

FEDERALLY FUNDED RESEARCH AND DEVELOPMENT (FFRDC) TECHNICAL EXECUTION PLAN (TEP)

U.S. Department of Homeland Security

Title: Analytic Support to the Office of Immigration Statistics

**Component/Office: Office of Immigration Statistics
FFRDC: Homeland Security Operational Analysis Center (HSOAC)**

Version: 1.0

Date: June 28, 2022

1. Challenge

Immigration is a subject that continues to dominate the national discourse. The ability of the U.S. Government to implement an effective immigration strategy has been sometimes hampered by a lack of concerted analytic efforts, including collection and analysis of relevant data and information on all stages and aspects of the immigration process to inform policy decisions. Congress has funded a wide range of analytic and modeling initiatives across the Department of Homeland Security (DHS) components for years, including immigration related analytics. However, many of these efforts are confined to program offices and are not incorporated into internal DHS budget processes. This means they are not included in annual budget requests to Congress. Increasing and improving emphasis of immigration data analytics is necessary for both Congress and DHS to make better informed budget decisions.

2. Outcome(s)

The outcomes of this study include: (1) data- and evidence-based policy and resource decisions for the U.S. immigration system, (2) further maturing of the analytic capabilities of the DHS Office of Immigration Statistics (OIS), and (3) better coordination with other DHS Components whose mission sets include immigration administration, enforcement, and other equities.

3. Background

In the House of Representatives June 15, 2021 Report accompanying the FY 2022 DHS Appropriations bill, Congress recommended that DHS establish a Migration Analysis Center (MAC). The objective of the MAC is to create an interagency body that will conduct data and evidence-based modeling and analysis in order to inform policy and resource decisions

Page 1 of 28

Distribution is authorized to U.S. government agencies only. This document contains sensitive information exempt from mandatory disclosure under the Freedom of Information Act, 5 U.S.C. 552(b)(2). Do not release without prior approval of the Department of Homeland Security's Science and Technology Directorate.

impacted by the U.S. Immigration system. The MAC will aid DHS in developing annual and emergency budget submissions. Additionally, the MAC will serve to integrate policy analysis and data collection requirements across all relevant components and agencies, and objectively evaluate policies and programs that impact immigration. The House Report also suggests that the MAC utilize DHS OIS statistical immigration data systems of records to address deficiencies or weaknesses that may exist in current DHS immigration datasets, repositories, and databases.

In addition to DHS internal efforts, the House Report suggests that the MAC should include participation not only across the Department, but also with other agencies whose missions intersect with immigration-related policies and programs. Moreover, the MAC should engage with academia; state, local, tribal, and territorial communities; the private and non-profit sectors; and research communities to better understand migration-related issues. The MAC should also work to establish an independent peer-review process for its models and other work products to improve and strengthen their validity and utility for decision making. As referenced in the House Report, the MAC would be a primary customer of the modeling and analysis performed by DHS S&T and would require the support of DHS PA&E to improve the quality and utility of other existing models. Correspondingly, the MAC should have a broad focus with respect to migration analysis and, as such, these models would serve as a subset of the library of tools needed by the MAC to accomplish its mission. OIS's efforts related to the MAC cover a broad series of topics. Expertise is needed by OIS to respond to several current key challenges.

Additionally, Secretary Mayorkas signed a decision memo on September 6, 2022, supporting the expansion of OIS into the Office of Homeland Security Statistics (OHSS). These relatively recent and increased expectations for the statistical reporting work that OIS has traditionally done exceeds OIS's historical knowledge base and will require additional expertise that this HSOAC contract can provide in a timely manner while OIS develops expertise and implementation plans to expand to OHSS. Relatedly, OMB tasked OIS and Science and Technology to begin the stand up of an office for statistical reporting on domestic terrorism and targeted violence (DTTV) in fiscal year 2023.

4. Task Objective(s)

To assist DHS OIS in its efforts related to the MAC, HSOAC will deliver expertise on and analysis of immigration-related topics. This analysis will help OIS address a variety of analytic challenges and further strengthen OIS's ability provide data- and evidence-based decision-making tools and analyses to inform policy and resource decisions. HSOAC will provide analysis on potential racial bias in immigration enforcement as well as analysis on several other key issues (e.g., overstays, estimates of successful unlawful border crossings, improvements to existing population estimates) to improve OIS's analytic ability for future year needs.

5. Technical Approach / Analytic Methodology

HSOAC proposes the following two tasks to meet OIS's objectives for this effort.

5.1 Analysis of possible racial bias in immigration enforcement

HSOAC shall conduct a rigorous, objective analysis to explore whether there is evidence of differential treatment based on race in immigration enforcement, which might be due to possible racial bias. Such an analysis would examine whether non-citizens of different races are systematically treated differently at different points in the enforcement cycle, in ways that are unaccounted for by other known factors. This study will require the following:

- Agreement and coordination with OIS on the definition of racial bias and the relation of the research questions to that definition;
- access to all the relevant immigration enforcement data, and any data outside the immigration enforcement cycle, if needed;
- agreement with OIS on a method to impute or infer race, if race is not otherwise identified;
- agreement with OIS on which enforcement decisions to consider (e.g., bond, release, detention, etc.)

HSOAC will consider a range of statistical modeling approaches to identify differential treatment of individuals of different races and to take into account other factors that are expected to correlate with such treatment (for example, criminal history, nature of immigration violation, and so on). HSOAC will document its findings and methods in a brief report or white paper.

5.2 Research on Topics Identified by OIS

HSOAC and OIS will jointly determine pertinent immigration-related research topics that require in-depth analysis and expert support. The research topics may include, but are not limited to:

- Analysis of probability and length of nonimmigrant overstay
- Potential legal pathways as alternatives to unauthorized flows
- Analysis of push and pull factors (structural and short-term/acute) that underlie unauthorized migration
- Improvements to existing estimates of successful unlawful border crossings
- Critical review of OIS's regression-based encounter projections
- Improvements to existing population estimates, including adjustments to methodology necessitated by pandemic-related changes to the Census and migrant processing

OIS shall provide as much guidance and detail as possible about the topics of interest, as well as the type of analysis, review, or consultation that would be of greatest utility to accomplishing the task. When OIS determines a topic for analysis, review, or consultation, HSOAC will propose

Page 3 of 28

Distribution is authorized to U.S. government agencies only. This document contains sensitive information exempt from mandatory disclosure under the Freedom of Information Act, 5 U.S.C. 552(b)(2). Do not release without prior approval of the Department of Homeland Security's Science and Technology Directorate.

a research approach, timeline, and anticipated type of deliverable. HSOAC shall also assemble a team of researchers with domain expertise to begin research and provide consulting support, leveraging all pertinent skills, data, and tools. A research topic can be quantitative (e.g., modeling and simulation), qualitative (e.g., doctrine and policy), or hybrid. Once a research topic is determined, OIS shall provide all necessary information, including relevant documents, data, and codes. HSOAC will document each research topic, associated approach, deliverable, and projected deadline in the updated Project Management Plan (PMP).

The number of research topics that can be studied depends on the topics' level of complexity and available resources. HSOAC shall coordinate closely with OIS to determine the reasonable number of topics that can be studied within the period of performance.

The type of deliverables depends on the nature of the research topic and OIS's needs. Because of the dynamic nature of this analytic support to meet OIS's goals and objectives, deliverables may be in written form, in-line comments to existing documents/artifacts, or in oral form. The types of deliverables can include, but not limited to, the following, where the last type is *not* written:

- Reports – Within an agreed upon timeframe (to be set), HSOAC shall provide research reports addressing the topics of interest. The scope of these reports shall be agreed upon by OIS and HSOAC prior to initiation of the research.
- White papers – Within an agreed upon timeframe (to be set), HSOAC shall prepare white papers addressing the topics of interest. White papers are less elaborate than reports but generally would still include sufficient technical details. The length and the corresponding timeline of a white paper greatly depend on a topic's nature and complexity. White papers could include review and/or analysis of certain subjects. For a topic that is more complex or where a more in-depth analysis is desired by OIS, then the corresponding white paper shall be prepared on a longer, mutually agreeable timeframe and with more contents.
- Memoranda - Within an agreed upon timeframe (to be set), HSOAC shall provide a memorandum detailing the review, observations, recommendations, or other relevant response for a selected issue. Memoranda are less elaborate and shorter than white papers and typically do not involve original research.
- Policy/Guidance/Document Reviews – Within an agreed upon timeframe (to be set), HSOAC shall prepare written reviews, either through in-line comments in the document or an informal summary of a few pages, of existing or draft DHS policy, guidance, or other documents (e.g., technical descriptions of various modeling tools) of interest, determined in consultation with OIS. These reviews shall provide substantive feedback and/or recommendations.
- Briefings – Within an agreed upon timeframe (to be set), HSOAC shall provide briefings on the topics of interest, to summarize the results of the HSOAC team's research. For subjects that require analysis, the briefings generally would include problem statements, objectives, data, approaches, results, and caveats.

- Expert Discussion –HSOAC shall be available to attend formal or informal meetings or discussions for which OIS requires subject matter expertise and support. As part of the notice requirement, OIS shall provide an appropriate communication (e.g., email) concerning the topic of the meeting or discussion, and the type of input or contribution, if any, the HSOAC team is expected to provide. If necessary, HSOAC will provide a short, informal summary.

As previously mentioned, the decisions on research topics and the associated approaches, schedules, and deliverables shall be clearly documented in the study's PMP.

5.3 OHSS Organizational and Analytical Studies

HSOAC will support OIS's efforts to expand the office into an Office of Homeland Security Statistics (OHSS). The OHSS will be responsible for the Department's statistical data processing, data governance, and data quality; modeling and analysis; and reporting. HSOAC will assist OIS in expanding these functions to other Department data domains. The scope and maturity of the other data domains across the Department are not fully understood by OIS and HSOAC will assist with data calls and research to develop OIS knowledge about the other data domains. Additionally, HSOAC will assist OIS in developing a prioritization, timeline and staffing plan for the other data domains under OHSS.

5.4 Project Completion Memo

At the conclusion of the project, HSOAC will provide a projection completion memo to OIS listing the efforts and deliverables from throughout the year.

6. Key Words

Type of Work

Data-driven, integrated policy analysis; operations analysis; enforcement evaluation.

Benefit of Work

Evidence-based budget planning, equitable immigration enforcement.

Subject of Interest

Border and immigration, statistical analysis, data analytics, modeling and simulation.

7. Focus Area and Mission Alignment

Table 1 below aligns the percent of the total projected staff years of technical effort (STE) allocations to the IDIQ focus areas and DHS Quadrennial Homeland Security Review (QHSR) missions.

FFRDC proposed total STE:_____

DHS Management Directive 143-04, “Establishing or Contracting with FFRDCs and National Laboratories” defines a STE as 1,810 hours of paid effort for technical services.

Table 1: Focus Areas to the QHSR Mission Areas Relationship Matrix

At the intersection of the appropriate Focus Area row and QHSR Mission column, enter a percentage of the total STE.

HSOAC Focus Areas	Mission 1: Prevent Terrorism and Enhance Security	Mission 2: Secure and Manage Our Borders	Mission 3: Enforce and Administer Our Immigration Laws	Mission 4: Safeguard and Secure Cyberspace	Mission 5: Strengthen National Preparedness and Resilience	Mission 6: Maturing and Strengthening Homeland Security
1: Acquisition Studies	0%	0%	0%	0%	0%	0%
2: Preparedness, Response, and Recovery	0%	0%	0%	0%	0%	0%
3: Innovation and Technology Acceleration	0%	0%	0%	0%	0%	0%
4: Homeland Security Threat and Opportunity Studies	0%	0%	0%	0%	0%	0%
5: Personnel Policy and Management Studies	0%	0%	0%	0%	0%	0%
6: Operational Studies	0%	50%	0%	0%	0%	0%
7: Organizational Studies	0%	0%	0%	0%	0%	0%
8: Regulatory, Doctrine, and Policy Studies	0%	0%	0%	0%	0%	0%
9: Research and Development (R&D) Studies	0%	50%	0%	0%	0%	0%

8. Deliverables and Schedule

The FFRDC shall provide the following deliverables (predicated in calendar days) according to Table below, and the most current Project Management Plan (PMP), as approved by the Project Manager and DHS Contracting Officer or COR.

Table 2: Deliverables

Scope Ref.	Deliverable Name	Delivery Date
5.0.1	Project Management Plan (PMP) (Draft)	15 days after award

5.0.2	Project Management Plan (PMP) (Final)	30 days after award
5.0.3	Task Order Project Kickoff Briefing	Within 30 days of award date
5.1	Draft racial bias analysis (in a format mutually agreed upon by OIS and HSOAC)	9 months after award
5.1	Final racial bias analysis (in a format mutually agreed upon by OIS and HSOAC)	11 months after award
5.2	Expert analysis (at least product by the end of the period of performance)	As required and documented in the PMP
5.3.1	Analysis of other DHS statistical activities and how other federal statistical agencies were established and operate	As required and documented in the PMP
5.3.2	Based on 5.3.1, develop a proposed long term implementation plan to include staffing and resources necessary for OHSS and a structure for OHSS to work with counterparts in Components	As required and documented in the PMP
5.4	Project Completion Memorandum	End of period of performance

The FFRDC shall provide all deliverables under this task order directly to the S&T FFRDC PMO [REDACTED] the Task Order PM, TPOC, and Task Order COR. An unclassified abstract, 100 to 200 words in length, and at least five keywords, or a completed Standard Form 298, "Report Documentation Page," shall accompany each deliverable as indicated in Table 2. deliverable. Note that the Report Documentation Page will identify the approved release distribution level (e.g., distribution is unlimited; distribution authorized to US Government agencies only; etc.).

The FFRDC shall deliver a monthly status report by the 15th for HSOAC of the following month containing metrics pertaining to financial, schedule, technical progress, deliverable status, and risk information related to the task. The FFRDC task lead and the task order COR as needed will discuss relevant issues in evaluating the task priorities for the next period; and update the program plan as necessary.

9. Assumptions

The Government and HSOAC consider this project to be non-severable. The nature and scope of HSOAC projects makes categorization of them as non-severable most appropriate. A non-severable undertaking constitutes a specific, entire job or single undertaking with a defined end-product (such as a final report of research) that cannot feasibly be subdivided for separate performance. Per Comptroller General/Government Accountability Office decisions, a non-severable undertaking must be financed entirely out of the appropriation current at the time of

award, even though performance may extend into future fiscal years. Contracts for a non-severable undertaking cannot be incrementally funded (see 71 Comp Gen 428 (1992) and GAO Decision B-317139, Matter of Financial Crimes Enforcement Network).

Staff working on HSOAC FFRDC projects receive Fitness/Suitability, PIV/badges, DHS headquarters IT access, and security clearances under the IDIQ contract rather than having to wait to be cleared under each task order. This helps to ensure that the FFRDC can agilely respond to requirements and apply the full advantages that its open matrix structure provides the Department. It also saves the government valuable resources by leveraging active access and current investigations rather than performing additional investigations. This is keeping with the spirit of DHS Instruction 121-01-007-01, which states in part that “Reciprocity applies to the fullest extent possible” and “investigations and adjudications conducted by other federal agencies should be used whenever practicable to reduce the number of investigation requests, associated costs and unnecessary delays.” We assume that the sponsor will offer reciprocity of the Fitness they have through our primary sponsor, as is customary.

HSOAC’s proposed scope of work assumes that OIS will assist HSOAC in accessing all necessary data, including those that are collected by non-DHS departments (e.g., Justice, Health and Human Services, State) if such becomes necessary, in a timely manner. HSOAC assumes that delays in obtaining the data will result in extended timelines for performance.

10. Travel

Travel may be necessary to meet and coordinate interagency exchanges of information and to collect data for this task. The FFRDC shall provide trip reports to the task order COR for all non-local travel within 30 days of completion of travel.

Long Distance Travel

From	To	No. of Trips	No. of Days per Trip
Washington DC	El Paso, TX	2	3
Washington DC	Tucson, AZ	2	3
Washington DC	McAllen, TX	2	3
Los Angeles, CA	Washington, DC	3	3

- Total Number of Trips (All Travelers): 9
- Total Number of Travel Days (All Travelers): 27

The task order COR must approve all foreign travel. Foreign travel must be approved at least 30 days (for unclassified visits) or 45 days (for classified visits) in advance of the planned travel event.

Travel, including local non-commuting travel, shall be reimbursed in accordance with the Federal Travel Regulation. Daily commuting costs shall not be reimbursed. Long-distance travel not specified in this Task Order must be pre-approved by the Task Order CO or COR.

11. Period of Performance

The period of performance of this non-severable work is **24 months** from date of task order award.

Section F of the Indefinite-Delivery Indefinite-Quantity contract (70RSAT22D000000001) prescribes the following:

F.4 Task Order Performance Period and Pricing

Task Orders (TOs) may be issued at any time during the COP. The period of performance (PoP) for each TO will be specified in the TO and may include option periods and only extended within the allowable limitations of task severability and funding appropriation type. ***A task order PoP shall not be arbitrarily or unilaterally limited to 12 months.***

12. Security Requirements.

This Task Order will require access to the following information

- ☒ 1. Unclassified, no markings
- ☒ 2. Sensitive but Unclassified (SBU), For Official Use Only (FOUO)
- ☒ 3. Law Enforcement Sensitive (LES)
- ☒ 4. Personally Identifiable Information (PII)
- ☐ 5. Protected Critical Infrastructure Information (PCII)
- ☐ 6. Confidential (classified)
- ☐ 7. Secret (classified)
- ☐ 8. Top Secret (classified)
- ☐ 9. Top Secret/SCI (classified)
- ☒ 10. Sensitive Security Information (SSI)

12.1 Security requirement #2 (SBU, FOUO) – All unclassified “For Official Use Only” (FOUO) work is expected to occur at the “medium” level per the National Institute of Standards and Technology (NIST) 800-60 (Federal Information Processing Standard (FIPS) Security Categorization) and the Federal Information Security Management Act (FISMA). Any work at the “high” FOUO level per the FISMA, or any work at the classified level, shall be performed on a stand-alone computer system accredited in accordance with the FISMA and applicable DHS policies.

12.2 Security requirement # 2 (SBU, FOUO) – The FFRDC shall adhere to all applicable government laws, regulations, orders, guides, and directives pertaining to classified, Sensitive But Unclassified (SBU), FOUO, or personally identifiable information. The contractor shall safeguard SBU, FOUO information specifically in accordance with DHS Management Directive 11042.1 and in compliance with HSAR Class Deviation 15-01 Safeguarding of Sensitive Information.

12.3 The contractor shall use Science & Technology or another DHS Components' accredited General Support System (GSS) to accomplish this work, when applicable, until such time as HSSDI or HSOAC Accredited Enclave solution becomes available. If classified work is required under this Task Order, the Task Order COR shall provide specific guidance to the FFRDC as to which work will be conducted in a classified manner and at which classification level. If such DHS-guidance conflicts with other applicable guidelines (e.g., DOE, DOD, etc.), the FFRDC shall adhere to the more stringent guidelines as determined by the Task Order COR and DHS FFRDC PMO. The FFRDC shall also adhere to other applicable government orders, guides, and directives pertaining to classified or confidential work.

12.4 Authorized IT Environments

The FFRDC team will use their FFRDC corporate IT environment for FFRDC contracts management and administrative support for activities including:

- Time reporting
- Financial management
- Contract management
- Monthly status reports
- Non-DHS Sensitive project work

Sensitive FFRDC work described in the TEP will be performed in IT environment(s) authorized by DHS. These may include, a) FFRDC IT Enclave (following ATO by DHS), b) DHS infrastructure (e.g., LAN-A), and/or c) other authorized environment(s) (e.g., classified networks).

12.5 DHS Furnished Information

- a) DHS will provide unique information, materials, and forms to the Contractor as specified under this task order. Such DHS provided information, materials, and forms shall remain the property of DHS, unless otherwise indicated in writing by DHS, and may not be distributed beyond the FFRDC's project performers without DHS's prior written permission.

- b) The DHS COR identified in this task order will be the point of contact (POC) for identifying required information to be supplied by DHS.

12.6 FFRDC Furnished Information

Not Applicable

12.7 Privacy Compliance Requirements

The Government Program Manager will coordinate with the appropriate DHS component's Privacy Office (i.e., CBP, USCIS, S&T, etc.) to determine if a Privacy Threshold Analysis (PTA) is required prior to the start of performance. In those instances, the performer shall support the development of compliance related documentation and meet privacy requirements. Please have your privacy office reach out to S&T Privacy to see what documentation is available.

13. Safeguarding/Storage:

- a. No safeguarding/storage needed at the FFRDC.

14. Other Contract Details

In accordance with the language in the FFRDC contract, the following sections are repeated here for awareness and should not be changed. If they are changed, the language in the IDIQ takes precedence.

14.1 Inherently Governmental Functions

As defined under FAR subpart 7.503 (d) and additionally as described in the Office of Federal Procurement Policy (OFPP) Letter 11- 0 I, Performance of Inherently Governmental and Critical Functions (76 Fed Reg 56227), the FFRDC may perform certain closely associated with inherently Governmental functions. However, in accordance with Federal Acquisition Regulation (FAR) 7.503(c)(20) and Homeland Security Acquisition Manual 3037.103(e), the FFRDC shall not draft Congressional testimony, responses to Congressional correspondence, or agency responses to audit reports from the Inspector General, the Government Accountability Office, or other Federal audit entity. Furthermore, in accordance with FAR 7.503(c)(12)(ii), FFRDC employees, subcontractors, and/or consultants will not be voting members on any DHS source selections. When applicable, FAR clause 52.203-16, "Preventing Personal Conflicts of Interest," as included in the IDIQ contract, will apply to this Task Order.

14.2 Out of Scope Work

The following types of work are out of scope for the FFRDC to perform. More specific types of work that are out of scope are found in the relevant IDIQ contract:

Page 11 of 28

Distribution is authorized to U.S. government agencies only. This document contains sensitive information exempt from mandatory disclosure under the Freedom of Information Act, 5 U.S.C. 552(b)(2). Do not release without prior approval of the Department of Homeland Security's Science and Technology Directorate.

- Performance of any services and functions as defined under FAR Subpart 7.5 - “Inherently Governmental Functions,” specifically subparts 7.503 (a), (b) and (c).
- Performance of any Systems Engineering and Technical Assistance (SETA) type work, particularly where such work is directly for staff augmentation and of a general support nature where the specific type and quantity of deliverables are undefined.
- Preparation of any Independent Government Cost Estimates (IGCEs).
- Participation in any Source Selection Evaluation or any other membership body where voting and/or ranking of proposals will lead to a subsequent monetary or contract award. The FFRDC may provide independent technical evaluation of proposals in support to a Source Selection Evaluation body but may not provide any ranking, voting or other assigned ordering or selection criteria other than commenting on the technical merit of a particular proposal or proposal section(s). Use of the FFRDC in evaluating an offeror’s proposal MUST BE DISCLOSED IN THE SOLICITATION OF PROPOSALS and the offeror(s) given the opportunity to affect non-disclosure agreements and/or withdraw their offer(s), otherwise the FFRDC may not participate.
- Delivering recurring compliance training to DHS employees, particularly that which could reasonably be considered staff augmentation services, is not allowed. Training associated with the transfer of skills from the FFRDC to DHS is acceptable, as long as such training is non-recurring (i.e. train the trainer) and is not intended to be part of a formal established training program. Waivers to this may be requested from the FFRDC COR. Seminars, workshops, and short-courses intended to extend the access and awareness of FFRDC research, research methods, and data sets to practitioners across the Homeland Security Enterprise to assist them in improving mission effectiveness and efficiency is permissible.
- Software and/or hardware development or other manufacturing unless such development is associated with a prototype demonstration or other proof of concept system and not intended to be a permanent solution or in response to formal requirements.

15. Publications and Communications Concerning Work Performed

In accordance with the language in the FFRDC contract, the following statement is repeated here for awareness and should not be changed. If it is changed, the language in the IDIQ takes precedence.

The FFRDC shall mark all technical data or computer software pursuant to the terms of the IDIQ Contract. This will include, for copyrighted works, an appropriate notice acknowledging DHS’s sponsorship of the work, license rights, and the appropriate copyright notice as detailed in the IDIQ Contract.

Page 12 of 28

Distribution is authorized to U.S. government agencies only. This document contains sensitive information exempt from mandatory disclosure under the Freedom of Information Act, 5 U.S.C. 552(b)(2). Do not release without prior approval of the Department of Homeland Security’s Science and Technology Directorate.

The DHS desires widespread dissemination of the results of funded non-sensitive research and does not seek to undermine the independence or objectivity of the FFRDC or FFRDC operator in anyway. The FFRDC therefore will generally seek public release approval for the results of non-sensitive research. Thirty (30) days prior to release, the FFRDC will first ask for the task order COR's and CO's agreement that the research product is suitable for release. The FFRDC contract governs the scope of the review. Specifically, this review is strictly a mechanism by which the Department identifies the inclusion of Sensitive Information, as defined in the IDIQ contract, Section I.13(a). The review does not include a determination of the FFRDC's analytical conclusions, final findings, or analytical outcomes.

- Are you interested in releasing information publicly from this research? Possibly, depending on the specific work requested. Any public release of work will be scoped at the beginning of a requested task.
- If you don't want to release the results, is the FFRDC able to release info about the methodology to the other components or the public? It will depend on the audience. OIS will likely want to share its methodology with DHS Components and other relevant federal stakeholders with immigration responsibilities. Any release of the work will be scoped at the beginning of a requested task.
- What is the desired audience for the release of info? Component only/all of DHS/public release? The desired audience and any release will be scoped at the beginning of a requested task.
- Do you want an outreach event as part of the release? Depending on the scope and complexity of the work, OIS will determine whether an outreach event will be part of any release. If a release is necessary, it will be scoped at the beginning of a requested task.
- Would you be interested in having the PMO assist with the release of favorable results? Depending on the scope and complexity of the work, OIS will determine whether an outreach event will be part of any release. If a release is necessary, it will be scoped at the beginning of a requested task.

16. DHS Furnished Facilities, Supplies and Services

If work at the DHS Office of Immigration Statistics is necessary for the services being performed under this Task Order, such facilities will be provided at offices at the appropriate location. Parking facilities are not provided. Basic facilities such as work space and associated operating requirements (e.g., phones, desks, utilities, desktop computers, and consumable and general purpose office supplies) will be provided to FFRDC personnel.

DHS Furnished Property – a quarterly report of all S&T property should be submitted to the COR | FFRDC of all of the equipment purchased on behalf of the Government, and Government Furnished equipment being utilized by either FFRDC.


Subsequently a yearly report of all Government Furnished Equipment shall be provided to the COR | FFRDC. The COR | FFRDC will need a property form filled out for all S&T Contractor Acquired Equipment /Property or purchases on behalf of the Government for insertion into the S&T property management system (SAMS). This insertion will need to include the property form filled out in its entirety, paid invoice(s) showing the property purchase and a picture of the current state of that property.

- a) Additional DHS property will not be provided to the FFRDC unless otherwise agreed. If DHS property is provided to the FFRDC for task performance, the FFRDC shall maintain property records, sending a yearly report of all items currently attached to the task order to the COR| FFRDC and the Program Manager and a disposition of the property must be completed at the end of the period of performance.
- b) Before purchasing any individual item equal to or exceeding \$5,000 that is required to support technical tasks performed pursuant to this Task Order, that has not already been accepted by the Government with the issuance of the Task Order, the FFRDC shall obtain prior written consent from the Program Manager, DHS IDIQ Contracting Officer, and DHS IDIQ COR. The FFRDC shall maintain any such items according to the IDIQ Contract's property accountability procedures, and FAR Part 45.
- c) All DHS/GFP/GFE (IT equipment, building passes etc.) must be returned at the conclusion of the task order in accordance with component's procedures.
- d) If any GFP/GFE is not returned, a report of survey must be submitted to the COR and Project Manager, referencing the DHS equipment number, pass or card number, name of individual to whom equipment was issued, and the last known location of property. Contractors who lose a badge will be required to fill out an additional lost badge form.

17. Invoices

Invoices shall be submitted electronically to [REDACTED] with a courtesy copy to the Contracting Officer ([REDACTED] Contract Specialist [REDACTED] and to the Contracting Officer's Representative [REDACTED]

18. Points of Contact

Government POCs	Corresponding FFRDC POCs
	



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 e-mail notification shall state the required training has been completed for all Contractor and subcontractor employees.

(End of clause)

SAFEGUARDING OF SENSITIVE INFORMATION (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) *Definitions.* As used in this clause—

“Personally Identifiable Information (PII)” means information that can be used to distinguish or trace an individual's identity, such as name, social security number, or biometric records, either alone, or when combined with other personal or identifying information that is linked or linkable to a specific individual, such as date and place of birth, or mother's maiden name. The definition of PII is not anchored to any single category of information or technology. Rather, it requires a case-by-case assessment of the specific risk that an individual can be identified. In performing this assessment, it is important for an

Page 17 of 28

Distribution is authorized to U.S. government agencies only. This document contains sensitive information exempt from mandatory disclosure under the Freedom of Information Act, 5 U.S.C. 552(b)(2). Do not release without prior approval of the Department of Homeland Security's Science and Technology Directorate.

agency to recognize that non-personally identifiable information can become personally identifiable information whenever additional information is made publicly available—in any medium and from any source—that, combined with other available information, could be used to identify an individual.

PII is a subset of sensitive information. Examples of PII include, but are not limited to: name, date of birth, mailing address, telephone number, Social Security number (SSN), email address, zip code, account numbers, certificate/license numbers, vehicle identifiers including license plates, uniform resource locators (URLs), static Internet protocol addresses, biometric identifiers such as fingerprint, voiceprint, iris scan, photographic facial images, or any other unique identifying number or characteristic, and any information where it is reasonably foreseeable that the information will be linked with other information to identify the individual.

“Sensitive Information” is defined in HSAR clause 3052.204-71, Contractor Employee Access, as any information, which if lost, misused, disclosed, or, without authorization is accessed, or modified, could adversely affect the national or homeland security interest, the conduct of Federal programs, or the privacy to which individuals are entitled under section 552a of Title 5, United States Code (the Privacy Act), but which has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense, homeland security or foreign policy. This definition includes the following categories of information:

(1) Protected Critical Infrastructure Information (PCII) as set out in the Critical Infrastructure Information Act of 2002 (Title II, Subtitle B, of the Homeland Security Act, Public Law 107-296, 196 Stat. 2135), as amended, the implementing regulations thereto (Title 6, Code of Federal Regulations, Part 29) as amended, the applicable PCII Procedures Manual, as amended, and any supplementary guidance officially communicated by an authorized official of the Department of Homeland Security (including the PCII Program Manager or his/her designee);

(2) Sensitive Security Information (SSI), as defined in Title 49, Code of Federal Regulations, Part 1520, as amended, “Policies and Procedures of Safeguarding and Control of SSI,” 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 his/her designee);

(3) Information designated as “For Official Use Only,” which is unclassified information of a sensitive nature and the unauthorized disclosure of which could adversely impact a person’s privacy or welfare, the conduct of Federal programs, or other programs or operations essential to the national or homeland security interest; and

(4) Any information that is designated “sensitive” or subject to other controls, safeguards or protections in accordance with subsequently adopted homeland security information handling procedures.

“Sensitive Information Incident” is an incident that includes the known, potential, or suspected exposure, loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or unauthorized access or attempted access of any Government system, Contractor system, or sensitive information.

“Sensitive Personally Identifiable Information (SPII)” is a subset of PII, which if lost, compromised or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. Some forms of PII are sensitive as stand-alone elements. Examples of such PII include: Social Security numbers (SSN), driver’s license or state identification number, Alien Registration Numbers (A-number), financial account number, and biometric identifiers such as fingerprint, voiceprint, or iris scan. Additional examples include any groupings of information that contain an individual’s name or other unique identifier plus one or more of the following elements:

- (1) Truncated SSN (such as last 4 digits)
- (2) Date of birth (month, day, and year)
- (3) Citizenship or immigration status
- (4) Ethnic or religious affiliation
- (5) Sexual orientation
- (6) Criminal History
- (7) Medical Information
- (8) System authentication information such as mother’s maiden name, account passwords or personal identification numbers (PIN)

Other PII may be “sensitive” depending on its context, such as a list of employees and their performance ratings or an unlisted home address or phone number. In contrast, a business card or public telephone directory of agency employees contains PII but is not sensitive.

(c) *Authorities.* The Contractor shall follow all current versions of Government policies and guidance accessible at <http://www.dhs.gov/dhs-security-and-training-requirements-contractors>, or available upon request from the Contracting Officer, including but not limited to:

- (1) DHS Management Directive 11042.1 Safeguarding Sensitive But Unclassified (for Official Use Only) Information

- (2) DHS Sensitive Systems Policy Directive 4300A
- (3) DHS 4300A Sensitive Systems Handbook and Attachments
- (4) DHS Security Authorization Process Guide
- (5) DHS Handbook for Safeguarding Sensitive Personally Identifiable Information
- (6) DHS Instruction Handbook 121-01-007 Department of Homeland Security Personnel Suitability and Security Program
- (7) DHS Information Security Performance Plan (current fiscal year)
- (8) DHS Privacy Incident Handling Guidance
- (9) Federal Information Processing Standard (FIPS) 140-2 Security Requirements for Cryptographic Modules accessible at <http://csrc.nist.gov/groups/STM/cmvp/standards.html>
- (10) National Institute of Standards and Technology (NIST) Special Publication 800-53 Security and Privacy Controls for Federal Information Systems and Organizations accessible at <http://csrc.nist.gov/publications/PubsSPs.html>
- (11) NIST Special Publication 800-88 Guidelines for Media Sanitization accessible at <http://csrc.nist.gov/publications/PubsSPs.html>

(d) *Handling of Sensitive Information.* Contractor compliance with this clause, as well as the policies and procedures described below, is required.

(1) Department of Homeland Security (DHS) policies and procedures on Contractor personnel security requirements are set forth in various Management Directives (MDs), Directives, and Instructions. *MD 11042.1, Safeguarding Sensitive But Unclassified (For Official Use Only) Information* describes how Contractors must handle sensitive but unclassified information. DHS uses the term “FOR OFFICIAL USE ONLY” to identify sensitive but unclassified information that is not otherwise categorized by statute or regulation. Examples of sensitive information that are categorized by statute or regulation are PCII, SSI, etc. The *DHS Sensitive Systems Policy Directive 4300A* and the *DHS 4300A Sensitive Systems Handbook* provide the policies and procedures on security for Information Technology (IT) resources. The *DHS Handbook for Safeguarding Sensitive Personally Identifiable Information* provides guidelines to help safeguard SPII in both paper and electronic form. *DHS Instruction Handbook 121-01-007 Department of Homeland Security Personnel Suitability and Security Program* establishes procedures, program responsibilities, minimum standards, and reporting protocols for the DHS Personnel Suitability and Security Program.

(2) The Contractor shall not use or redistribute any sensitive information processed, stored, and/or transmitted by the Contractor except as specified in the contract.

(3) All Contractor employees with access to sensitive information shall execute *DHS Form 11000-6, Department of Homeland Security Non-Disclosure Agreement (NDA)*, as a condition of access to such information. The Contractor shall maintain signed copies of the NDA for all employees as a record of

compliance. The Contractor shall provide copies of the signed NDA to the Contracting Officer's Representative (COR) no later than two (2) days after execution of the form.

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

(e) *Authority to Operate.* The Contractor shall not input, store, process, output, and/or transmit sensitive information within a Contractor IT system without an Authority to Operate (ATO) signed by the Headquarters or Component CIO, or designee, in consultation with the Headquarters or Component Privacy Officer. Unless otherwise specified in the ATO letter, the ATO is valid for three (3) years. The Contractor shall adhere to current Government policies, procedures, and guidance for the Security Authorization (SA) process as defined below.

(1) Complete the Security Authorization process. The SA process shall proceed according to the *DHS Sensitive Systems Policy Directive 4300A* (Version 11.0, April 30, 2014), or any successor publication, *DHS 4300A Sensitive Systems Handbook* (Version 9.1, July 24, 2012), or any successor publication, and the *Security Authorization Process Guide* including templates.

(i) **Security Authorization Process Documentation.** SA documentation shall be developed using the Government provided Requirements Traceability Matrix and Government security documentation templates. SA documentation 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). During the development of SA documentation, the Contractor shall submit a signed SA package, validated by an independent third party, to the COR for acceptance by the Headquarters or Component CIO, or designee, at least thirty (30) days prior to the date of operation of the IT system. The Government is the final authority on the compliance of the SA package and may limit the number of resubmissions of a modified SA package. Once the ATO has been accepted by the Headquarters or Component CIO, or designee, the Contracting Officer shall incorporate the ATO into the contract as a compliance document. The Government's acceptance of the ATO does not alleviate the Contractor's responsibility to ensure the IT system controls are implemented and operating effectively.

(ii) **Independent Assessment.** Contractors shall have an independent third party validate the security and privacy controls in place for the 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 Special Publication 800-53 Security and Privacy Controls for Federal Information Systems and Organizations*. The Contractor shall address all deficiencies before submitting the SA package to the Government for acceptance.

(iii) Support the completion of the Privacy Threshold Analysis (PTA) as needed. As part of the SA process, the Contractor may be required to support the Government in the completion of the PTA. The requirement to complete a PTA is triggered by the creation, use, modification, upgrade, or disposition of a Contractor IT system that will store, maintain and use PII, and must be renewed at least every three (3) years. Upon review of the PTA, the DHS Privacy Office determines whether a Privacy Impact Assessment (PIA) and/or Privacy Act System of Records Notice (SORN), or modifications thereto, are required. The Contractor shall provide all support necessary to assist the Department in completing the PIA in a timely manner and shall ensure that project management plans and schedules include time for the completion of the PTA, PIA, and SORN (to the extent required) as milestones. Support in this context includes responding timely to requests for information from the Government about the use, access, storage, and maintenance of PII on the Contractor's system, and providing timely review of relevant compliance documents for factual accuracy. Information on the DHS privacy compliance process, including PTAs, PIAs, and SORNs, is accessible at <http://www.dhs.gov/privacy-compliance>.

(2) *Renewal of ATO*. Unless otherwise specified in the ATO letter, the ATO shall be renewed every three (3) years. The Contractor is required to update its SA package as part of the ATO renewal process. The Contractor shall update its SA package by one of the following methods: (1) Updating the SA documentation in the DHS automated information assurance tool for acceptance by the Headquarters or Component CIO, or designee, at least 90 days before the ATO expiration date for review and verification of security controls; or (2) Submitting an updated SA package directly to the COR for approval by the Headquarters or Component CIO, or designee, at least 90 days before the ATO expiration date for review and verification of security controls. The 90 day review process is independent of the system production date and therefore it is important that the Contractor build the review into project schedules. The reviews may include onsite visits that involve physical or logical inspection of the Contractor environment to ensure controls are in place.

(3) *Security Review*. The Government may elect to conduct random periodic reviews to ensure that the security requirements contained in this contract are being implemented and enforced. The Contractor shall afford DHS, the Office of the Inspector General, and other Government organizations access to the Contractor's facilities, installations, operations, documentation, databases and personnel used in the performance of this contract. The Contractor shall, through the Contracting Officer and COR, contact the Headquarters or Component CIO, or designee, to coordinate and participate in review and inspection activity by Government organizations external to the DHS. Access shall be provided, to the extent necessary as determined by the Government, 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) *Continuous Monitoring.* All Contractor-operated systems that input, store, process, output, and/or transmit sensitive information shall meet or exceed the continuous monitoring requirements identified in the *Fiscal Year 2014 DHS Information Security Performance Plan*, or successor publication. The plan is updated on an annual basis. The Contractor shall also store monthly continuous monitoring data at its location for a period not less than one year from the date the data is created. The data shall be encrypted in accordance with *FIPS 140-2 Security Requirements for Cryptographic Modules* and shall not be stored on systems that are shared with other commercial or Government entities. The Government may elect to perform continuous monitoring and IT security scanning of Contractor systems from Government tools and infrastructure.

(5) *Revocation of ATO.* In the event of a sensitive information incident, the Government may suspend or revoke an existing ATO (either in part or in whole). If an ATO is suspended or revoked in accordance with this provision, the Contracting Officer may direct the Contractor to take additional security measures to secure sensitive information. These measures may include restricting access to sensitive information on the Contractor IT system under this contract. Restricting access may include disconnecting the system processing, storing, or transmitting the sensitive information from the Internet or other networks or applying additional security controls.

(6) *Federal Reporting Requirements.* Contractors operating information systems on behalf of the Government or operating systems containing sensitive information shall comply with Federal reporting requirements. Annual and quarterly data collection will be coordinated by the Government. Contractors shall provide the COR with requested information within three (3) business days of receipt of the request. Reporting requirements are determined by the Government and are defined in the *Fiscal Year 2014 DHS Information Security Performance Plan*, or successor publication. The Contractor shall provide the Government with all information to fully satisfy Federal reporting requirements for Contractor systems.

(f) *Sensitive Information Incident Reporting Requirements.*

(1) All known or suspected sensitive information incidents shall be reported to the Headquarters or Component Security Operations Center (SOC) within one hour of discovery in accordance with *4300A Sensitive Systems Handbook Incident Response and Reporting* requirements. When notifying the Headquarters or Component SOC, the Contractor shall also notify the Contracting Officer, COR, Headquarters or Component Privacy Officer, and US-CERT using the contact information identified in the contract. If the incident is reported by phone or the Contracting Officer's email address is not immediately available, the Contractor shall contact the Contracting Officer immediately after reporting

the incident to the Headquarters or Component SOC. The Contractor shall not include any sensitive information in the subject or body of any e-mail. To transmit sensitive information, the Contractor shall use *FIPS 140-2 Security Requirements for Cryptographic Modules* compliant encryption methods to protect sensitive information in attachments to email. Passwords shall not be communicated in the same email as the attachment. A sensitive information incident shall not, by itself, be interpreted as evidence that the Contractor has failed to provide adequate information security safeguards for sensitive information, or has otherwise failed to meet the requirements of the contract.

(2) If a sensitive information incident involves PII or SPII, in addition to the reporting requirements in *4300A Sensitive Systems Handbook Incident Response and Reporting*, 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) Data Universal Numbering System (DUNS);
- (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, email);
- (v) Contracting Officer POC (address, telephone, email);
- (vi) Contract clearance level;
- (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 sensitive information resided at the time of the incident, both at the Contractor and subcontractor level;
- (xii) Description of the Government PII and/or SPII contained within the system;
- (xiii) Number of people potentially affected and the estimate or actual number of records exposed and/or contained within the system; and
- (xiv) Any additional information relevant to the incident.

(g) Sensitive Information Incident Response Requirements.

(1) All determinations related to sensitive information incidents, including response activities, notifications to affected individuals and/or Federal agencies, and related services (e.g., credit monitoring) will be made in writing by the Contracting Officer in consultation with the Headquarters or Component CIO and Headquarters or Component Privacy 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 sensitive information 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, and
- (iv) Data analyses and processing.

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

(h) Additional PII and/or SPII Notification Requirements.

(1) The Contractor shall have in place procedures and the capability to notify any individual whose PII resided in the Contractor IT system at the time of the sensitive information incident not later than 5 business days after being directed to notify individuals, unless otherwise approved by the Contracting Officer. The method and content of any notification by the Contractor shall be coordinated with, and subject to prior written approval by the Contracting Officer, in consultation with the Headquarters or Component Privacy Officer, utilizing the *DHS Privacy Incident Handling Guidance*. The Contractor shall not proceed with notification unless the Contracting Officer, in consultation with the Headquarters or Component Privacy Officer, has determined in writing that notification is appropriate.

(2) Subject to Government analysis of the incident and the terms of its instructions 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 and 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;

- (v) What the Contractor and/or the Government are doing to investigate the incident, to mitigate the incident, and to protect against any future incidents; and
- (vi) Information identifying who individuals may contact for additional information.

(i) *Credit Monitoring Requirements.* In the event that a sensitive information incident involves PII or SPII, the Contractor may be required to, as directed by the Contracting Officer:

(1) Provide notification to affected individuals as described above; and/or

(2) Provide credit monitoring services to individuals whose data was under the control of the Contractor or resided in the Contractor IT system at the time of the sensitive information 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; and/or

(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 FAQs, approved in writing by the Contracting Officer in coordination with the Headquarters or Component Chief Privacy Officer; and
- (vi) Information for registrants to contact customer service representatives and fraud resolution representatives for credit monitoring assistance.

(j) *Certification of Sanitization of Government and Government-Activity-Related Files and Information.* As part of contract closeout, the Contractor shall submit the certification to the COR and the Contracting Officer following the template provided in *NIST Special Publication 800-88 Guidelines for Media Sanitization*.

(End of clause)

CONTRACTOR EMPLOYEE ACCESS (SEP 2012)

(a) *Sensitive Information*, as used in this clause, means any information, which if lost, misused, disclosed, or, without authorization is accessed, or modified, could adversely affect the national or homeland security interest, the conduct of Federal programs, or the privacy to which individuals are entitled under section 552a of title 5, United States Code (the Privacy Act), but which has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense, homeland security or foreign policy. This definition includes the following categories of information:

(1) Protected Critical Infrastructure Information (PCII) as set out in the Critical Infrastructure Information Act of 2002 (Title II, Subtitle B, of the Homeland Security Act, Public Law 107-296, 196 Stat. 2135), as amended, the implementing regulations thereto (Title 6, Code of Federal Regulations, Part 29) as amended, the applicable PCII Procedures Manual, as amended, and any supplementary guidance officially communicated by an authorized official of the Department of Homeland Security (including the PCII Program Manager or his/her designee);

(2) Sensitive Security Information (SSI), as defined in Title 49, Code of Federal Regulations, Part 1520, as amended, "Policies and Procedures of Safeguarding and Control of SSI," 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 his/her designee);

(3) Information designated as "For Official Use Only," which is unclassified information of a sensitive nature and the unauthorized disclosure of which could adversely impact a person's privacy or welfare, the conduct of Federal programs, or other programs or operations essential to the national or homeland security interest; and

(4) Any information that is designated "sensitive" or subject to other controls, safeguards or protections in accordance with subsequently adopted homeland security information handling procedures.

(b) "Information Technology Resources" include, but are not limited to, computer equipment, networking equipment, telecommunications equipment, cabling, network drives, computer drives, network software, computer software, software programs, intranet sites, and internet sites.

(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

Page 27 of 28

Distribution is authorized to U.S. government agencies only. This document contains sensitive information exempt from mandatory disclosure under the Freedom of Information Act, 5 U.S.C. 552(b)(2). Do not release without prior approval of the Department of Homeland Security's Science and Technology Directorate.

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 sensitive information or IT 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 sensitive information. Therefore, the Contractor shall not disclose, orally or in writing, any sensitive information to any person unless authorized in writing by the Contracting Officer. For those Contractor employees authorized access to sensitive information, the Contractor shall ensure that these persons receive training concerning the protection and disclosure of sensitive information both during and after contract performance.

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

(End of clause)