**United States Attorney’s Office**

**Northern District of Alabama**

**1801 Fourth Avenue North**

**Birmingham, AL 35203**

**Contracting Officer/P.O.C.: Carmen M. Richardson**

**Phone: 205-244-2051 Email:** **Carmen.Richardson@usdoj.gov**

**RFQ# 15JA01-21-Q-00000007**

**Open Period: Wednesday, August 18, 2021 at 10:00 a.m. CT to Friday, August 28, 2021 at 10:00 a.m. CT**

**STATEMENT OF WORK**

**Project Safe Neighborhood**

**BACKGROUND**

The Department of Justice (DOJ), United States Attorney’s Office (USAO), Northern District of Alabama (NDAL) has a requirement for Project Safe Neighborhood (PSN) Data Analysis in our Birmingham office. Addressing crime and successfully identifying offenders requires substantial use of data from multiple data sets. Criminal justice data is often incomplete and messy; and typically, does not cross over different parts of the system (or even within the same system). Increased capacity to track offenses and offenders over multiple data systems is needed to increase the effectiveness and efficiency of addressing crime. The USAO requires contractor support services to assist the Community Outreach Coordinator with crime prevention analytics.

**SCOPE OF WORK**

The contractor will assist the Community Outreach Coordinator to develop and execute the crime prevention strategies for the USAO-NDAL. The contractor will (1) coordinate with the USAO and justice agencies to determine desired data integration; (2) determine what systems are currently integrated and obtain approval for data release and delivery; and (3) assist the Outreach Coordinator in developing and organizing data samples to design an integration.

**STATEMENT OF WORK/TASKS**

The contract employee shall have the knowledge, skills, and abilities to perform the duties as specified herein. Typical duties will include:

1. Coordinate with USAO and justice agencies to determine desired data integration.
2. Determine what systems that are currently integrated.
3. Obtain approvals for data release and delivery (Data Use Agreements).
4. Obtain data samples to design an integration process.
5. Test data integration process and debug as necessary.
6. Distribute test dataset among stakeholders to ensure completeness.
7. Obtain complete data sets from agencies
8. Conduct and test large scale integration.
9. Establish process for regular delivery of data and maintenance of integrated data set.
10. Train justice agency personnel as needed.
11. Establish sunset of records and datasets.
12. **Place of Performance**

United States Attorney’s Office

Northern District of Alabama

1801 Fourth Avenue North

Birmingham, AL 35203-2101

The period of performance for this assignment is anticipated to last approximately 1 year, maybe longer depending on funding in future fiscal years. The period of performance should start on September 1, 2021, thru August 31, 2022. The contractor shall perform duties at the 1801 Fourth Avenue N. in Birmingham, Alabama as well as offsite at planning meetings and special events. The contractor shall work from 8:30 a.m. to 5:00 p.m., Monday through Friday, except Federal holidays and may be required to work evening hours during special programs.

1. **Scope of Work**

The statement of work encompasses PSN data analysis.

The contractor shall be able to solicit and hire a candidate that meets the following requirements:

 Key Requirements:

* Must be a U.S. Citizen
* Background and/or Security Investigation Required
* Available for Part-Time Work
* Relocation Expenses are not authorized
1. **Deliverables/Performance Standards**

Contractor performance will be monitored and assessed by the COR, or other designated government representative, by periodically sampling and reviewing documentation and records for quality and timeliness of work accomplished. The COR shall inform the Contractor of any problems as they arise.

Specific deliverables will include:

* Data Use Agreement signed by all parties for each agency Month 1 after start
* Data samples provided for test integration Month 2
* Completed test integrated data set Month 6
* Data set delivered to stakeholders Month 6
* Obtain complete data sets from agencies Month 8
* Delivery of complete data set to agencies Month 10
* Establish protocols for data deletion and sunset Month 11
* Final report Month 12
1. **Certifications, License, Physical Requirements or Other Expertise Required**

The contractor must have good communication and organizational skills, the ability to deliver high quality work under pressure, and knowledge of software used by the USAO (or the ability to acquire knowledge about the USAO’s computer systems).

The contractor must have the ability to prove U.S. citizenship and meet the Department of Justice residency requirements.

1. **Contracting Officer**

The Contracting Officer for this contract is:

Attn: Carmen M. Richardson, Contracting Officer

United States Attorney’s Office

Northern District of Alabama

1801 Fourth Avenue North

Birmingham, AL 35203-2101

Written communications shall make reference to the contract number and shall be emailed to Carmen.Richardson@usdoj.gov or mailed to the address above.

1. **Contract Type**

This will be a firm fixed price contract with hourly rates.

1. **Government Furnished Support/Information**

The USAO will assist in coordination of justice agencies and contacts and will assist in obtaining approvals for and receipt of data from the agencies.

**DOJ Ethics -** All contract employees must view the Department of Justice ethics presentation entitled, “Pardon the Ethics Interruption,” within the first two weeks of employment. Copies of his presentation may be obtained from the on-site USAO employee in charge of directing the work of the contract employee. The employee should notify the government manager upon completion task. The government manager will notify the COR, who will maintain a record of completion of this training in the official file.

All contract employees must complete the U.S. Office of Government Ethics online training module entitled, “Interacting with Government Employees for Contractors,” within the first two weeks of employment. The contractor should notify the government manager upon completion of this training module. The government manager will notify the COR, who will maintain a record of completion of this training in the official file.

**Confidentiality Requirements –** Signature of a Nondisclosure Agreement is required of all contractor employees. This Agreement must be signed the first day of employment. All signed forms shall be retained in the official file by the COR.

1. **Employee Qualifications and Conduct**

The Government reserves the right to require the Contractor to reassign from this contract any Contractor employee(s) who is deemed incompetent, careless, unsuitable, or otherwise objectionable, or whose continued use under the contract is deemed contrary to the best interests of the Government.

The Contractor shall remove any employee from performance of contract work within five (5) working days of receiving notice from the Contracting Officer that the employee’s performance is unsatisfactory. The Contractor shall immediately remove any Contractor employee found to represent a threat to the safety of government records, government employees, or other Contractor employees. In instances where the removal of an employee is for substandard performance or behavior negatively impacting delivery of services, the Contractor will be given an opportunity to address the situation prior to removing the employee.

1. **Data Rights**

With prior project approval, incumbent is permitted to use the integrated data for research projects to improve crime and justice application and in better understanding offender behavior. In no case will individual level data be released or included in any publication or other document or data set.

1. **Invoicing Instructions**

To constitute a proper invoice, invoices must be submitted on a monthly basis in accordance with FAR 52.212-4(g). The Government will not pay for services not yet received, accepted or pre-approved, as applicable.

The USAO will process invoices under the Prompt Payment guidelines to pay within thirty days of receipt of the services or receipt of the invoice. The payment will be made via Electronic Funds Transfer (EFT) to the financial institution ac­count in the System for Award Management (SAM) database.

Invoices should be addressed to:

United States Attorney’s Office

Northern District of Alabama

ATTN: BUDGET OFFICE

1801 Fourth Avenue North

Birmingham, AL 35203-2101

1. **Local Clauses**

**Notice of Contractor Personnel Security Clearance Requirements (May 2016)**

Where performance under this contract/task or delivery order/call requires contractor personnel to have access to Department of Justice (DOJ) information, systems or facilities, contractor personnel will be subject to the background clearance requirements of Homeland Security Presidential Directive (HSPD)-12, OMB Guidance Memorandum M-05-24, FIPS Publication 201 and DOJ policy implementing HSPD-12 requirements.

Background clearance requirements are determined by the risk level of each position, type of access and length of access required. Further information on background security clearance requirements applicable to contractor personnel proposed for performance on this contract/order/call may be obtained from the Contracting Officer.

All contractor personnel must meet the DOJ Residency Requirements. He/She must have lived in the United States three of the last five years immediately prior to start of performance on this contract/order/call, and/or worked for the United States overseas in a federal or military capacity, and/or be a dependent of a federal or military employee serving overseas. Specific limited waiver request requirements - contractor personnel performing duties for a cumulative total of 14 days or less where there is a critical need for their specialized and unique skills (as solely determined by the Government) may be proposed for a waiver of the Residency Requirement by the contractor. Contractor personnel who are non-US citizens proposed for such a waiver of the Residency Requirement must be from a country allied with the United States (Since the countries on the Allied Countries List are subject to change, the contractor may review the following website for current information:

<http://www.opm.gov>

For contracts/orders/calls where access to DOJ information systems is involved, non-US citizens are not permitted to have access to or assist in the development, operation, management or maintenance of any DOJ IT system, unless a waiver is granted by the head of the Component, with concurrence of the Department Security Officer (DSO) and DOJ Chief Information Officer (CIO). Any such waiver must be in writing and be obtained prior to allowing any contractor employee who is the subject of the waiver request to begin work under this contract/order/call.

The above requirements apply to any and all contractor employees requiring access to DOJ information systems or facilities, including subcontractor personnel, if applicable.

(end of clause)

**Security of Department Information and Systems (April 2015)**

**I. Applicability to Contractors and Subcontractors**

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

**II. General Definitions**

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

A. **Information** means any communication or representation of knowledge such as facts, data, or opinions, in any form or medium, including textual, numerical, graphic, cartographic, narrative, or audiovisual. Information includes information in an electronic format that allows it be stored, retrieved or transmitted, also referred to as “data,” and “personally identifiable information” (“PII”), regardless of form.

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

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

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

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

**III. Confidentiality and Non-disclosure of DOJ Information**

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

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

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

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

1. 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)

**Continuing Contract Performance During a Pandemic Influenza or other National Emergency (October 2007)**

During a Pandemic or other emergencies 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 contractor’s 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)

**Provisions and Clauses Incorporated by Full Text**

52.217-5, Evaluation of Options (Jul 1990)

Except when it is determined in accordance with FAR 17.206(b) not to be in the Government’s best interests, the Government will evaluate offers 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 Provision)

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 42 months.

(End of Clause)

52.252-1, Solicitation Provisions Incorporated by Reference (Feb 1998)

This solicitation incorporates one or more solicitation provisions by reference, with the same force and effect as if they were given in full text. Upon request, the Contracting Officer will make their full text available. The offeror is cautioned that the listed provisions may include blocks that must be completed by the offeror and submitted with its quotation or offer. In lieu of submitting the full text of those provisions, the offeror may identify the provision by paragraph identifier and provide the appropriate information with its quotation or offer. Also, the full text of a solicitation provision may be accessed electronically at this/these address(es): <http://www.acquisition.gov/far/> and <http://farsite.hill.af.mil/vffar1.htm>

(End of Provision)

52.252-2, Clauses Incorporated by Reference (Feb 1998)

This contract incorporates one or more clauses by reference, with the same force and effect as if they were given in full text. Upon request, the Contracting Officer will make their full text available. Also, the full text of a clause may be accessed electronically at this/these address(es): <http://www.acquisition.gov/far/> and <http://farsite.hill.af.mil/vffar1.htm>

(End of Clause)

**Provisions and Clauses Incorporated by Reference**

52.204-3, Tax Identification Number (OCT 98) - If known, please indicate your Tax Identification Number (TIN). \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

52.204-6, Unique Entity Identifier (OCT 2016) - If known, please indicate your Contractor Identification Number (DUNS #) \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

52.204-10, Reporting Executive compensation and First-Tier Subcontract Awards (OCT 2016) (Pub. L. 109-282) (31 U.S.C. 6101 note).

52.209-2, Prohibition on Contracting with Inverted Domestic Corporations - Representation (NOV 2015).

52.209-6, Protecting the Government’s Interest When Subcontracting with Contractors Debarred, Suspended, or Proposed for Debarment (OCT 2015) (31 U.S.C. 6101 note).

52.209-10, Prohibition on Contracting with Inverted Domestic Corporations (NOV 2015).

52.212-1, Instructions to Offerors -- Commercial Items (JAN 2017)

52.212-3, Offeror Representations and Certifications -- Commercial Items (JAN 2017)

52.212-4, Contract Terms and Conditions -- Commercial Items (JAN 2017) – Alternate I (JAN 2017)

52.212-5, Contract Terms and Conditions Required to Implement Statutes or Executive Orders -- Commercial Items (JAN 2017)

52.219-4, Notice of Price Evaluation Preference for HUBZone Small Business Concerns (OCT 2014) (15 U.S.C. 657a).

52.219-28, Post Award Small Business Program Representation (JUL 2013) (15 U.S.C. 632(a)(2)).

52.222-3, Convict Labor (JUN 2003) (E.O. 11755).

52.222-17, Nondisplacement of Qualified Workers (May 2014).

52.222-21, Prohibition of Segregated Facilities (APR 2015).

52.222-26, Equal Opportunity (SEP 2016) (E.O. 11246).

52.222-36, Equal Opportunity for Workers with Disabilities (JUL 2014) (29 U.S.C. 793).

52.222-50, Combating Trafficking in Persons (MAR 2015) (22 U.S.C. 7104(g)).

52.223-18, Encouraging Contractor Policies to Ban Text Messaging while Driving (AUG 2011) (E.O. 13513).

52.224-3, Privacy Training (JAN 2017)

52.225-13, Restrictions on Certain Foreign Purchases (JUN 2008) (E.O.’s, proclamations, and statutes administered by the Office of Foreign Assets Control of the Department of the Treasury).

52.232-33, Payment by Electronic Funds Transfer— System for Award Management (JUL 2013) (31 U.S.C. 3332).

52.239-1, Privacy or Security Safeguards (AUG. 1996) (5 U.S.C. 552a).