Performance Work Statement

FOR

ENTERPRISE SERVICES TRANSFORMATION

AT

U.S. IMMIGRATION AND CUSTOMS ENFORCEMENT

Table of Contents

Section I

1.0 Description of Services

1.1 General

U.S. Immigration and Customs Enforcement (ICE) was established within the Department of Homeland Security (DHS) in 2002 through a merger of the investigative and interior enforcement elements of the former U.S. Customs Service and the Immigration and Naturalization Service. With more than 20,000 law enforcement and support personnel in over 400 offices across the United States and around the world, ICE protects our country from national security and public safety threats by enforcing immigration and customs laws.

1.1.1 Background

ICE's mission success relies on effective delivery and implementation of its enterprise services, including human resources (position management and hiring), facilities management, asset management, budget formulation and execution, enterprise risk management, enterprise requirements development, Freedom of Information Act compliance, and leadership and career development. ICE's enterprise services mechanisms are decentralized, lacking integration, and largely non-standardized with respect to distribution of roles and responsibilities, processes, and use of technology. These services are implemented by all programs throughout the agency, both in headquarters and ICE's field offices, across a varied and complex range of mission spaces by personnel with diverse skillsets and competencies.

ICE's mission requirements and resources have grown but growth in the agency's enterprise services – its mission-enabling functions – have not kept pace. Recognizing that the current state of ICE's enterprise services is not optimal, ICE launched the Enterprise Transformation Initiative (ETI)—a multi-year effort to strategically transform the way ICE delivers enterprise services worldwide. ETI's primary objectives are to increase the effectiveness and efficiency of the full range of ICE's enterprise services in phases by diagnosing root causes of systemic challenges and developing and implementing strategies for sustained improvement.

To achieve ETI's goals, ICE requires highly specialized, expert consultation and support informed by extensive experience successfully partnering with similarly-scaled corporations and agencies to develop and implement transformational strategies and implementation plans to resolve highly complex challenges involving and impacting the entire organization. Success requires strategies and actionable plans that: focus on people, process, and technology; reflect an understanding of ICE's culture(s) and address culture-informed change management as a cornerstone; translate and incorporate best practices and lessons learned from all sectors; maximize use of ICE's personnel resources; and enable ICE to harness data to measure, plan, decide, and continuously improve in a fully integrated manner.

1.2 Scope

ICE seeks strategic partnership and wraparound support to thoroughly assess its enterprise services and design and execute comprehensive strategies that sustainably improve operational effectiveness; create and sustain data-driven decision making; accelerate solution implementation; enhance stakeholder relationships; and manage enterprise risks.

ICE has almost completed its first assessment focused on position management and hiring and is currently working toward building a blueprint to improve those functions, with expected delivery of a near-final draft on September 11, 2024. This activity does not scratch the surface of the step transformation needed at ICE for the remaining enterprise services, nor does it address change management, which ICE anticipates will be exceedingly complex.

Program Goals: To optimize the delivery and implementation of ICE's mission-enabling enterprise services. ICE intends to examine all aspects of its enterprise services, inclusive of organizational design, roles and responsibilities, processes, and technology and determine and implement needed changes to sustainably increase overall effectiveness.
Program Efficiencies (possible change): ICE has established a governance framework for the program to secure ongoing executive and senior-level awareness, collaboration, and participation in decision-making. The two governance bodies are operable and have the potential to be instrumental in the agency's successful transformation, especially with respect to change management, with some focused maturation.
Change Areas: This transformation effort will bring step change to every program in the agency. Changes are likely needed with respect to distribution of roles and responsibilities, resource alignment, technology, and processes throughout the enterprise. ICE anticipates an emphasis on culture change – specifically, improving the psychosocial environment – will be a focus area, as well.
Program Risks: The consequences of failure are a compromised ability to accomplish the ICE mission, low morale, recruiting and retention challenges, erosion of public confidence, compromised stakeholder relationships, and an inability to advocate for ICE's needs. The most significant risk to the ETI currently centers on change management. The ETI program office needs expert, deeply experienced partnership and support to reliably foster the conditions for the agency to adopt lasting change; maintain interest and momentum for transformation during protracted assessment and recommendations development processes; navigate fears of "losing" as a result of this effort; and keep agency executives and personnel engaged and informed at the right levels and the right times. The ETI program office also has a lack of dedicated personnel and relies predominantly on contractor support to accomplish the full range of its objectives; lack of expertise and lack of continuity in personnel are significant risks.

Due to the dynamic nature of transformations, modifications to increase the level of support are highly likely. The contractor should be prepared to increase support based on the needs of the Government. Any increase in scope will have to be determined fair and reasonable.

Section II

2.0 Problem Statement

ICE's enterprise services mechanisms are not optimized to effectively support the agency's mission requirements. These services are implemented by all programs throughout the agency, both in headquarters and ICE's field offices, across a varied and complex range of mission spaces by personnel with diverse skillsets and competencies. The functions are lacking

integration and largely non-standardized with respect to distribution of roles and responsibilities, processes, and use of technology.

The Contractor shall provide all services, materials, supplies, equipment, travel, and project supervision, as required in connection with this Performance Work Statement (PWS).

2.1 Applicable Regulations

In addition to federal laws, regulations, and policies generally applicable to federal executive agencies, ICE is subject to DHS directives, which, in some cases, prescribe delegated authorities, processes and constraints.

2.2 Objective(s)

ICE's overarching objective is to design and execute strategies and plans to demonstrably and sustainably improve its enterprise services.

2.2.1 Mandatory Assessment Period (Maximum 60 days from contract award)

The contractor shall complete an assessment of the program to ensure the proposed solution is the most advantageous. After completing the assessment, the contractor can make a one-time adjustment to the proposed solution with up to 15% increase or unlimited decrease in price or tasks. Contractor shall meet with both enterprise services governance bodies to understand leadership priorities, objectives, current strengths and improvement areas Enterprise Transformation Initiative (ETI) seeks to address.

- Contractor shall begin analysis of cultural psychosocial environment to inform change management strategy.
- Contractor shall deliver assessment brief.

2.2.2 Change Management Strategy and Support

ICE requires a change management strategy and hands-on execution support to ensure the agency's people and culture are ready, willing, and able to adopt the changes necessary to improve ICE's enterprise services, beginning with position management and hiring capabilities. It is critical that its culture and protocols enable sustained improvement.

- Contractor shall host a kick-off meeting with ICE senior leadership and ETI governance bodies to understand leadership priorities, objectives, current strengths, and improvement areas the Enterprise Transformation Initiative (ETI) seeks to address.
- Contractor shall host a kick-off meeting with FFRDC study leadership to gather information and understand ICE current state for position management and hiring initiatives.
- Contractor shall gather and review the FFRDC, draft blueprint, progress reports and preliminary data and other relevant background materials.
- Contractor shall initiate the development a draft change management strategy for the position management and hiring enterprise function utilizing the draft blueprint, progress reports, and preliminary data gathered from the FFRDC study and other discrete position management and hiring transformation efforts underway within various program offices (e.g., Office of the Chief Information Officer, Office of Human Capital, Office of the Chief Financial Officer). The change management strategy will be adaptable to other enterprise service transformation efforts.

- Contractor shall review the FFRDC draft blueprint and create the draft change management strategy.
- Contractor shall incorporate revisions and deliver the final change management strategy.
- Contractor shall update the final change management strategy based on receipt of the final blueprint (if required).
- Contractor shall develop a strategic communication plan as part of the change management strategy for informing employees about the change, the goals of the position management and hiring transformation strategy, and resources to assist them with during the transition.
- Contractor shall launch the position management and hiring change management and strategic communication plan to build stakeholder awareness, buy-in, and adoption.
- Contractor shall provide ongoing change management support as part of the transformation plan and implementation support execution.

2.2.3 Transformation Plan and Implementation Support – Position Management and Hiring

ICE requires a plan for socializing and obtaining feedback from senior leadership on its draft blueprint to improve position management and hiring, which ICE will receive on September 11, 2024, designed to ensure ICE is able to finalize the blueprint by December 11, 2024. ICE also requires a detailed transformation plan containing specific actions the contractor will derive from recommendations contained in the blueprint, and that incorporates the Change Management Strategy described in Objective 2.2.2. ICE expects its blueprint to be comprehensive; however, the transformation plan may also include additional actions the contractor determines beneficial to ICE's transformation.

- Contractor shall meet with the ETI governance bodies in the lead up to the receipt of the draft blueprint to identify key stakeholders for socializing the blueprint.
- Contractor shall create a senior leadership socialization and feedback plan with ETI governance bodies and ICE leadership.
- Contractor shall conduct feedback sessions following the draft release of blueprint.
- Contractor shall conduct an environmental scan to understand relevant position management and hiring regulations, policies, and directives, including ongoing initiatives, dynamics, and technology advances.
- Contractor shall develop a draft transformation plan incorporating the draft blueprint recommendations and feedback from socialization sessions. The plan will be in compliance with ongoing regulations, policies, and directives and include designated workstreams, priorities, and timelines.
- Contractor shall develop draft key performance indicators (KPIs) for measuring success of the transformation initiative utilizing qualitative and quantitative methods with associated benchmarks and targets.
- Contractor shall solicit feedback from the draft transformation plan and KPIs from ICE Leadership and ETI governance bodies to identify strategic priorities, validate timelines, prepare communications, deconflict initiatives, and review objectives outlined in the transformation plan and KPIs and submit final deliverables.
- Contractor shall incorporate draft revisions and deliver final transformation plan.

- Contractor shall support implementation activities in accordance with the developed transformation plan.
- Contractor shall monitor KPIs and regularly report progress.

Optional Tasks: The following objectives should be included in optional CLINs. Each of the remaining enterprise services – facilities management, asset management, budget formulation and execution, enterprise risk management, enterprise requirements development, Freedom of Information Act compliance, and leadership and career development – can be addressed separately or together for purposes of structuring the optional CLINs. The number and structure of optional CLINs will be based on the contractor's proposed solution. The optional CLINs will be exercised depending on the availability of funding.

2.2.4 Assessment of Current (As-Is) State (*Other Enterprise Services – Optional Tasks*)

ICE requires comprehensive assessments of its remaining enterprise service capabilities: facilities and asset management, budget formulation and execution, enterprise risk management, enterprise requirements development, Freedom of Information Act compliance, and leadership and career development. The assessments should cover the full complement of factors agency-wide that affect the efficacy of these functions including but not necessarily limited to people, process, data, and technology. The assessments should also fully consider inter-agency and other external factors and equities.

- Contractor shall analyze the current state of ICE as it relates to its six remaining enterprise service capabilities with a focus on people, process, data, and technology practices.
- Contractor shall complete an environmental scan to understand relevant regulations, policies and directives, ongoing DHS or governmentwide initiatives and macro trends such as global migration patterns, technology advances, and policy changes.
- Contractor shall analyze inter-agency relationships, including relationships with stakeholders, program offices, and other federal agencies. This may be done via document review, process reviews, or stakeholder interviews.
- Contractor shall categorize the findings produced in the current state assessment into key focus areas including people and the distribution of roles and responsibilities and resource alignment, processes, data, and technology.
- Contractor shall synthesize findings into assessment briefing with supplemental data, analysis, and insight.
- Contractor shall produce a Current State Assessment, detailing the focus areas, data, findings, and insights produced by the current state analysis.

2.2.5 Definition of Future (To-Be) State (*Other Enterprise Services – Optional Tasks*)

ICE requires defined realistic future states for its remaining enterprise services that reflect industry and government standards and best practices; take into account any and all relevant assignments of authorities; address the full scope of changes necessary to organizational design, processes, and technology that will enable ICE both to maximize resources and fully meet mission demands; improve customer experience; enable enduring business process governance,

continuous improvement, and data-driven decision-making; and allow the agency to measure and monitor organizational performance.

- Contractor shall develop a list of recommendations to enhance the future state of ICE's enterprise functions.
- Contractor shall identify similar scaled commercial companies and federal agencies and document best practices.
- Contractor shall confirm relevancy of best practices to ICE and ICE's mission with ETI Advisory Committee.
- Contractor shall conduct workshops with relevant stakeholders to validate proposed future state.
- Contractor shall conduct workshops to co-create the Definition of Future State.
- Contractor shall develop a Definition of Future State that incorporates opportunities to streamline the service delivery model while improving mission efficiencies and outcomes.
- Contractor shall recommend updates or identify new performance metrics to inform performance tracking, monitoring, and continuous improvement of the transformation efforts.

2.2.6 Transformation Strategy (*Other Enterprise Services – Optional Tasks*)

ICE requires transformation strategies from current state to future state for its remaining enterprise services. The strategies should address the full scope of factors affecting ICE's ability to successfully implement enterprise services. The strategies should also address culture and change management, demonstrate return on investment, map out applicable qualitative and quantitative measures and metrics and evaluation methodologies; should be informed by and integrated with related efforts across the broader DHS enterprise; and should ensure ICE is effectively engaging with key external stakeholders.

- Contractor shall conduct a gap analysis between the current state and desired future state vision for each of the ETI initiatives.
- Contractor shall co-create with ICE leadership a draft initial list of potential change activities.
- Contractor shall ensure list of potential change initiatives are in compliance with broader DHS enterprise and government wide regulations and initiatives.
- Contractor shall develop a level of effort and level of impact estimate for each potential change activity.
- Contractor shall work with ICE leadership to refine and validate the prioritized initiatives based on perceived value and return on investment in alignment with ICE defined future state.
- Contractor shall develop draft key performance indicators (KPIs) for measuring success of the transformation initiative utilizing qualitative and quantitative methods with associated benchmarks and targets.
- Contractor shall develop a change management strategy based on the proposed change initiatives with a focus on sustained improvement.
- Contractor shall develop a communications plan to build stakeholder awareness and adoption.
- Contractor shall deliver the Transformation Strategy outlining the changes needed across people, processes, data, and technology to improve mission efficiencies.

2.2.7 Implementation Plan and Support (*Other Enterprise Services – Optional Tasks*)

ICE requires detailed implementation plans for the transformation strategies delivered under Objective 2.2.6 that identify and prioritize specific actions and define timelines, milestones, dependencies, and other elements needed to fully and successfully implement the transformation strategies. ICE also requires comprehensive implementation support.

- Contractor shall develop and deliver an implementation plan that includes multi-year timelines, key milestones, dependencies, and intended outcomes for prioritized activities.
- Contractor shall validate the implementation plan with ICE leadership.
- Contractor shall stand-up a program management office (PMO) with government and contractor resources to manage the implementation plan, maintain implementation dashboards, coordinate stakeholders and activities, and facilitate the Transformation Strategy
- Contractor shall provide implementation support in accordance with the implementation plan.
- Contractor shall monitor KPIs and regularly report progress.
- Contractor shall develop performance dashboards to track progress, performance, and risks, issues, and opportunities (RIOs).

2.3 Final Outcome

ICE will have executed effective change management strategies to sustainably improve its enterprise services. ICE will also have implemented a comprehensive plan that demonstrably improves its position management and hiring functions and will have clear and implementable mechanisms for measuring the effectiveness of these functions. Finally, subject to funds availability, ICE will have implemented transformation strategies that will demonstrably and sustainably improve its other enterprise services.

- Contractor shall develop a draft and final sustainability report.
- Contractor shall package all deliverables in accordance with PWS and submit package to ICE for final review and feedback.
- Contractor shall revise deliverables based on feedback from ICE.
- Contractor shall package all deliverables in accordance with PWS and submit package to ICE for final approval and acceptance.
- Contractor shall brief any additional ICE leadership and stakeholders on the results from the project.
- Contractor shall conduct any additional project closeout activities that ICE requires.

Appendix A. SOO Sections 3.0 through 7.0

SECTION III

3.0 PERFORMANCE THRESHOLDS

All deliverables and performance that fall below the outlined thresholds below will be re-performed at no cost to the Government. Any task, performance, or deliverable(s) that is not corrected greater than 95% acceptance for accuracy and timeliness will be reflected negatively on the contractor's past performance. Any task or deliverable that is corrected at a level higher than 95% for accuracy and timeliness will be reflected positively on the contractor's performance.

Performance Objective	SOO Paragraph	Performance Threshold	Method of Surveillance
SS – 1 Performance Metrics	2.2	The contractor shall establish a baseline with objective criteria to measure transformation progression. This is an iterative process. Changes are expected along the transformation journey. These metrics will be re-assed at the mid-point of the determined transformation timeline. The final Performance Metrics will provide the Government with a way to clearly measure transformation success/failure and how to minimally maintain the change and/or adjust based on the performance metrics put in place.	100% Surveillance
SS – 2 Program Assessment	2.2.1	The contractor shall complete an assessment of the program to ensure the proposed solution is the most advantageous.	100% Surveillance
SS – 3 Change Management Strategy and Support	2.2.2	The contractor shall provide a comprehensive change management strategy and hands-on, ongoing execution support that enables ICE to be successful in transforming its enterprise services.	100% Surveillance
SS – 4 Transformation Plan and Implementation Support – Position Management and Hiring	2.2.3	The contractor shall provide a plan for socializing and obtaining feedback from senior leadership on its draft blueprint to improve position management and hiring, which ICE will receive on	100% Surveillance

		September 11, 2024, to support ICE's finalization of its blueprint by December 11, 2024. The contractor shall also provide a detailed transformation plan that the agency can realistically implement using, at minimum, the blueprint and Change Management Strategy, and provide comprehensive support to ICE to successfully implement the plan.	
SS – 5 Assessment of Current (As-Is) State	2.2.4	The contractor shall provide a comprehensive assessment of ICE's remaining enterprise service capabilities that covers the full complement of agency-wide factors affecting successful implementation.	100% Surveillance
SS – 6 Future State Definition	2.2.5	The contractor shall provide a definition of a realistic future state for ICE's remaining enterprise services that considers the complexities referenced and others ICE may not be aware of.	100% Surveillance
SS – 7 Transformation Strategy	2.2.6	The contractor shall provide a comprehensive strategy to transform ICE's remaining enterprise services from the current state to the defined future state.	100% Surveillance
SS – 8 Implementation Plan and Support	2.2.7	The contractor shall provide detailed, realistic implementation plans for each transformation strategy and shall provide comprehensive support to ICE to successfully implement the plans.	100% Surveillance
SS – 6 Sustainability	2.3	At the end of the performance period, the contractor will have helped ICE to measurably and sustainably improve its position management and hiring functions. Further, if optional tasks are exercised, the contractor will have helped ICE to measurably and sustainably improve its remaining enterprise services.	100% Surveillance

SECTION IV

4.0 DELIVERABLES / ACCEPTANCE CRITERIA

The Contractor shall provide deliverable(s) in a format mutually agreed upon by the Government and the Contractor. The following deliverables are not expected to change. Due date intervals are not expected to change but actual dates may need to be revised depending on actual contract start date.

Deliverables and Performance are not considered acceptable until the Government provides written notice of acceptance. This can be in the Monthly Status Report (bi-lateral signatures from the contractor and COR) and/or written acceptance via email.

Contractor proposed timeline best suited to meet the requirement.

DELIVERABLE – Acceptance Criteria	DUE DATE	SOO Paragraph	DELIVERY METHOD
Assessment Brief – acceptable when the briefing provides defendable recommendations to update/change the initial solution	NLT 60 days after award	2.2.1	By email to COR in PowerPoint/PDF briefing format
Performance Metrics – acceptable when the performance measures are objective, executable, traceable, repeatable, and reliant on authoritative data	DRAFT 1 – NLT 60 days after award DRAFT 2 – NLT 30 days after mid-point of performance FINAL – NLT 30 days prior to end of task order period of performance	2.2	By email to COR in mutually agreed upon format
Change Management Strategy	DRAFT – NLT 30 days after receipt of the draft blueprint (expected September 11, 2024) FINAL – NLT 40 days after receipt of the draft blueprint (expected September 11, 2024)	2.2.2	By email to COR in mutually agreed upon format.

	UPDATE (if needed) – NLT 10 days after receipt of the final blueprint (expected December 11, 2024)		
Change Management Support	Ongoing	2.2.2	Direct support to ETI Program Management Office
Blueprint Senior Leadership Socialization and Feedback Plan	DRAFT – NLT 10 days after award. FINAL – NLT 13 days after award	2.2.3	By email to COR in mutually agreed upon format
Transformation Plan – Position Management and Hiring	DRAFT – NLT 30 days after receipt of draft blueprint (expected September 11, 2024) FINAL – NLT 40 days after receipt of draft blueprint (expected September 11, 2024) UPDATE (if needed) – NLT 10 days after receipt of final blueprint (expected December 11, 2024)	2.2.3	By email to COR in mutually agreed upon format
Implementation Support – Position Management and Hiring	Ongoing	2.2.3	Direct support to ETI Program Management Office
Assessment of Current (As-Is) state – Other Enterprise Services (Optional Task)	NLT 45 days after applicable Optional CLIN is exercised.	2.2.4	By email to COR in mutually agreed upon format
Definition of Future (To-Be) State – Other Enterprise Services (Optional Task)	NLT 45 days after Optional CLIN is exercised.	2.2.5	By email to the COR in mutually agreed upon format
Transformation Strategy – Other Enterprise Services (Optional Task)	NLT 30 days after delivery of Definition	2.2.6	By email to the COR in mutually agreed upon format

	of Future (To-Be) State		
Implementation Plan – Other Enterprise Services (Optional Task)	NLT 30 days after delivery of Transformation Strategy	2.2.7	By email to the COR in mutually agreed upon format
Implementation Support – Other Enterprise Services (Optional Task)	Ongoing	2.2.7	Direct support to ETI Program Management Office
Final Sustainability Report	DRAFT 1 – NLT 60 days prior to end of task order period of performance FINAL - NLT 30 days prior to end of task order period of performance	2.3	By email to the COR in PDF format

Several deliverables are required and described in the IDIQ Scope and Ordering Guide such the Monthly Status Report, Trip Report, etc. DO NOT repeat deliverables already required

SECTION V

5.0 TIMELINE, STAKEHOLDER (collaborating offices)

5.1 Timeline. Contractor proposed timeline best suited to meet the requirement.

5.2 Stakeholders (Collaborating Offices).

ICE carries out its mission through three operational directorates—Enforcement and Removal Operations (ERO), Homeland Security Investigations (HSI), and the Office of the Principal Legal Advisor (OPLA). A fourth directorate—M&A—supports the three operational branches to advance the ICE mission. The Office of Professional Responsibility (OPR) is responsible for upholding the agency's professional standards.

Enforcement and Removal Operations (ERO) enforces our Nation's immigration laws by identifying, arresting, detaining, and removing criminal noncitizens and those subject to removal. To ensure the national security and public safety of the United States, ICE law enforcement officers take enforcement actions against individuals present in the United States in violation of immigration law.

Homeland Security Investigations (HSI) conducts criminal investigations to protect the United States against terrorists and other transnational criminal organizations (TCOs) through criminal and civil enforcement of Federal laws governing border control, customs, trade, and immigration.

Office of the Principal Legal Advisor (OPLA) is the largest legal component within DHS working in 83 locations throughout the United States and at ICE Headquarters. OPLA serves as the exclusive representative of DHS in immigration removal proceedings before the Executive

Office for Immigration Review (EOIR), litigating all removal cases including those against criminal noncitizens, terrorists, and human rights abusers.

Office of Professional Responsibility (OPR): OPR is responsible for upholding ICE's professional standards through a multi-disciplinary approach of security, inspections, and investigations. OPR is responsible for ICE's entire security portfolio, conducting independent reviews of ICE programs and operations, impartially investigating allegations of criminal and/or serious misconduct and other wrongdoing impacting ICE personnel and operations, as well as internal and external threats.

Management and Administration (M&A): M&A governs all administrative and managerial lines of business and components to strategically address the administrative challenges faced in today's law enforcement environment, while keeping pace with the dynamic growth in other ICE programs to most effectively meet ICE mission requirements, address customer needs and ensure sound stewardship of ICE resources in accordance with all legal, regulatory and policy requirements.

The eight M&A subordinate functional offices are as follows:

Office of Acquisition Management (OAQ): Partners with internal and external organizations to deliver quality acquisition solutions and serves as a strategic asset dedicated to improving overall business performance in support of ICE's mission.

Office of Asset and Facilities Management (OAFM): Maximizes the operational and mission support value of assets, including fleet and facilities, through cost-effective life-cycle management and fostering a positive culture of safety and occupational health.

Office of the Chief Financial Officer (OCFO): Provides effective and efficient management of ICE resources by implementing best business practices and linking strategic planning, budgeting, and performance reporting to financial decision-making.

Office of the Chief Information Officer (OCIO): Delivers innovative information technology and business solutions that enable ICE to protect and secure our nation.

Office of Human Capital (OHC): Positions ICE for successful mission completion by recruiting and hiring high-performing talent and by delivering human capital programs that support employee engagement and wellness.

Office of Information Governance and Privacy (OIGP): Oversees the management, sharing, protection, and disclosure of ICE data and information in accordance with law, policy, and standards. IGP implements the Freedom of Information Act (FOIA) and collaborates with ICE and DHS partners to build privacy protections into ICE programs and systems and develops data governance solutions.

Office of Investment and Program Accountability (OIPA): Develops, implements, and oversees ICE acquisition management processes, policies, and procedures, and coordinates across DHS to support and align acquisition program execution activities and oversight.

Office of Leadership and Career Development (OLCD): Delivers quality training and professional development opportunities that build on and enhance employee knowledge, skills, and abilities, preparing them to perform their duties at the highest level.

M&A is also supported by the Office of the Strategic Resourcing Advisor (SRAD), which serves as the primary mission support apparatus assisting M&A leadership with executive oversight, prioritization, resource management, and strategic direction for the Mission Support program, project, or activity (PPA) resources. Similarly, HSI, ERO, OPLA and OPR each have their own mission support directorates that provide the same services to their respective programs in coordination with M&A's eight functional offices. These mission support directorates vary in organizational structure and staffing levels, functions performed, procedures and processes, and in some cases policies that are specific to their mission requirements.

Additionally, ICE works directly with the Department of Homeland Security (DHS) Headquarters and its corresponding Management Directorate (MD) offices, such as the Office of the Chief Human Capital Officer (OCHCO).

SECTION VI

6.0 GENERAL INFORMATION

In support of the DHS/ICE mission, the identified tasks and/or outputs may take the form of information, advice, opinions, alternatives, analyses, evaluations, training, processes to eliminate waste, standardize best practices, reduce cycle times and reduce the cost of doing business, or recommendations to complement the Government's technical expertise in accomplishing its mission and day-to-day activities. The contractor shall provide a work force possessing the skills, knowledge and training to satisfactorily perform the services required under this contract. The primary work location for contractor personnel will be at ICE HQ in Washington, DC. Other CONUS work locations or travel will rarely be required.

Contractor employees performing services under this contract shall be controlled, directed and supervised at all times by management personnel of the contractor. The contractor's management shall ensure that employees properly comply with the performance standards outlined in this Performance Work Statement and as required by the contracting officer or the contracting officer's representative (COR). Contractor employees shall be capable of performing independently and without the assistance of Government personnel. Actions of contractor employees shall not be interpreted or implemented in any manner which results in a contractor employee creating, modifying or violating Federal policy, obligating the appropriated funds of the U.S. Government, overseeing the work of Federal employees, providing direct personal services to any Federal employee or otherwise violating the prohibitions set forth in Parts 7.5 and 37.1 of the Federal Acquisition Regulation (FAR). If the contractor feels that any actions constitute or are perceived to constitute personal services, it shall be the contractor's responsibility to notify the COR immediately.

No contractor personnel will perform any work on this contract that can be defined as inherently governmental according to FAR Subpart 7.503(c). Contractor personnel will be performing tasks under FAR Subpart 7.503(d); however, contract personnel will be in a

supporting role to the Government task lead and will not be in a decision-making role. The Government will be the sole authority for decisions.

6.1 Location

Regular onsite support will be required at ICE HQ located at Potomac Center North (PCN) 500 12th St SW, Washington, DC 20024. Telework is permitted, though both regular and ad hoc on-site presence in ICE facilities in Washington, DC will be required.

6.2 Travel (TDYs)

Below are the known travel requirements at this time. In the event travel additional travel is required, the Government will modify the contract to increase the price to cover travel. Price shall be determined fair and reasonable.

Location	Dates	Max Contractor Participants
[redacted]	Once per year	4

6.3 Identify Known or Possible Conflicts of Interest

The contractor is not expected to have access to data that can be perceived as competition sensitive contract information or support the development of acquisition strategies.

Performance on any of the task orders awarded under the Air Force Strategic Transformation Support contract MAY, by definition in FAR 9.5, be a Conflict of Interest as either Impaired Objectivity or Unfair Competitive Advantage (unequal access to information). Due to the unknown task requests, it is impossible to complete a focused OCI plan at the IDIQ level; however, if vendors either during the TOPR process, during the performance of a task order, or at any time become aware of an OCI, they shall immediately inform the Contracting office. This may result in a work stoppage until (if) the OCI can be neutralized or mitigated. If it cannot, the task order will be terminated immediately and re-competed. If a vendor does not inform the Contracting officer of an OCI that it has been made aware of, the Contracting office may terminate the task order, may remove the vendor as an AFSTS awardee, or request debarment.

If an OCI is discovered during the TOPR process, provide (in writing) the nature of the OCI and why the OCI is precluding the vendor from proposing. The CO will determine if the OCI is mitigated and provide a response in writing, notifying the vendor if they are exempt from the offering. If the vendor is exempted from submitting by the CO, it does not count toward the vendor's annual “no-bid” limit. If the CO does not exempt the vendor, the vendor is required to propose. If the vendor determines not to offer, it will be counted as a “no-bid” against the vendor's annual “no-bid” limit.

6.4 Security and Training Requirements

This Order is unclassified and 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)

The full security and training details are found in Appendix 1 below – Section 7.3. There are three referenced training requirements in the security language:

1) Security Training Requirements.

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) 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.

3) Cybersecurity Awareness Training (CSAT) will be required upon initial access and annually thereafter. CSAT training will be provided by the appropriate component agency of DHS. Contractor employees, who are involved with management, use, or operation of any IT systems that handle sensitive information within or under the supervision of the Department, shall receive periodic training at least annually in security awareness and accepted security practices, systems rules of behavior, to include Unauthorized Disclosure Training, available on the ICE Training System (ITS) or by contacting [redacted]. Contractor employees with significant security responsibilities shall receive specialized training specific to their security responsibilities annually. The level of training shall be commensurate with

the individual's duties and responsibilities and is intended to promote a consistent understanding of the principles and concepts of telecommunications and IT systems security.

6.5 Data Rights

The copies of any Contractor generated records, files, documents, data, and work papers, provided to the Government in performance of this task order shall become and remain Government property and shall be maintained and disposed of IAW Air Force Manual 33-363, Management of Records, and are disposed of in accordance with the Air Force Records Disposition Schedule which is located in the Air Force Records Information Management System; and other regulations, as applicable. The copies of any Government generated records, files, documents, data, and work papers, provided to the Contractor in performance of this task order, or derivatives thereof, are and shall remain Government property, and shall be returned to the Government at the completion of this contract. Software licensing terms shall not conflict with Federal law or regulation. In according with the Defense Federal Acquisition Regulation Supplement 239.7602-1, "DoD shall acquire cloud computing services using commercial terms and conditions that are consistent with Federal law, and an agency's need. Contracting officers shall incorporate any applicable service provider terms and conditions into the contract by attachment or other appropriate mechanism." The Government shall not be bound by any licensing terms or other restrictions on the use, modification, reproduction, release, performance, or disclosure of software not incorporated by attachment or other appropriate mechanism.

SECTION VII

7.0 APPENDIX 1

7.1 DEFINITIONS, ABBREVIATIONS, AND ACRONYMS

Contracting Officer (CO). The duly appointed Government agent authorized to award or administer contracts. The contracting officer is the only person authorized to contractually obligate the Government.

Statement of Objective (SOO). A formal contracting document used to describe the goals and objectives expected from soliciting contractor work.

Organizational Conflict of Interest (OCI). Unequal access and competitive advantage are two conflicts that the government is aware of that could result from Non-Financial Recommendations (NFR) Performance Threshold. The minimum performance level of a performance objective required by the Government.

7.2 ACRONYMS

Enterprise Transformation Initiative (ETI)

Enforcement and Removal Operations (ERO)

Homeland Security Investigations (HSI)

Office of the Principal Legal Advisor (OPLA)

Management & Administration (M&A)

Office of Professional Responsibility (OPR)

Management and Administration (M&A)

Office of Acquisition Management (OAQ)

Office of Asset and Facilities Management (OAFM)

Office of the Chief Financial Officer (OCFO)

Office of the Chief Information Officer (OCIO)

Office of Human Capital (OHC)

Office of Information Governance and Privacy (OIGP)

Office of Investment and Program Accountability (OIPA)

Office of Leadership and Career Development (OLCD)

Strategic Resourcing Advisor (SRAD)

INFORMATION TECHNOLOGY SECURITY AWARENESS TRAINING (JULY 2023)

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

(b) *Security Training Requirements*.

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

Subsequent training certificates to satisfy the annual training requirement shall be submitted to the COR via e-mail notification not later than October 31st of each year. The e-mail notification shall state the required training has been completed for all Contractor and subcontractor employees.

(2) The DHS Rules of Behavior apply to every DHS employee, Contractor and subcontractor that will have access to DHS systems and sensitive information. The DHS Rules of Behavior shall be signed before accessing DHS systems and sensitive information. The DHS Rules of Behavior is a document that informs users of their responsibilities when accessing DHS systems and holds users accountable for actions taken while accessing DHS systems and using DHS Information Technology resources capable of inputting, storing, processing, outputting, and/or transmitting sensitive information. The DHS Rules of Behavior is accessible at http://www.dhs.gov/dhs-security-and-training-requirements-contractors. Unless otherwise specified, the DHS Rules of Behavior shall be signed within thirty (30) days of contract award. Any new Contractor employees assigned to the contract shall also sign the DHS Rules of

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

(End of clause)

PRIVACY REQUIREMENTS FOR CONTRACTOR AND PERSONNEL

In addition to FAR 52.224-1 Privacy Act Notification (APR 1984), 52.224-2 Privacy Act (APR 1984), FAR 52.224-3 Privacy Training (JAN 2017), and HSAR Clauses, the following instructions must be included in their entirety in all contracts.

Limiting Access to Privacy Act and Other Sensitive Information

In accordance with FAR 52.224-1 Privacy Act Notification (APR 1984), and FAR 52.224-2 Privacy Act (APR 1984), if this contract requires contractor personnel to have access to information protected by the Privacy Act of 1974, the contractor is advised that the relevant DHS system of records notices (SORNs) applicable to this Privacy Act information may be found at https://www.dhs.gov/system-records-notices-sorns. Applicable SORNS of other agencies may be accessed through the agencies' websites or by searching GovInfo, available at https://www.govinfo.gov that replaced the FDsys website in December 2018. SORNs may be updated at any time.

Prohibition on Performing Work Outside a Government Facility/Network/Equipment

The Contractor shall perform all tasks on authorized Government networks, using Government-furnished IT and other equipment and/or Workplace as a Service (WaaS) if WaaS is authorized by the statement of work. Government information shall remain within the confines of authorized Government networks at all times. Except where telework is specifically authorized within this contract, the Contractor shall perform all tasks described in this document at authorized Government facilities; the Contractor is prohibited from performing these tasks at or removing Government-furnished information to any other facility; and Government information shall remain within the confines of authorized Government facilities at all times. Contractors may only access classified materials on government furnished equipment in authorized government owned facilities regardless of telework authorizations.

Prior Approval Required to Hire Subcontractors

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

Separation Checklist for Contractor Employees

Contractor shall complete a separation checklist before any employee or Subcontractor employee terminates working on the contract. The separation checklist must verify: (1) return of any Government-furnished equipment; (2) return or proper disposal of sensitive personally

identifiable information (PII), in paper or electronic form, in the custody of the employee or Subcontractor employee including the sanitization of data on any computer systems or media as appropriate; and (3) termination of any technological access to the Contractor's facilities or systems that would permit the terminated employee's access to sensitive PII.

In the event of adverse job actions resulting in the dismissal of an employee or Subcontractor employee, the Contractor shall notify the Contracting Officer's Representative (COR) within 24 hours. For normal separations, the Contractor shall submit the checklist on the last day of employment or work on the contract.

As requested, contractors shall assist the ICE Point of Contact (ICE/POC), Contracting Officer, or COR with completing ICE Form 50-005/Contractor Employee Separation Clearance Checklist by returning all Government-furnished property including but not limited to computer equipment, media, credentials and passports, smart cards, mobile devices, PIV cards, calling cards, and keys and terminating access to all user accounts and systems.

Contractor's Commercial License Agreement and Government Electronic Information Rights

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

(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, Pub. L. 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 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, and 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.

(g) Before receiving access to IT resources under this contract the individual must receive a security briefing, which the Contracting Officer's Technical Representative (COTR) will arrange and complete any nondisclosure agreement furnished by DHS.

(h) The Contractor shall have access only to those areas of DHS information technology resources explicitly stated in this contract or approved by the COTR in writing as necessary for performance of the work under this contract. Any attempts by Contractor personnel to gain access to any information technology resources not expressly authorized by the statement of work, other terms and conditions in this contract, or as approved in writing by the COTR, is strictly prohibited. In the event of violation of this provision, DHS will take appropriate actions with regard to the contract and the individual(s) involved.

(i) Contractor access to DHS networks from a remote location is a temporary privilege for mutual convenience while the Contractor performs business for the DHS Component. It is not a right, a guarantee of access, a condition of the contract, or Government Furnished Equipment (GFE).

(j) Contractor access will be terminated for unauthorized use. The Contractor agrees to hold and save DHS harmless from any unauthorized use and agrees not to request additional time or money under the contract for any delays resulting from unauthorized use or access.

(k) Non-U.S. citizens shall not be authorized to access or assist in the development, operation, management or maintenance of Department IT systems under the contract, unless a waiver has been granted by the Head of the Component or designee, with the concurrence of both the Department's Chief Security Officer (CSO) and the Chief Information Officer (CIO) or their designees. Within DHS Headquarters, the waiver may be granted only with the approval of both the CSO and the CIO or their designees. In order for a waiver to be granted:

(1) There must be a compelling reason for using this individual as opposed to a U.S. citizen; and

(2) The waiver must be in the best interest of the Government.

(l) Contractors shall identify in their proposals the names and citizenship of all non-U.S. citizens proposed to work under the contract. Any additions or deletions of non-U.S. citizens after contract award shall also be reported to the Contracting Officer.

(End of clause)

Compliance with DHS Security Policy Terms and Conditions:

All hardware, software, and services provided under this task order must be compliant with *DHS 4300A DHS Sensitive System Policy and DHS 4300A Sensitive Systems Handbook.*

Security Review Terms and Conditions

The Government may elect to conduct periodic reviews to ensure that the security requirements contained in this contract are being implemented and enforced. The Contractor shall afford ICE, including the organization of ICE Office of the Chief Information Officer, the Office of the Inspector General, authorized Contracting Officer Representative (COR), and other government oversight organizations, access to the Contractor's facilities, installations, operations, documentation, databases and personnel used in the performance of this contract. The Contractor will contact ICE Chief Information Security Officer to coordinate and participate in the review and inspection activity of government oversight organizations external to ICE. Access shall be provided to the extent necessary 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 ICE data or the function of computer system operated on behalf of ICE, and to preserve evidence of computer crime.

Contractor IT Resource Access (Sep 2012)

1) Before receiving access to IT resources under this contract the individual must receive a security briefing, which the Contracting Officer's Representative (COR) will arrange, and complete any nondisclosure agreement furnished by DHS.

2) The Contractor shall have access only to those areas of DHS information technology resources explicitly stated in this contract or approved by the COR in writing as necessary for performance of the work under this contract. Any attempts by Contractor personnel to gain access to any information technology resources not expressly authorized by the statement of work, other terms and conditions in this contract, or as approved in writing by the COR, is strictly prohibited. In the event of violation of this provision, DHS will take appropriate actions with regard to the contract and the individual(s) involved.
3) Contractor access to DHS networks from a remote location is a temporary privilege for mutual convenience while the Contractor performs business for DHS Component. It is not a right, a guarantee of access, a condition of the contract, or Government Furnished Equipment (GFE).
4) Contractor access will be terminated for unauthorized use. The Contractor agrees to hold and save DHS harmless from any unauthorized use and agrees not to request additional time or money under the contract for any delays resulting from unauthorized use or access.
5) Non-U.S. citizens shall not be authorized to access or assist in the development, operation, management or maintenance of Department IT systems under the contract, unless a waiver has been granted by the Head of the Component or designee, with the concurrence of both the Department's Chief Security Officer (CSO) and the Chief Information Officer (CIO) or their designees. Within DHS Headquarters, the waiver may be granted only with the approval of both the CSO and the CIO or their designees. In order for a waiver to be granted:
    a) There must be a compelling reason for using this individual as opposed to a U. S. citizen; and
    b) The waiver must be in the best interest of the Government.
6) Contractors shall identify in their proposals the names and citizenship of all non-U.S. citizens proposed to work under the contract. Any additions or deletions of non-U.S. citizens after contract award shall also be reported to the contracting officer.

SECURITY REQUIREMENTS

GENERAL

The United States Immigration and Customs Enforcement (ICE) has determined that performance of the tasks as described in this contract requires that the Contractor, subcontractor(s), vendor(s), etc. (herein known as Contractor) have access to sensitive DHS information, and that the Contractor will adhere to the following.

PRELIMINARY FITNESS DETERMINATION

ICE will exercise full control over granting, denying, withholding, or terminating unescorted government facility and/or sensitive Government information access for Contractor applicants/employees, based upon the results of a Fitness screening process. ICE may, as it deems appropriate, authorize and make a favorable expedited preliminary Fitness determination based on preliminary security checks. The preliminary Fitness determination will allow the Contractor employee to commence work temporarily prior to the completion of a Full Field Background Investigation. The granting of a favorable preliminary Fitness shall not be considered as assurance that a favorable final Fitness determination will follow as a result thereof. The granting of preliminary Fitness or final Fitness shall in no way prevent, preclude, or bar the withdrawal or termination of any such access by ICE, at any time during the term of the

contract. No employee of the Contractor shall be allowed to enter on duty and/or access sensitive information or systems without a favorable Fitness determination by the Office of Professional Responsibility (OPR), Personnel Security Division (PSD). No employee of the Contractor shall be allowed unescorted access to a Government facility without a favorable Fitness determination by OPR PSD. Contract employees are processed under DHS Instruction 121-01-007-001, Personnel Security, Suitability and Fitness Program, dated June 14, 2017, or successor thereto; those having direct contact with Detainees will also have 6 CFR § 115.117 considerations made as part of the Fitness screening process. Sexual Abuse and Assault Prevention Standards implemented pursuant to Public Law 108-79 (Prison Rape Elimination Act (PREA) of 2003)).

BACKGROUND INVESTIGATIONS

Contractor employees (to include applicants, temporary, part-time and replacement employees) under the contract, needing access to sensitive information and/or ICE Detainees, shall undergo a position sensitivity analysis based on the duties each individual will perform on the contract. The results of the position sensitivity analysis shall identify the appropriate background investigation to be conducted. Background investigations will be processed through OPR PSD. Contractor applicant/employees are nominated by a Contracting Officer Representative (COR) for consideration to support this contract via submission of the DHS Form 11000-25 and ICE Supplement to the DHS Form 11000-25 to the PSD. This contract shall submit the following security vetting documentation to OPR PSD, through the COR, within 10 days of notification of initiation of an Electronic Questionnaire for Investigation Processing (e-QIP), or successor thereto, in the Office of Personnel Management (OPM) automated on-line system:

1. Standard Form 85P (Standard Form 85PS (with supplement to 85P required for those with direct contact with detainees or armed positions)), "Questionnaire for Public Trust Positions" form completed online and archived by the Contractor applicant/employee in their OPM e-QIP account.
2. Signature Release Forms (Three total) generated by OPM e-QIP upon completion of Questionnaire (e-signature recommended/acceptable). Completed online and archived by the Contractor applicant/employee in their OPM e-QIP account.
3. Electronic fingerprints taken at an approved facility OR two (2) SF 87 Fingerprint Cards (current revision) sent to OPR PSD. Additional information regarding fingerprints will be sent to the Contractor applicant/employee from OPR PSD.
4. Optional Form 306 Declaration for Federal Employment. This document is sent as an attachment in an e-mail to the Contractor applicant/employee from OPR PSD. Completed online and archived by the Contractor applicant/employee in their OPM e-QIP account.
5. If occupying PREA designated position: Questionnaire regarding conduct defined under 6 CFR § 115.117 (Sexual Abuse and Assault Prevention Standards). This document is sent as an attachment in an e-mail to the Contractor applicant/employee from OPR PSD. Completed online and archived by the Contractor applicant/employee in their OPM e-QIP account.
6. One additional document may be applicable if the Contractor applicant/employee was born abroad. If applicable, the document will be sent as an attachment in an e-mail to the Contractor applicant/employee from OPR PSD. Completed online and archived by the Contractor applicant/employee in their OPM e-QIP account.

Contractor employees who have an adequate, current investigation by another Federal Agency may not be required to submit complete security packages; the investigation may be accepted under reciprocity. The questionnaire related to 6 CFR § 115.117 listed above in item 5 will be required for positions designated under PREA.

An adequate and current investigation is one where the investigation was favorably adjudicated within 5 years and not to exceed 7 years, meets the contract risk level requirement, and applicant has not had a break in service of more than two years. (Executive Order 13488 amended under Executive Order 13764/DHS Instruction 121-01-007-01)

Required information for submission of security packet will be provided by OPR PSD at the time of award of the contract. Only complete packages will be accepted by OPR PSD as notified by the COR. To ensure adequate background investigative coverage, Contractor applicants/employees must currently reside in the United States or its Territories. Additionally, Contractor applicants/employees are required to have resided within the United States or its Territories for three or more years out of the last five (ICE retains the right to deem a Contractor applicant/employee ineligible due to insufficient background coverage). This timeline is assessed based on the signature date of the standard form questionnaire submitted for the applied position. Contractor employees falling under the following situations may be exempt from the residency requirement: 1) work or worked for the U.S. Government in foreign countries in federal civilian or military capacities; 2) were or are dependents accompanying a federal civilian or a military employee serving in foreign countries so long as they were or are authorized by the U.S.

Government to accompany their federal civilian or military sponsor in the foreign location; 3) worked as a Contractor employee, volunteer, consultant or intern on behalf of the federal government overseas, where stateside coverage can be obtained to complete the background investigation; 4) studied abroad at a U.S. affiliated college or university; or 5) have a current and adequate background investigation (commensurate with the position risk/sensitivity levels) completed for a Federal or Contractor employee position, barring any break in federal employment or federal sponsorship.

Only U.S. citizens and Legal Permanent Residents are eligible for employment on contracts requiring access to DHS sensitive information unless an exception is granted as outlined under DHS Instruction 121-01-007-001. Per DHS Sensitive Systems Policy Directive 4300A, only U.S. citizens are eligible for positions requiring access to DHS Information Technology (IT) systems or positions that are involved in the development, operation, management, or maintenance of DHS IT systems, unless an exception is granted as outlined under DHS Instruction 121-01-007-001.

CONTINUED ELIGIBILITY

ICE reserves the right and prerogative to deny and/or restrict facility and information access of any Contractor employee whose actions conflict with Fitness standards contained in DHS Instruction 121-01-007-01, Chapter 3, paragraph 6.B or who violate standards of conduct under 6 CFR § 115.117. The Contracting Officer or their representative can determine if a risk of compromising sensitive Government information exists or if the efficiency of service is at risk and may direct immediate removal of a Contractor employee from contract support.

OPR PSD will conduct periodic reinvestigations every 5 years, or when derogatory information is received, to evaluate continued Fitness of Contractor employees.

The Federal Government is transitioning to Trusted Workforce (TW) 2.0. TW 2.0 is a whole-of-government background investigation reform effort overhauling the personnel vetting process by creating a government-wide system that allows transfer of trust across organizations. All contractor employees will be subjected to the transition and will be enrolled into continuous vetting at a date to be determined and via a to be determined continuous vetting system. Enrollment will include multiple requirements from all personnel and potential changes to processes, procedures, and systems. This contract will comply with all requirements that facilitate the mandated transition to TW 2.0.

REQUIRED REPORTS

The Contractor will notify OPR PSD, via the COR providing an ICE Form 50-005, Contractor Employee Separation Clearance Checklist, of all terminations/resignations of Contractor employees under the contract within five days of occurrence to the [redacted] The Contractor will return any expired ICE issued identification cards and building passes of terminated/resigned employees to the COR. If an identification card or building pass is not available to be returned, a report must be submitted to the COR referencing the pass or card number, name of individual to whom issued, the last known location and disposition of the pass or card. The COR will return the identification cards and building passes to the responsible ID Unit.

The Contractor will report any adverse information coming to their attention concerning Contractor employees under the contract to OPR PSD, via the COR, as soon as possible. Reports based on rumor or innuendo should not be made. The subsequent termination of employment of an employee does not obviate the requirement to submit this report. The report shall include the Contractor employees' name and social security number, along with the adverse information being reported.

The Contractor will provide, through the COR, a Quarterly Report (on a Microsoft Excel Spreadsheet) containing the names of Contractor employees who are actively serving on their contract. The list shall include the Name, Position and SSN (Last Four) and should be derived from system(s) used for Contractor payroll/voucher processing to ensure accuracy. This list is what ICE Industrial Security uses to reconcile the contract quarterly. **CORs will submit reports to [redacted] no later than the 10th day of each January, April, July and October.**

Contractors, who are involved with management and/or use of information/data deemed "sensitive" to include 'law enforcement sensitive" are required to complete the DHS Form 11000-6-Sensitive but Unclassified Information Non-Disclosure Agreement (NDA) for Contractor employee access to sensitive information. The NDA will be administered by the COR to all contract personnel within 10 calendar days of the entry on duty date. The completed form shall remain on file with the COR for purpose of administration and inspection.

Sensitive information as defined under the Computer Security Act of 1987, Public Law 100-235 is information not otherwise categorized by statute or regulation that if disclosed could have an adverse impact on the welfare or privacy of individuals or on the welfare or conduct of Federal programs or other programs or operations essential to the national interest. Examples of sensitive information include personal data such as Social Security numbers; trade secrets; system vulnerability information; pre-solicitation procurement documents, such as statements of work; and information pertaining to law enforcement investigative methods; similarly, detailed reports related to computer security deficiencies in internal controls are also sensitive information because of the potential damage that could be caused by the misuse of this information. All sensitive information must be protected from loss, misuse, modification, and unauthorized access in accordance with DHS Management Directive 11042.1, **DHS Policy for Sensitive Information and ICE Policy 4003, Safeguarding Law Enforcement Sensitive Information."**

Any unauthorized disclosure of information will be reported to [redacted]

SECURITY MANAGEMENT

The Contractor shall appoint a senior official to act as the Corporate Security Officer. The individual will interface with OPR PSD through the COR on all security matters, to include physical, personnel, and protection of all Government information and data accessed by the Contractor.

The COR and OPR shall have the right to inspect the procedures, methods, and facilities utilized by the Contractor in complying with the security requirements under this contract. Should the COR determine that the Contractor is not complying with the security requirements of this contract, the Contractor will be informed in writing by the Contracting Officer of the proper action to be taken to effect compliance with such requirements.

INFORMATION TECHNOLOGY SECURITY

When sensitive government information is processed on Department telecommunications and automated information systems, the contract company agrees to provide for the administrative control of sensitive data being processed and to adhere to the procedures governing such data as outlined in DHS MD 4300.1, *Information Technology Systems Security* (or its replacement). Contractor employees must have favorably adjudicated background investigations commensurate with the defined sensitivity level.

Contractor employees who fail to comply with Department security policy are subject to having their access to Department IT systems and facilities terminated, regardless if the failure results in criminal prosecution. Any person who improperly discloses sensitive information is subject to criminal and civil penalties and sanctions under a variety of laws (e.g., Privacy Act).

INFORMATION TECHNOLOGY SECURITY TRAINING AND OVERSIGHT

In accordance with Office of the Chief Information Officer (OCIO) requirements and provisions, all Contractor employees accessing Department IT systems or processing DHS sensitive data via an IT system will require an ICE issued/provisioned Personal Identity Verification (PIV) card. Additionally, Cybersecurity Awareness Training (CSAT) will be required upon initial access and annually thereafter. CSAT training will be provided by the appropriate component agency of DHS.

Contractor employees, who are involved with management, use, or operation of any IT systems that handle sensitive information within or under the supervision of the Department, shall receive periodic training at least annually in security awareness and accepted security practices, systems rules of behavior, to include Unauthorized Disclosure Training, available on the ICE Training System (ITS) or by contacting [redacted]. Contractor employees with significant security responsibilities shall receive specialized training specific to their security responsibilities annually. The level of training shall be commensurate with the individual's duties and responsibilities and is intended to promote a consistent understanding of the principles and concepts of telecommunications and IT systems security.

All personnel who access Department information systems will be continually evaluated while performing these duties. System Administrators should be aware of any unusual or inappropriate behavior by personnel accessing systems. Any unauthorized access, sharing of passwords, or other questionable security procedures should be reported to the local Security Office or Information System Security Officer (ISSO).

OCIO/ Data Management Unit (DMU) - Data Ownership Contract Requirements Language

1. Accessibility of Government-owned Data

All stored program data associated with this acquisition shall be owned by the Government. As such, it shall be made accessible to the Government in accordance with the Minimum Data Access Capability described below. This accessibility is required to allow full data transparency, flexibility in performing data analytics, and integration with data from other government programs.

In addition to the Minimum Data Access Capability, the Government prefers, but does not require, that program data be accessible via Enhanced Access Capabilities as described below.

Definition of "program data": Program Data refers to any data resulting from ICE and DHS organizational activity. Examples of such data include but are not limited to administrative data resulting from human resource, management, and financial actions, as well as operational data resulting from performance of the ICE mission.

Definition of "associated with this acquisition": Program Data is associated with an acquisition if it is created by DHS organizational activity that is facilitated by the contractor. Examples of how a contractor might facilitate organizational activity follow:

- Program data is stored by contractor personnel.
- Program data is stored by software that is managed, developed, or used by the contractor.
- Program data is stored in a repository that is managed, developed, or used by the contractor.

2. Minimum Data Access Capability

- The current version of all Program Data is accessible to the Government within 24 hours of request, as well as on any pre-defined schedule as required by the Government.

  Data access can occur by various means, provided that Government security requirements are met, and data is accessible in a format that is acceptable to the Government. Examples include but are not limited to APIs that are consumable by the Government, files made available for Government download (e.g., Excel Spreadsheets), or direct database query by federal or contractor personnel.

- The contractor shall format program data accessed by the Government to anticipate the maximum file size of any data to be accessed. File size shall be small enough to assure rapid processing by government applications.
- The contractor shall provide the means for the Government to interpret accessible Program Data as follows:
  - Data elements and groupings of data elements shall be clearly identifiable by labels embedded in the data itself, or by a separate schema or file layout which allows such elements and groupings to be identified.

In the case of a relational database schema defined through Data Definition Language (DDL), data elements would be represented as columns, and groupings of data would be represented as tables. In addition, relationships between tables would be described as foreign key relations.

- Labels or names used to identify data elements and groupings of data elements shall be approved by the Government. In addition, each label or name shall be associated with a government approved definition which describes the content of data held therein.
- Program data delivered to the Government shall conform to the Government approved definition for each data element and grouping of data elements.
- All data accessible by the Government shall be both machine readable and human-readable in plain text.
- All reference data associated with Program Data also needs to be accessible to the Government. Such reference data is required to provide complete understanding of a record.

Reference Data Example: Program data may include a city code which uniquely identifies a city. Reference data associated with a city code may include its name, geographic boundaries, population, median income, etc. This example is provided for clarification of the meaning of reference data and may or may not apply to this specific acquisition. Examples of other reference data codes would include codes representing eye color, gender, country of origin, etc.

3. Enhanced Access Capabilities

The Government prefers that sharing of program data take place via an Application Programming Interface (API) or multiple APIs. APIs allow the Government to efficiently consume data via a widely recognized standard where the data has been completely abstracted from the technology platform that produces it.

In addition, the Government prefers that sharing of program data take place using techniques that enhance efficiency, such as Change Data Capture (CDC). CDC enhances efficiency of data transfer by providing only incremental updates to program data as opposed to providing all program data each time data is shared.