U.S. Immigration and Customs Enforcement

Department of Homeland Security

Immigration and Customs Enforcement

Statement of Work

for
Zero Trust Research Library, Strategic Advisory Services, Training and Certification

May 31, 2023

For Official Use Only

CONTENTS

1.0 BACKGROUND

Immigration and Customs Enforcement (ICE) is the Department of Homeland Security (DHS) component responsible for enforcing immigration laws to preserve national security and public safety. Within ICE, the Office of the Chief Information Officer (OCIO) is responsible for providing mission-critical Information Technology (IT) services and products that enable ICE and DHS to meet their respective missions.

DHS ICE OCIO Information Assurance Division (IAD) has a need for Cybersecurity and Zero Trust Strategic Advisory Services, Research Library, Training and Certification Services, which will allow OCIO Management to find leading technological solutions and services in the market. These services must provide OCIO leadership with access to extensive research on Zero Trust and other cybersecurity issues, as well as offer training and certification in Zero Trust for select users.

These services must provide process-driven strategic planning, rather than a technology-based solution, meaning that it can be applied to ICE's legacy systems, and is product agnostic and creates clear recommendations for requirements to guide the adoption of emerging technology.

2.0 SCOPE

ICE requires research, advisory, and professional services from an experienced, objective, Contractor with proven experience aligning both deep technical expertise and system design best practices to provide OCIO with support that will inform its strategic decisions. The work included in this SOW does not include or require implementation of any solutions. All advisory services will be external from the ICE network (e.g, ICE network access will not be provided).

ICE needs to continue progress in meeting compliance and deadlines within Cyber Executive Order 14028 and NIST SP 800-207. These compliance deadlines require ICE to develop an agency specific roadmap to guide implementation of Zero Trust architecture and concepts. Furthermore, ICE requires ongoing support to continue to drive cultural change, avoid backsliding, and ensure future investments align with the security policy.

Thus, ICE requires the expertise and analysis of industry-recognized Zero Trust analysts, consultants and practitioners with proven experience, deep technical expertise, and research-backed knowledge of system design best practices to support continuous improvement. This program support should include insights based on long-standing quantitative and qualitative Zero Trust research and thought leadership, including in-depth network discovery, information system analysis, documentation, diagrams, and recommendations based on industry best practices and primary research on implementing a Zero Trust Framework. Through this expertise, ICE requires that designated staff be able to obtain an industry-recognized Zero Trust Certification to ensure ICE staff can also nurture in-house expertise for ongoing priorities.

3.0 TASKS

The Contractor shall provide the following:

3.1 Research Library Access

The Contractor shall provide seven (7) named IAD users with unlimited individual access to a research library consisting of business, strategy, and cybersecurity related research available to designated users that

includes market forecasts, customer insights, and technology and service provider landscapes. ICE has identified 3 types of users (executive, strategic, technical). Only one license required at the executive level. ICE anticipate 3 users at the strategic level and 3 at the technical level. Note, contractors may propose alternate tiers and structures as long as the intent of the user role is equivalent to the below:

- Executive Level – concierge level aimed at executive level leadership, strategic planning support, executive partner support.
- Strategic – Leadership-level strategic guidance sessions
- Technical – Technical/SME stakeholder support for organization's technical employees.

While licenses may be tiered, all tiers should have access to research, document review/research, and advisory services however the levels of access may vary based on tiers.

Research should be on Zero Trust and include topics such as customer experience, product management, security and risk, and additional topics. The research library shall include research on Zero Trust /cybersecurity topics from at least five (5) or more years of data and should include products such as research, reports, studies, foundational artifacts, and best practices across industry. It is mandatory for the contractor to have its own managed research library. The research should be conducted by the awarded vendor.

This research should demonstrate deep technical expertise across the full spectrum of technologies including, but not limited to: best case analysis; customer experience and business-value metrics; vendor assessments; toolkits; and other analysis that will ensure recommendations that consider the realities of the OCIO's existing environment.

3.2 Strategic Advisory Services

The Contractor shall provide insights and recommendations gathered from helping other Federal, State, and local agencies align their people, process, and technology in a way that both improves mission-partner experience while maximizing the value of spend. The citizen, employee, and Federal partner insights should be based on a long-standing quantitative baseline of analytics identifying the changing expectations, behaviors, and attitudes of internal and external customers, and be product-agnostic.

The Contractor shall provide advisory services that includes a Zero Trust/cybersecurity methodology that provides actionable and **product-agnostic** recommendations to improve cybersecurity posture.

The Contractor shall provide strategic advisory and consulting services that may focus on, but are not limited to, the following priorities, as determined by the Government:

- Assist ICE OCIO in the transition from Zero Trust strategy to execution that may include:
    - Documents review and feedback (such as Government SOWs unrelated to this action, products provided by other contractors (e.g. Zero Trust Roadmap) or other reviews relating to Zero Trust. Document review sessions will be limited to twenty pages or less per session.
    - Research, where the contractor uses their existing research to provide Zero Trust-related products to the Government on specified topics. These products may include white papers, slide decks/presentations, market research, or other relevant products as determined by Government need. All research for these products shall be based on the research completed by the Vendor in their research library.

    - The Government will plan each year's expected reviews/research needs at the beginning of each period of performance in coordination with the Contractor, however additional Ad Hoc sessions may be required.
- Provide Executive partner advisory and strategy sessions on topics that may include, but are not limited to:
    - Guiding product-agnostic development of a solution architecture and roadmap
    - Securing data/assets through their lifecycle
    - Quantum Encryption
        - Planning and budgeting for future quantum capabilities
    - Driving a risk-driven decision-making culture through ICE and aiding progression toward a quantifiable risk model
    - Building a high-performing security organization
        - Continued education/training, including certification in Zero Trust, across ICE
        - Unlimited access to research, document reviews, webinars, and other information in a library style format

All strategic and advisory service must be product/tool agnostic, and holistic in an approach that accounts for technology, people, and processes These services shall be advisory only, based on extensive (10+ years) experience in Zero Trust.

3.3 Zero Trust Courses and Zero Trust Certifications

The Contractor shall provide Zero Trust courses leading to a Zero Trust certification for the seven (7) users listed in 4.1. Certification should be specific to Zero Trust and grounded in Zero Trust research. Certification must already be established, but does not need to be accredited. The courses should be online and self-paced, though occasional virtual discussions with group/cohort is expected if required. The Contractor shall provide at minimum an introductory, intermediate, and expert courses already available.

Courses may cover subjects such as adoption of Zero Trust, developing use cases for Zero Trust, and/or leading a customer-focused approach. The focus is on advancing interagency Zero Trust collaboration, increasing agency-specific expertise and implementation readiness, and building a cross-agency cadre of informal advisors in the Federal Government. These courses can include a series of interactive webinars as well as live training.

3.4 Optional Tasks

The Government may expand upon the research library and inclusive advisory access requirements and choose to purchase additional strategic advisory time. These Optional tasks are described below:

3.4.1 Optional Strategic Advisory Consulting

The Government may require dedicated consulting resources to support a targeted engagement designed to advance ICE's efforts to advance the goals established in EO 14028. To meet its needs, OCIO requires a solution that can rapidly assess how well ICE is approaching, designing, communicating and executing its Zero Trust initiatives. The consulting support will apply existing research, concepts, and ideas to OCIO challenges. Upon exercise, the Contractor will deliver working sessions requiring moderate customization including an intake session to identify current challenges; evaluation and application of research content to those challenges;

and a road map discussing general themes and next steps. Timelines and scheduling for these sessions will be agreed upon between the Vendor and the Government. Areas of focus for the engagement may include:

- **Reference Architecture Refinement:** Refining the visual representation of the Zero Trust reference architectures to include clear identification of data, telemetry, control and policy flows, aggregation and signaling. Application of these approaches to critical use cases.

- **Zero Trust Technology Landscape Awareness**: Understanding the technologies capabilities required to design a Zero Trust architecture. Elucidation of the primary vendors within each capability space and their relative strengths and weaknesses relative to specific ICE use cases. Identification of key capabilities and technologies that ICE will require as part of its future roadmap.

- **Micro-Segmentation Strategy:** Assessment of ICE's access management status quo. Review of primary strategies for establishing micro-segmentation within complex environments. Identification of key milestones and sequencing of essential activities for the implementation of micro-segmentation at ICE.

The Government anticipates that the above services will be performed by the following resources:

- Principal:
    - 5 years experience with Zero Trust
    - Bachelor's Degree
    - Program Management/Executive experience
    - Experience with strategic planning for Government organizations
- Consultant:
    - Experience with Project Management and Zero Trust
    - Research Analysis experience

Government anticipates a maximum of 9 days for the Principal and 10 days for the Consultant each year. A day is defined as 8 hours and the Government contemplates that the contractor may invoice after completion of each day. The Government and contractor may agree to a project which is less than the 8 hours.

Note that ICE does not intend for the above roles to be Full Time Equivalents, nor does ICE intend for any personnel to be submitted for Entrance on Duty (EOD). The two roles specified are only for SOW section 3.4.1.

3.4.2 Optional Research Library Licenses

The Government may require additional research licenses, equivalent to the strategic or technical level, during the option years of this Task Order and reserves the right to order an additional 5 licenses of each type.

4.0 DELIVERABLES

All deliverables will be electronically submitted to the Contracting Officer's Representative and the ICE Task Manager/Program Manager.

Deliverable	Frequency	Date of Submission
Licenses - The Contractor shall provide seven (7) annual licenses (1 Executive Level, 3 Strategic Level and 3 Technical Level).	Annual	As determined by the Program Manager (PM) or the Contracting Officer's Representative (COR)
Documents Research - The Contractor shall research, develop, provide, update, and distribute (if requested) documents requested by the ICE Task Manager/PM or the COR.	As needed	As needed
Analyst Services - The Contractor shall provide analyst/advisory services.	As needed	As needed
Webinars – The Contractor shall provide webinars, or live training, as needed	As needed	As needed
Certification/training	Self-paced	As needed

5.0 PLACE OF PERFORMANCE

The vendor shall perform the described services for ICE within the National Capital Region and/or remotely.

6.0 PERIOD OF PERFORMANCE

The period of performance is one (1) 12-month base period with four (4) 12-month Option Periods.

7.0 ADDITIONAL CONSTRAINTS

- Use electronic technologies to reduce paper copies of program information generated throughout the life of this contract (unless paper copy is requested).
- Use secure electronic technologies to communicate and pass data between Government and contractor organizations, when requested and whenever possible.
- The Government does not foresee the need for travel in the fulfillment of this contract. Any travel expenses incurred, shall not be reimbursed.

Appendix A: General Cybersecurity Contract Requirements

1. ICE CYBERSECURITY REQUIREMENTS

1.1 Compliance with DHS Security Policy Terms and Conditions

All hardware, software, and services provided under this task order must be compliant with *DHS 4300A Information Security Systems Directive version 13.3 2023 DHS Sensitive System Policy* and *DHS 4300A Information Security Systems Directive version 13.3 2023 Sensitive Systems Handbook.***In accordance with ITAR 4.5.3.4 and ITAR 4.5.4.4 – Security Review**
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 Technical Representative (COTR), 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.

1.2 In accordance with ITAR 4.5.3.7 – Supply Chain Risk Management

Supply Chain Risk Management Terms and Conditions
The Contractors supplying the Government hardware and software shall provide the manufacturer's name, address, state and/or domain of registration, and the Data Universal Numbering System (DUNS) number for all components comprising the hardware and software. If subcontractors or subcomponents are used, the name, address, state, and/or domain of registration and DUNs number of those suppliers must also be provided. Subcontractors are subject to the same general requirements and standards as prime contractors. Contractors employing subcontractors shall perform due diligence to ensure that these standards are met.
The Government shall be notified when a new contractor/subcontractor/service provider is introduced to the supply chain, or when suppliers of parts or subcomponents are changed.
Contractors shall provide, implement, and maintain a Supply Chain Risk Management Plan that addresses internal and external practices and controls employed to minimize the risk posed by counterfeits and vulnerabilities in systems, components, and software.
The Plan shall describe the processes and procedures that will be followed to ensure appropriate supply chain protection of information system resources developed, processed, or used under this contract.
The Supply Chain Risk Management Plan shall address the following elements:

i. How risks from the supply chain will be identified;

ii. What processes and security measures will be adopted to manage these risks to the system or system components; and

i. How the risks and associated security measures will be updated and monitored.

The Supply Chain Risk Management Plan shall remain current through the life of the contract or period of performance. The Supply Chain Risk Management Plan shall be provided to the Contracting Officer Representative (COR/CO) 30 days post award.

The Contractor acknowledges the Government's requirement to assess the Contractors Supply Chain Risk posture. The Contractor understands and agrees that the Government retains the right to cancel or terminate the contract, if the Government determines that continuing the contract presents a risk to national security.

The Contractor shall disclose, and the Government will consider, relevant industry standard certifications, recognitions and awards, and acknowledgments.

The Contractor shall provide only new equipment unless otherwise expressly approved, in writing, by the CO. Contractors shall provide only Original Equipment Manufacturer (OEM) parts to the Government. In the event that a shipped OEM part fails, all replacement parts must be OEM parts.

The Contractor shall be excused from using new OEM (i.e. "grey market, "previously used) components only with formal Government approval. Such components shall be procured from their original source and have them shipped only from manufacturers authorized shipment points.

For software products, the contractor shall provide all OEM software updates to correct defects for the life of the product (i.e., until the “end of life"). Software updates and patches must be made available to the government for all products procured under this contract.

Contractors shall employ formal and accountable transit, storage, and delivery procedures (i.e., the possession of the component is documented at all times from initial shipping point to final destination, and every transfer of the component from one custodian to another is fully documented and accountable) for all shipments to fulfill contract obligations with the Government.

All records pertaining to the transit, storage, and delivery will be maintained and available for inspection for the lessor of the term of the contract, the period of performance, or one calendar year from the date the activity occurred.

These records must be readily available for inspection by any agent designated by the U.S. Government as having the authority to examine them.

This transit process shall minimize the number of times en route components undergo a change of custody and make use of tamper-proof or tamper-evident packaging for all shipments. The supplier, at the Government's request, shall be able to provide shipping status at any time during transit.

The Contractor is fully liable for all damage, deterioration, or losses incurred during shipping and handling, unless the damage, deterioration, or loss is due to the Government. The Contractor shall provide a packing slip which shall accompany each container or package with the information identifying the contract number, the order number, a description of the hardware/software enclosed (Manufacturer name, model number, serial number), and the customer point of contact. The contractor shall send a shipping notification to the intended government recipient or contracting officer. This shipping notification shall be sent electronically and will state the contract number, the order number, a description of the hardware/software being ship (manufacturer name, model number, serial number), initial shipper, shipping date and identifying (tracking) number.

Sensitive Information Limited to U.S. Citizens and Lawful Permanent Residents (JUN 2006)

1. Each individual employed under the contract shall be a citizen of the United States of America, or an alien who has been lawfully admitted for permanent residence as evidenced by a Permanent Resident Card (USCIS I-551). Any exceptions must be approved by the Department's Chief Security Officer or designee.

2. 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

1.3 In accordance with White House Digital Government BYODTK – Privacy Expectations

Privacy Expectations

Government contractor employees do not have a right, nor should they have an expectation, of privacy while using Government provided devices at any time, including accessing the Internet and using e-mail and voice communications. To the extent that employees wish that their private activities remain private, they should avoid using the Government provided device for limited personal use. By acceptance of the government provided device, employees imply their consent to disclosing and/or monitoring of device usage, including the contents of any files or information maintained or passed -through that device.

2. SECTION 508 REQUIREMENTS

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

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

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

2.1 Section 508 Requirements for Technology Products

Section 508 applicability to Information and Communications Technology (ICT): Web based research library

Applicable Exception: N/A Authorization #: N/A

Applicable Functional Performance Criteria: Does not apply

Applicable 508 requirements for electronic content features and components (including but not limited to Electronic training materials): Does not apply

Applicable 508 requirements for software features and components: Does not apply

Applicable 508 requirements for hardware features and components: Does not apply

Applicable 508 requirements for support services and documentation: All requirements in Chapter 6 apply

2.2 Section 508 Deliverables

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

3. ENTERPRISE ARCHITECTURE (EA) COMPLIANCE LANGUAGE

This is a list of EA Architecture Compliance language agreed upon between Components and HQ DHS to be used in preparing SOW, PWS & SOO for IT acquisitions & services. The following Components (CBP, TSA & USCG) have their own customized version listed below that must be used. All other Components must use the DHS Enterprise Architecture Compliance language that follows: DHS Enterprise Architecture Compliance All solutions and services shall meet DHS Enterprise Architecture policies, standards, and procedures. Specifically, the contractor shall comply with the following Homeland Security (HLS) EA requirements: - All developed solutions and requirements shall be compliant with the HLS EA principles - All IT hardware and software shall be compliant with the HLS EA Technical Reference Model (TRM) Standards and Products Profile ; all products are subject to DHS Enterprise Architectural approval. No products may be utilized in any production environment that is not included in the HLS EA TRM Standards and Products Profile. - Description information for all data assets, information exchanges and data standards, whether adopted or developed, shall be submitted to the Enterprise Data Management Office (EDMO) for review, approval and insertion into the

DHS Data Reference Model and Enterprise Architecture Information Repository. - Development of data assets, information exchanges and data standards will comply with the DHS Data Management Policy MD 103-01 and all data-related artifacts will be developed and validated according to DHS data management architectural guidelines. - Applicability of Internet Protocol Version 6 (IPv6) to DHS-related components (networks, infrastructure, and applications) specific to individual acquisitions shall be in accordance with the DHS Enterprise Architecture (per OMB Memorandum M-05- 22, August 2, 2005) regardless of whether the acquisition is for modification, upgrade, or replacement. All EA-related component acquisitions shall be IPv6 compliant as defined in the U.S. Government Version 6 (USGv6) Profile (National Institute of Standards and Technology (NIST) Special Publication 500-267) and the corresponding declarations of conformance defined in the USGv6 Test Program

4. PRIVACY REQUIREMENTS FOR CONTRACTOR AND PERSONNEL

4.1 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.

4.2 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.

4.3 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.

4.4 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.

4.5 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.

4.6 Privacy Lead Requirements

If the contract involves an IT system build or substantial development or changes to an IT

system that may require privacy documentation, the Contractor shall assign or procure a Privacy Lead, to be listed under the SOW or PWS's required Contractor Personnel section. The Privacy Lead shall be responsible for providing adequate support to DHS to ensure DHS can complete any required PTA, PIA, SORN, or other supporting documentation to support privacy compliance. The Privacy Lead shall work with personnel from the program office, the ICE Privacy Unit, the Office of the Chief Information Officer, and the Records and Data Management Unit to ensure that the privacy documentation is kept on schedule, that the answers to questions in the PIA are thorough and complete, and that questions asked by the ICE Privacy Unit and other offices are answered in a timely fashion.

The Privacy Lead:

- Must have excellent writing skills, the ability to explain technology clearly for a non-technical audience, and the ability to synthesize information from a variety of sources.
- Must have excellent verbal communication and organizational skills.
- Must have experience writing PIAs. Ideally the candidate would have experience writing PIAs for DHS.
- Must be knowledgeable about the Privacy Act of 1974 and the E-Government Act of 2002.
- Must be able to work well with others.

If a Privacy Lead is already in place with the program office and the contract involves IT system builds or substantial changes that may require privacy documentation, the requirement for a separate Private Lead specifically assigned under this contract may be waived provided the Contractor agrees to have the existing Privacy Lead coordinate with and support the ICE Privacy POC to ensure privacy concerns are proactively reviewed and so ICE can complete any required PTA, PIA, SORN, or other supporting documentation to support privacy compliance if required. The Contractor shall work with personnel from the program office, the ICE Office of Information Governance and Privacy, and the Office of the Chief Information Officer to ensure that the privacy documentation is kept on schedule, that the answers to questions in any privacy documents are thorough and complete, that all records management requirements are met, and that questions asked by the ICE Privacy Unit and other offices are answered in a timely fashion.

5. OCIO/ DATA MANAGEMENT UNIT (DMU) - DATA OWNERSHIP CONTRACT REQUIREMENTS LANGUAGE

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

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.

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.