionally, Contractor shall cooperate with DOJ's efforts to ensure, maintain, and safeguard the security, confidentiality, integrity, and availability of DOJ Information.

E. The use of Contractor-owned laptops or other portable digital or electronic media to process or store DOJ Information covered by this clause is prohibited until Contractor provides a letter to the DOJ CO, and obtains the CO's approval, certifying compliance with the following requirements:

1. Media must be encrypted using a NIST FIPS 140-2 approved product;

2. Contractor must develop and implement a process to ensure that security and other applications software is kept up-to-date;

3. Where applicable, media must utilize antivirus software and a host-based firewall mechanism;

4. Contractor must log all computer-readable data extracts from databases holding DOJ Information and verify that each extract including such data has been erased within 90 days of extraction or that its use is still required. All DOJ Information is sensitive information unless specifically designated as non-sensitive by the DOJ; and,

5. A Rules of Behavior ("ROB") form must be signed by users. These rules must address, at a minimum, authorized and official use, prohibition against unauthorized users and use, and the protection of DOJ Information. The form also must notify the user that he or she has no reasonable expectation of privacy regarding any communications transmitted through or data stored on Contractor-owned laptops or other portable digital or electronic media.

F. Contractor-owned removable media containing DOJ Information shall not be removed from DOJ facilities without prior approval of the DOJ CO or COR.

G. When no longer needed, all media must be processed (sanitized, degaussed, or destroyed) in accordance with DOJ security requirements.

H. Contractor must keep an accurate inventory of digital or electronic media used in the performance of DOJ contracts.

I. Contractor must remove all DOJ Information from Contractor media and return all such information to the DOJ within 15 days of the expiration or termination of the contract, unless otherwise extended by the CO, or waived (in part or whole) by the CO, and all such information

shall be returned to the DOJ in a format and form acceptable to the DOJ. The removal and return of all DOJ Information must be accomplished in accordance with DOJ IT Security Standard requirements, and an official of the Contractor shall provide a written certification certifying the removal and return of all such information to the CO within 15 days of the removal and return of all DOJ Information.

J. DOJ, at its discretion, may suspend Contractor's access to any DOJ Information, or terminate the contract, when DOJ suspects that Contractor has failed to comply with any security requirement, or in the event of an Information System Security Incident (see Section V.E. below), where the Department determines that either event gives cause for such action. The suspension of access to DOJ Information may last until such time as DOJ, in its sole discretion, determines that the situation giving rise to such action has been corrected or no longer exists. Contractor understands that any suspension or termination in accordance with this provision shall be at no cost to the DOJ, and that upon request by the CO, Contractor must immediately return all DOJ Information to DOJ, as well as any media upon which DOJ Information resides, at Contractor's expense.

V. Cloud Computing

A. **Cloud Computing** means an Information System having the essential characteristics described in NIST SP 800-145, *The NIST Definition of Cloud Computing.* For the sake of this provision and clause, Cloud Computing includes Software as a Service, Platform as a Service, and Infrastructure as a Service, and deployment in a Private Cloud, Community Cloud, Public Cloud, or Hybrid Cloud.

B. Contractor may not utilize the Cloud system of any CSP unless:

1. The Cloud system and CSP have been evaluated and approved by a 3PAO certified under FedRAMP and Contractor has provided the most current Security Assessment Report ("SAR") to the DOJ CO for consideration as part of Contractor's overall System Security Plan, and any subsequent SARs within 30 days of issuance, and has received an ATO from the Authorizing Official for the DOJ component responsible for maintaining the security confidentiality, integrity, and availability of the DOJ Information under contract; or,

2. If not certified under FedRAMP, the Cloud System and CSP have received an ATO signed by the Authorizing Official for the DOJ component responsible for maintaining the security, confidentiality, integrity, and availability of the DOJ Information under the contract.

C. Contractor must ensure that the CSP allows DOJ to access and retrieve any DOJ Information processed, stored or transmitted in a Cloud system under this Contract within a reasonable time of any such request, but in no event less than 48 hours from the request. To ensure that the DOJ can fully and appropriately search and retrieve DOJ Information from the Cloud system, access shall include any schemas, meta-data, and other associated data artifacts.

VI. Information System Security Breach or Incident

A. Definitions

1. **Confirmed Security Breach** (hereinafter, "Confirmed Breach") means any confirmed unauthorized exposure, loss of control, compromise, exfiltration, manipulation, disclosure, acquisition, or accessing of any Covered Information System or any DOJ Information accessed by, retrievable from, processed by, stored on, or transmitted within, to or from any such system.

2. **Potential Security Breach** (hereinafter, "Potential Breach") means any suspected, but unconfirmed, Covered Information System Security Breach.

3. **Security Incident** means any Confirmed or Potential Covered Information System Security Breach.

B. Confirmed Breach. Contractor shall immediately (and in no event later than within 1 hour of discovery) report any Confirmed Breach to the DOJ CO and the CO's Representative ("COR"). If the Confirmed Breach occurs outside of regular business hours and/or neither the DOJ CO nor the COR can be reached, Contractor must call DOJ-CERT at 1-866-US4-CERT (1-866-874-2378) immediately (and in no event later than within 1 hour of discovery of the Confirmed Breach), and shall notify the CO and COR as soon as practicable.

C. Potential Breach.

1. Contractor shall report any Potential Breach within 72 hours of detection to the DOJ CO and the COR, *unless* Contractor has (a) completed its investigation of the Potential Breach in accordance with its own internal policies and procedures for identification, investigation and mitigation of Security Incidents and (b) determined that there has been no Confirmed Breach.

2. If Contractor has not made a determination within 72 hours of detection of the Potential Breach whether an Confirmed Breach has occurred, Contractor shall report the Potential Breach to the DOJ CO and COR within one-hour (i.e., 73 hours from detection of the Potential Breach). If the time by which to report the Potential Breach occurs outside of regular business hours and/or neither the DOJ CO nor the COR can be reached, Contractor must call the DOJ Computer Emergency Readiness Team (DOJ-CERT) at 1-866-US4-CERT (1-866-874-2378) within one-hour (i.e., 73 hours from detection of the Potential Breach) and contact the DOJ CO and COR as soon as practicable.

D. Any report submitted in accordance with paragraphs (B) and (C), above, shall identify (1) both the Information Systems and DOJ Information involved or at risk, including the type, amount, and level of sensitivity of the DOJ Information and, if the DOJ Information contains PII, the estimated number of unique instances of PII, (2) all steps and processes being undertaken by Contractor to minimize, remedy, and/or investigate the Security Incident, (3) any and all other information as required by the US-CERT Federal Incident Notification Guidelines, including the functional impact, information impact, impact to recoverability, threat vector, mitigation details, and all available incident details; and (4) any other information specifically requested by the DOJ. Contractor shall continue to provide written updates to the DOJ CO regarding the status of the Security Incident at least every three (3) calendar days until informed otherwise by the DOJ CO.

E. All determinations regarding whether and when to notify individuals and/or federal agencies potentially affected by a Security Incident will be made by DOJ senior officials or the DOJ Core Management Team at DOJ's discretion.

F. Upon notification of a Security Incident in accordance with this section, Contractor must provide to DOJ full access to any affected or potentially affected facility and/or Information System, including access by the DOJ OIG and Federal law enforcement organizations, and undertake any and all response actions DOJ determines are required to ensure the protection of DOJ Information, including providing all requested images, log files, and event information to facilitate rapid resolution of any Security Incident.

G. DOJ, at its sole discretion, may obtain, and Contractor will permit, the assistance of other federal agencies and/or third party contractors or firms to aid in response activities related to any Security Incident. Additionally, DOJ, at its sole discretion, may require Contractor to retain, at Contractor's expense, a Third Party Assessing Organization (3PAO), acceptable to DOJ, with expertise in incident response, compromise assessment, and federal security control requirements, to conduct a thorough vulnerability and security assessment of all affected Information Systems.

H. Response activities related to any Security Incident undertaken by DOJ, including activities undertaken by Contractor, other federal agencies, and any third-party contractors or firms at the request or direction of DOJ, may include inspections, investigations, forensic reviews, data analyses and processing, and final determinations of responsibility for the Security Incident and/or liability for any additional response activities. Contractor shall be responsible for all costs and related resource allocations required for all such response activities related to any Security Incident, including the cost of any penetration testing.

VII. Personally Identifiable Information Notification Requirement

Contractor certifies that it has a security policy in place that contains procedures to promptly notify any individual whose Personally Identifiable Information ("PII") was, or is reasonably determined by DOJ to have been, compromised. Any notification shall be coordinated with the DOJ CO and shall not proceed until the DOJ has made a determination that notification would not impede a law enforcement investigation or jeopardize national security. The method and content of any notification by Contractor shall be coordinated with, and subject to the approval of, DOJ. Contractor shall be responsible for taking corrective action consistent with DOJ Data Breach Notification Procedures and as directed by the DOJ CO, including all costs and expenses associated with such corrective action, which may include providing credit monitoring to any individuals whose PII was actually or potentially compromised.

VIII. Pass-through of Security Requirements to Subcontractors and CSPs

The requirements set forth in the preceding paragraphs of this clause apply to all subcontractors and CSPs who perform work in connection with this Contract, including any CSP providing services for any other CSP under this Contract, and Contractor shall flow down this clause to all subcontractors and CSPs performing under this contract. Any breach by any subcontractor or CSP of any of the provisions set forth in this clause will be attributed to Contractor.

(End of Clause)

ATF-50 LIMITATIONS ON SUBCONTRACTING UNDER SMALL BUSINESS SET-ASIDES (May 24, 2019)

In conjunction with the requirements of FAR 52.219-14, Limitations on Subcontracting, contractors shall certify the level of

subcontracting proposed, prior to award of any portion of the contract set-aside or partially set-aside for a small business or 8(a)

participant. Contractors shall also certify the level of subcontracting actually achieved prior to exercising any option period.

(Offerors shall indicate "N/A" for lines that are Not Applicable.)

1) Services (except construction). Contractor's proposed percent of the cost of contract performance incurred for personnel shall be

expended for employees of concern: _____ (must be at least 50%).

2) Supplies (other than procurement from a non-manufacturer of such supplies). Contractor's proposed work to be performed as

percent of the cost of manufacturing the supplies, not including the cost of materials: _____ (must be at least 50%).

3) General construction. Offeror's proposed work to be performed as percent of the cost of the contract, not including the cost of

materials, with its own employees: _____ (must be at least 15%).

4) Construction by special trade contractors. Offeror's proposed work to be performed as percent of the cost of the contract, not

including the cost of materials, with its own employees: _____ (must be at least 25%).

(End of Clause)

52.204-24 Representation Regarding Certain Telecommunications and Video Surveillance Services or Equipment.

As prescribed in 4.2105(a), insert the following provision:

Representation Regarding Certain Telecommunications and Video Surveillance Services or Equipment (Nov 2021)

The Offeror shall not complete the representation at paragraph (d)(1) of this provision if the Offeror has represented that it "does not provide covered telecommunications equipment or services as a part of its

offered products or services to the Government in the performance of any contract, subcontract, or other contractual instrument" in paragraph (c)(1) in the provision at 52.204-26, Covered Telecommunications Equipment or Services—Representation, or in paragraph (v)(2)(i) of the provision at 52.212-3, Offeror Representations and Certifications-Commercial Products or Commercial Services. The Offeror shall not complete the representation in paragraph (d)(2) of this provision if the Offeror has represented that it "does not use covered telecommunications equipment or services, or any equipment, system, or service that uses covered telecommunications equipment or services" in paragraph (c)(2) of the provision at 52.204-26, or in paragraph (v)(2)(ii) of the provision at 52.212-3.

(a) Definitions. As used in this provision—

Backhaul, covered telecommunications equipment or services, critical technology, interconnection arrangements, reasonable inquiry, roaming, and substantial or essential component have the meanings provided in the clause 52.204-25, Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment.

(b) Prohibition. (1) Section 889(a)(1)(A) of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Pub. L. 115-232) prohibits the head of an executive agency on or after August 13, 2019, from procuring or obtaining, or extending or renewing a contract to procure or obtain, any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system. Nothing in the prohibition shall be construed to—

(i) Prohibit the head of an executive agency from procuring with an entity to provide a service that connects to the facilities of a third-party, such as backhaul, roaming, or interconnection arrangements; or

(ii) Cover telecommunications equipment that cannot route or redirect user data traffic or cannot permit visibility into any user data or packets that such equipment transmits or otherwise handles.

(2) Section 889(a)(1)(B) of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Pub. L. 115-232) prohibits the head of an executive agency on or after August 13, 2020, from entering into a contract or extending or renewing a contract with an entity that uses any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system. This prohibition applies to the use of covered telecommunications equipment or services, regardless of whether that use is in performance of work under a Federal contract. Nothing in the prohibition shall be construed to—

(i) Prohibit the head of an executive agency from procuring with an entity to provide a service that connects to the facilities of a third-party, such as backhaul, roaming, or interconnection arrangements; or

(ii) Cover telecommunications equipment that cannot route or redirect user data traffic or cannot permit visibility into any user data or packets that such equipment transmits or otherwise handles.

(c) Procedures. The Offeror shall review the list of excluded parties in the System for Award Management (SAM) (https://www.sam.gov) for entities excluded from receiving federal awards for "covered telecommunications equipment or services".

(d) Representation. The Offeror represents that—

(1) It □ will, □ will not provide covered telecommunications equipment or services to the Government in the performance of any contract, subcontract or other contractual instrument resulting from this solicitation. The Offeror shall provide the additional disclosure information required at paragraph (e)(1) of this section if the Offeror responds "will" in paragraph (d)(1) of this section; and

(2) After conducting a reasonable inquiry, for purposes of this representation, the Offeror represents that—

It □ does, □ does not use covered telecommunications equipment or services, or use any equipment, system, or service that uses covered telecommunications equipment or services. The Offeror shall provide the additional disclosure information required at paragraph (e)(2) of this section if the Offeror responds "does" in paragraph (d)(2) of this section.

(e) Disclosures. (1) Disclosure for the representation in paragraph (d)(1) of this provision. If the Offeror has responded "will" in the representation in paragraph (d)(1) of this provision, the Offeror shall provide the following information as part of the offer:

(i) For covered equipment—

(A) The entity that produced the covered telecommunications equipment (include entity name, unique entity identifier, CAGE code, and whether the entity was the original equipment manufacturer (OEM) or a distributor, if known);

(B) A description of all covered telecommunications equipment offered (include brand; model number, such as OEM number, manufacturer part number, or wholesaler number; and item description, as applicable); and

(C) Explanation of the proposed use of covered telecommunications equipment and any factors relevant

to determining if such use would be permissible under the prohibition in paragraph (b)(1) of this provision.

(ii) For covered services—

(A) If the service is related to item maintenance: A description of all covered telecommunications services offered (include on the item being maintained: Brand; model number, such as OEM number, manufacturer part number, or wholesaler number; and item description, as applicable); or

(B) If not associated with maintenance, the Product Service Code (PSC) of the service being provided; and explanation of the proposed use of covered telecommunications services and any factors relevant to determining if such use would be permissible under the prohibition in paragraph (b)(1) of this provision.

(2) Disclosure for the representation in paragraph (d)(2) of this provision. If the Offeror has responded "does" in the representation in paragraph (d)(2) of this provision, the Offeror shall provide the following information as part of the offer:

(i) For covered equipment—

(A) The entity that produced the covered telecommunications equipment (include entity name, unique entity identifier, CAGE code, and whether the entity was the OEM or a distributor, if known);

(B) A description of all covered telecommunications equipment offered (include brand; model number, such as OEM number, manufacturer part number, or wholesaler number; and item description, as applicable); and

(C) Explanation of the proposed use of covered telecommunications equipment and any factors relevant to determining if such use would be permissible under the prohibition in paragraph (b)(2) of this provision.

(ii) For covered services—

(A) If the service is related to item maintenance: A description of all covered telecommunications services offered (include on the item being maintained: Brand; model number, such as OEM number, manufacturer part number, or wholesaler number; and item description, as applicable); or

(B) If not associated with maintenance, the PSC of the service being provided; and explanation of the proposed use of covered telecommunications services and any factors relevant to determining if such use would be permissible under the prohibition in paragraph (b)(2) of this provision.

(End of provision)

52.204-26 Covered Telecommunications Equipment or Services-Representation.

As prescribed in 4.2105(c), insert the following provision:

Covered Telecommunications Equipment or Services-Representation (Oct 2020)

(a) Definitions. As used in this provision, "covered telecommunications equipment or services" and "reasonable inquiry" have the meaning provided in the clause 52.204-25, Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment.

(b) Procedures. The Offeror shall review the list of excluded parties in the System for Award Management (SAM) (https://www.sam.gov) for entities excluded from receiving federal awards for "covered telecommunications equipment or services".

(c) (1) Representation. The Offeror represents that it □ does, □ does not provide covered telecommunications equipment or services as a part of its offered products or services to the Government in the performance of any contract, subcontract, or other contractual instrument.

(2) After conducting a reasonable inquiry for purposes of this representation, the offeror represents that it □ does, □ does not use covered telecommunications equipment or services, or any equipment, system, or service that uses covered telecommunications equipment or services.

(End of provision)

52.209-5 Certification Regarding Responsibility Matters.

As prescribed in 9.104-7(a), insert the following provision:

Certification Regarding Responsibility Matters (Aug 2020)

(a) (1) The Offeror certifies, to the best of its knowledge and belief, that—

(i) The Offeror and/or any of its Principals–

(A) Are □ are not □ presently debarred, suspended, proposed for debarment, or declared ineligible for the award of contracts by any Federal agency;

(B) Have □ have not □, within a three-year period preceding this offer, been convicted of or had a civil judgment rendered against them for: commission of fraud or a criminal offense in connection with obtaining, attempting to obtain, or performing a public (Federal, State, or local) contract or subcontract; violation of Federal or State antitrust statutes relating to the submission of offers; or commission of embezzlement, theft, forgery, bribery, falsification or destruction of records, making false statements, tax evasion, violating Federal criminal tax laws, or receiving stolen property (if offeror checks "have", the offeror shall also see 52.209-7, if included in this solicitation);

(C) Are □ are not □ presently indicted for, or otherwise criminally or civilly charged by a governmental entity with, commission of any of the offenses enumerated in paragraph (a)(1)(i)(B) of this provision;

(D) Have □, have not □, within a three-year period preceding this offer, been notified of any delinquent Federal taxes in an amount that exceeds the threshold at 9.104-5(a)(2) for which the liability remains unsatisfied.

(1) Federal taxes are considered delinquent if both of the following criteria apply:

(i) The tax liability is finally determined. The liability is finally determined if it has been assessed. A liability is not finally determined if there is a pending administrative or judicial challenge. In the case of a judicial challenge to the liability, the liability is not finally determined until all judicial appeal rights have been exhausted.

(ii) The taxpayer is delinquent in making payment. A taxpayer is delinquent if the taxpayer has failed to pay the tax liability when full payment was due and required. A taxpayer is not delinquent in cases where

enforced collection action is precluded.

(2) Examples.

(i) The taxpayer has received a statutory notice of deficiency, under I.R.C. § 6212, which entitles the taxpayer to seek Tax Court review of a proposed tax deficiency. This is not a delinquent tax because it is not a final tax liability. Should the taxpayer seek Tax Court review, this will not be a final tax liability until the taxpayer has exercised all judicial appeal rights.

(ii) The IRS has filed a notice of Federal tax lien with respect to an assessed tax liability, and the taxpayer has been issued a notice under I.R.C. § 6320 entitling the taxpayer to request a hearing with the IRS Office of Appeals contesting the lien filing, and to further appeal to the Tax Court if the IRS determines to sustain the lien filing. In the course of the hearing, the taxpayer is entitled to contest the underlying tax liability because the taxpayer has had no prior opportunity to contest the liability. This is not a delinquent tax because it is not a final tax liability. Should the taxpayer seek tax court review, this will not be a final tax liability until the taxpayer has exercised all judicial appeal rights.

(iii) The taxpayer has entered into an installment agreement pursuant to I.R.C. § 6159. The taxpayer is making timely payments and is in full compliance with the agreement terms. The taxpayer is not delinquent because the taxpayer is not currently required to make full payment.

(iv) The taxpayer has filed for bankruptcy protection. The taxpayer is not delinquent because enforced collection action is stayed under 11 U.S.C. 362 (the Bankruptcy Code).

(ii) The Offeror has □ has not □, within a three-year period preceding this offer, had one or more contracts terminated for default by any Federal agency.

(2) "Principal," for the purposes of this certification, means an officer, director, owner, partner, or a person having primary management or supervisory responsibilities within a business entity (e.g., general manager; plant manager; head of a division or business segment; and similar positions).

This Certification Concerns a Matter Within the Jurisdiction of an Agency of the United States and the Making of a False, Fictitious, or Fraudulent Certification May Render the Maker Subject to Prosecution Under Section 1001, Title 18, United States Code.

(b) The Offeror shall provide immediate written notice to the Contracting Officer if, at any time prior to

contract award, the Offeror learns that its certification was erroneous when submitted or has become erroneous by reason of changed circumstances.

(c) A certification that any of the items in paragraph (a) of this provision exists will not necessarily result in withholding of an award under this solicitation. However, the certification will be considered in connection with a determination of the Offeror's responsibility. Failure of the Offeror to furnish a certification or provide such additional information as requested by the Contracting Officer may render the Offeror nonresponsible.

(d) Nothing contained in the foregoing shall be construed to require establishment of a system of records in order to render, in good faith, the certification required by paragraph (a) of this provision. The knowledge and information of an Offeror is not required to exceed that which is normally possessed by a prudent person in the ordinary course of business dealings.

(e) The certification in paragraph (a) of this provision is a material representation of fact upon which reliance was placed when making award. If it is later determined that the Offeror knowingly rendered an erroneous certification, in addition to other remedies available to the Government, the Contracting Officer may terminate the contract resulting from this solicitation for default.

(End of provision)

52.209-7 Information Regarding Responsibility Matters.

As prescribed at 9.104-7(b), insert the following provision:

Information Regarding Responsibility Matters (Oct 2018)

(a) Definitions. As used in this provision—

Administrative proceeding means a non-judicial process that is adjudicatory in nature in order to make a determination of fault or liability (e.g., Securities and Exchange Commission Administrative Proceedings, Civilian Board of Contract Appeals Proceedings, and Armed Services Board of Contract Appeals Proceedings). This includes administrative proceedings at the Federal and State level but only in connection with performance of a Federal contract or grant. It does not include agency actions such as contract audits, site visits, corrective plans, or inspection of deliverables.

Federal contracts and grants with total value greater than $10,000,000 means—

(1) The total value of all current, active contracts and grants, including all priced options; and

(2) The total value of all current, active orders including all priced options under indefinite-delivery, indefinite-quantity, 8(a), or requirements contracts (including task and delivery and multiple-award Schedules).

Principal means an officer, director, owner, partner, or a person having primary management or supervisory responsibilities within a business entity (e.g., general manager; plant manager; head of a division or business segment; and similar positions).

(b) The offeror □ has □ does not have current active Federal contracts and grants with total value greater than $10,000,000.

(c) If the offeror checked "has" in paragraph (b) of this provision, the offeror represents, by submission of this offer, that the information it has entered in the Federal Awardee Performance and Integrity Information System (FAPIIS) is current, accurate, and complete as of the date of submission of this offer with regard to the following information:

(1) Whether the offeror, and/or any of its principals, has or has not, within the last five years, in connection with the award to or performance by the offeror of a Federal contract or grant, been the subject of a proceeding, at the Federal or State level that resulted in any of the following dispositions:

(i) In a criminal proceeding, a conviction.

(ii) In a civil proceeding, a finding of fault and liability that results in the payment of a monetary fine, penalty, reimbursement, restitution, or damages of $5,000 or more.

(iii) In an administrative proceeding, a finding of fault and liability that results in–

(A) The payment of a monetary fine or penalty of $5,000 or more; or

(B) The payment of a reimbursement, restitution, or damages in excess of $100,000.

(iv) In a criminal, civil, or administrative proceeding, a disposition of the matter by consent or compromise with an acknowledgment of fault by the Contractor if the proceeding could have led to any of the outcomes specified in paragraphs (c)(1)(i), (c)(1)(ii), or (c)(1)(iii) of this provision.

(2) If the offeror has been involved in the last five years in any of the occurrences listed in (c)(1) of this provision, whether the offeror has provided the requested information with regard to each occurrence.

(d) The offeror shall post the information in paragraphs (c)(1)(i) through (c)(1)(iv) of this provision in FAPIIS as required through maintaining an active registration in the System for Award Management, which can be accessed via https://www.sam.gov (see 52.204-7).

(End of provision)

52.209-11 Representation by Corporations Regarding Delinquent Tax Liability or a Felony Conviction under any Federal Law.

As prescribed in 9.104-7(d), insert the following provision:

Representation by Corporations Regarding Delinquent Tax Liability or a Felony Conviction under any Federal Law (Feb 2016)

(a) As required by sections 744 and 745 of Division E of the Consolidated and Further Continuing Appropriations Act, 2015 (Pub. L. 113-235), and similar provisions, if contained in subsequent appropriations acts, the Government will not enter into a contract with any corporation that–

(1) Has any unpaid Federal tax liability that has been assessed, for which all judicial and administrative remedies have been exhausted or have lapsed, and that is not being paid in a timely manner pursuant to an agreement with the authority responsible for collecting the tax liability, where the awarding agency is aware of the unpaid tax liability, unless an agency has considered suspension or debarment of the corporation and made a determination that suspension or debarment is not necessary to protect the interests of the Government; or

(2) Was convicted of a felony criminal violation under any Federal law within the preceding 24 months, where the awarding agency is aware of the conviction, unless an agency has considered suspension or debarment of the corporation and made a determination that this action is not necessary to protect the interests of the Government.

(b) The Offeror represents that–

(1) It is □ is not □ a corporation that has any unpaid Federal tax liability that has been assessed, for which all judicial and administrative remedies have been exhausted or have lapsed, and that is not being paid in a timely manner pursuant to an agreement with the authority responsible for collecting the tax liability; and

(2) It is □ is not □ a corporation that was convicted of a felony criminal violation under a Federal law within the preceding 24 months.

(End of provision)

52.222-22 Previous Contracts and Compliance Reports.

As prescribed in 22.810(a)(2), insert the following provision:

Previous Contracts and Compliance Reports (Feb 1999)

The offeror represents that-

It □ has, □ has not participated in a previous contract or subcontract subject to the Equal Opportunity clause of this solicitation;

It □ has, □ has not filed all required compliance reports; and

Representations indicating submission of required compliance reports, signed by proposed subcontractors, will be obtained before subcontract awards.

(End of provision)

52.212-2 Evaluation—Commercial Products and Commercial Services.

As prescribed in 12.301(c), the Contracting Officer may insert a provision substantially as follows:

Evaluation—Commercial Products and Commercial Services (Nov 2021)

(a) The Government will award a contract resulting from this solicitation to the responsible offeror whose offer conforming to the solicitation will be most advantageous to the Government, price and other factors considered. The following factors shall be used to evaluate offers:

Technical capability and price.

Technically capable is defined as meeting or exceeding the specifications found in the Statement of Work and solicitation instructions.

Price will be evaluated in accordance with FAR 13.106-3 for fair and reasonableness determination.

(b) Options. The Government will evaluate offers for award purposes by adding the total price for all options to the total price for the basic requirement. The Government may determine that an offer is unacceptable if the option prices are significantly unbalanced. Evaluation of options shall not obligate the Government to exercise the option(s).

(c) A written notice of award or acceptance of an offer, mailed or otherwise furnished to the successful offeror within the time for acceptance specified in the offer, shall result in a binding contract without further action by either party. Before the offer's specified expiration time, the Government may accept an offer (or part of an offer), whether or not there are negotiations after its receipt, unless a written notice of withdrawal is received before award.

(End of provision)