– Validation and Modeling Support

SECTION I – SUPPLIES OR SERVICES AND PRICE/COSTS

CONTRACT TYPE

The Government is awarding a Labor Hour BPA task order under the Department of Homeland Security's Office of Chief Financial Officer (OCFO) Strategic Sourcing Vehicle for Manpower Modeling Blanket Purchasing Agreement (BPA) to provide Validation and Modeling Support to the Department of Homeland Security (DHS), Office of Program Accountability and Risk Management (PARM).

All terms and conditions of the Contractor's DHS Manpower Modeling BPA remain unchanged and in full force and effect, unless specifically stated otherwise herein.

TRAVEL

The Contractor may be required to travel within the Washington, DC metropolitan area or to other DHS Components within a fifty (50) mile radius of the duty location in the performance of work on this requirement. All travel within a fifty (50) mile radius of the duty location is local travel. The Contractor will not be reimbursed for local travel.

End of Section I
[Remainder of Page Blank]

– Validation and Modeling Support

SECTION II - STATEMENT OF WORK

1.0 GENERAL

1.1 Background

In Fiscal Year (FY) 2017, The Department of Homeland Security (DHS) initiated implementation of the requirements of the DHS Instruction 102-01-006, Acquisition Program Management Staffing. This instruction requires each DHS major acquisition program and Component Acquisition Executives (CAEs) to develop and maintain a multi-year staffing plan which documents staffing needed to be sufficiently staffed, critical positions, staffing gaps, and an association mitigation strategy to address staffing gaps. The Office of Program Accountability and Risk Management (PARM) is responsible for reviewing staffing plans for completeness and analyzing staffing gaps and mitigation strategies; consolidating staffing plans across DHS for Department-level acquisition workforce requirements analysis; and performing program staffing analysis and assessments to provide recommendations on staffing. To ensure these staffing plans are based on defensible data driven estimates, which can be submitted as part of the Resource Allocation Plan (RAP) submission, PARM requires a workforce requirement model capable of identifying staffing gaps to help determine relationships between staffing levels and program performance.

1.2 Objective

To successfully carry out the responsibilities described in this SOW, the Contractor shall provide DHS PARM support and guidance in developing and sustaining a predictive manpower requirements model with analytical capability to aid leadership decision making in staffing resource allocations.

1.3 Scope

The scope of this requirement in providing analysis and developing and/or improving analytical tools related to the DHS Component manpower plans, programs, and budgets. The contractor shall develop and provide advice on analytical protocols used to understand manpower requirements models. This includes providing in depth studies and analysis to validate existing manpower requirements models and staffing plans used for estimating staffing requirements, validating the underlying models for generating requirements, tables, and graphic illustrations, and verifying that the data used in the models is accurate and can be manipulated in a repeatable way so it can be presented to leadership in a clear and concise manner to aid in leadership decision making. Additionally, the contractor shall possess the capability to review human capital, operational, and cost data to help Components develop analytical manpower requirements models that provide leadership with projected multi-year requirements and costs associated with staffing resources. The contractor shall have the capability to make iterative improvements utilizing advanced analytics to the model. Finally, the contractor must have the knowledge to recommend a standardized approach to manpower analysis and data collection processes that is extendible to both existing models and related staffing plans, along with future improvements, which can be easily implementable across Components. Improvements shall include, but is not limited to the following:

1. The capability for scenario-based analysis allowing programs to predict staffing resources based on planned future work across the acquisition lifecycle.
2. Iterative improvements to MS Power Apps based applications staffing data collection tools or similar application data collection tool based on feedback from user community and other

– Validation and Modeling Support

stakeholders.

3. Extract data from staffing plan or staffing model data sources and put them into consolidated database for use in modeling or staffing plan analysis and reporting. Previously this has been done using R-Script.

4. Deliver continuous process improvements to develop and maintain the current "Ratio-based" model. This includes but is not limited to the capability to generate reports, data visualization dash boards, and a predictive ability for staffing resource needs for new programs.

1.4 Applicable Documents

The following documents are applicable to this BPA Call:

- Workforce Requirements Instruction 106-01-001

– Validation and Modeling Support

- Workforce Requirements Instruction 106-01-001
- DUSM Workforce Requirements Model Verification, Validation, and Accreditation Memo
- Chief Financial Officers (CFO) Act of 1990 (P.L. 101-576)
- Federal Acquisition Regulations
- DHS Strategic Plan
- GAO Standards for Estimating Staffing Requirements
- OMB Circular A-11 *Preparation, Submission and Execution of the Budget*
- DHS Instruction 102-01-001
- Directive 101-01 Planning, Programming, Budgeting, and Execution

2.0 TASKS

The Contractor shall provide support to DHS PARM to increase level of internal controls by analyzing, validating existing manpower requirements models, developing manpower requirements models, and making improvements to include:

2.1 TASK ONE: Maintain and Sustain: The Contractor shall develop an accurate acquisition workforce staffing requirement model(s) depicting the number and type of acquisition professionals needed by major acquisition programs across the acquisition lifecycle of a program. The contractor shall provide the model(s) in complete entirety to PARM along with accompanying operation, maintenance, and training documentation (i.e., electronic User Manual with screenshots for general users, guidance for utilizing and updating the model for admin users). The activities will leverage existing DHS systems, software, processes, and products to the maximum extent possible. The analysis and modeling shall include but is not limited to:

2.1.1 (Maintain): The Contractor shall make recommendations, define requirements to support business process improvements and provide iterative improvement support to the multi-year staffing plan submitted by Components. The Contractor shall facilitate the staffing plan collection process by updating the necessary data parameters in the power application tool used by PARM to collect annual staffing plans.

2.1.2 (Maintain): Develop an understanding of DHS and Component organizational structure, management and acquisition mission support responsibilities, functions, existing and future workload. Inventory existing products, tools, and data collection methods. Provide input to improve data collection processes currently in use. Perform Gap Analysis to determine capabilities and needs for workload.

2.1.3 (Maintain): Build and validate annual updates to Requirements Models or iterations of any existing models covering acquisition workforce, as approved by COR. Calculate baseline staffing requirements and iterate on the data visualization platform – currently a Power BI output-based model, which compares historic workload data to current staffing needs to establish a shortfall or surplus. Models shall be compatible with the current PARM annual staffing plan process. Models shall document or catalog staffing requirements in accordance with the PA&E Verification, Validation, and Accreditation (VV&A) process.

2.1.4 (Maintain): In support of the existing output-based model and related staffing plans; develop, maintain, and iteratively improve the existing work break down structure, data

– Validation and Modeling Support
collection application and associated processes necessary to create an output-based staffing model with inputs collected and validated annually.

2.1.5 (Maintain): The contractor shall develop a tool for use by government personnel which provides status updates on current and future contractor activities relating to model progress, development, and planned improvements. This tool shall contain any planned updates and improvement statuses of the data collection tool (currently Power-BI app).

2.1.6 (Maintain): The Contractor shall develop training materials, continuity documentation and conduct training for Federal personnel.

2.2 TASK TWO: Operationalize and Integrate: The Contractor shall provide recommendations, support, and guidance on how to operationalize and integrate the model(s) with existing and related DHS acquisition workforce activities including data collection efforts and Staffing Plan analysis and reporting requirements.

2.2.1 (Integrate): Conduct analysis using current and historic DHS staffing, data, and acquisition lifecycle activities to identify and distinguish which positions are in the acquisition workforce and which positions are currently covered by existing models.

2.2.2 (Integrate): The Contractor shall support acquisition staffing oversight activities by providing analysis of available staffing models and other relevant data sources including annual staffing plans.

2.2.3 (Integrate): Integrate additional elements as directed by COR into existing staffing model WBS to capture acquisition work more accurately being completed by programs. As an example, add a new element to the existing a program identifies as work not previously covered in the WBS.

2.2.4 (Integrate): Determine how to integrate additional parameters that would benefit modeling to produce more accurate projections. As an example, utilization of cost data provided by other DHS Lines of Business (LOB).

2.2.5 (Integrate): The Contractor shall prepare the Model for DHS formal Verification, Validation, and Accreditation (VV&A).

3.0 USE OF SURGE OPTIONS
All Optional Surge CLINs can be exercised unilaterally in accordance with FAR 17.202 for an increase in quantity of support for the task areas.

3.1 Optional Surge Task: Development and Iterative Improvements

3.1.1 (Surge): Deliver a program calculator reporting tool based on existing baseline ratio / output modeling data that can estimate future staffing needs that is tailorable to individual DHS components and programs to analyze patterns, needs and current resources and to forecast workforce demands, trends, and needs based on historical trends, seasonal fluctuations, and other factors influencing acquisition programs, departments, or units. Acquisition workforce forecasting capabilities shall also align to DHS Acquisition Lifecycle Framework (ALF) scheduling activities to enable the production of better, more timely and accurate program staffing plans. The tool shall have the ability to report or export the modeled output.

– Validation and Modeling Support

3.1.2 (Surge): The Contractor shall use statistics and/or other analytical tools approved for use by DHS to analyze the data from the model and staffing plans to determine if and how staffing levels play a role in determining program success.

3.1.3. (Surge): Develop multi-year forecast for staffing /manpower needs.

3.1.4. (Surge): Develop tailored applications based on customer (component program /CAE requests and / or to integrate data to and from other data sources) or for partner funded applications as directed by the COR.

3.2 Optional Surge Task: Operationalize and Integrate. The Contractor shall provide recommendations, support, and guidance on how to operationalize and integrate the model(s) with existing and related DHS acquisition workforce activities including data collection efforts and Staffing Plan analysis and reporting requirements.

4.0 CONTRACTOR PERSONNEL

4.1 Key Personnel

The following Contractor personnel is designated as Key for this requirement.

- Manager/Project Manager

The Manager/Project Manager is designated as *Key* by the Government. Before replacing any individual designated as *Key* by the Government, the Contractor shall notify the Contracting Officer no less than 15 business days in advance, submit *Key* person being replaced, unless otherwise approved by the Contracting Officer. The Contractor shall not replace *Key* Contractor personnel without approval from the Contracting Officer.

The Project Manager shall be a single point of contact for the Contracting Officer and the Contracting Officer's Representative (COR). The name of the Manager/Project Manager, and the name(s) of any alternate(s) who shall act for the Contractor in the absence of the Manager/Project Manager, shall be provided to the Government as part of the Contractor's proposal. During any absence of the Manager/Project Manager, only one alternate shall have full authority to act for the Contractor on all matters relating to work performed under this BPA Call.

4.2 Qualified Personnel

The Contractor shall provide qualified personnel in accordance with ATTACHMENT III – LABOR CATEGORY DESCRIPTIONS AND QUALIFICATIONS to perform all requirements specified in this SOW. The Contractor shall maintain the personnel, organization, and administrative control necessary to ensure that the work delivered meets the Government's specifications and requirements.

4.3 Continuity of Support

The Contractor shall ensure that the contractually required level of support for this requirement is always maintained. The Contractor shall ensure that all contract support personnel are present for all hours of the workday as defined in this BPA call. If for any reason the Contractor staffing levels are not maintained due to vacation, leave, appointments, etc., and replacement personnel will not be provided, the Contractor shall provide e-mail notification no later than 2 business days in advance to the COR prior to planned employee absence and as soon as possible for

– Validation and Modeling Support

unplanned absences along with mitigation strategies for planned work for personnel not present. Otherwise, the Contractor shall provide a fully qualified replacement during time of absence.

4.4 Employee Identification

Contractor employees visiting Government facilities shall wear an identification badge that, at a minimum, displays the Contractor name, the employee's photo, name, clearance-level and badge expiration date. Visiting Contractor employees shall comply with all Government escort rules and requirements. All Contractor employees shall identify themselves as Contractors when their status is not readily apparent and always display all identification and visitor badges in plain view above the waist.

Contractor employees working on-site at Government facilities shall wear a Government issued identification badge. All Contractor employees shall identify themselves as Contractors when

– Validation and Modeling Support

their status is not readily apparent (in meetings, when answering Government telephones, in e-mail messages, etc.)

4.5 Employee Conduct

Contractor's employees shall comply with all applicable Government regulations, policies, and procedures (e.g., fire, safety, sanitation, environmental protection, security, "off limits" areas, wearing of parts of DHS uniforms, and possession of weapons) when visiting or working at Government facilities. The Contractor shall ensure Contractor employees always present a professional appearance and that their conduct shall not reflect discredit on the United States or the Department of Homeland Security. The Project Manager shall ensure Contractor employees understand and abide by Department of Homeland Security established rules, regulations and policies concerning safety and security.

4.6 Removing Employees for Misconduct or Security Reasons

The Government may, at its sole discretion (via the Contracting Officer*), direct the Contractor to remove any Contractor employee from DHS facilities for misconduct or security reasons. Removal does not relieve the Contractor of the responsibility to continue providing the services required under the contract. The Contracting Officer will provide the Contractor with a written explanation to support any request to remove an employee.

End of Section II
[Remainder of Page Blank]

– Validation and Modeling Support

SECTION III – DELIVERIES OR PERFORMANCE

1.0 PERIOD OF PERFORMANCE

The BPA call period of performance is a12-month base period and three (3) 12-month option period.

The performance period of this BPA Call may not extend more than 12-months beyond the OCFO Strategic Sourcing Vehicle for Manpower Modeling contract unless the contract has been modified to extend the period of performance.

2.0 PLACE OF PERFORMANCE

The primary place of performance for work under this effort is the Contractor's facility or designated location (i.e., telework).

Contractor personnel may be required to attend occasional large meetings at the DHS facility located in the TSA HQ building 6595 Springfield Center Drive, Springfield, VA 22150, or other designated federal facilities as necessary.

3.0 HOURS OF OPERATION

Contractor employees shall generally perform all work between the hours of 8:00 am and 5:30 pm ET, Monday through Friday (except Federal holidays). However, there may be occasions when Contractor employees shall be required to work other than normal business hours, including weekends and holidays, to fulfill requirements under this SOW.

Services will generally not be required on the following Federal holidays (or any other holidays declared by the Government); however, the Contractor may be required to provide services on these days in support of mission critical situations.

- New Year's Day – January 1
- Martin Luther King's Birthday – January 20
- Inauguration Day – January 20
- Washington's Birthday – February 17
- Memorial Day - May 26
- Juneteenth National Independence Day – 19 June (or as observed)
- Independence Day - 4 July (or as observed)
- Labor Day - September 1
- Columbus Day - October 13
- Veterans Day - 11 November (or as observed)
- Thanksgiving Day - 4th Thursday in November (November 27)
- Christmas Day - 25 December (or as observed)

No work shall be performed by Contractor personnel on Government facilities on Federal holidays or other non-workdays without prior written approval of the COR.

– Validation and Modeling Support

4.0 DELIVERABLES AND DELIVERY SCHEDULE

Item	SOW Reference	Deliverable / Event	Due by	Recipient/ Approver
1	Section IV, 1.0	Post Award Conference	Within 10 days after the date of award or as coordinated by the Contracting Officer.	Contracting Officer, COR
2	Section IV, 2.0	Kick-Off Meeting	Provided after award by COR or held concurrently with Post Award.	Contracting Officer, COR
3	Section VI, 10.3	Business Continuity Plan	Within 10 business days after award.	COR
4	Section III, 5.1	Monthly Progress Report	5th business day of the month following the month being reported.	COR, CO
5	Section III, 5.2	Monthly Status Meeting	Within 10 business days of the month following the month being reported. Frequency may be reduced at the COR's direction.	COR
6	Section III, 5.2	Meeting Minutes Report	Within 5 business days after each Status Meeting	COR
7	Section II, 2.0	Models and staffing plans	Within 10 business days after the Government's acceptance and approval of the model and / or related staffing plans or iterative development of model and / or related staffing plans	COR
8	Section II, 2.1	Training materials	Within 20 business days of model completion. Due date may be extended at COR's direction.	COR
9	Section III, 5.3	Draft Ad-Hoc Reports	Within 5 business days upon the Government's request	COR
10	Section III, 5.3	Final Ad-Hoc Reports	Within 10 business days after Government's acceptance and approval of Draft Ad Hoc Report.	COR

4.1 Government Acceptance Period

The COR/CO will review deliverables prior to acceptance and provide the contractor with an e-

mail that provides documented reasons for non-acceptance. If the deliverable is acceptable, the COR will send an e-mail to the Contractor notifying it that the deliverable has been accepted.

The COR/CO will have the right to reject or require correction of any deficiencies found in the deliverables that are contrary to the information contained in the Contractor's accepted proposal. In the event of a rejected deliverable, the Contractor will be notified in writing by the COR of the specific reasons for rejection. The Contractor may have an opportunity to correct the rejected deliverable and return it per delivery instructions.

The COR/CO will have 15 business days to review deliverables and make comments. The Contractor shall have 15 business days to make corrections and redeliver.

All other review times and schedules for deliverables shall be agreed upon by the parties based on the final approved Project Plan. The Contractor shall be responsible for timely delivery to Government personnel in the agreed upon review chain, at each stage of the review. The Contractor shall work with personnel reviewing the deliverables to assure that the established schedule is maintained.

5.0 REPORTING REQUIREMENTS

5.1 Monthly Progress Report

The Project Manager shall provide a monthly progress report to the Contracting Officer and COR via electronic mail on the 5th business day of the month following the month being reported. This report shall include a summary of all Contractor work performed, including a breakdown of labor hours by labor category, schedule status, and any Contractor concerns or recommendations for the previous reporting period. The status report shall also identify the work in progress such as the number of actions completed or processed and a projection of work to be started and completed in the following month. In addition, the monthly progress report shall include the BPA Call Number and Contractor's BPA Number. The format will be as agreed upon by the COR.

5.2 Monthly Status Meetings

The Contractor shall meet with the Contracting Officer and the COR monthly to present deliverables, discuss progress, exchange information, and resolve emerging problems and issues. These meetings shall take place at 6595 Springfield Center Drive, Springfield, VA, 22150 or via teleconference.

The Contractor shall submit a meeting minutes report summarizing the key discussions, decisions, and subsequent action items no later than 5 business days after the meeting.

5.3 Ad-Hoc Report

Upon the Government's request, the Project Manager shall submit to the COR, electronically, a "Draft" Ad Hoc Report within 5 business days. The "Final" Ad Hoc Report shall be submitted within 10 business days after the Government's acceptance and approval of the "Draft" Ad Hoc Report. Ad Hoc Reports consists of documentation for any or all of the sections of the requirement as requested by the COR.

– Validation and Modeling Support

5.4 Section 508 Requirements

Section 508 of the Rehabilitation Act (classified to 29 U.S.C. § 794d) requires that when Federal agencies develop, procure, maintain, or use information and communications technology (ICT), it shall be accessible to people with disabilities. Federal employees and members of the public with disabilities must be afforded access to and use of information and data comparable to that of Federal employees and members of the public without disabilities.

All products, platforms and services delivered as part of this work statement that, by definition, are deemed ICT shall conform to the revised regulatory implementation of Section 508 Standards, which are located at 36 C.F.R. § 1194.1 & Appendixes A, C & D, and available at https://www.ecfr.gov/cgi-bin/text-dx?SID=e1c6735e25593339a9db63534259d8ec&mc=true&node=pt36.3.1194&rgn=div5. In the revised regulation, ICT replaced the term electronic and information technology (EIT) used in the original 508 standards. ICT includes IT and other equipment.

Exceptions for this work statement have been determined by DHS and only the exceptions described herein may be applied. Any request for additional exceptions shall be sent to the Contracting Officer and a determination will be made according to DHS Directive 139-05, Office of Accessible Systems and Technology, dated November 12, 2018, and DHS Instruction 139-05-001, Managing the Accessible Systems and Technology Program, dated November 20, 2018, or any successor publication.

1.1 Section 508 Requirements for Technology Services

1. When developing or modifying ICT, the Contractor is required to validate ICT deliverables for conformance to the applicable Section 508 requirements. Validation shall occur on a frequency that ensures Section 508 requirements is evaluated within each iteration and release that contains user interface functionality.
2. When modifying, installing, configuring, or integrating commercially available or government-owned ICT, the Contractor shall not reduce the original ICT Item's level of Section 508 conformance.
3. When developing or modifying ICT deliverables that contain the ability to automatically generate electronic documents and forms in Microsoft Office and Adobe formats, or when the capability is provided to enable end users to design and author web based electronic content (i.e. surveys, dashboards, charts, data visualizations, etc.), the Contractor shall demonstrate the ability to ensure these outputs conform to the applicable Section 508 standards (including WCAG 2.0 Level A and AA Success Criteria). The Contractor shall demonstrate conformance by conducting testing and reporting test results based on representative sample outputs. For outputs produced as Microsoft Office and Adobe PDF file formats, the Contractor shall use the test methods published under "Accessibility Tests for Documents", which are published at https://www.dhs.gov/compliance-test-processes. For outputs produced as web based electronic content, the Contractor shall use the DHS Trusted Tester for Web Methodology Version 5.0, or successor versions. This methodology is published at https://www.dhs.gov/trusted-tester

– Validation and Modeling Support

4. Contractor personnel shall possess the knowledge, skills and abilities necessary to address the accessibility requirements in this work statement.

1.2 Section 508 Deliverables

1. **Section 508 Test Plans**: When developing or modifying ICT pursuant to this contract, the Contractor shall provide a detailed Section 508 Conformance Test Plan. The Test Plan shall describe the scope of components that will be tested, an explanation of the test process that will be used, when testing will be conducted during the project development life cycle, who will conduct the testing, how test results will be reported, and any key assumptions.

2. **Section 508 Test Results**: When developing or modifying ICT pursuant to this contract, the Contractor shall provide test results in accordance with the Section 508 Requirements for Technology Services provided in this solicitation.

3. **Section 508 Accessibility Conformance Reports**: For each ICT item offered through this contract (including commercially available products, and solutions consisting of ICT that are developed or modified pursuant to this contract), the Offeror shall provide an Accessibility Conformance Report (ACR) to document conformance claims against the applicable Section 508 standards. The ACR shall be based on the Voluntary Product Accessibility Template Version 2.0 508 (or successor versions). The template can be found at https://www.itic.org/policy/accessibility/vpat. Each ACR shall be completed by following all of the instructions provided in the template, including an explanation of the validation method used as a basis for the conformance claims in the report.

4. **Other Section 508 Documentation:** The following documentation shall be provided upon request for ICT items offered through this contract:
    - Documentation of features provided to help achieve accessibility and usability for people with disabilities.
    - Documentation on how to configure and install the ICT Item to support accessibility.
    - Documentation of core functions that cannot be accessed by persons with disabilities.
    - Documentation of remediation plans to address non-conformance to the Section 508 standards

End of Section III
[Remainder of Page Blank]

– Validation and Modeling Support

SECTION IV – BPA CALL ADMINISTRATION DATA

1.0 POST AWARD CONFERENCE

The Contractor shall attend a Post Award Conference with the Contracting Officer and the COR within 10 days after the date of award or as coordinated by the Contracting Officer. The Post Award Conference will be held at the Government's facility, 6595 Springfield Center Drive, Springfield, VA, 22150 or via teleconference. The date, time, and location will be provided after award.

2.0 KICK-OFF MEETING

The Contractor shall attend a kickoff meeting for this BPA call as requested following award. The purpose of the Kick-Off Meeting is to discuss technical objectives of the BPA call and review the Contractor's draft project plan. The kick-off meeting, which will be chaired by the COR, will be held at the Government's facility or via teleconference. The date, time, and location will be provided after award by the COR and may be held concurrently with the Post Award Conference.

3.0 Contract Administration

3.1 Contracting Officer

The Contracting Officer is the only individual who can legally commit or obligate the Government for the expenditure of public funds and authorize revisions of the terms and conditions of this BPA Call. The Contracting Officer shall authorize any such revision in writing. If the contractor makes any BPA Call changes at the direction of any person other than the Contracting Officer, the change will be considered to have been made without authority and no adjustment will be made in the BPA Call to cover any increases in changes that may result. The Contracting Officer has the authority to perform any and all post-award functions in administering and enforcing the BPA Call in accordance with its terms and conditions.

The Contracting Officer is

[redacted]
Department of Homeland Security
Office of Procurement Operations
Phone: [redacted]
Email: [redacted]

The Contract Specialist is:

Department of Homeland Security
Office of Procurement Operations
Phone: [redacted]
Email: [redacted]

– Validation and Modeling Support

3.2 Contracting Officer's Representative (COR)

[redacted]
Department of Homeland Security
Office of Program Accountability and Risk Management
Phone: [redacted]
Email: [redacted]

The COR is responsible for the technical administration of the BPA Call and technical liaison between the Contractor and the Government. The COR is not authorized to change the scope of work or specifications stated in the BPA Call, to make any commitments, or otherwise obligate the Government or authorize any changes which affect the BPA Call price, delivery schedule, period of performance, or other terms and conditions. The COR for this BPA Call will be provided after BPA Call award.

End of Section IV
[Remainder of Page Blank]

– Validation and Modeling Support

SECTION V – INVOICE AND PAYMENT PROVISIONS

INVOICING

Invoices shall be prepared in accordance with FAR Clauses 52.232-1 Payments. In addition to invoice preparation as required by the FAR, the Contractor's invoice shall include the following information:

a) Cover sheet identifying DHS;
b) BPA Call and Associated BPA Number;
c) Modification Number, if any;
d) DUNS Number;
e) Month services provided; and
f) CLIN and Accounting Classifications.

Invoices shall be submitted not less than once per month and shall be received no later than the 5th business day of each month (or as otherwise approved by the COR) following the services provided. The Contractor shall invoice for services rendered in accordance with the final pricing Schedule. Supporting documentation shall include labor categories, rates, and hours burned for the billing period; contractor employee name; total cumulative hours to date and dollar amount for contractor employees. The Contractor shall indicate the associated CLIN and dollar amount invoiced.

INVOICE SUBMISSION

The Contractor shall submit the invoice electronically to the address below:

E-mail: [redacted]

Simultaneously provide an electronic copy of the invoice to the following individuals at the addresses below:

a) ATTN: Office of Procurement Operations/ (Contract Specialist) E-mail:

b) ATTN: Office of Procurement Operations/ [redacted] (Contracting Officer) E-mail: [redacted]

b) ATTN: Office of Program Accountability and Risk Management (PARM)/ [redacted]
E-mail [redacted]

End of Section V
[Remainder of Page Blank]

– Validation and Modeling Support

SECTION VI – SPECIAL CONTRACT REQUIREMENTS

1.0 PROTECTION OF INFORMATION

Contractor access to sensitive but unclassified information is required under this SOW. Contractor employees shall safeguard this information against unauthorized disclosure or dissemination in accordance with DHS MD 11042.1, Safeguarding Sensitive but Unclassified (For Official Use Only) Information. The Contractor shall ensure that all Contractor personnel having access to business or procurement-sensitive information sign a non-disclosure agreement (DHS Form 11000-6).

2.0 Personal Identification Verification (PIV) Credential Compliance

Authorities:

- HSPD-12 "Policies for a Common Identification Standard for Federal Employees and Contractors"
- OMB M-11-11 "Continued Implementation of Homeland Security Presidential Directive (HSPD) 12 – Policy for a Common Identification Standard for Federal Employees and Contractors"
- OMB M-06-16 "Acquisition of Products and Services for Implementation of HSPD-12"
- NIST FIPS 201 "Personal Identity Verification (PIV) of Federal Employees and Contractors"
- NIST SP 800-63 "Electronic Authentication Guideline"
- OMB M-10-15 "FY 2010 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management"

Procurements for products, systems, services, hardware, or software involving controlled facility or information system shall be PIV-enabled by accepting HSPD-12 PIV credentials as a method of identity verification and authentication.

3.0 REQUESTS FOR EXCEPTION TO U.S. CITIZENSHIP REQUIREMENT

Special procedures apply for exception to the requirement that persons accessing DHS systems be U.S. citizens. Under normal circumstances, only U.S. citizens are allowed access to DHS systems and networks; but there is a need at times to grant access to foreign nationals. Access for foreign nationals is normally a long-term commitment, and exceptions to citizenship requirements are treated differently from security policy waivers. Exceptions to the U.S. citizenship requirement should be requested by completing a Foreign National Visitor Access Request, DHS Form 11052-1, which is available online or through the DHS Office of the Chief Security Officer (OCSO). Components who have access may file their request via the Foreign National Vetting Management System (FNVMS), a part of the DHS OCSO Integrated Security Management System's (ISMS). For further information regarding the citizenship exception process, contact the DHS OCSO.

This Policy Directive and the DHS 4300A Sensitive Systems Handbook apply to all DHS employees, contractors, detailees, others working on behalf of DHS, and users of DHS information systems that collect, generate, process, store, display, transmit, or receive DHS

information unless an approved waiver has been granted. This includes prototypes, telecommunications systems, and all systems in all phases of the Systems Engineering Life Cycle (SELC).

4.0 POST-AWARD INSTRUCTIONS REGARDING SECURITY REQUIREMENTS FOR CONTRACTS/ORDERS

All contractor and subcontractor personnel are required to complete a suitability/background investigation with the DHS Office of Security, Personnel Security Division.

The procedures outlined below shall be followed for the DHS Security Office to process background investigations and suitability determinations, as required, in a timely and efficient manner.

Carefully read the security clauses in the Order. Compliance with the security clauses in the contract is not optional.

Contract employees (to include applicants, temporaries, part-time and replacement employees) under the contract, requiring access to sensitive information, shall undergo a position sensitivity analysis based on the duties each individual will perform on the contract. The results of the position sensitivity analysis shall identify the appropriate background investigation to be conducted. All background investigations will be processed through the DHS Security Office. Prospective Contractor employees shall submit the following completed forms to the DHS Security Office. The Standard Form 85P will be completed electronically, through the Office of Personnel Management's e-QIP SYSTEM. The completed forms must be given to the DHS Security Office no less than thirty (30) days before the start date of the contract or thirty (30) days prior to entry on duty of any employees, whether a replacement, addition, subcontractor employee, or vendor:

- Standard Form 85P, "Questionnaire for Public Trust Positions"
- FD Form 258, "Fingerprint Card" (2 copies)
- DHS Form 11000-6 "Conditional Access To Sensitive But Unclassified Information
- Non-Disclosure Agreement"
- DHS Form 11000-9, "Disclosure and Authorization Pertaining to Consumer Report is Pursuant to the Fair Credit Reporting Act"

Only complete packages will be accepted by the DHS Security Office. Specific instructions on submission of packages will be provided upon award of the contract.

DHS may, as it deems appropriate, authorize, and grant a favorable entry on duty (EOD) decision based on preliminary suitability checks. The favorable EOD decision would allow the employees to commence work temporarily prior to the completion of the full investigation. The granting of a favorable EOD decision shall not be considered as assurance that a full employment suitability authorization will follow. A favorable EOD decision or a full employment suitability

determination shall in no way prevent, preclude, or bar DHS from withdrawing or terminating access to government facilities or information, at any time during the term of the contract. No employee of the Contractor shall be allowed unescorted access to a Government facility without a favorable EOD decision or suitability determination by the Security Office.

Limited access to Government buildings is allowable prior to the EOD decision if the Contractor is escorted by a Government employee. This limited access is to allow Contractors to attend briefings and non-recurring meetings to begin transition work.

The DHS Security Office shall be notified of all terminations /resignations within five (5) days of occurrence. The Contractor shall return to the Contracting Officer Representative (COR) all DHS issued identification cards and building passes that have either expired or have been collected from terminated employees. If an identification card or building pass is not available to be returned, a report shall be submitted to the COR, referencing the pass or card number, name of individual to who it was issued and the last known location and disposition of the pass or card.

When sensitive Government information is processed on Department telecommunications and automated information systems, the Contractor shall provide for the administrative control of sensitive data being processed. Contractor personnel must have favorably adjudicated background investigations commensurate with the defined sensitivity level. Contractors who fail to comply with Department security policy are subject to having their access to Department IT systems and facilities terminated, whether or not the failure results in criminal prosecution. Any person who improperly discloses sensitive information is subject to criminal and civil penalties and sanctions under a variety of laws (e.g., Privacy Act).

Failure to follow these instructions may delay the completion of suitability determinations and background checks. Note that any delays in this process that are not caused by the government do not relieve a contractor from performing under the terms of the contract.

5.0 SAFEGUARDING OF CONTROLLED UNCLASSIFIED INFORMATION (JULY 2023)

(a) *Definitions*. As used in this clause—

Adequate Security means security protections commensurate with the risk resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of information. This includes ensuring that information hosted on behalf of an agency and information systems and applications used by the agency operate effectively and provide appropriate confidentiality, integrity, and availability protections through the application of cost-effective security controls.

Controlled Unclassified Information (CUI) is any information the Government creates or possesses, or an entity creates or possesses for or on behalf of the Government (other than classified information) that a law, regulation, or Governmentwide policy requires or permits an agency to handle using safeguarding or dissemination controls. This definition includes the following CUI categories and subcategories of information:

(1) Chemical-terrorism Vulnerability Information (CVI) as defined in 6 CFR part 27, "Chemical Facility Anti-Terrorism Standards," and as further described in supplementary guidance issued by an authorized

official of the Department of Homeland Security (including the Revised Procedural Manual "Safeguarding Information Designated as Chemical-Terrorism Vulnerability Information" dated September 2008);

(2) Protected Critical Infrastructure Information (PCII) as set out in the Critical Infrastructure Information Act of 2002 (title XXII, subtitle B of the Homeland Security Act of 2002 as amended through Pub. L. 116–283), PCII's implementing regulations (6 CFR part 29), the PCII Program Procedures Manual, and any supplementary guidance officially communicated by an authorized official of the Department of Homeland Security, the PCII Program Manager, or a PCII Program Manager Designee;

(3) Sensitive Security Information (SSI) as defined in 49 CFR part 1520, "Protection of Sensitive Security Information," as amended, and any supplementary guidance officially communicated by an authorized official of the Department of Homeland Security (including the Assistant Secretary for the Transportation Security Administration or designee), including Department of Homeland Security MD 11056.1, "Sensitive Security Information (SSI)" and, within the Transportation Security Administration, TSA MD 2810.1, "SSI Program";

(4) Homeland Security Agreement Information means information the Department of Homeland Security receives pursuant to an agreement with State, local, Tribal, territorial, or private sector partners that is required to be protected by that agreement. The Department receives this information in furtherance of the missions of the Department, including, but not limited to, support of the Fusion Center Initiative and activities for cyber information sharing consistent with the Cybersecurity Information Sharing Act of 2015;

(5) Homeland Security Enforcement Information means unclassified information of a sensitive nature lawfully created, possessed, or transmitted by the Department of Homeland Security in furtherance of its immigration, customs, and other civil and criminal enforcement missions, the unauthorized disclosure of which could adversely impact the mission of the Department;

(6) International Agreement Information means information the Department of Homeland Security receives that is required to be protected by an information sharing agreement or arrangement with a foreign government, an international organization of governments or any element thereof, an international or foreign public or judicial body, or an international or foreign private or non-governmental organization;

(7) Information Systems Vulnerability Information (ISVI) means:

> (i) Department of Homeland Security information technology (IT) systems data revealing infrastructure used for servers, desktops, and networks; applications name, version, and release; switching, router, and gateway information; interconnections and access methods; and mission or business use/need. Examples of ISVI are systems inventories and enterprise architecture models. Information pertaining to national security systems and eligible for classification under Executive Order 13526 will be classified as appropriate; and/or
>
> (ii) Information regarding developing or current technology, the release of which could hinder the objectives of the Department, compromise a technological advantage or countermeasure, cause a denial of service, or provide an adversary with sufficient information to clone, counterfeit, or circumvent a process or system;

(8) Operations Security Information means Department of Homeland Security information that could be collected, analyzed, and exploited by a foreign adversary to identify intentions, capabilities, operations, and vulnerabilities that threaten operational security for the missions of the Department;

(9) Personnel Security Information means information that could result in physical risk to Department of Homeland Security personnel or other individuals whom the Department is responsible for protecting;

(10) Physical Security Information means reviews or reports illustrating or disclosing facility infrastructure or security vulnerabilities related to the protection of Federal buildings, grounds, or property. For example, threat assessments, system security plans, contingency plans, risk management plans, business impact analysis studies, and certification and accreditation documentation;

(11) Privacy Information includes both Personally Identifiable Information (PII) and Sensitive Personally Identifiable Information (SPII). PII refers to 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; and SPII is a subset of PII that if lost, compromised, or disclosed without authorization could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. To determine whether information is PII, the DHS will perform an assessment of the specific risk that an individual can be identified using the information with other information that is linked or linkable to the individual. In performing this assessment, it is important to recognize that information that is not PII can become PII whenever additional information becomes available, in any medium or from any source, that would make it possible to identify an individual. Certain data elements are particularly sensitive and may alone present an increased risk of harm to the individual.

(i) Examples of stand-alone PII that are particularly sensitive include: Social Security numbers (SSNs), driver's license or State identification numbers, Alien Registration Numbers (A-numbers), financial account numbers, and biometric identifiers.

(ii) Multiple pieces of information may present an increased risk of harm to the individual when combined, posing an increased risk of harm to the individual. SPII may also consist of any grouping of information that contains an individual's name or other unique identifier plus one or more of the following elements:

(A) Truncated SSN (such as last 4 digits);
(B) Date of birth (month, day, and year);
(C) Citizenship or immigration status;
(D) Ethnic or religious affiliation;
(E) Sexual orientation;
(F) Criminal history;
(G) Medical information; and
(H) System authentication information, such as mother's birth name, account passwords, or personal identification numbers (PINs).

(iii) Other PII that may present an increased risk of harm to the individual depending on its context, such as a list of employees and their performance ratings or an unlisted home address or phone number. The context includes the purpose for which the PII was collected, maintained, and used. This assessment is critical because the same information in different contexts can reveal additional information about the impacted individual.

Federal information means information created, collected, processed, maintained, disseminated, disclosed, or disposed of by or for the Federal Government, in any medium or form.

Federal information system means an information system used or operated by an agency or by a Contractor of an agency or by another organization on behalf of an agency.

Handling means any use of controlled unclassified information, including but not limited to marking, safeguarding, transporting, disseminating, re-using, storing, capturing, and disposing of the information.

Incident means an occurrence that—

(1) Actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or

(2) Constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies.

Information Resources means information and related resources, such as personnel, equipment, funds, and information technology.
Information Security means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide—

(1) Integrity, which means guarding against improper information modification or destruction, and includes ensuring information nonrepudiation and authenticity;

(2) Confidentiality, which means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; and

(3) Availability, which means ensuring timely and reliable access to and use of information.

Information System means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

(b) *Handling of Controlled Unclassified Information.*

(1) Contractors and subcontractors must provide adequate security to protect CUI from unauthorized access and disclosure. Adequate security includes compliance with DHS policies and procedures in effect at the time of contract award. These policies and procedures are accessible at https://www.dhs.gov/dhs-security-and-training-requirements-contractors.

(2) The Contractor shall not use or redistribute any CUI handled, collected, processed, stored, or transmitted by the Contractor except as specified in the contract.

(3) The Contractor shall not maintain SPII in its invoicing, billing, and other recordkeeping systems maintained to support financial or other administrative functions. It is acceptable to maintain in these systems the names, titles, and contact information for the Contracting Officer's Representative (COR) or other government personnel associated with the administration of the contract, as needed.

(4) Any government data provided, developed, or obtained under the contract, or otherwise under the control of the Contractor, shall not become part of the bankruptcy estate in the event a Contractor and/or subcontractor enters bankruptcy proceedings.

(c) *Incident Reporting Requirements.*

(1) Contractors and subcontractors shall report all known or suspected incidents to the Component Security Operations Center (SOC) in accordance with Attachment F, *Incident Response*, to DHS Policy Directive 4300A *Information Technology System Security Program, Sensitive Systems*. If the Component SOC is not available, the Contractor shall report to the DHS Enterprise SOC. Contact information for the DHS Enterprise SOC is accessible at https://www.dhs.gov/dhs-security-and-training-requirements-contractors. Subcontractors are required to notify the prime Contractor that it has reported a known or suspected incident to the Department. Lower tier subcontractors are required to likewise notify their higher tier

subcontractor, until the prime contractor is reached. The Contractor shall also notify the Contracting Officer and COR using the contact information identified in the contract. If the report is made by phone, or the email address for the Contracting Officer or COR is not immediately available, the Contractor shall contact the Contracting Officer and COR immediately after reporting to the Component or DHS Enterprise SOC.

(2) All known or suspected incidents involving PII or SPII shall be reported within 1 hour of discovery. All other incidents shall be reported within 8 hours of discovery.

(3) CUI transmitted via email shall be protected by encryption or transmitted within secure communications systems. CUI shall be transmitted using a *FIPS 140-2/140-3 Security Requirements for Cryptographic Modules* validated cryptographic module identified on https://csrc.nist.gov/projects/cryptographic-module-validation-program/validated-modules. When this is impractical or unavailable, for Federal information systems only, CUI may be transmitted over regular email channels. When using regular email channels, Contractors and subcontractors shall not include any CUI in the subject or body of any email. The CUI shall be included as a password-protected attachment with the password provided under separate cover, including as a separate email. Recipients of CUI information will comply with any email restrictions imposed by the originator.

(4) An incident shall not, by itself, be interpreted as evidence that the Contractor or Subcontractor has failed to provide adequate information security safeguards for CUI or has otherwise failed to meet the requirements of the contract.

(5) If an incident involves PII or SPII, in addition to the incident reporting guidelines in Attachment F, *Incident Response*, to DHS Policy Directive 4300A *Information Technology System Security Program, Sensitive Systems*, Contractors shall also provide as many of the following data elements that are available at the time the incident is reported, with any remaining data elements provided within 24 hours of submission of the initial incident report:

(i) Unique Entity Identifier (UEI);
(ii) Contract numbers affected unless all contracts by the company are affected;
(iii) Facility CAGE code if the location of the event is different than the prime Contractor location;
(iv) Point of contact (POC) if different than the POC recorded in the System for Award Management (address, position, telephone, and email);
(v) Contracting Officer POC (address, telephone, and email);
(vii) Name of subcontractor and CAGE code if this was an incident on a subcontractor network;
(viii) Government programs, platforms, or systems involved;
(ix) Location(s) of incident;
(x) Date and time the incident was discovered;
(xi) Server names where CUI resided at the time of the incident, both at the Contractor and subcontractor level;
(xii) Description of the government PII or SPII contained within the system; and
(xiii) Any additional information relevant to the incident.

(d) *Incident Response Requirements.*

(1) All determinations by the Department related to incidents, including response activities, will be made in writing by the Contracting Officer.

(2) 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 incidents.

(3) Incident response activities determined to be required by the Government may include, but are not limited to, the following:

(i) Inspections;
(ii) Investigations;
(iii) Forensic reviews;
(iv) Data analyses and processing; and
(v) Revocation of the Authority to Operate (ATO), if applicable.

(4) The Contractor shall immediately preserve and protect images of known affected information systems and all available monitoring/packet capture data. The monitoring/packet capture data shall be retained for at least 180 days from submission of the incident report to allow DHS to request the media or decline interest.

(5) The Government, at its sole discretion, may obtain assistance from other Federal agencies and/or third-party firms to aid in incident response activities.

(e) *Certificate of Sanitization of Government and Government-Activity-Related Files and Information.* Upon the conclusion of the contract by expiration, termination, cancellation, or as otherwise indicated in the contract, the Contractor shall return all CUI to DHS and/or destroy it physically and/or logically as identified in the contract unless the contract states that return and/or destruction of CUI is not required. Destruction shall conform to the guidelines for media sanitization contained in NIST SP 800–88, *Guidelines for Media Sanitization*. The Contractor shall certify and confirm the sanitization of all government and government-activity related files and information. The Contractor shall submit the certification to the COR and Contracting Officer following the template provided in NIST SP 800–88, *Guidelines for Media Sanitization*, Appendix G.

(f) *Other Reporting Requirements.* Incident reporting required by this clause in no way rescinds the Contractor's responsibility for other incident reporting pertaining to its unclassified information systems under other clauses that may apply to its contract(s), or as a result of other applicable statutory or regulatory requirements, or other U.S. Government requirements.

(g) *Subcontracts.* The Contractor shall insert this clause in all subcontracts and require subcontractors to include this clause in all lower tier subcontracts when subcontractor employees will have access to CUI; CUI will be collected or maintained on behalf of the agency by a subcontractor; or a subcontractor information system(s) will be used to process, store, or transmit CUI.

(End of clause)

ALTERNATE I (JULY 2023)

When Federal information systems, which include Contractor information systems operated on behalf of the agency, are used to collect, process, store, or transmit CUI, add the following paragraphs:

(h) *Authority to Operate*. The Contractor shall not collect, process, store, or transmit CUI within a Federal information system until an ATO has been granted by the Component or Headquarters CIO, or designee. Once the ATO has been granted by the Government, the Contracting Officer shall incorporate the ATO into the contract as a compliance document. Unless otherwise specified in the ATO letter, the ATO is valid for 3 years. An ATO is granted at the sole discretion of the Government and can be revoked at any time. Contractor receipt of an ATO does not create any contractual right of access or entitlement. The Government's grant of an ATO does not alleviate the Contractor's responsibility to ensure the information system controls are implemented and operating effectively.

(1) *Complete the Security Authorization process.* The Security Authorization (SA) process shall proceed according to DHS Policy Directive 4300A *Information Technology System Security Program, Sensitive*

Systems (Version 13.3, February 13, 2023), or any successor publication; and the *Security Authorization Process Guide*, including templates. These policies and templates are accessible at https://www.dhs.gov/dhs-security-and-training-requirements-contractors.

(i) *Security Authorization Package.* The SA package shall be developed using the government-provided Security Requirements Traceability Matrix and SA templates. The SA package consists of the following: Security Plan, Contingency Plan, Contingency Plan Test Results, Configuration Management Plan, Security Assessment Plan, Security Assessment Report, and Authorization to Operate Letter. Additional documents that may be required include a Plan(s) of Action and Milestones and Interconnection Security Agreement(s). The Contractor shall submit a signed copy of the SA package, validated by an independent third party, to the COR for review and approval by the Component or Headquarters CIO, or designee, at least 30 days prior to the date of operation of the information system. The Government is the final authority on the compliance of the SA package and may limit the number of resubmissions of modified documents.

(ii) *Independent Assessment.* Contractors shall have an independent third party validate the security and privacy controls in place for the information system(s). The independent third party shall review and analyze the SA package, and report on technical, operational, and management level deficiencies as outlined in NIST SP 800–53, *Security and Privacy Controls for Information Systems and Organizations*, or successor publication, accessible at *https://csrc.nist.gov/publications/sp.* The Contractor shall address all deficiencies before submitting the SA package to the COR for review.

(2) *Renewal of ATO.* Unless otherwise specified in the ATO letter, the Contractor shall renew the ATO every 3 years. The Contractor is required to update its SA package as part of the ATO renewal process for review and verification of security controls. Review and verification of security controls is independent of the system production date and may include onsite visits that involve physical or logical inspection of the Contractor environment to ensure controls are in place. The updated SA package shall be submitted for review and approval by the Component or Headquarters CIO, or designee, at least 90 days before the ATO expiration date. The Contractor shall update its SA package by one of the following methods:

(i) Updating the SA package in the DHS Information Assurance Compliance System; or
(ii) Submitting the updated SA package directly to the COR.

(3) *Security Review.* The Government may elect to conduct periodic reviews to ensure that the security requirements contained in the contract are being implemented and enforced. The Government, at its sole discretion, may obtain assistance from other Federal agencies and/or third-party firms to aid in security review activities. The Contractor shall afford DHS, the Office of the Inspector General, other government organizations, and Contractors working in support of the Government access to the Contractor's facilities, installations, operations, documentation, databases, networks, systems, and personnel used in the performance of this contract. The Contractor shall, through the Contracting Officer and COR, contact the Component or Headquarters CIO, or designee, to coordinate and participate in review and inspection activity by government organizations external to DHS. Access shall be provided, to the extent necessary as determined by the Government (including providing all requested images), for the Government to carry out a program of inspection, investigation, and audit to safeguard against threats and hazards to the integrity, availability, and confidentiality of government data or the function of computer systems used in performance of this contract and to preserve evidence of computer crime.

(4)*Federal Reporting and Continuous Monitoring Requirements.* Contractors operating information systems on behalf of the Government shall comply with Federal reporting and information system continuous monitoring requirements. Reporting requirements are determined by the Government and are defined in the Fiscal Year 2015 DHS Information Security Performance Plan, or successor publication, accessible at https://www.dhs.gov/dhs-security-and-training-requirements-contractors. The plan is updated on an annual

basis. Annual, quarterly, and monthly data collection will be coordinated by the Government. The Contractor shall provide the Government with all information to fully satisfy Federal reporting requirements for information systems. The Contractor shall provide the COR with requested information within 3 business days of receipt of the request. Unless otherwise specified in the contract, monthly continuous monitoring data shall be stored at the Contractor's location for a period not less than 1 year from the date the data are created. The Government may elect to perform information system continuous monitoring and IT security scanning of information systems from government tools and infrastructure.

(End of clause)

6.0 INFORMATION TECHNOLOGY SECURITY AND PRIVACY TRAINING (MAR 2015)

(a) Applicability. This clause applies to the Contractor, its subcontractors, and Contractor employees (hereafter referred to collectively as "Contractor"). The Contractor shall insert the substance of this clause in all subcontracts.

(b) Security Training Requirements.

(1) All users of Federal information systems are required by Title 5, Code of Federal Regulations, Part 930.301, Subpart C, as amended, to be exposed to security awareness materials annually or whenever system security changes occur, or when the user's responsibilities change. The Department of Homeland Security (DHS) requires that Contractor employees take an annual Information Technology Security Awareness Training course before accessing sensitive information under the contract. Unless otherwise specified, the training shall be completed within thirty (30) days of contract award and be completed on an annual basis thereafter not later than October 31st of each year. Any new Contractor employees assigned to the contract shall complete the training before accessing sensitive information under the contract. The training is accessible at http://www.dhs.gov/dhs-security-and-training-requirements-contractors. The Contractor shall maintain copies of training certificates for all Contractor and subcontractor employees as a record of compliance. Unless otherwise specified, initial training certificates for each Contractor and subcontractor employee shall be provided to the Contracting Officer's Representative (COR) not later than thirty (30) days after contract award. Subsequent training certificates to satisfy the annual training requirement shall be submitted to the COR via e-mail notification not later than October 31st of each year. The e-mail notification shall state the required training has been completed for all Contractor and subcontractor employees.

(2) The DHS Rules of Behavior apply to every DHS employee, Contractor and subcontractor that will have access to DHS systems and sensitive information. The DHS Rules of Behavior shall be signed before accessing DHS systems and sensitive information. The DHS Rules of Behavior is a document that informs users of their responsibilities when accessing DHS systems and holds users accountable for actions taken while accessing DHS systems and using DHS Information Technology resources capable of inputting, storing, processing, outputting, and/or transmitting sensitive information. The DHS Rules of Behavior is accessible at http://www.dhs.gov/dhs-

security-and-training-requirements-contractors. Unless otherwise specified, the DHS Rules of Behavior shall be signed within thirty (30) days of contract award. Any new Contractor employees assigned to the contract shall also sign the DHS Rules of Behavior before accessing DHS systems and sensitive information. The Contractor shall maintain signed copies of the DHS Rules of Behavior for all Contractor and subcontractor employees as a record of compliance. Unless otherwise specified, the Contractor shall e-mail copies of the signed DHS Rules of Behavior to the COR not later than thirty (30) days after contract award for each employee. The DHS Rules of Behavior will be reviewed annually, and the COR will provide notification when a review is required.

(c) Privacy Training Requirements. All Contractor and subcontractor employees that will have access to Personally Identifiable Information (PII) and/or Sensitive PII (SPII) are required to take Privacy at DHS: Protecting Personal Information before accessing PII and/or SPII. The training is accessible at http://www.dhs.gov/dhs-security-and-training-requirements-contractors.

Training shall be completed within thirty (30) days of contract award and be completed on an annual basis thereafter not later than October 31st of each year. Any new Contractor employees assigned to the contract shall also complete the training before accessing PII and/or SPII. The Contractor shall maintain copies of training certificates for all Contractor and subcontractor employees as a record of compliance. Initial training certificates for each Contractor and subcontractor employee shall be provided to the COR not later than thirty (30) days after contract award. Subsequent training certificates to satisfy the annual training requirement shall be submitted to the COR via e-mail notification not later than October 31st of each year. The email notification shall state the required training has been completed for all Contractor and subcontractor employees. (End of Clause)

7.0 GOVERNMENT FURNSHED RESOURCES

The Contractor shall use government furnished information, data, and documents only for the performance of work under this BPA call. It is the Contractor's responsibility to return all government furnished information and data and documents to the Government at the end of the performance period. The Contractor shall not release government furnished information and data and documents to outside parties without the prior and explicit consent of the Contracting Officer.

8.0 GOVERNMENT FURNISHED PROPERTY

The Government will provide the workspace, computer workstations, cubicles, access to duplicating machines, miscellaneous office supplies, and phones necessary to perform the on-site portion of Contractor services required in this BPA call, unless specifically stated otherwise in this work statement. The phones shall be used for work purposes only or for emergency calls. The Contractor shall use government furnished facilities, property, equipment and supplies only for the performance of work under this BPA call and shall be responsible for returning all government furnished facilities, property, and equipment in good working condition, subject to normal wear and tear. The Government will provide all necessary information and data and documents to the Contractor for work required under this BPA call.

9.0 ORGANIZATIONAL CONFLICT OF INTEREST NOTICE

The Contractor shall be aware that the type of work required by this BPA call may give rise to an Organizational Conflict of Interest (OCI) that may restrict the Contractor's ability to compete for follow-on work. These types of OCI do not generally lend themselves to successful mitigation (see FAR 9.5, Organizational and Consultant Conflicts of Interest). The Contractor shall carefully examine and comply with HSAR 3052.209-73, Limitation of Future Contracting, found in Section VII of this Request for Quotation. A Contractor's eligibility or ineligibility to participate in a future acquisition is determined by the Contracting Officer.

10.0 OPERATIONS DURING EMERGENCY SITUATIONS

10.1 Emergencies and Special Events

The contractor shall respond to emergencies as governed by procedures prescribed by the DHS in accordance with its applicable statutes, regulations, orders, policies, and guidelines. The DHS may have the need to extend contractor tour of duties, hours, and bringing on additional cleared contractor personnel in the event of a major emergency. The contractor shall provide surge personnel support, as directed by the COR or CO, in response to emergencies or special events. Emergencies may consist of natural disasters, terrorist threats or events, elevation of the DHS threat level or as designated by the Department. In the event of any emergency, the CO may initiate contractor action by a verbal authorization.

10.2 Extreme Weather Conditions

Extreme weather conditions and natural disasters (such as tornados, flooding, snow, and ice) may warrant temporary office evacuation or office closure. The contractor shall respond to extreme weather conditions according to DHS direction and shall inform all employees of these instructions. During normal duty hours, the normal chain of management will provide notification of facility closures. During non-duty hours, local radio and television channels will provide notification. Facility closings shall in no way interfere with the contractor operation and maintenance of the critical systems. All contractor employees identified as essential personnel shall remain on duty or report for duty in accordance with the Emergency Situations and relevant Continuity of Operations (COOP), IT Contingency, IT Disaster Recovery/Business Continuity Plan.

10.3 Business Continuity Plan

The Contractor shall prepare and submit a Business Continuity Plan (BCP) to the Government. The BCP Plan shall be due 10 business days after the date of award and will be updated on an annual basis. The BCP shall document Contractor plans and procedures to maintain support during an emergency, including natural disasters and acts of terrorism. The BCP, at a minimum, shall include the following:

- A description of the Contractor's emergency management procedures and policy;
- A description of how the Contractor will account for their employees during an emergency;
- How the Contractor will communicate with the Government during emergencies; and

- A list of primary and alternate Contractor points of contact, each with:
- Telephone numbers
- E-mail addresses

10.3.1 Individual BCPs shall be activated immediately after determining that an emergency has occurred, shall be operational within 12 hours of activation or as directed by the Government, and shall be sustainable until the emergency situation is resolved and normal conditions are restored or the contract is terminated, whichever comes first. In case of a life-threatening emergency, the COR shall immediately make contact with the Contractor Project Manager to ascertain the status of any Contractor personnel who were located in Government controlled space affected by the emergency. When any disruption of normal, daily operations occurs, the Contractor Project Manager and the COR shall promptly open an effective means of communication and verify:

- Key points of contact (Government and Contractor)
- Temporary work locations (alternate office spaces, telework, virtual offices, etc.)
- Means of communication available under the circumstances (e.g. email, webmail, telephone, FAX, courier, etc.)
- Essential Contractor work products expected to be continued, by priority

10.3.2 The Government and the designated Project Manager shall make use of the resources and tools available to continue contracted functions to the maximum extent possible under emergency circumstances. Contractors shall obtain approval from the Contracting Officer prior to incurring costs over and above those costs allowed for under the terms of this contract. Regardless of contract type, and of work location, Contractors performing work in support of authorized tasks within the scope of their contract shall charge those hours accurately in accordance with the terms of this BPA Call.

End of Section VI [Remainder of Page Blank]

– Validation and Modeling Support

SECTION VII – BPA CALL CLAUSES

BPA AND GSA SCHEDULE CLAUSES

The Contractor's AICSS BPA clauses and GSA Schedule contract clauses are incorporated into this BPA call.

BPA CLAUSES

The Contractor shall note that the term "contract" as used in the FAR clauses below is synonymous with "BPA Call."

52.252-2 Clauses Incorporated by Reference (Feb 1998)

The contract incorporates one or more clauses by reference with the same force and effect as if they were given in full text in accordance with the Federal Acquisition Regulation (FAR) Clause 52.252-2, "CLAUSES INCORPORATED BY REFERENCE." Upon request, the Contracting Officer will make their full text available. Also, the full text of a clause may be accessed electronically at this address: **HTTP://ACQUISITION.GOV/FAR/** or for DHS specific clauses at **HTTP://FARSITE.HILL.AF.MIL/VMHSARA.HTM**

Clause	Title	Date
FAR Clauses Incorporated by Reference		
52.203-5	Covenant Against Contingent Fees	May 2014
52.203-16	Preventing Personal Conflicts of Interest	Jun 2020
52.203-17	Contractor Employee Whistleblower Rights and Requirement To Inform Employees of Whistleblower Rights	Apr 2014
52.204-2	Security Requirements	Aug 1996
52.204-9	Personal Identity Verification of Contractor Personnel	Jan 2011
52.204-25	Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment	Aug 2020
52.209-10	Prohibition on Contracting with Inverted Domestic Corporations	Nov 2015
52.222-50	Combating Trafficking in Persons	Mar 2015
52.224-1	Privacy Act Notification	Apr 1984
52.224-2	Privacy Act	Apr 1984
52.224-3	Privacy Training – Alternate I (DEVIATION 17-03)	Jul 2023
52.227-14	Rights in Data – General	Jun 1987
52.232-1	Payments	Apr 1984
52.232-39	Unenforceability of Unauthorized Obligations	Jun 2013
52.243-3	Changes-Time-and-Materials or Labor-Hour	Sep 2000
HSAR Clauses Incorporated by Reference		
30521.205-70	Advertisements, Publicizing Awards and Releases	Sept 2012

– Validation and Modeling Support

3052.242-72	Contracting Officer's Technical Representative	Dec 2003
3052.204-71	Contractor Employee Access	July 2023
3052.204-72	Safeguarding of Controlled Unclassified Information	July 2023
3052.204-73	Notification and Credit Monitoring Requirements for Personally Identifiable Information Incidents	July 2023
Class Deviation 15-01, Revision 1 – Special Clause	Information Technology Security Awareness Training	July 2023

FAR AND HSAR CLAUSES INCORPORATED BY FULL TEXT

FAR Clauses:

FAR 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 30 days of contract period expiration. (End of clause)

FAR 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 1 calendar day; 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 30 months. (End of clause)

FAR 52.224-3 Privacy Training – Alternate I (DEVIATION 17-03) (July 2023)

(a) *Definition.* As used in this clause, 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. (See Office of Management and Budget (OMB) Circular A–130, Managing Federal Information as a Strategic Resource).

(b) The Contractor shall ensure that initial privacy training, and annual privacy training, thereafter, is completed by contractor employees who—

(1) Have access to a system of records;

(2) Create, collect, use, process, store, maintain, disseminate, disclose, dispose, or otherwise handle personally identifiable information on behalf of an agency; or

– Validation and Modeling Support

(3) Design, develop, maintain, or operate a system of records (see also FAR subpart 24.1 and 39.105).

(c) The contracting agency will provide initial privacy training, and annual privacy training thereafter, to Contractor employees for the duration of this contract. Contractor employees shall satisfy this requirement by completing *Privacy at DHS: Protecting Personal Information* accessible at *http://www.dhs.gov/dhs-security-and-training-requirements-contractors.* Training shall be completed within 30 days of contract award and be completed on an annual basis thereafter not later than October 31st of each year.

(d) The Contractor shall maintain and, upon request, provide documentation of completion of privacy training to the Contracting Officer.

(e) The Contractor shall not allow any employee access to a system of records, or permit any employee to create, collect, use, process, store, maintain, disseminate, disclose, dispose or otherwise handle personally identifiable information, or to design, develop, maintain, or operate a system of records unless the employee has completed privacy training, as required by this clause.

(f) The substance of this clause, including this paragraph (f), shall be included in all subcontracts under this contract, when subcontractor employees will—

(1) Have access to a system of records;

(2) Create, collect, use, process, store, maintain, disseminate, disclose, dispose, or otherwise handle personally identifiable information; or

(3) Design, develop, maintain, or operate a system of records.

(End of clause)

HOMELAND SECURITY ACQUISITION REGULATION (HSAR) CLAUSES

HSAR 3052.215-70 Key Personnel or Facilities (Dec 2003)

(a) The personnel or facilities specified below are considered essential to the work being performed under this contract and may, with the consent of the contracting parties, be changed from time to time during the course of the contract by adding or deleting personnel or facilities, as appropriate.

(b) Before removing or replacing any of the specified individuals or facilities, the Contractor shall notify the Contracting Officer, in writing, before the change becomes effective. The Contractor shall submit sufficient information to support the proposed action and to enable the Contracting Officer to evaluate the potential impact of the change on this contract. The Contractor shall not remove or replace personnel or facilities until the Contracting Officer approves the change.

The Key Personnel or Facilities under this Contract: Manager/Project Manager (End of Clause)

HSAR 3052.204-71 Contractor Employee Access (July 2023)

(a) Controlled Unclassified Information (CUI) is any information the Government creates or possesses, or an entity creates or possesses for or on behalf of the Government (other than classified information) that a law, regulation, or Governmentwide policy requires or permits an agency to handle using safeguarding or dissemination controls. This definition includes the following CUI categories and subcategories of information:

– Validation and Modeling Support

(1) Chemical-terrorism Vulnerability Information (CVI) as defined in 6 CFR part 27, "Chemical Facility Anti-Terrorism Standards," and as further described in supplementary guidance issued by an authorized official of the Department of Homeland Security (including the Revised Procedural Manual "Safeguarding Information Designated as Chemical-Terrorism Vulnerability Information" dated September 2008);

(2) Protected Critical Infrastructure Information (PCII) as set out in the Critical Infrastructure Information Act of 2002 (title XXII, subtitle B of the Homeland Security Act of 2002 as amended through Pub. L. 116–283), PCII's implementing regulations (6 CFR part 29), the PCII Program Procedures Manual, and any supplementary guidance officially communicated by an authorized official of the Department of Homeland Security, the PCII Program Manager, or a PCII Program Manager Designee;

(3) Sensitive Security Information (SSI) as defined in 49 CFR part 1520, "Protection of Sensitive Security Information," as amended, and any supplementary guidance officially communicated by an authorized official of the Department of Homeland Security (including the Assistant Secretary for the Transportation Security Administration or designee), including Department of Homeland Security MD 11056.1, "Sensitive Security Information (SSI)" and, within the Transportation Security Administration, TSA MD 2810.1, "SSI Program";

(4) Homeland Security Agreement Information means information the Department of Homeland Security receives pursuant to an agreement with State, local, Tribal, territorial, or private sector partners that is required to be protected by that agreement. The Department receives this information in furtherance of the missions of the Department, including, but not limited to, support of the Fusion Center Initiative and activities for cyber information sharing consistent with the Cybersecurity Information Sharing Act of 2015;

(5) Homeland Security Enforcement Information means unclassified information of a sensitive nature lawfully created, possessed, or transmitted by the Department of Homeland Security in furtherance of its immigration, customs, and other civil and criminal enforcement missions, the unauthorized disclosure of which could adversely impact the mission of the Department;

(6) International Agreement Information means information the Department of Homeland Security receives that is required to be protected by an information sharing agreement or arrangement with a foreign government, an international organization of governments or any element thereof, an international or foreign public or judicial body, or an international or foreign private or non-governmental organization;

(7) Information Systems Vulnerability Information (ISVI) means:

(i) Department of Homeland Security information technology (IT) systems data revealing infrastructure used for servers, desktops, and networks; applications name, version, and release; switching, router, and gateway information; interconnections and access methods; and mission or business use/need. Examples of ISVI are systems inventories and enterprise architecture models. Information pertaining to national security systems and eligible for classification under Executive Order 13526 will be classified as appropriate; and/or

(ii) Information regarding developing or current technology, the release of which could hinder the objectives of the Department, compromise a technological advantage or

– Validation and Modeling Support
countermeasure, cause a denial of service, or provide an adversary with sufficient information to clone, counterfeit, or circumvent a process or system;

(8) Operations Security Information means Department of Homeland Security information that could be collected, analyzed, and exploited by a foreign adversary to identify intentions, capabilities, operations, and vulnerabilities that threaten operational security for the missions of the Department;

(9) Personnel Security Information means information that could result in physical risk to Department of Homeland Security personnel or other individuals whom the Department is responsible for protecting;

(10) Physical Security Information means reviews or reports illustrating or disclosing facility infrastructure or security vulnerabilities related to the protection of Federal buildings, grounds, or property. For example, threat assessments, system security plans, contingency plans, risk management plans, business impact analysis studies, and certification and accreditation documentation;

(11) Privacy Information includes both Personally Identifiable Information (PII) and Sensitive Personally Identifiable Information (SPII). PII refers to 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; and SPII is a subset of PII that if lost, compromised, or disclosed without authorization could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. To determine whether information is PII, DHS will perform an assessment of the specific risk that an individual can be identified using the information with other information that is linked or linkable to the individual. In performing this assessment, it is important to recognize that information that is not PII can become PII whenever additional information becomes available, in any medium or from any source, that would make it possible to identify an individual. Certain data elements are particularly sensitive and may alone present an increased risk of harm to the individual.

(i) Examples of stand-alone PII that are particularly sensitive include: Social Security numbers (SSNs), driver's license or State identification numbers, Alien Registration Numbers (A-numbers), financial account numbers, and biometric identifiers.

(ii) Multiple pieces of information may present an increased risk of harm to the individual when combined, posing an increased risk of harm to the individual. SPII may also consist of any grouping of information that contains an individual's name or other unique identifier plus one or more of the following elements:

(A) Truncated SSN (such as last 4 digits);
(B) Date of birth (month, day, and year);
(C) Citizenship or immigration status;
(D) Ethnic or religious affiliation;
(E) Sexual orientation;
(F) Criminal history;
(G) Medical information; and
(H) System authentication information, such as mother's birth name, account passwords, or personal identification numbers (PINs).

– Validation and Modeling Support

(iii) Other PII that may present an increased risk of harm to the individual depending on its context, such as a list of employees and their performance ratings or an unlisted home address or phone number. The context includes the purpose for which the PII was collected, maintained, and used. This assessment is critical because the same information in different contexts can reveal additional information about the impacted individual.

(b) Information Resources means information and related resources, such as personnel, equipment, funds, and information technology.

(c) Contractor employees working on this contract must complete such forms as may be necessary for security or other reasons, including the conduct of background investigations to determine suitability. Completed forms shall be submitted as directed by the Contracting Officer. Upon the Contracting Officer's request, the Contractor's employees shall be fingerprinted or subject to other investigations as required. All Contractor employees requiring recurring access to government facilities or access to CUI or information resources are required to have a favorably adjudicated background investigation prior to commencing work on this contract unless this requirement is waived under Departmental procedures.

(d) The Contracting Officer may require the Contractor to prohibit individuals from working on the contract if the Government deems their initial or continued employment contrary to the public interest for any reason, including, but not limited to, carelessness, insubordination, incompetence, or security concerns.

(e) Work under this contract may involve access to CUI. The Contractor shall access and use CUI only for the purpose of furnishing advice or assistance directly to the Government in support of the Government's activities, and shall not disclose, orally or in writing, CUI for any other purpose to any person unless authorized in writing by the Contracting Officer. For those Contractor employees authorized to access CUI, the Contractor shall ensure that these persons receive initial and refresher training concerning the protection and disclosure of CUI. Initial training shall be completed within 60 days of contract award and refresher training shall be completed every 2 years thereafter.

(f) The Contractor shall include this clause in all subcontracts at any tier where the subcontractor may have access to government facilities, CUI, or information resources.

(End of clause)

HSAR 3052.204-73 Notification and Credit Monitoring Requirements for Personally Identifiable Information Incidents (July 2023)

(a) *Definitions.* Privacy Information includes both Personally Identifiable Information (PII) and Sensitive Personally Identifiable Information (SPII). PII refers to 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; and SPII is a subset of PII that if lost, compromised, or disclosed without authorization could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. To determine whether information is PII, the DHS will perform an assessment of the specific risk that an individual can be identified using the information with other information that is linked or linkable to the individual. In performing this assessment, it is important to recognize that information that is not PII can become PII whenever additional information becomes available, in any medium or from any source, that would make it possible to identify an individual. Certain data elements are particularly sensitive
and may alone present an increased risk of harm to the individual.

– Validation and Modeling Support

(1) Examples of stand-alone PII that are particularly sensitive include: Social Security numbers (SSNs), driver's license or State identification numbers, Alien Registration Numbers (A-numbers), financial account numbers, and biometric identifiers.

(2) Multiple pieces of information may present an increased risk of harm to the individual when combined, posing an increased risk of harm to the individual. SPII may also consist of any grouping of information that contains an individual's name or other unique identifier plus one or more of the following elements:

(i) Truncated SSN (such as last 4 digits);
(ii) Date of birth (month, day, and year);
(iii) Citizenship or immigration status;
(iv) Ethnic or religious affiliation;
(v) Sexual orientation;
(vi) Criminal history;
(vii) Medical information; and
(viii) System authentication information, such as mother's birth name, account passwords, or personal identification numbers (PINs).

(3) Other PII that may present an increased risk of harm to the individual depending on its context, such as a list of employees and their performance ratings or an unlisted home address or phone number. The context includes the purpose for which the PII was collected, maintained, and used. This assessment is critical because the same information in different contexts can reveal additional information about the impacted individual.

(b) *PII and SPII Notification Requirements.*

(1) No later than 5 business days after being directed by the Contracting Officer, or as otherwise required by applicable law, the Contractor shall notify any individual whose PII or SPII was either under the control of the Contractor or resided in an information system under control of the Contractor at the time the incident occurred. The method and content of any notification by the Contractor shall be coordinated with, and subject to prior written approval by, the Contracting Officer. The Contractor shall not proceed with notification unless directed in writing by the Contracting Officer.

(2) All determinations by the Department related to notifications to affected individuals and/or Federal agencies and related services (e.g., credit monitoring) will be made in writing by the Contracting Officer.

(3) Subject to government analysis of the incident and direction to the Contractor regarding any resulting notification, the notification method may consist of letters to affected individuals sent by first-class mail, electronic means, or general public notice, as approved by the Government. Notification may require the Contractor's use of address verification and/or address location services. At a minimum, the notification shall include:

(i) A brief description of the incident;
(ii) A description of the types of PII or SPII involved;
(iii) A statement as to whether the PII or SPII was encrypted or protected by other means;
(iv) Steps individuals may take to protect themselves;

– Validation and Modeling Support

(v) What the Contractor and/or the Government are doing to investigate the incident, mitigate the incident, and protect against any future incidents; and

(vi) Information identifying who individuals may contact for additional information.

(c) *Credit Monitoring Requirements.* The Contracting Officer may direct the Contractor to:

(1) Provide notification to affected individuals as described in paragraph (b).

(2) Provide credit monitoring services to individuals whose PII or SPII was under the control of the Contractor or resided in the information system at the time of the incident for a period beginning the date of the incident and extending not less than 18 months from the date the individual is notified. Credit monitoring services shall be provided from a company with which the Contractor has no affiliation. At a minimum, credit monitoring services shall include:

(i) Triple credit bureau monitoring;

(ii) Daily customer service;

(iii) Alerts provided to the individual for changes and fraud; and

(iv) Assistance to the individual with enrollment in the services and the use of fraud alerts.

(3) Establish a dedicated call center. Call center services shall include:

(i) A dedicated telephone number to contact customer service within a fixed period;

(ii) Information necessary for registrants/enrollees to access credit reports and credit scores;

(iii) Weekly reports on call center volume, issue escalation (i.e., those calls that cannot be handled by call center staff and must be resolved by call center management or DHS, as appropriate), and other key metrics;

(iv) Escalation of calls that cannot be handled by call center staff to call center management or DHS, as appropriate;

(v) Customized Frequently Asked Questions, approved in writing by the Contracting Officer in coordination with the Component or Headquarters Privacy Officer; and

(vi) Information for registrants to contact customer service representatives and fraud resolution representatives for credit monitoring assistance.

(End of clause)

– Validation and Modeling Support

HSAR 3052.209-73 Limitation of Future Contracting (Jun 2006) (Modified)

(a) The Contracting Officer has determined that this acquisition may give rise to a potential organizational conflict of interest. Accordingly, the attention of prospective offerors is invited to FAR Subpart 9.5--Organizational Conflicts of Interest.

(b) The nature of this conflict is the vendor is allowed access to Component staffing data and the staffing analysis of that data by the Acquisition Workforce Staffing Division (AWSD) of PARM, and access to the recommended number of full time equivalent staff needed to complete planned work. This information would bar the vendor from competing on any future procurement with DHS offices of which the vendor accessed program planning and budget information.

(c) Conflicts of interest are evaluated on a case-by-case for each task order under this BPA. If a conflict cannot be mitigated, then the anticipated restrictions on future contracting would be as follows:

(1) If the Contractor, under the terms of this contract, or through the performance of tasks pursuant to this contract, has access to DHS program planning and budgeting information, the Contractor shall be ineligible to perform the work described in solicitations resulting from acquisitions from those program plans and budgets as a prime or first tier-contractor. This restriction shall remain in effect for a reasonable time, as agreed to by the Contracting Officer and the Contractor, sufficient to avoid unfair competitive advantage or potential bias (this time shall in no case be less than the duration of the initial production contract).

(2) To the extent that the work under this contract requires access to proprietary, business confidential, or financial data of other companies, and as long as these data remain proprietary or confidential, the Contractor shall protect these data from unauthorized use and disclosure and agrees not to use them to compete with those other companies.

(3) Contractors will not be awarded call orders to conduct assessments of their own work or the work of their primes, subs, or teaming partners. (End of clause)

HSAR Class Deviation 15-01, Revision 1 (Special Clause) – Information Technology Security Awareness Training (July 2023)

(a) *Applicability.* This clause applies to the Contractor, its subcontractors, and Contractor employees (hereafter referred to collectively as "Contractor"). The Contractor shall insert the substance of this clause in all subcontracts.

(b) *Security Training Requirements*.

(1) All users of Federal information systems are required by Title 5, Code of Federal Regulations, Part 930.301, Subpart C, as amended, to be exposed to security awareness materials annually or whenever system security changes occur, or when the user's responsibilities change. The Department of Homeland Security (DHS) requires that Contractor employees take an annual Information Technology Security Awareness Training course before accessing sensitive information under the contract. Unless otherwise specified, the training shall be completed within

– Validation and Modeling Support

thirty (30) days of contract award and be completed on an annual basis thereafter not later than October 31st of each year. Any new Contractor employees assigned to the contract shall complete the training before accessing sensitive information under the contract. The training is accessible at http://www.dhs.gov/dhs-security-and-training-requirements-contractors. The Contractor shall maintain copies of training certificates for all Contractor and subcontractor employees as a record of compliance. Unless otherwise specified, initial training certificates for each Contractor and subcontractor employee shall be provided to the Contracting Officer's Representative (COR) not later than thirty (30) days after contract award. Subsequent training certificates to satisfy the annual training requirement shall be submitted to the COR via e-mail notification not later than October 31st of each year. The e-mail notification shall state the required training has been completed for all Contractor and subcontractor employees.

(2) The DHS Rules of Behavior apply to every DHS employee, Contractor and subcontractor that will have access to DHS systems and sensitive information. The DHS Rules of Behavior shall be signed before accessing DHS systems and sensitive information. The DHS Rules of Behavior is a document that informs users of their responsibilities when accessing DHS systems and holds users accountable for actions taken while accessing DHS systems and using DHS Information Technology resources capable of inputting, storing, processing, outputting, and/or transmitting sensitive information. The DHS Rules of Behavior is accessible at http://www.dhs.gov/dhs-security-and-training-requirements-contractors. Unless otherwise specified, the DHS Rules of Behavior shall be signed within thirty (30) days of contract award. Any new Contractor employees assigned to the contract shall also sign the DHS Rules of Behavior before accessing DHS systems and sensitive information. The Contractor shall maintain signed copies of the DHS Rules of Behavior for all Contractor and subcontractor employees as a record of compliance. Unless otherwise specified, the Contractor shall e-mail copies of the signed DHS Rules of Behavior to the COR not later than thirty (30) days after contract award for each employee. The DHS Rules of Behavior will be reviewed annually, and the COR will provide notification when a review is required.

(End of clause)

End of Section VII
[Remainder of Page Blank]

– Validation and Modeling Support

SECTION VIII - LIST OF DOCUMENTS, EXHIBITS AND OTHER ATTACHMENTS

Attachment #	Title	No. of pages
Attachment I	**Pricing Table**	2
Attachment II	**Non-Disclosure Agreement** DHS Form 11000-6 The Contractor awarded the BPA Call must complete the form at both the organizational level and the personnel level. All completed forms must be returned to the DHS COR with a copy sent to the Contacting Officer).	3
Attachment III	**Labor Category Descriptions and Qualifications**	3

End of Section VIII
[Remainder of Page Blank]