FEDERALLY FUNDED RESEARCH AND DEVELOPMENT CENTER (FFRDC)

Homeland Security Systems Engineering and Development Institute (HSSEDI)

TECHNICAL EXECUTION PLAN (TEP)

Title: ICE Information Governance and Privacy Program Support

U.S. Department of Homeland Security
U.S Immigration and Customs Enforcement (ICE)
Office of Information Governance and Privacy (OIGP)

Version: 6.4 – TEP43-23-0244 – Cost Proposal P23-724

Date: September 14, 2023

1. Challenge

The ICE Office of Information Governance and Privacy is facing a series of unprecedented short, mid, and long-term challenges to achieving its mission. Some examples include implementing privacy protections into upcoming ICE Body Worn Camera audio, video, and records, transitioning from a compliance-based to risk-based privacy framework, and automating privacy functions to accomplish more work with fewer staff and smaller budgets.

Some ICE operational and enterprise-wide programs may be required to pause activities if privacy policies and requirements are not addressed, and the resulting lack of access to personal information will have a detrimental impact on mission goals and objectives.

HSSEDI has a strong track record of helping ICE and other DHS components evaluate new and evolving technologies, identifying privacy gaps and risks, and working with the Privacy Officer to develop strategies and plans to improve privacy protections within the agency.

2. Outcome(s)

At the completion of this task order the OIGP executive leadership team will have improved privacy strategy guidance and awareness throughout the agency and will effectively coordinate with internal and external government partners on matters impacting ICE's handling of sensitive personally identifiable information (PII).

3. Background

ICE is the largest investigative agency in the Department of Homeland Security (DHS) and was formally established March 1, 2003. ICE's primary mission is to protect national security, public safety, and the

integrity of the US borders through the criminal and civil enforcement of federal laws governing border control, customs, trade, and immigration.

As a part of ICE, the OIGP oversees the management, sharing, protection and access to ICE data, and ensures the information ICE maintains meets legal and policy requirements. OIGP's functional components include the Privacy Unit and the Freedom of Information Act (FOIA) Unit.

The ICE Privacy Unit oversees the implementation of privacy protections and the transparency of government operations while supporting the ICE mission. The Unit is responsible for ensuring ICE compliance with the Privacy Act of 1974 and the e-Government Act of 2002, analyzing, and managing privacy risk associated with ICE programs that collect, use, or share personally identifiable information (PII), some of which may be sensitive.

4. Task Objective(s)

For this task, HSSEDI will act as an independent trusted advisor to the OIGP Assistant Director, Deputy Assistant Director, and the ICE Privacy Officer.

In the Base Period, HSSEDI will work with OIGP to:

- Identify short, mid, and long-term ICE privacy risks and compliance challenges that may detrimentally impact ICE operations and recommend mitigation strategies;
- Evaluate existing agency privacy and information management policies/guidance and recommend actions to address gaps.
- Assess Privacy program workflows and develop business and technical requirements for a comprehensive workflow and knowledge management, stakeholder coordination, and decision-making support tool;
- Evaluate and recommend IT solutions and develop funding requirements;
- Develop a framework, roadmap, and supporting materials for an agency-wide privacy competency and capacity-building program; and
- Assess gaps in the agency's approach to compliance with 8 USC §1367 and asylum confidentiality requirements and recommend strategies for increasing compliance and awareness.

In the Option Period, HSSEDI will build on the accomplishments of the Base Period, working with OIGP to:

- Draft an agency Privacy Compliance Directive and Instruction or Handbook;
- Draft updates to agency policies to address identified privacy gaps and decrease risk;
- Assess enterprise risk and identify privacy risks to be included in ICE's Enterprise Risk Register;
- Support implementation of a privacy workflow and knowledge management tool, identifying opportunities to refine workflows and requirements; recommend privacy program metrics that support program evaluation and decision-making and align to privacy risks identified in previous Tasks;
- Develop a workflow and knowledge management standardization plan;

- Evaluate the effectiveness of the initial launch of the privacy competency- and capacity-building program designed during the Base Period and identify opportunities for immediate and continuous improvement and program maturity; and
- Develop a comprehensive Risk Mitigation Strategy for 8 USC §1367 and asylum confidentiality.

5. Technical Approach / Analytic Methodology

HSSEDI's technical approach leverages subject matter experts to assess ICE's privacy environment to act as an independent advisor to the OIGP executive leadership team to identify data collaboration opportunities and make recommendations which increase compliance and better protect sensitive information. HSSEDI will also participate in discussions with ICE privacy professionals, cross-cutting working groups (e.g., IPTs, communities of interest) and other stakeholders, while providing guidance in needed technical areas.

6. Base Period – Establish Environment for Capability Enhancement (1.28 STE)

6.1 Privacy Risk Mitigation Assessment

HSSEDI will provide privacy subject matter expertise in reviewing agency policies and other documents involving privacy and personal information; appraising privacy compliance practices and ascertaining methods for transitioning to privacy risk management practices; providing substantive and qualitative strategy recommendations for further mitigating privacy risks, as needed; and enabling appropriate and effective law enforcement data collection and sharing by ensuring ICE initiatives align with applicable legal and regulatory frameworks (e.g., the Privacy Act, E-Government Act). HSSEDI will:

- Conduct an inventory of federal government privacy policies, standards, and processes and identify gaps leading to non-compliance with applicable laws and policies and risk to the agency;
- Evaluate ICE directives and related instructions or handbooks and recommend options to transition from a privacy compliance approach to a privacy risk management approach in general and specific to planned agency initiatives (e.g., body worn cameras, use of privacy sensitive technologies); and
- Develop a roadmap for addressing identified gaps and moving to a risk management approach through changes to policies and processes.

6.2 Internal Workflow/Knowledge Management and Collaboration Platform

HSSEDI will conduct an analysis of current Privacy Unit workflows, assessing inputs and outputs, and establish baselines for collaboration and integration with stakeholders to support synchronization of priority tasks within expected deliverables and timeframes. HSSEDI will:

- Develop draft requirements for an internal workflow/knowledge management and collaboration platform that ensures all stakeholder's equities are fully integrated, the workflow is correct and reduces identified privacy risks, and data about the Privacy Unit's level of effort is available to OIGP leadership for reporting and resource allocation purposes;
- Advise on technical and process requirements to standardize and support privacy workflows, privacy program management, and the integration of privacy equities into agency processes and

workflows

- to increase efficiency, and to incorporate automation into the privacy compliance process, where possible; and
- Research, evaluate, and recommend tools that meet requirements and provide recommendations and funding requirements.

6.3 Privacy Liaison Program

HSSEDI will develop guidance and provide recommendations for the framework of a Liaison Program to build privacy competency and support privacy program implementation across the organization. HSSEDI will:

- Provide guidance and design recommendations for the framework of a Privacy Liaison Program to build privacy capacity throughout ICE to support an increase in awareness throughout the agency of responsibilities and techniques for protecting individual information and serve as a force multiplier for the ICE Privacy Unit;
- Develop draft privacy resources for OIGP delivery to collateral Privacy Liaison Officers; and
- Develop a draft roadmap for the initial launch of the Privacy Liaison Program including selection criteria and process, evaluation of industry certification programs for consideration, and ongoing communication and feedback plans.

6.4 8 USC §1367 and Asylum Confidentiality Gap Analysis and Recommendations

HSSEDI will conduct a gap analysis of existing 8 USC §1367 ("Section 1367) and asylum confidentiality procedures, practices, and agency awareness measures (e.g., training materials, rules of behavior) and develop a roadmap and informational materials to address gaps. To support this effort, HSSEDI will:

- Engage with Section 1367 and asylum SMEs within USCIS and ICE and review existing statutes, policies, requirements, and procedures to gain a baseline understanding of Section 1367 and asylum confidentiality policies;
- Develop a gap analysis to inform ICE on risks associated with its handling of Section 1367 and asylum information and a roadmap for addressing identified gaps; and
- Develop a standardized baseline for knowledge of Section 1367 and asylum confidentiality requirements;
- Develop a draft roadmap for deployment of the Section 1367 and asylum confidentiality related materials to all ICE personnel interacting with protected information.

7. Continued Support to OIGP [Option Year 1 (1.26 STE)]

In Option year 1, the HSSEDI Team will continue to aid in the advancement of the proposed 8 USC §1367 disclosure limitation and Asylum Confidentiality strategies through an evaluation of compliance gaps. HSSEDI will also provide final roadmap for workflow/knowledge management and collaboration platform and recommendations for maturing the privacy liaison program. The team will:

7.1 Privacy Risk Mitigation Assessment

HSSEDI will provide privacy subject matter expertise in conducting an inventory of agency policies and other documents involving privacy and personal information; appraising privacy compliance practices and ascertaining methods to draft updates and revisions for the ICE directives and related instructions or handbooks, and an enterprise privacy assessment to identify executives and key stakeholders, define their key objectives, and establish how risks/unplanned events that could impact the organization's ability to achieve them. HSSEDI will:

Based on Task 6.1 deliverables, HSSEDI will:

- Develop a draft ICE Privacy Compliance directive and related instruction or handbook to support an increase in awareness throughout the agency of responsibilities and techniques for protecting individual information;
- Develop draft updates and revisions for ICE directives and related instructions or handbooks to support an increase in privacy compliance throughout the agency as well as awareness of responsibilities and techniques for protecting individual information;
- Review and recommend updates to existing policies to address ICE operational social media guidance, and/or draft new policy if circumstances require it;
- Review and recommend updates to existing policies to address AI-related risks so they align with and support ICE's 2021-2025 Strategic Plan; and

Additionally, HSSEDI will conduct an Enterprise Risk Management assessment to identify privacy risks that should be rolled into the ICE enterprise risk register.

7.2 Support for Workflow/Knowledge Management and Collaboration Platform

Based on the Task 6.2 deliverables, HSSEDI will advise on technical and process requirements to further standardize privacy workflows, privacy program management, and the integration of privacy equities into agency processes and workflows to increase efficiency. HSSEDI will:

- Develop proposed privacy program metrics based on anticipated or actual data available to support comprehensive understanding of privacy program effectiveness and decision-making on resource allocation and alignment of metrics to specific privacy risks;
- Develop a Workflow/Knowledge Management Standardization Plan to document approaches for sharing knowledge and linking insights and key findings across the enterprise; and
- Identify opportunities to refine workflows and technical requirements.

7.3 Privacy Liaison Program

HSSEDI will evaluate effectiveness of initial launch of the Privacy Liaison Program (PLP) based on the framework developed in Task 6.3 and develop guidance and provide recommendations for the maturation of the PLP across the organization. HSSEDI will:

- Evaluate the effectiveness of the initial launch, identifying lessons learned, and formulating recommendations and roadmap for maturing the program over time; and
- Identify gaps and develop a roadmap, as well as additional resources and artifacts, to mature the PLP.

7.4 8 USC §1367 Disclosure Limitation and Asylum Confidentiality Recommendations

HSSEDI will utilize the gap analysis of existing 8 USC §1367 ("Section 1367") disclosure limitation and asylum documentation and Roadmap developed during the Base Period (Task 6.4) and develop a Section 1367 and Asylum Confidentiality Risk Mitigation Strategy and related materials to enable OIGP to enhance the protection of Section 1367 and asylum information across the ICE enterprise.

8. Key Words

Type of Work
Privacy
Policy
Compliance

Benefit of Work
Improved privacy awareness
Increased information sharing
Knowledge transfer

Subject of Interest
Legal and regulatory frameworks
International Data Protection

9. 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.

HSSEDI proposed total STE: 1.28 STE Base year and 1.26 Option year

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

	QHSR Missions					
HSSEDI 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 Resi.	Mission 6: Maturing and Strengthening
1. Acquisition Planning and Development	0%	0%	0%	0%	0%	0%
2. Emerging Threats, Concept Exploration, Experimentation and Evaluation	0%	0%	0%	0%	0%	0%
3. Information Technology and Communications	0%	0%	100%	0%	0%	0%
4. Cyber Solutions / Operations	0%	0%	0%	0%	0%	0%
5. Systems Engineering, System Architecture, and Integration	0%	0%	0%	0%	0%	0%
6. Technical Quality and Performance	0%	0%	0%	0%	0%	0%
7. Independent Test and Evaluation	0%	0%	0%	0%	0%	0%

10. Deliverables and Schedule

HSSEDI shall provide the following deliverables (predicated in calendar days) according to Table 2 below, and the most current Project Management Plan (PMP), as approved by the Project Manager and DHS Contracting Officer or COR.

Table 2: Base Period Deliverables

Scope Ref.	Deliverable Name	Delivery Date
4	Project Management Plan (PMP) (Draft)	15 days after award
4.1	Project Management Plan (PMP) (Final)	30 days after award
4.1	Task Order Project Kickoff Briefing	Within 30 days of project award date
6.1	ICE Privacy Compliance Gap Analysis (Draft)	Within 90 days after award
6.2	Workflow/Knowledge Management and Collaboration Platform Requirements Analysis and Recommendations (Draft)	Within 150 days after award
6.2	Workflow/Knowledge Management and Collaboration Platform Requirements Analysis and Recommendations (Final)	Within 180 days after award
6.4	8 USC §1367 Disclosure Limitation and Asylum Confidentiality Gap Analysis, Roadmap, and Knowledge-Building Materials (Draft)	Within 210 days after award
6.4	8 USC §1367 Disclosure Limitation and Asylum Confidentiality Gap Analysis, Roadmap, and Knowledge-Building Materials (Final)	Within 270 days after award
6.1	ICE Privacy Compliance Gap Analysis (Final) and Roadmap	Within 300 days after award
6.3	Privacy Liaison Program Framework and Roadmap (Draft)	Within 330 days after award
6.3	Privacy Liaison Program Framework and Roadmap (Final)	Within 345 days after award

Table 3: Option Year Deliverables

Scope Ref.	Deliverable Name	Delivery Date
4	Project Management Plan (PMP) (Draft)	15 days after project award
4.4	Project Management Plan (PMP) (Final)	30 days after project award
4.4	Task Order Project Kickoff Briefing	Within 30 days of project award
7.1	ICE Privacy Compliance Directive and Related Instruction/Handbook Summary	60 days after award
7.2	Workflow/Knowledge Management and Collaboration Platform: Metrics and Standardization Plan (Draft)	Within 90 days of project award
7.2	Workflow/Knowledge Management and Collaboration Platform: Metrics and Standardization Plan (Final)	Within 180 days of project award
7.3	Privacy Liaison Program Assessment and Program Maturation Roadmap (Draft)	Within 180 days of project award
7.1	Enterprise Risk Management Assessment	Within 240 days of project award
7.3	Privacy Liaison Program Assessment and Program Maturation Roadmap (Final)	Within 240 days of project award
7.4	8 USC §1367 Disclosure Limitation and Asylum Confidentiality Risk Mitigation Strategy (Draft)	Within 300 days of project award
7.1	Draft updates to directives/instructions	Within 345 days of project award
7.4	8 USC §1367 Disclosure Limitation and Asylum Confidentiality Risk Mitigation Strategy (Final)	15 days prior to the end of period of performance

HSSEDI shall provide all deliverables under this task order directly to the ICE FFRDC PMO (via hssedi.deliverable@hq.dhs.gov), 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.).

HSSEDI shall deliver a monthly status report by the 23rd of the following month containing metrics pertaining to financial, schedule, technical progress, deliverable status, and risk information related to the task. The HSSEDI 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.

11. Assumptions

- Deliverables will be primarily electronic unless otherwise directed by the task sponsor.
- The current estimate is based on information to date. HSSEDI will work collaboratively with the government to clarify and adjust if needed, focus and/or resource needs associated with the specific tasks, subtasks, and formal deliverables, informed by budget and schedule constraints, while remaining within overall project scope.
- The government will be responsible for managing any necessary formal government review and concurrence process that may derive from deliverables associated with these tasks.
- Integration with/of third-party applications, models, or environments will be facilitated by the government via formal request/direction to the third party. Any/all costs associated with requests will be documented by the third party and included in any contractual changes required by/for the third party to participate. Schedules associated with third party integration activities will be agreed and presented for consideration jointly between HSSEDI and the third party(ies).
- FAR Section 4.7 Contractor Records Retention requires contractors to maintain records for three (3) years following the final payment on a task order. Along with this and other audit obligations, MITRE must maintain a record of all unclassified deliverables, formal and informal. To meet these requirements, HSSEDI intends to use its archive site (known as DOV) located in the HSSEDI Enclave to collect and store all unclassified deliverables, regardless of where the deliverables are developed.

12. Travel

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

Long Distance Travel base and option

From	To	No. of Trips	No of Staff	No. of Days per Trip
Bedford, MA	Washington, DC	2	2	5
Tampa, Florida	Washington, DC	2	1	5

- Total Number of Trips: 6
- Total Number of Travel Days (All Travelers): 30

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.

13. Period of Performance

The period of performance is 12 months from date of task order award with an optional 12-month period of performance for continued specified support to OIGP to be exercised at the discretion of the government.

14. 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)

14.1 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.

14.2 Security requirement # 5 (PCII) – The FFRDC shall comply with all requirements of the Protected Critical Infrastructure Information (PCII) Program set out in the PCII Act, in the implementing regulations published in the Interim Rule, and in the PCII Procedures Manual as they may be amended from time to time and shall safeguard PCII in accordance with the procedures contained therein.

14.3 Security requirement # 5 (PCII) – The FFRDC shall ensure that each of its employees, consultants, and subcontractors who work on the PCII Program have executed non-disclosure agreements (NDAs) in a form prescribed by the PCII Program Manager. The FFRDC shall ensure that each of its employees, consultants and subcontractors has executed an NDA and agrees that none of its employees, consultants or sub-contractors shall be given access to PCII without having previously executed an NDA.

14.4 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.

14.5 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.

14.6 Authorized IT Environments

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

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

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

14.7 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.

14.8 HSSEDI Furnished Information

14.9 Privacy Compliance Requirements

The Government Program Manager will coordinate with the ICE Privacy Office 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.

15. Safeguarding/Storage:

a. No safeguarding/storage needed at the FFRDC.

16. Other Contract Details

In accordance with the language in the HSSEDI 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.

16.1 FFRDC Personnel

Personnel provided by the FFRDC will have the skills and technical background necessary to successfully complete the tasks described in this plan. The FFRDC shall implement and manage the technical approach, organizational resources, management, and quality controls to be employed to meet the cost, performance and schedule requirements throughout task order execution.

16.2 Food and Drink.

The FFRDC shall not charge any expense for food, snacks, or drink as part of holding task related meetings, conferences, or gatherings; however, this prohibition does not prevent the contractor from charging meals and incidental expenses as part of authorized travel expenses.

16.3 Meetings and Workshops

All necessary conference approvals should take place prior to the FFRDC's attendance at any conference in support of the sponsoring component. The component user should follow the conference approval process per the guidance set-forth under DHS Financial Management Policy Manual (FMPM Section 7.10) and any component-specific policies and procedures and provide a copy approval(s) to the FFRDC.

The FFRDC may interview and conduct workshops of recognized subject-matter experts, including non-federal experts, to gather the expert's individual knowledge and experience regarding the current state of the art of the technical issues relating to this task, and to foster the building of a long-term collaboration between the individual subject matter experts and the FFRDC on the issues relating to the experts' areas of expertise. The workshops or other interaction with non-Federal experts will be for the purpose of collecting the views of the individual experts, not to result in a consensus of those experts. The FFRDC shall produce an objective assessment on the technical merits of the data and/or experts' views espoused in these meetings; and include an evaluation of the strengths and weaknesses of the various discussion points provided by individuals.

The FFRDC may organize meetings/workshops related to the task with federal officials on behalf of the user; however, federal government personnel will approve the agenda and will chair any federal intra-agency/inter-agency meetings. The FFRDC shall produce an objective assessment on the technical merits of individual and any consensus findings and

recommendations discussed in these meetings; and include an evaluation of their strengths and weaknesses of the various discussion points.

16.4 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 l, 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.

16.5 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:

- 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.

17. Publications and Communications Concerning Work Performed

In accordance with the language in the HSSEDI 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.

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?

  No, at the time of award no research is intended to be released. If this changes during the conduct of this research effort, HSSEDI will use the appropriate Public Release Process to gain concurrence.

- If you don't want to release the results, is HSSEDI able to release info about the methodology to the other components or the public?

  No, not currently due to the sensitive nature of ICE immigration data which is LE Sensitive.

- What is the desired audience for the release of info? Component only/all DHS/public release?

  ICE only

- Do you want an outreach event as part of the release?

  No

- Would you be interested in having the ICE FFRDC PMO assist with the release of favorable results?

  No

18. DHS Furnished Facilities, Supplies and Services

If work at **ICE HSI** 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 workspace and associated operating requirements (e.g., phones, desks, utilities, desktop computers, and consumable and general-purpose office supplies) will be provided to HSSEDI personnel.

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

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 ICE Contractor Acquired Equipment /Property or purchases on behalf of the Government for insertion into the ICE 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, HSSEDI shall obtain prior written consent from the Program Manager, task order Contracting Officer, and task order COR. HSSEDI 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.

19. Invoices

20. Points of Contact

Government POCs	Corresponding HSSEDI POCs
[redacted] Deputy Assistant Director Information Governance and Privacy U.S. Immigration and Customs Enforcement [redacted]	[redacted] Program Manager HSSEDI P713 [redacted]

Program Manager [redacted] Deputy Assistant Director Information Governance and Privacy U.S. Immigration and Customs Enforcement [redacted]	**HSSEDI Task Lead** [redacted] Principal Privacy Engineer [redacted]
Contracting Officer's Representative Nelson Molina Contract Officer Representative202-322-9151 nelson.molina@ice.dhs.gov	**HSSEDI Department Manager** [redacted] Department Manager [redacted]
Contract Officer [redacted] Contract Officer Office of Acquisition Management (OAQ) [redacted]	.**HSSEDI Contracts Lead/Manager** [redacted] Contracts Lead [redacted]
Suitability/Fitness Point of Contact [redacted] Division Chief Personnel Security Division [redacted]	**HSSEDI Security Staff** [redacted] Senior Personnel Security Specialist [redacted]