15JA0522Q00000103

STATEMENT OF WORK
ACE Fraud Investigator Support Services
United States Attorney's Office
Location XXX

1. PURPOSE.

The Department of Justice, United States Attorney's Office (USAO) - Location XXX has a requirement for an Affirmative Civil Enforcement (ACE) Fraud Investigator to work within the ACE program designed to advance and protect the financial and programmatic interests of the United States through civil investigations and litigation.

2. BACKGROUND.

The ACE Program at the USAO for the NDNY uses federal civil enforcement laws to combat fraud, waste, and abuse in federal programs, and to pursue enforcement actions against those who violate federal environmental and civil rights laws. The NDNY will be assigning cases and matters that vary in scope and complexity, but characteristically involve difficult and complex financial and regulatory issues and schemes giving rise to civil actions within the jurisdiction of the USAO NDNY.

3. SCOPE OF WORK.

The Contractor shall provide one (1) ACE Fraud Investigator to perform the following job duties:

- Based upon the general direction provided by the Assistant United States Attorney (AUSA) to whom a case is assigned, the investigator assists with the planning and conducting of investigations of a highly complex and difficult nature. Perform quantitative, qualitative, and other analyses of relevant facts, data, account information, etc., and prepares the results to support the mission of the USAO NDNY's ACE Program. Investigations may be conducted solely by the USAO, or more typically, in conjunction with other agencies.

- Manage complex investigations from beginning to end, including attending and conducting intake meetings, background research, and summarizing findings for AUSAs.

- Document investigative findings and recommendations.

- Identify anomalies or other "red flags" in complex data (e.g., healthcare billing and claims data; procurement payment data; etc.) to build proactive investigations and triage existing investigations.

- Develop an understanding of the civil False Claims Act, the Controlled Substances Act, and other laws to the extent necessary to make sound decisions on direction and scope of investigations and case development.

- In conjunction with assigned AUSAs, establish investigative plans for gathering evidence in investigations.

- Provide specialized skills and investigative analysis relevant to violations of federal law.

- Communicate with federal, state, and local officials, and other organizations and individuals related to subject of investigation for the purpose of gathering facts, obtaining statements, learning sequences of events, obtaining explanations, and otherwise advancing investigative objectives.

- Prepare draft subpoenas for testimony, documents and written discovery, and other forms of requests for information, and serves the approved instrument.

- Examine financial records, corporate documents, books, ledgers, payrolls, cost reports, medical records, billing statements, invoices, correspondence, computer data and other records pertaining to the transactions, events, or allegations under investigation.

- Establish and/or verify relationships of all facts and evidence obtained or presented to confirm authenticity of documents, corroborate witness statements, and otherwise build proof necessary for successful litigation.

- Secure the storage, preservation, organization, filing and indexing of voluminous documentary evidence and aids in the review of such evidence.

- Use provided electronic databases to identify assets, verify employment and conduct financial analyses.

- Prepare interim and final reports on progress of investigations for use by AUSAs. Include significant findings and conclusions, recommendations for additional investigative actions and candid assessments of strengths and weaknesses of witnesses, documentary evidence or other aspects of the case.

- Prepare summaries and digests of pertinent data, depositions, and other transcripts, compile indexes, assist in the creation of charts, graphs, videotapes and other audio-visual materials for use by AUSAs for motions, depositions, and in mediations, and trials. Assist AUSAs with selection of witnesses and ensure their attendance through subpoena or otherwise.

- Meet and coordinate with designated agency personnel for the purpose of investigating

allegations. - Other related duties as assigned and within scope.

4. BASIC QUALIFICATIONS

The Contractor shall provide a candidate that possesses the following qualifications:

- Four (4) year undergraduate degree in criminal justice, law enforcement, statistical/data analysis, finance, accounting, or other related field or higher
- Minimum three (3) years of professional work experience planning and conducting complex civil investigations
- Proficient in Microsoft Office applications (Word, PowerPoint, Excel)
- U.S. Citizenship and ability to obtain adjudication for the requisite background investigation - Experience and expertise in performing the requisite services in Section 3

Preferred qualifications:

- Related experience working with a federal or state legal or law enforcement entity
- Experience reviewing and understanding medical records and/or knowledge of medical billing procedures, accounting principles, or statistical/data analysis
- Experience analyzing, organizing, and presenting a large volume of data such as bank records, financial records, healthcare claims, tax records, etc., through the use of common software programs

5. CONTRACT TYPE.

Firm Fixed Price. Monthly rates shall include wages, overhead, general and administrative expenses, and profit.

6. PERIOD OF PERFORMANCE.

The period of performance will include a base year and four consecutive one-year options as

follows: Base Year: September 28 2022 – September 27 2023

Option Year I: September 28 2023 – September 27 2024
Option Year II: September 28 2024 – September 27 2025
Option Year III: September 28 2025 – September 27 2026
Option Year IV: September 28 2026 – September 27 2027

7. PLACE OF PERFORMANCE.

The assigned work location shall be:

XXX

OR

XXX

Place of performance will be one of the two USAO offices listed. One of the two USAO offices will be selected at time of contract award based on the location of the prospective awardee candidate location.

Off-site performance of work may be permitted dependent upon Program Manager or COR approval. Any approval for off-site work shall not be considered permanent unless specifically authorized in writing by the Contracting Officer.

8. HOURS OF PERFORMANCE.

The Contractor shall generally be required to perform duties during normal, core business hours of Monday – Friday, 8:30 a.m. to 5:00 p.m except Federal Holidays. Based on office needs, some scheduling flexibility may be necessary and will be authorized in advance.

The Contractor shall not perform work at Government facilities on Federal holidays or other non-work days without prior approval of the Contracting Officer and/or COR. Work performed on holidays, weekends, or other non-work days, shall be billable at regular approved rates unless otherwise

negotiated and approved by the CO in accordance with GSAM 552.212-4. Overtime shall not be worked without prior approval of the Contracting Officer and/or COR. The Government observes the following Federal holidays as non-work days:

- New Year's Day
- Martin Luther King's Birthday
- Washington's Birthday
- Memorial Day
- Juneteenth National Independence Day
- Independence Day
- Labor Day
- Columbus Day
- Veteran's Day
- Thanksgiving Day
- Christmas Day

There are certain types of irregularly occurring circumstances that prompt the Government to close its offices where Contractor personnel are working, either on a national or local basis (i.e., bomb threats, inclement

weather, power outages, death of a national figure, or funding lapses). Contractor personnel shall not work if the Government is closed. Non-work due to the Government closing its facility is not an expense directly reimbursable to the Contractor.

9. GOVERNMENT FURNISHED SUPPORT.

The Government will provide Contractor personnel with access to the facilities during normal business hours from 8:30 a.m. to 5:30 p.m., or otherwise as needed. The Government will provide the Contractor

with access to office space, desk, computer, telephone, facsimile machines, copiers, supplies, and other general office equipment necessary to perform the requested work.

10. POINTS OF CONTACT.

Contracting Officer Representative (COR)

TBD

Contracting Officer (CO).

Contracting Officer
Executive Office for U.S. Attorneys (EOUSA)

Written communications shall make reference to the Contract number and shall be e-mailed to .

11. TRAVEL.

Travel may be required within the district or occasionally outside the district as-needed to perform job duties as directed by the USAO. When travel is required, it shall be pre-approved by the Contracting Officer, COR, or Civil Chief. Local travel (within 50 miles of the place of performance) and travel time will not be reimbursed by the Government. All travel expenses shall be reimbursed in accordance with Federal Travel Regulations (FTR). Contractors are expected to incur expenses prudently. Travel shall be submitted with back-up documentation and receipts provided as required by the FTR.

12. TRAINING

The Contractor shall ensure its employees on this Contract are trained on "contract-specific" issues such as Department of Justice ethics, standards of conduct, individual conflict of interest, confidentiality requirements, Department of Justice security requirements, understanding the function

of reporting, and the importance of quality control and quality assurance. In addition, Contractor managers shall be educated in the terms and conditions of the Contract.

DOJ Ethics - All Contractor personnel must view the Department of Justice ethics presentation within the first two weeks of performance. The Contractor shall notify the COR upon completion of the task. The COR will maintain a record of completion of this training in the official file.

Cybersecurity Awareness Training (CSAT) – All Contractor personnel having access to a Department Information System shall be required to complete the annual Cybersecurity Awareness Training.

13. SECURITY REQUIREMENTS.

Contractor Personnel will be required to undergo requisite security clearance and background investigations as directed by the USAO. The vendor shall pre-screen applicants and only offer candidates who are capable and expected to pass these screenings.

14. ACCEPTANCE CRITERIA.

The Government will assess performance continuously during this Contract. The Government will evaluate the work performed based on the degree to which the Contractor fulfills the requirements identified in the Scope of Work. Assigned tasks are completed according to agreed upon due dates.

If at any time during this Contract the Government finds that the quality of service does not fulfill the requirements identified in the Statement of Work, the Contracting Officer or COR will provide official written notification to the Contractor and require rework.

Replacement of any key personnel is subject to the prior written consent from the Government. The Contractor shall notify the Contracting Officer 14 business days prior to making any changes in key personnel, or not later than 10 business days if the change was not anticipated. The Contractor must
demonstrate that the qualifications of the prospective replacement personnel are equal to, or better than, the qualifications of the personnel being replaced by submitting resumes for approval by the CO's authorized Government representative. All replacement personnel must be qualified to assume the duties and responsibilities of the position, provide the same levels of effort as the replaced staff.

15. INVOICE INSTRUCTIONS.

Invoices shall be submitted no more often than monthly to . All travel reimbursement shall comply with allowable, published Federal rates and shall be in compliance with FTR.

Each invoice shall contain the following information:

- Contractor Name
- Tax Identification Number
- Contractor's Mailing Address
- Telephone Number
- Contract/Order Number
- Date of Invoice
- Invoice Number
- Total Invoice Amount
- Description of services provided, including dates services were rendered

Invoices that are not properly submitted, or that contain incorrect data, will be returned/rejected for revision. **16. CONFIDENTIALITY.**

The Contractor shall not reveal, divulge, or disseminate any oral or written information obtained as a result of execution of this Contract or performance of work hereunder. All client records are confidential. Improper disclosure of information is a violation of the Privacy Act. The Contractor shall

be required to sign a non-disclosure agreement.

17. GOVERNMENT-CONTRACTOR RELATIONSHIP

The Government and the Contractor understand and agree that the support services under this Contract are for non-personal services and the Contractor will not be paid for performing personal service functions.

Local Clauses & Provisions

Electronic Signatures (May 2019)

(a) The Department of Justice is committed to doing business in the most efficient and effective way possible, and to facilitate paperless processes. In furtherance of this goal, the Contracting Officer may apply their digital signature to procurement documents in the Portable Document Format (PDF) through the use of their government issued Personal Identity Verification (PIV) Card with a valid public key certificate. A digital signature made with these certificates is evidence that a specific individual signed the electronic record and that it was not altered. The recipient of a signed document can rely on the digital signature as evidence for a third party that the signature was generated by the claimed signer.
(b) For procurement documents that require a signature from a representative of the Contractor, the Contractor may utilize manual or electronic signature. Should the Contractor utilize an electronic signature, by returning

the document with an electronic symbol affixed to the appropriate signature block, the Contractor representative signing on behalf of the Contractor certifies that:
(1) Electronic Form of Signature: The Contractor representative has knowingly adopted, applied or affixed an electronic symbol to the document;
(2) Intent to Sign: The Contractor representative has applied an electronic symbol with the intent to legally bind the Contractor;
(3) Association of Signature to Record: the Contractor representative's signature is attached to the electronic record being signed;
(4) Identification and Authentication of Signer: The Contractor has a means to identify and authenticate a particular person as the signer; and
(5) Integrity of Signed Record: The Contractor can attest to the integrity of the signed record between the time of signature and the returned record to the government.
(c) This clause applies to this document and any subsequent documents (e.g., modifications, task/delivery orders) associated with this action.

(End of clause)

2852.201-70 Contracting Officer's Representative (COR) – (EOUSA modified, March 2014)

(a) **To be determined (TBD) at time of award** Mr./Ms. (Name) of (Organization) (Room No.), (Building), (Address), (Area Code & Telephone No.), is hereby designated to act as Contracting Officer's Representative (COR) under this contract.
(b) The COR is responsible, as applicable, for: receiving all deliverables, inspecting and accepting the supplies or services provided hereunder in accordance with the terms and conditions of this contract; providing direction to the contractor which clarifies the contract effort, fills in details or otherwise serves to accomplish the contractual Scope of Work; evaluating performance; and certifying all invoices/vouchers for acceptance of the supplies or services furnished for payment.
(c) The COR does not have the authority to alter the contractor's obligations under the contract, and/or modify any of the expressed terms, conditions, specifications, or cost of the agreement. If as a result of technical discussions it is desirable to alter/change contractual obligations or the Scope of Work, the Contracting Officer shall issue such changes.

(End of clause)

EOUSA AI-10-1B - 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)

EOUSA AI-10-1D - Continuing Contract Performance During a Pandemic Influenza or other National Emergency (October 2007)

During a Pandemic or other emergency we understand that our contractor workforce will experience the same high levels of absenteeism as our federal employees. Although the Excusable Delays and Termination for Default clauses used in government contracts list epidemics and quarantine restrictions among the reasons to excuse delays in contract performance, we expect our contractors to make a reasonable effort to keep performance at an acceptable level during emergency periods.

The Office of Personnel Management (OPM) has provided guidance to federal managers and employees on the kinds of actions to be taken to ensure the continuity of operations during emergency periods. This guidance is also applicable to our contract workforce. Contractors are expected to have reasonable policies in place for continuing

work performance, particularly those performing mission critical services, during a pandemic influenza or other emergency situation.

The types of actions a federal contractor should reasonably take to help ensure performance are:
Encourage employees to get inoculations or follow other preventive measures as advised by the public health service.

Contractors should cross-train workers as backup for all positions performing critical services. This is particularly important for work such as guard services where telework is not an option.

Implement telework to the greatest extent possible in the workgroup so systems are in place to support successful remote work in an emergency.

Communicate expectations to all employees regarding their roles and responsibilities in relation to remote work in the event of a pandemic health crisis or other emergency.

Establish communication processes to notify employees of activation of this plan.

Integrate pandemic health crisis response expectations into telework agreements.

With the employee, assess requirements for working at home (supplies and equipment needed for an extended telework period). Security concerns should be considered in making equipment choices; agencies or contractors may wish to avoid use of employees' personal computers and provide them with PCs or laptops as appropriate.
Determine how all employees who may telework will communicate with one another and with

management to accomplish work.

Practice telework regularly to ensure effectiveness.

Make it clear that in emergency situations, employees must perform all duties assigned by management, even if they are outside usual or customary duties.

Identify how time and attendance will be maintained.

It is the contractor's responsibility to advise the government contracting officer if they anticipate not being able to perform and to work with the Department to fill gaps as necessary. This means direct communication with the contracting officer or in his/her absence, another responsible person in the contracting office via telephone or email messages acknowledging the contractors notification. The incumbent contractor is responsible for assisting the Department in estimating the adverse impacts of nonperformance and to work diligently with the Department to develop a strategy for maintaining the continuity of operations.

The Department does reserve the right in such emergency situations to use federal employees. employees of other agencies, contract support from other existing contractors, or to enter into new contracts for critical support services. Any new contracting efforts would be acquired following the guidance in the Office of federal Procurement Policy issuance "Emergency Acquisitions", May, 2007 and Subpart 18.2. Emergency Acquisition Flexibilities, of the Federal Acquisition Regulations.

(End of clause)

Notification to Employees of Whistleblower Rights, Remedies, and other Information

Pursuant to clause 52.203-17 titled “Contractor Employee Whistleblower Rights and Requirement to Inform Employees of Whistleblower Rights”, which is incorporated into this contract/modification action by reference, the Contractor must comply with the requirement to inform its employees of their whistleblower rights and protections

by distributing a copy of the document entitled “Whistleblower Information for Department of Justice Contractors, Subcontractors, and Grantees”. Following is a link to the document for electronic distribution to your employees: (https://oig.justice.gov/hotline/docs/NDAA-brochure.pdf).

(End of provision)

DOJ-02 Contractor Privacy Requirements (November 2021)

A. Limiting Access to Privacy Act and Other Sensitive Information

(1) Privacy Act Information

In accordance with FAR 52.224-1 Privacy Act Notification (APR 1984) and FAR 52.224-2 Privacy Act (APR 1984), if this contract requires Contractor personnel to have access to information protected by the Privacy Act of 1974, the contractor is advised that the relevant DOJ system of records notices (SORNs) applicable to this Privacy Act information may be found at https://www.justice.gov/opcl/doj-systems-records.[1] Applicable SORNs published by other agencies may be accessed through those agencies’ websites or by searching the Federal Digital System (FDsys) available at http://www.gpo.gov/fdsys/. SORNs may be updated at any time.

(2) Prohibition on Performing Work Outside a Government Facility/Network/Equipment

The Contractor shall perform all tasks on authorized Government networks, using Government-furnished IT and other equipment and/or Workplace as a Service (WaaS), if WaaS is authorized by the statement of work. Government information shall remain within the confines of authorized Government networks at all times. Except where remote work is specifically authorized within this contract, the Contractor shall perform all tasks described in this document at authorized Government facilities; the Contractor is prohibited from performing

these tasks at or removing Government-furnished information to any other facility; and Government information shall remain within the confines of authorized Government facilities at all times. Contractors may only access classified materials on government furnished equipment in authorized government owned facilities regardless of remote work authorizations.

(3) Prior Approval Required to Hire Subcontractors

The Contractor is required to obtain the Contracting Officer's approval prior to engaging in any contractual relationship (Subcontractor) in support of this contract requiring the disclosure of information, documentary material and/or records generated under or relating to this contract. The Contractor (and any Subcontractor) is required to abide by Government and Agency guidance for protecting sensitive and proprietary information.

(4) Separation Checklist for Contractor Employees

The Contractor shall complete and submit an appropriate separation checklist to the Contracting Officer before any employee or Subcontractor employee terminates working on the contract. The Contractor must submit the separation checklist on or before the last day of employment or work on the contract. The separation checklist must verify: (1) return of any Government-furnished equipment; (2) return or proper disposition of personally identifiable information (PII)[2], in paper or electronic form, in the custody of the employee or Subcontractor employee including the sanitization of data on any computer systems or media as appropriate; and (3) termination of any technological access to the Contractor’s facilities or systems that would permit the terminated employee’s access to PII or other sensitive information.

In the event of adverse job actions resulting in the dismissal of a Contractor or Subcontractor employee before the separation checklist can be completed, the Prime Contractor must notify the Contracting Officer within 24 hours and confirm receipt of the notification. In the case the Contractor is unable to notify the Contracting Officer, then the Contractor should notify the Contract Officer’s Representative (COR).

Contractors must complete the separation checklist with the Contracting Officer or COR by returning all Government-furnished property including, but not limited to, computer equipment, media, credentials and passports, smart cards, mobile devices, Personal Identity Verification (PIV) cards, calling cards, and keys and terminating access to all user accounts and systems. Unless the Contracting Officer requests otherwise, the relevant Program Manager or other Key Personnel designated by the Contracting Officer or COR may facilitate the return of equipment.

B. Privacy Training, Safeguarding, and Remediation

(1) Required Security and Privacy Training for Contractors

The Contractor must ensure that all employees take appropriate privacy training, including Subcontractors who have access to PII as well as the creation, use, dissemination and/or destruction of PII at the outset of the employee's work on the contract and every year thereafter. Training must include procedures on how to properly handle PII, including heightened security requirements for the transporting or transmission of sensitive PII, and reporting requirements for a suspected breach or loss of PII. These courses, along with more information about DOJ security and training requirements for Contractors, are available at https://www.justice.gov/jmd/learndoj. The Federal Information Security Modernization Act of 2014 (FISMA) requires all individuals accessing DOJ information to complete training on records management, cybersecurity awareness, and information system privacy awareness. Contractor employees are required to sign the "Privacy Rules of Behavior," acknowledging and agreeing to abide by privacy law, policy, and certain privacy safeguards, prior to accessing DOJ information. These Rules of Behavior are made available to all new users of DOJ's computer network and to trainees at the conclusion of DOJ-OPCL-CS 0005.

The Contractor should maintain copies of certificates as a record of compliance and must submit an email notification annually to the COR verifying that all employees working under this contract have completed the required privacy and cybersecurity training.

(2) Safeguarding PII Requirements

Contractor employees must comply with DOJ Order 0904 and other guidance published to the

publicly-available Office of Privacy and Civil Liberties (OPCL) Resources page[3] relating to the safeguarding of PII, including the use of additional controls to safeguard sensitive PII (e.g., the encryption of sensitive PII). This requirement flows down from the Prime Contractor to all Subcontractors and lower tiered subcontracts.

(3) Non-Disclosure Agreement Requirement

Prior to commencing work, all Contractor personnel that may have access to PII or other sensitive information shall be required to sign a Non-Disclosure Agreement (NDA) and the DOJ IT Rules of Behavior. The Non-Disclosure Agreement:

(a) prohibits the Contractor from retaining or divulging any PII or other sensitive information, or derivatives therefrom, furnished by the Government or to which they may otherwise come in contact as a result of their performance of work under the contract/task order that is otherwise not publicly available, whether or not such information has been reduced to writing; and

(b) requires the Contractor to report any loss of control, compromise, unauthorized disclosure, or unauthorized acquisition of PII or other sensitive information to the component-level or headquarters Security Operations Center within one (1) hour of discovery.

The Contractor should maintain signed copies of the NDA for all employees as a record of compliance. The Contractor should also provide copies of each employee's signed NDA to the Contracting Officer before the employee may commence work under the contract/task order.

(4) Prohibition on Use of PII in Vendor Billing and Administrative Records

The Contractor's invoicing, billing, and other financial or administrative records or databases is not authorized

to regularly store or include any sensitive PII or other confidential government information that is created, obtained, or provided during the performance of the contract without the written permission of the Senior Component Official for Privacy (SCOP). It is acceptable to list the names, titles and contact information for the Contracting Officer, COR, or other personnel associated with the administration of the contract in the invoices as needed.

(5) Reporting Actual or Suspected Data Breach

Contractors must report any actual or suspected breach of PII within one hour of discovery.[4] A "breach" is an incident or occurrence that involves 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 PII or (2) an authorized user accesses or potentially accesses PII for an other than authorized purpose. The report of a breach must be made to DOJ. The Contractor must cooperate with DOJ's inquiry into the incident and efforts to minimize risks to DOJ or individuals, including remediating any harm to potential victims.

(a) The Contractor must develop and maintain an internal process by which its employees and Subcontractors are trained to identify and report the breach, consistent with DOJ Instruction 0900.00.01[5], Reporting and Response Procedures for a Breach of Personally Identifiable Information.

(b) The Contractor must report any such breach by its employees or Subcontractors to the DOJ Security Operations Center (xxxx); Component-level Security Operations Center and Component-level Management Team, where appropriate; the COR; and the Contracting Officer within one (1) hour of the initial

(c) The Contractor must provide a written report to the DOJ Security Operations Center (xxxx) within 24 hours of discovery of the breach by its employees or Subcontractors. The report must contain the following information:

(i) Narrative or detailed description of the events surrounding the suspected loss or compromise of information.[6] Date, time, and location of the incident.

(ii) Amount, type, and sensitivity of information that may have been lost or compromised, accessed without authorization, etc.

(iii) Contractor's assessment of the likelihood that the information was compromised or lost and the reasons behind the assessment.[7]

(iv) Names and classification of person(s) involved, including victim, Contractor employee/Subcontractor and any witnesses.

(v) Cause of the incident and whether the company's security plan was followed and, if not, which specific provisions were not followed.[8]
(vi) Actions that have been or will be taken to minimize damage and/or mitigate further compromise. (vii) Recommendations to prevent similar situations in the future, including whether the security plan needs to be modified in any way and whether additional training may be required.

(d) The Contractor shall provide full access and cooperation for all activities determined by the Government to be required to ensure an effective incident response, including providing all requested images, log files, and event information to facilitate rapid resolution of sensitive information incidents.

(e) At the Government's discretion, Contractor employees or Subcontractor employees may be identified as no longer eligible to access PII or to work on that contract based on their actions related to the loss or compromise of PII.

(6) Victim Remediation

At DOJ's request, the Contractor is responsible for notifying victims and providing victim remediation services in the event of a breach of PII held by the Contractor, its agents, or its Subcontractors, under this contract. Victim remediation services shall include at least 18 months of credit monitoring and, for serious or large incidents as determined by the Government, call center help desk services for the individuals whose PII was lost or compromised. When DOJ requests notification, the Department Chief Privacy and Civil Liberties Officer and SCOP

will direct the Contractor on the method and content of such notification to be sent to individuals whose PII was breached. By performing this work, the Contractor agrees to full cooperation in the event of a breach. The Contractor should be self-insured to the extent necessary to handle any reasonably foreseeable breach, with another source of income, to fully cover the costs of breach response, including but not limited to victim remediation.

C. Government Records Training, Ownership, and Management

(1) Records Management Training and Compliance

(a) The Contractor must ensure that all employees and Subcontractors that have access to PII as well as to those involved in the creation, use, dissemination and/or destruction of PII take the DOJ Records and Information Training for New Employees (RIM) training course or another training approved by the Contracting Officer or COR. This training will be provided at the outset of the Subcontractor's/employee's work on the contract and every year The Contractor shall maintain copies of certificates as a record of compliance and must submit an email notification annually to the COR verifying that all employees working under this contract have completed the required records management training.

(b) The Contractor agrees to comply with Federal and Agency records management policies, including those policies associated with the safeguarding of records containing PII and those covered by the Privacy Act of 1974. These policies include the preservation of all records created or received regardless of format, mode of transmission, or state of

(2) Records Creation, Ownership, and Disposition

(a) The Contractor shall not create or maintain any records not specifically tied to or authorized by the contract using Government IT equipment and/or Government records or that contain Government Agency information. The Contractor shall certify, in writing, the appropriate disposition or return of all Government information at the conclusion of the contract or at a time otherwise specified in the contract. In accordance with 36 CFR 1222.32, the Contractor shall maintain and manage all Federal records created in the course of performing the contract in accordance with Federal law. Records may not be removed from the legal custody of DOJ or destroyed except in accordance with the provisions of the agency records schedules.

(b) Except as stated in the Performance Work Statement and, where applicable, the Contractor's Commercial License Agreement, the Government Agency owns the rights to all electronic information (electronic data, electronic information systems or electronic databases and all supporting documentation and associated metadata created as part of this contract. All deliverables (including all data and records) under the contract are the property of the U.S. Government and may be considered federal records, for which the Agency shall have unlimited rights to use, dispose of, or disclose such data contained therein. The Contractor must deliver

sufficient technical documentation with all data deliverables to permit the agency to use the data.

(c) The Contractor shall not retain, use, sell, disseminate, or dispose of any government data/records or deliverables without the express written permission of the Contracting Officer or Contracting Officer's Representative. The Agency and its contractors are responsible for preventing the alienation or unauthorized destruction of records, including all forms of mutilation. Willful and unlawful destruction, damage or alienation of Federal records is subject to the fines and penalties imposed by 18 U.S.C. § 2701. Records may not be removed from the legal custody of the Agency or destroyed without regard to the provisions of the Agency records

D. Data Privacy and Oversight

(1) Restrictions on Testing or Training Using Real Data Containing PII

The use of real data containing PII from any source for testing or training purposes is generally prohibited. The Contractor shall use synthetic or de-identified real data for testing or training whenever feasible.

(2) Requirements for Contractor IT Systems Hosting Government Data

The Contractor is required to obtain an Authority To Operate (ATO) for any IT environment owned or controlled by the Contractor or any Subcontractor on which Government data shall reside for the purposes of IT system development, design, data migration, testing, training, maintenance, use, or disposal.

(3) Requirement to Support Privacy Compliance

(a) If this contract requires the development, maintenance or administration of information technology[9], the Contractor shall support the completion of the Initial Privacy Assessment (IPA) document, if requested by

Department personnel. An IPA is the first step in a process to identify potential privacy issues and mitigate privacy risks. The IPA asks basic questions to help components assess whether additional privacy protections may be needed in designing or implementing a project[10] to mitigate privacy risks, and whether compliance work may be needed. Upon review of the IPA, the OPCL determines whether a Privacy Impact Assessment (PIA) document and/or SORN, or modifications thereto, are required. The Contractor shall provide adequate support to complete the applicable risk assessment and PIA document in a timely manner, and shall ensure that project management plans and schedules include the IPA, PIA, and SORN (to the extent required) as milestones. Additional information on the privacy compliance process at DOJ, including IPAs, PIAs, and SORNs, is located on the DOJ OPCL website (https://dojnet.doj.gov/privacy/), including DOJ Order 0601, Privacy and Civil Liberties. The Privacy Impact Assessment Guidance and Template outline the requirements and format for the PIA.

(b) If the contract involves an IT system build or substantial development or changes to an IT system that may require privacy risk assessment and documentation, the Contractor shall provide adequate support to DOJ to ensure DOJ can complete any required assessment, and IPA, PIA, SORN, or other supporting documentation to support privacy compliance. The Contractor shall work with personnel from the program office, OPCL, the Office of the Chief Information Officer (OCIO), and the Office of Records Management and Policy to ensure that the privacy assessments and documentation are kept on schedule, that the answers to questions in the documents are thorough and complete, and that questions asked by the OPCL and other offices are answered in a timely fashion. The Contractor must ensure the completion of required PIAs and documentation of privacy controls consistent with federal law and standards, e.g. NIST 800-53, Rev. 5; and compliance with the Privacy Act of 1974, E-Government Act of 2002, Federal Information Security Modernization Act of 2014, and key OMB guidelines, e.g., OMB Circular A-130.

[1] "[T]he term 'record' means any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, his education, financial transactions, medical history, and criminal or employment history and that contains his name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph." 5 U.S.C. § 552a(a)(4). "[T]he term 'system of records' means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual." 5 U.S.C. § 552a(a)(5).
[2] As stated in FAR 52.224-3 and Office of Management and Budget (OMB) Circular A-130, Managing Federal Information as a Strategic Resource (2016), "'personally identifiable information' means

information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is
linked or linkable to a specific individual." Regarding "sensitive PII," "[t]he sensitivity level of the PII will depend on the context, including the purpose for which the PII is created, collected, used, processed, stored, maintained, disseminated, disclosed, or disposed. For example, the sensitivity level of a list of individuals' names may depend on the source of the information, the other information associated with the list, the intended use of the information, the ways in which the information will be processed and shared, and the ability to access the information." OMB Circular A-130, at App. II-2.
[3] The DOJ OPCL Resources page is available at https://www.justice.gov/opcl/resources. [4] As stated in DOJ Instruction 0900, "Contractors must notify the Contracting Officer, the Contracting Officer's Representative, and JSOC (or component-level SOC) within 1 hour of discovering any incidents, including breaches, consistent with this Instruction, guidance issued by the CPCLO, NIST standards and guidelines, and the US-CERT notification guidelines."
[5] https://www.justice.gov/file/4336/download
[6] As stated in DOJ Instruction 0900, the description should include the type of information that constitutes PII; purpose for which PII is collected, maintained, and used; extent to which PII identifies a peculiarly vulnerable population; the determination of whether the information was properly encrypted or rendered partially or completely

inaccessible by other means; format of PII (e.g., whether PII was structured or unstructured); length of time PII was exposed; any evidence confirming that PII is being misused or that it was never accessed. [7] As stated in DOJ Instruction 0900, the report should include the nature of the cyber threat (e.g., Advanced Persistent Threat, Zero Day Threat, data exfiltration) for cyber incidents.
[8] As stated in DOJ Instruction 0900, the report should include analysis on whether the data is accessible, usable, and intentionally targeted.
[9] As defined in 40 U.S.C. § 11101, the term "information technology" means any equipment or interconnected system or subsystem of equipment, used in the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or

information by the executive agency, if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency that requires the use (i) of that equipment or (ii) of that equipment to a significant extent in the performance of a service or the furnishing of a product; includes computers, ancillary equipment (including imaging peripherals, input, output, and storage devices necessary for security and surveillance), peripheral equipment designed to be controlled by the central processing unit of a computer, software, firmware and similar procedures, services (including support services), and related resources; but does not include any equipment acquired by a federal contractor incidental to a federal contract. [10] In this instance, the term "project" is used to scope the activities (e.g., creating, collecting, using, processing, storing, maintaining, disseminating, disclosing, or disposing of information) covered by an IPA. A project is intended to be technology-neutral, and may include an information system, a digital service, an information technology, a combination thereof, or some other activity that may create potential privacy issues or privacy risks that would benefit from an IPA. The scope of a project covered by an IPA is discretionary, but components should work with their SCOP and OPCL.

(End of clause)

DOJ-03 - Personnel Security Requirements For Contractor Employees (Nov 2021)

Work performed under this contract will involve any one or more of the following: access to DOJ Information, which may include Controlled Unclassified Information (CUI), i.e., unclassified, sensitive DOJ information, and/or access to DOJ Information Technology (IT) systems, and/or unescorted access to DOJ space or facilities. Contractor employees will occupy Public Trust Positions, unless clause alternates are applied.

1.1 General Requirements

(a) (1) All references to "contract(or) personnel" and "contract(or) employee" in this clause means all individuals, without limitation, to include individuals employed by the contractor, team member, subcontractor, consultant, and/or independent contractor, who will have access to information of the Department of Justice (DOJ) or information that is within the custody and control of the DOJ, access to DOJ IT systems, and/or unescorted access to DOJ facilities/space in connection with the performance of this contract. "Employment" as used herein does not create nor imply an employer/employee relationship between the DOJ and contractor employees.

(b) (1) The type of security investigation required for each contractor employee will be governed by the type and risk level of information made available to the contractor employee. The contractor will not be permitted to commence performance under this contract until a sufficient number of its personnel, as determined by the Security Programs Manager (SPM), in consultation with the Contracting Officer's Representative if one is appointed, have received the requisite security approval.

(c) Except where specifically noted otherwise, the federal government will be responsible for the cost and conduct of the investigation.

(d) The contractor shall ensure that no contractor employee commences performance prior to receipt of a written authorization from the contracting officer, COR, or the SPM that performance by the respective contractor employee is authorized.

(e) The data and other information to which the contractor may have access as a result of this contract is the property of, and/or within the custody and control of, the Department, and its disclosure to third parties is governed by various statutes and regulations, the violation of which may subject the discloser to criminal penalties.

1.2 Citizenship and Residency Requirements

(a) **Residency Requirement**. (1) Contractor employees in Public Trust positions, both U.S. citizens and non U.S. citizens, must meet the Department's residency requirement if they will require access to DOJ information, IT systems, or unescorted access to facilities. For three years (not necessarily consecutive years) out of the last five years immediately prior to employment under the Department contract the contractor employee musthave: (i) resided in the U.S.; (ii) worked for the U.S. in a foreign country as either an employee or contractor in a federal civilian or military capacity; or, (iii) been a dependent of a federal civilian or military

employee or contractor working for the U.S. in a foreign country. At the Department's sole discretion, the residency requirement may be waived by the Department Security Officer (DSO) for contractor employees on a case-by-case basis where justified by extenuating circumstances. The residency requirement does not apply to contractor employees residing in foreign countries that are hired to work in American embassies/consulates/missions located outside of the United States and who require access to DOJ information, IT systems, or unescorted access *provided that* an adequate background investigation can be conducted, with favorable adjudication, as determined by the DSO.

(b) **Citizenship.** (1) Aside from the specific exceptions set forth in Section 1.2(b)(2), for Public Trust positions, the DOJ requires that contractor employees be U.S. citizens and nationals, or lawful permanent residents seeking U.S. citizenship. Any prospective non-U.S. citizen contractor employee who requires access to DOJ information
systems, DOJ information, and/or unescorted facilities access must also have been granted a waiver as described in paragraphs 1.2(d) and/or (e) below. The contractor is responsible for verifying that the non-U.S. citizens working under this contract are lawful permanent residents seeking U.S. citizenship.

(2) **Exception for Certain Non-U.S. Citizen Contractor Employees:** (i) Non-U.S. citizen expert witnesses, litigative consultants, and interpreters in rare foreign languages are not required to be lawful permanent residents seeking U.S. citizenship. However, they must be granted a waiver for access to unclassified DOJ information, whether CUI or not, DOJ IT systems, and/or unescorted facility access, as described in paragraph 1.2(d) and (e) below, regardless of the duration of their duties. (ii) Non-U.S. Citizen contractor employees residing in foreign countries who are hired to work for the Department of Justice in American embassies/consulates/missions outside of the United States are not required to be lawful permanent residents seeking U.S. citizenship.

(c) **Dual Citizenship.** (1) U.S. citizens who hold dual citizenship with a foreign country are considered U.S. citizens within the meaning of this clause, and may be considered for, but are not entitled to, contract employment as U.S. citizens consistent with this clause. The means by which the contractor employee obtained or exercises his or her dual citizenship status will be a consideration in the Public Trust Investigation (PTI) adjudication, and/or waiver approval processes discussed in this clause.

(d) **Access to DOJ Information Technology Systems.** Non-U.S citizens are not authorized to access DOJ information technology (IT) systems or assist in the development, operation, management, or maintenance

of DOJ IT systems, including providing IT system support, unless a waiver has been granted by the Head of the DOJ component or designee, with the prior concurrence of both the DSO and the DOJ Chief Information Officer, allowing computer access by the non-U.S. citizen. Such a waiver will be granted only in exceptional and unique circumstances on a case-by-case basis. It should be noted that the Justice Consolidated Office Network (JCON) is a sensitive DOJ IT system and any contractor employee who will need access to JCON must be a U.S. citizen or have received a waiver. In order for a waiver to be considered for approval: (1) There must be a compelling reason for using this individual as opposed to a U.S. citizen; (2) The type of personnel security vetting that has been conducted on the individual, and vetting results, that would mitigate risk; and (3) The waiver must be in the best interest of the federal government.

2. Access to Unclassified DOJ Information and Unescorted Access to DOJ Facilities or Space.
(1) Except as provided under 1.2(b)(2), non-U.S citizens are not authorized to access DOJ information and/or

unescorted access to DOJ facilities or space, unless a waiver has been granted by the DSO, allowing access by the non-U.S. citizen. Such a waiver will be granted on a case-by-case basis where justified at the discretion of the DSO.

2.2 Background Investigation Requirements

(a) (1) Unless otherwise stated below, all contractor personnel are subject to a Public Trust Investigation (PTI). The SPM will determine the type of investigation for each contractor employee based on the risk category (i.e., the nature of the position and degree of harm that could be caused by the individual in that position) and whether the position is long-term or short-term. The PTI risk categories are listed below.

(i) High Risk Positions. The minimum background investigation required is a Tier 4 (T4) investigation, and the five year reinvestigation required is a Tier 4R (T4R) investigation.

The 2017 version of the Standard Form (SF) 85P, Questionnaire for Public Trust Positions, is required.

(ii) Moderate Risk Positions. The minimum background investigation required is a Tier 2 (T2) investigation. The five year reinvestigation required is a Tier 2R (T2R) investigation. The 2017 version of the SF-85P is required.

(iii) Low Risk/Non-Sensitive Positions. The minimum background investigation required for Low Risk/Non-Sensitive positions is a Tier 1 (T1) investigation and the required five year reinvestigation is also a Tier 1 (T1) investigation. The SF 85, Questionnaire for Non Sensitive Positions, is required.

(b) **Exception for Expert Witnesses.** Expert Witnesses, litigative consultants, and interpreters in rare foreign languages may not be subject to full background investigation requirements if alternative security requirements are approved by the DSO.

(c) **Short-Term U.S. Citizen Contractor Employees**. Other than the exception in Section 1.3(b), short-term contractor employees (6 months or less) who are U.S. citizens are not subject to a full background investigation, however, must receive an approved pre-employment background investigation waiver. The required forms to complete and submit are listed in Section 1.4(b) and (c)(2).

(d) **Long-Term U.S. Citizen Contractor Employees**. Other than the exception in Section 1.3(b), all long term U.S. citizen employees (longer than 6 months) are subject to a full background investigation in the risk category appropriate to the position they will hold.

(e) **Non U.S. Citizen Contractor Employees**. Other than the exception in 1.3(b), all non-U.S. citizen contractor employees regardless of performance duration (short or long term) are subject to a full background investigation in the risk category appropriate to the position they will hold.

(f) **Reciprocity.** A Public Trust Investigation will be accepted under reciprocity if it meets the following guidelines: (i) the investigation is current (investigations are considered current if completed within the last five years) and favorably adjudicated, or the reinvestigation has been deferred; (ii) the investigation meets or exceeds the level of investigation required for the DOJ contractual instrument; (iii) there has been no

continuous (not cumulative) break in federal contract/service employment of two years or more; (iv) there is no derogatory information since the favorable fitness determination or adjudication that calls into question the individual's fitness based on character or conduct; and (v) the investigative record does not show conduct that is incompatible with the core duties of the new contract position. A "core duty" is a continuing responsibility that is of particular importance to the relevant covered position or the achievement of an agency's mission. Core duties will vary from position to position.

2.3 Background Investigation Process

(a) **e-QIP (or its successor)**. Public Trust background investigations/reinvestigations of contractor employees

will be performed by the DCSA. The investigative process requires contractor employees to complete the Electronic Questionnaires for Investigations Processing (e-QIP) and provide additional information as specified in paragraph 1.4(b) below. Immediately after contract award, the contractor shall designate an employee as its "e-QIP Initiator" and provide the name of this person to the SPM. The e-QIP Initiator must have, at a minimum, a favorably adjudicated Tier 1 investigation and the appropriate DOJ security approval before being given access to e-QIP. After the e-QIP Initiator's security approval is granted, the Contractor will be configured in e-QIP as a sub-agency to DOJ. The contractor will then be responsible for initiating investigations for all contract personnel, whose previous investigation does not meet reciprocity, in e-QIP for completion of the security questionnaire form and forwarding the electronic form with the remainder of the security package to the SPM. Subject to the prior written approval of the SPM, the contractor may designate an e-QIP Initiator for each subcontractor. Subcontractor e-QIP Initiators must have, at a minimum, a favorably adjudicated Tier 1 investigation and the appropriate DOJ security approval before being provided access to e-QIP.

(b) **Additional Documentation.** (1) In addition to completing the e-QIP questionnaire (see paragraph 1.4(a) above), the contractor shall ensure that each contractor employee occupying Public Trust Positions, including short-term employees, completes and submits the following information through the

contractor's Corporate Security Officer:

(i) Digital Fingerprinting/FD-258 Applicant Fingerprint Card. Two sets are required per applicant. The contractor may schedule appointments with the SPM to be digitally fingerprinted; otherwise, fingerprinting by the FBI or other law enforcement entity, as approved by the SPM, is required to ensure the identity of the person being fingerprinted and for printing quality. All pertinent information must be completed by the individual taking the fingerprints (FBI or other). Use of the physical FD-258 Applicant Fingerprint Card should only be used in extenuating circumstances.

(ii) DOJ-555 Fair Credit Reporting Act Disclosure. Authorizes DOJ to obtain one or more consumer/credit reports on the individual. This form will be required if the Component SPM determines a credit check is necessary for its Low Risk Level 1 contractor positions.

(iii) OF-306, Declaration for Federal Employment.

(iv) Foreign National Relatives or Associates Statement. This is only required if foreign national relatives or associates were not disclosed on the security questionnaire form.

(v) Self-Reporting Requirements for All Contractor Personnel. This is an acknowledgement and acceptance statement that every contractor must sign.

(vi) Additional information as may be required based on the review of the security questionnaire form.

The contractor shall review all forms/documents to ensure each is complete, accurate and meets all DOJ requirements, including applicable residency and citizenship requirements. The contractor shall resolve any issues or discrepancies with the contractor employee, including resubmission of corrected forms or documentation. Completed forms/documents shall be submitted to the SPM (or designee, which may include the COR) within five (5) calendar days after being finalized.

(c) **Adjudication and Pre-Employment Background Investigation Waivers**

(1) Except as set forth in this section, background investigations must be conducted and favorably adjudicated for each contractor employee prior to commencing their work on this contract. Where programmatic needs do not permit the federal government to wait for completion of the entire background investigation, a pre-employment background investigation waiver for ***public trust contractors*** can be granted by the SPM, in consultation with the cognizant COR. Pre-employment waivers cannot be used to circumvent delays in clearing classified contractors through the DCSA, if access to classified information is required.

(2) As directed by the SPM, the contractor shall initiate pre-employment waivers for Public Trust Positions when necessary. This may entail performing credit history checks and submission of these checks as part of the security package, including satisfactory resolution of any issues prior to submission to the federal government. A waiver will be disapproved if it develops derogatory information that cannot be resolved in the contractor employee's favor. When a waiver has been disapproved, the CO, in consultation with the SPM and COR, will determine (i) whether the contractor employee will no longer be considered for work on a DOJ contract or (ii) whether to wait for the completion and favorable adjudication of the background investigation before the contractor employee commences work on a Department contract. Pre-employment background investigation waiver requirements include:

1. Verification of citizenship (copy of a birth certificate, naturalization certificate, or U.S. passport);
2. Verification of compliance with the *DOJ Residency Requirement* of this Clause;
3. Favorable review of the security questionnaire form;
4. Favorable FBI fingerprint results;
5. Favorable credit report;
6. Favorable review of the OF-306 form, Declaration for Federal Employment;

7. Verification of the initiation of the appropriate background investigation (for long term personnel); and
8. Receipt of the signed DOJ *Self-Reporting Requirements for All Contractor Personnel* (see Section 1.6, below).

(3) The investigating agency (DCSA) will provide the SPM with the results of each proposed contractor employee's Public Trust investigation. Upon receipt of the investigation and any other pertinent documents from the investigating agency, the SPM will determine whether each proposed contractor employee should be granted employment security approval.

(4) The COR will notify the contractor of the results of Public Trust background investigations as they are completed and adjudicated, including any individual who is found ineligible for employment security approval. For any individual found ineligible for employment on a Department contract, the contractor shall propose a replacement and initiate the background investigation process consistent with this clause.

1.5 Identity Proofing and Badging

(a) Access to DOJ Information, federally-controlled IT systems, and/or unescorted access to federally-controlled facilities or space (regardless of whether the contractor employee will be issued a DOJ PIV card or building access badge) shall be made available after each respective contractor employee has (1) met the identity proofing requirements outlined below, and (2) completed all other security requirements stated elsewhere in this contract.

(b) Public Trust contractor employees must appear in person at least once before a DOJ official or an official of a trusted contract company (i.e., has a facility security clearance) who is responsible for checking two forms of identification in original form prior to commencement of work by the contractor employee and PIV card or building access badge issuance (as applicable). Approval will be documented by the DOJ official or an official of a trusted contract company. (Acceptable documents are listed in Form I-9, Employment Eligibility Verification, and at least one document must be a valid state or federal government issued picture ID).

(c) All contractor employees requiring unescorted access to a DOJ controlled facility or space shall comply with the PIV card or building access badge requirements outlined below:

(i) When any contractor employee enters a DOJ building for the first time, he/she shall allow one hour for security processing and the creation and issuance of a building access badge. PIV cards require additional processing time and will not likely be issued on the same day.

(ii) Building access badges shall be subject to periodic review by the contractor employee's supervisor and checked against his/her personal identification. The contractor employees shall present

themselves for the issuance of renewed badges when required by the government as scheduled by the COR or his/her designee. The contractor shall notify the COR when contractor employee badges are lost, and must immediately apply for reissuance of a replacement badge. The contractor shall pay for
reissued building access badges at no cost to the government. It is the contractor employee's responsibility to return badges to the COR or his/her designee when a contractor employee is dismissed, terminated or assigned to duties not within the scope of this contract.

1.6 Employee Reporting Requirements

(a) All contractor employees must sign the DOJ *Self-Reporting Requirements for All Contractor Personnel* statement acknowledging and accepting the DOJ requirement that they immediately self-report certain information using the Department's iReport system. The COR or SPM will provide the Self-Reporting statement as well as a list of reportable information, which varies by position sensitivity designation, to the contractor employee before commencing work under the contract. If the contractor employee does not have access to the DOJ iReport System, the COR or SPM will provide a fillable form for the contractor employee to complete and submit.

(b) The COR and SPM will review the written report and documentation and make a determination regarding continued employment on a DOJ contract.

(c) DOJ reporting requirements are in addition to the DCSA reporting requirements and the contractor's internal reporting requirements.

1.7 Replacement Personnel

(a) The contractor shall make every effort to avoid costs to the government for security investigations for replacement of contractor employees, and in so doing shall ensure that otherwise satisfactorily performing and physically able contractor employees remain in contract performance for the duration of the contract. The contractor shall take all necessary steps to ensure that contractor personnel who are selected for assignment to this contract are professionally qualified and personally reliable, of reputable background and sound character, and able to meet all other requirements stipulated in the contract.

(b) The fact that the government performs security investigations shall not in any manner relieve the contractor of its responsibility to ensure that all contract personnel are reliable and of reputable background and sound character. Should a security investigation conducted by the government and/or a contractor's self-report or failure to self-report render ineligible a contractor employee, the contracting officer will determine whether the contractor has violated this clause. The contracting officer may direct the contractor, at its own expense, to remove and replace any contractor personnel who fails to comply with or violates applicable requirements of this contract. Such action may be taken at the government's direction without prejudice to its rights under any other provision of this contract, including termination for default, and the contractor may be held liable, at a minimum, for all reasonable and necessary costs incurred by the government to (i) provide coverage (performance) through assignment of individuals employed by the government or third parties in those cases where absence of contractor personnel would cause either a security threat or DOJ program disruption and (ii) conduct security investigations in excess of those which would otherwise be required.

(c) Nothing in this clause shall require the contractor to bear costs involved in the conduct of security investigations for replacement of a contractor employee who separates from the contractor of his/her own accord, is incapacitated, or is deceased.

(d) The contractor shall comply with the terms and conditions set forth under this clause and assumes all liability for failure to comply. The rights and remedies conferred upon the government by this clause are in addition to all and other rights and remedies pursuant to the contract and as established by law.

(End of clause)

JAR Clauses & Provisions

2852.223-70 - Unsafe Conditions Due to the Presence of Hazardous Material (June 1996)

(a) "Unsafe condition" as used in this clause means the actual or potential exposure of contractor or Government employees to a hazardous material as defined in Federal Standard No. 313, and any revisions thereto during the term of this contract, or any other material or working condition designated by the Contracting Officer's Technical Representative (COTR) as potentially hazardous and requiring safety controls.

(b) The Occupational Safety and Health Administration (OSHA) is responsible for issuing and administering regulations that require contractors to apprise its employees of all hazards to which they may be exposed in the course of their employment; proper conditions and precautions for safe use and exposure; and related symptoms and emergency treatment in the event of exposure.

(c) Prior to commencement of work, contractors are required to inspect for and report to the contracting officer or designee the presence of, or suspected presence of, any unsafe condition including asbestos or other hazardous materials or working conditions in areas in which they will be working.

(d) If during the performance of the work under this contract, the contractor or any of its employees, or subcontractor employees, discovers the existence of an unsafe condition, the contractor shall immediately notify the contracting officer, or designee, (with written notice provided not later than three (3) working days thereafter) of the existence of an unsafe condition. Such notice shall include the contractor's recommendations

for the protection and the safety of Government, contractor and subcontractor personnel and property that may be exposed to the unsafe condition.

(e) When the Government receives notice of an unsafe condition from the contractor, the parties will agree on a course of action to mitigate the effects of that condition and, if necessary, the contract will be amended. Failure to agree on a course of action will constitute a dispute under the Disputes clause of this contract.

(f) Nothing contained in this clause shall relieve the contractor or subcontractors from complying with applicable Federal, State, and local laws, codes, ordinances and regulations (including the obtaining of licenses and permits) in connection with hazardous material including but not limited to the use, disturbance, or disposal of such material.

(End of clause)

2852.233-70 - Protests Filed Directly with the Department of Justice (Jan 1998)

(a) The following definitions apply in this provision:

(1) "Agency Protest Official" means the official, other than the contracting officer, designated to review and decide procurement protests filed with a contracting activity of the Department of Justice.

(2) "Deciding Official" means the person chosen by the protestor to decide the agency protest; it may be either the Contracting Officer or the Agency Protest Official.

(3) "Interested Party" means an actual or prospective offeror whose direct economic interest would be affected by the award of a contract or by the failure to award a contract.

(b) A protest filed directly with the Department of Justice must:

(1) Indicate that it is a protest to the agency.

(2) Be filed with the Contracting Officer.

(3) State whether the protestor chooses to have the Contracting Officer or the Agency Protest Official decide the protest. If the protestor is silent on this matter, the Contracting Officer will decide the protest.

(4) Indicate whether the protestor prefers to make an oral or written presentation of arguments in support of the protest to the deciding official.

(5) Include the information required by FAR 33.103(d)(2):

(i) Name, address, facsimile number and telephone number of the protestor.

(ii) Solicitation or contract number.

(iii) Detailed statement of the legal and factual grounds for the protest, to include a description of resulting prejudice to the protestor.

(iv) Copies of relevant documents.

(v) Request for a ruling by the agency.

(vi) Statement as to the form of relief requested.

(vii) All information establishing that the protestor is an interested party for the purpose of filing a

protest. (viii) All information establishing the timeliness of the protest.

(c) An interested party filing a protest with the Department of Justice has the choice of requesting either that the Contracting Officer or the Agency Protest Official decide the protest.

(d) The decision by the Agency Protest Official is an alternative to a decision by the Contracting Officer. The Agency Protest Official will not consider appeals from the Contracting Officer's decision on an agency protest.

(e) The deciding official must conduct a scheduling conference with the protestor within five (5) days after the protest is filed. The scheduling conference will establish deadlines for oral or written arguments in support of the agency protest and for agency officials to present information in response to the protest issues. The deciding official may hear oral arguments in support of the agency protest at the same time as the scheduling conference, depending on availability of the necessary parties.

(f) Oral conferences may take place either by telephone or in person. Other parties may attend at the discretion of the deciding official.

(g) The protestor has only one opportunity to support or explain the substance of its protest. Department of Justice procedures do not provide for any discovery. The deciding official may request additional information from either the agency or the protestor. The deciding official will resolve the protest through informal presentations or meetings to the maximum extent practicable.

(h) An interested party may represent itself or be represented by legal counsel. The Department of Justice will not reimburse the protester for any legal fees related to the agency protest.

(i) The Department of Justice will stay award or suspend contract performance in accordance with FAR 33.103(f). The stay or suspension, unless overridden, remains in effect until the protest is decided, dismissed, or withdrawn.

(j) The deciding official will make a best effort to issue a decision on the protest within twenty (20) days after the filing date. The decision may be oral or written.

(k) The Department of Justice may dismiss or stay proceeding on an agency protest if a protest on the same or similar basis is filed with a protest forum outside the Department of Justice.

(End of clause)

FAR Clauses & Provisions

52.217-8 -- Option to Extend Services (Nov 1999)

The Government may require continued performance of any services within the limits and at the rates specified in the contract. These rates may be adjusted only as a result of revisions to prevailing labor rates provided by the Secretary of Labor. The option provision may be exercised more than once, but the total extension of performance hereunder shall not exceed 6 months. The Contracting Officer may exercise the option by written notice to the Contractor within 7 days.

(End of Clause)

52.217-9 -- Option to Extend the Term of the Contract (Mar 2000)

(a) The Government may extend the term of this contract by written notice to the Contractor within 7 days; provided that the Government gives the Contractor a preliminary written notice of its intent to extend at least 30 days before the contract expires. The preliminary notice does not commit the Government to an extension.

(b) If the Government exercises this option, the extended contract shall be considered to include this option clause.

(c) The total duration of this contract, including the exercise of any options under this clause, shall not exceed 66 months.

(End of Clause)

Addendums – FAR Clauses & Provisions

Addendum to 52.212-1 - Instructions, Conditions and Notices to Offerors (Jul 2021)

The Government plans to award a contract to the Offeror whose quote represents the best value solution. The CO may reasonably determine that the superior solution/approach merits a higher price, and therefore represents the best value to the Government. The CO, using sound business judgment will base the selection decision on the integrated assessment of the Statement of Work and the Offeror's capability as measured against the below evaluation factors. Quotation shall be prepared in accordance with and comply with the instructions contained within this RFQ. The technical submission will be evaluated separately from the price submission. Quotes will be evaluated in accordance with the evaluation factors listed herein.

Cover Page

Quote(s) shall be submitted with a cover page to include the following information:

- Company Name and Address
- Phone Number
- Point of Contact Name and E-Mail Address
- CAGE Code
- Small Business Qualification
- Contractor personnel location
- GSA Contract Number

In addition to the Cover Page, quotes(s) shall consist of three (3) separate volumes and contain the following information. The following factors shall be used to evaluate offerors, and the evaluation criteria for award are listed in order of importance as follows:

Volume I: Technical

Proposed Key Personnel - Offerors shall provide resumes of prospective key personnel. The proposed key personnel is:

- One (1) ACE Fraud Investigator

The key personnel shall perform the tasks identified in the Statement of Work. No more than two candidates with two (2) accompanying resumes shall be submitted for the key personnel position. The resume(s) shall demonstrate the key personnel's qualifications to provide the requested services and demonstrate experience in projects of similar size, scope, complexity and results. The resumes shall list the Key Personnel's security clearance level, location, and training, if any.

Offerors shall provide three (3) professional references for each proposed key personnel that can provide past performance information related to the type of work described in the Statement of Work.

Volume II: Past Performance

The Offeror will be evaluated based on their past performance experience. The Offeror shall submit up to three (3) past performance references of similar work and scope completed within three (3) years of this solicitation closing. Evaluation will be based on the relevancy of recent efforts accomplished by the Offeror. Other information that may be obtained, including how well the offeror cooperated with the client, the quality and timeliness of work delivered, and if costs were properly controlled (if applicable) will also be evaluated. Past performance information will also

be accessed by the Government from available online databases, including sources such as the Contractor Performance Assessment Rating System (CPARS) and Systems for Award Management. EOUSA will evaluate the breadth and depth of the Offeror's past performance and the degree to which the Offeror's past performance was positive, taking into consideration technical effectiveness, timeliness of performance, and

management effectiveness.

Volume III: Price

Offerors shall submit a complete price quote as reflected in Attachment 1 - Pricing Schedule, to be evaluated. Do not include asterisks with exceptions or comments on these pages. Only state the unit price and total CLIN amount for each CLIN item. Any additions to the pricing page other than the CLIN price in the space provided will not be considered. Quotes providing partial pricing shall be considered non-responsive and subsequently, ineligible for award.

All pricing and costs associated to provide the requisite services stated in this SOW herein shall be included within the pricing proposal. No additional line items nor additional charges will be added or considered post-award.

The Government will evaluate quotes for award purposes by adding the total price for all options to the total price for the basic requirement. Evaluation of options will not obligate the Government to exercise the option(s).

(End of addendum)

Addendum to 52.212-2 - Evaluation-Commercial Items (Oct 2014)

1 (Technical)
2 (Past Performance)
3 (Price)

Technical and past performance, when combined, are significantly more important than

price. (End of addendum)

Attachments

1. Pricing Schedule

Request for Quotation # 15JA0522O00000103

This is a combined synopsis/solicitation for Affirmative Civil Enforcement (ACE) Fraud Investigator Support Services (commercial items) prepared in accordance with FAR 8.405-2, as supplemented with additional information included in t[h]is notice. This announcement constitutes the only solicitation; quotes are being requested and a written solicitation will not be issued.

Specific instructions to offerors and minimum quote submission criteria are located in Addendum to 52.212-1- Instructions, Conditions and Notices to Offerors (Jul 2021)

Questions in regard to this solicitation are due August 18, 2022 at 1:00 PM Eastem to the Contracting Officer via email at XXX. Questions submitted after this deadline may not be responded to.

_ 9, 2022 at 10:00 Al'\1 Eastem to the Contracting Officer via email at

–

For further information regarding this solicitation, contact:

Contracting Officer
Executive Office for United States Attorneys

[redacted]

Attachment 1 - Pricing Schedule

SCHEDULE OF SUPPLIES/SERVICES

ITEM NO.	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
0001	ACE Fraud Investigator Support Services PSC: R499 **Line Period of Performance:** 09/28/2022 - 09/27/2023 Base Period	12	MO	$_____	$_____
ITEM NO.	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
0002	Travel in accordance with Federal Travel Regulation (FTR) Estimate, Not to Exceed PSC: R499 **Line Period of Performance:** 09/28/2022 - 09/27/2023 Base Period	1,000	EA	$___1.00____	$_____1,000.00_____
ITEM NO.	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
1001	ACE Fraud Investigator Support Services PSC: R499 **Line Period of Performance:** 09/28/2023 - 09/27/2024 Option Period	12	MO	$_____	$_____
ITEM NO.	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
1002	Travel in accordance with Federal Travel Regulation (FTR) Estimate, Not to Exceed	1,000	EA	$___1.00____	$_____1,000.00_____

	PSC: R499 **Line Period of Performance:** 09/28/2023 - 09/27/2024 Option Period				
ITEM NO.	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
2001	ACE Fraud Investigator Support Services PSC: R499 **Line Period of Performance:** 09/28/2024 - 09/27/2025 Option Period	12	MO	$_____	$_____
ITEM NO.	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
2002	Travel in accordance with Federal Travel Regulation (FTR) Estimate, Not to Exceed PSC: R499 **Line Period of Performance:** 09/28/2024 - 09/27/2025 Option Period	1,000	EA	$___1.00____	$_____1,000.00_____
ITEM NO.	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
3001	ACE Fraud Investigator Support Services PSC: R499	12	MO	$_____	$_____

	Line Period of Performance: 09/28/2025 - 09/27/2026 Option Period				
ITEM NO.	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
3002	Travel in accordance with Federal Travel Regulation (FTR) Estimate, Not to Exceed PSC: R499 **Line Period of Performance:** 09/28/2025 - 09/27/2026 Option Period	1,000	EA	$____1.00____	$_____1,000.00_____
ITEM NO.	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
4001	ACE Fraud Investigator Support Services PSC: R499 **Line Period of Performance:** 09/28/2026 - 09/27/2027 Option Period	12	MO	$_____	$_____
ITEM NO.	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
4002	Travel in accordance with Federal Travel Regulation (FTR) Estimate, Not to Exceed PSC: R499 **Line Period of Performance:** 09/28/2026 - 09/27/2027 Option Period	1,000	EA	$____1.00____	$_____1,000.00_____

Grand Total: $_____