Performance Work Statement

MAY 2021

Department of Homeland Security (DHS)
Immigration and Customs Enforcement (ICE)
Homeland Security Investigations (HSI)
Repository for Analytics in Virtualized Environment (RAVEN)
User Interface User Experience (UI/UX)

U.S. Immigration and Customs Enforcement

Procurement Sensitive

Table of Contents

1. Project Title

This requirement is for professional Information Technology (IT) services in support of the Repository for Analytics in Virtualized Environment (RAVEN) User Interface User Experience support on behalf of the Department of Homeland Security (DHS), Immigration and Customs Enforcement (ICE), Homeland Security Investigations (HSI) and the Innovation Lab.

2. Background

2.1. Homeland Security Investigations (HSI) is the principal investigative arm of Department of Homeland Security (DHS) and the second largest investigative agency in the Federal Government. HSI's primary mission is to promote homeland security and public safety through the criminal and civil enforcement of Federal laws governing border control, customs, trade, and immigration. The investigative mission is complex and ever evolving. HSI requires an investigative analytics platform that:

2.1.1. enables users to reveal criminal networks leveraging massive quantities of information obtained from 10,000s of different sources.

2.1.2. is flexible and can be adapted to address ever evolving threats.

2.1.3. enables the incorporation of best-in-class open source and Government off the shelf (GOTS) tools and process while relying minimally on commercial off the shelf tools (COTS);

2.1.4. automates routine business processes to drive down the time between collection and insight.

2.1.5. is comprised of reusable components which can be leveraged through adaptive maintenance to address the ever-evolving threats posed by criminal networks.

2.2. To meet this need HSI has transformed its investment approach and processes for acquiring and delivering investigative analytics capabilities. HSI has created the HSI Innovation Lab as the agent of change for the reimagination of what systems can and should be to better enable HSI to accomplish its mission.

2.3. The HSI Innovation Lab has built the Repository for Analytics in a Virtualized Environment (RAVEN) as the platform for investigative analytics. It is HSI's vision to provide expert analytic tools and services to ensure the employment of innovative analytic techniques to support investigations and to ensure customer value. Additionally, HSI seeks to make RAVEN a central component in DHS's efforts to operationalize Machine Learning in practical and responsible way.

2.4. The purpose of this Performance Work Statement (PWS) is to outline the Government's requirements for a Contractor to provide UIUX support for the HSI Innovation Lab's Repository for Analytics in a Virtualized Environment (RAVEN).

3. Scope of Work

The scope of this requirement is to provide User Interface and User Experience (UI/UX) support to the HSI Innovation Lab by performing the following functions:

3.1. The Government seeks to enhance HSI data analytics capability by developing web-based User Interfaces (UIs) which form a consistent User Experience (UX). All UIs will be developed to leverage other tools developed within RAVEn platform. The platform and all tools within it are designed to enable users to access information in ways that facilitate deriving meaning from information in ways far beyond what is currently available at HSI. This requires contract support services to design, develop, and improve UIs. The UIs will be developed to address specific high priority issues but the following tasks are representative of the types of requirements the UIs will be developed to address: Persistent Data Retrieval and Bring Your

Own Data, Data Ingest, Data Mapping (Flat Files), Data Mapping (Relational Databases), Graph Visualization, Timeline Visualization, Intuitive Search, Customized Reports, Mobile Device Accessible, Export, Logging and user interaction monitoring, Logging and user interaction monitoring, and Ease of Use.

3.2 Provide UI/UX support to the HSI Innovation Lab performing the following functions:

3.2.1. Leverage and enhance the modular architecture of the RAVEN platform so that thru adaptive maintenance RAVEN can continue to evolve to address the ever-changing threats posed by criminal networks. Special emphasis will be given in all enhancement activities to building solutions that are constructed of re-usable components.

3.2.2. Build solutions to automate the collection of publicly available information from the internet to support criminal investigations and investigative initiatives.

3.2.3. Build solutions to enhance HSIs ability to securely obtain information from private sector partners.

3.2.4. Build solutions to automate the ingestion of and connections to information in existing U.S. Government authoritative systems of record.

3.2.5. Build solutions to automate the extraction and transformation of information from data sources which traditionally require manual user intervention.

3.2.6. Build solutions to facilitate user's ability to bring data to RAVEN and fuse it with information currently in RAVEN.

3.2.7. Build solutions to facilitate robust fusion of information from many different sources so that a single comprehensive picture of the threat landscape can be assembled.

3.2.8. Build solutions to enable enhanced search which enable users to search across all available data for selectors (i.e. Phone Numbers, Addresses, People, Businesses) they know about.

3.2.9. Build solutions to facilitate search and exploration of all available RAVEN data to expose complex event interactions and criminal networks.

3.2.10. Build solutions to generate leads through robust multi-vector analytics.

3.2.11. Build solutions to prioritization through analytics which measure threat.

3.2.12. Build solutions to facilitate the rapid adaptation of the platform to address new or evolved threats.

3.2.13. Build solutions to facilitate the scalability of the platform to handle increases in user demand and size and/or velocity of incoming information.

3.2.14. The Government intends for this team to work closely with the solution development teams, comprised of members from the Data Analytics, UI/UX, DevSecOps, and PMO contracts, while maintaining an independent and objective position. The Government will leverage this team to ensure that only code meetings RAVEN's high standards as identified in the Attachment G – RAVEN Operational Requirements is allowed to be deployed.

4. Tasks

Section 4 of the PWS identifies the duties and responsibilities covered under the work covered this PWS. All requirements covered under **Section 4.1 RAVEN UI/UX Development** apply to the Tasks Identified in **Sections 4.2** through **4.5**.

Each Labor Category under these Tasks shall be Full Time, unless otherwise specified, and identified in the Line Item Description along with the associated Labor Rates. In the Base Period, these Tasks will be Time & Materials (T&M), and will convert to Firm-Fixed-Price (FFP) in Option Periods 1, 2, 3, and 4. HSI will not accept any invoices on these Tasks for any Personnel until they receive their Entry on Duty (EOD) Date from ICE Personnel Security. HSI expects the

Contractor to submit security packages for all new and/or replacement personnel within 30 days of Award. This includes any additional personnel upon exercise of any optional tasks or surge support.

The Contractor shall be aware that the Government and other Contractors are engaged in similar and supporting work as part of multiple solution development teams, requiring close cooperation. Contractors are expected to form a cohesive team to include the Government and other Contractors, by fostering transparency and information sharing for successful task execution. This task includes the following work:

4.1 RAVEN UI/UX Development.

The contractor will be required to provide qualified personnel with the appropriate skill mix and experience to support the design, develop and improvement of UI, web based analytic tools as described below and in **Section 3**. The contractor will be expected to staff this project with an appropriate mix of personnel. Additionally, the contractor will be required to staff this project with the key personnel as described in **Section 5.3**. All work conducted as part of this task is expected to align with ICE privacy and information assurance policies and regulations regarding the creation and maintenance of systems technology. The Contractor shall be aware that the Government and other contractors are engaged in similar and supporting work, requiring close cooperation. Contractors are expected to form a cohesive team to include the Government and other contractors, by fostering transparency and information sharing for successful task execution. The UIs will be developed to address specific high priority issues but the following tasks are representative of the types of requirements the UIs will be developed to address:

4.1.1. Persistent Data Retrieval and Bring Your Own Data: RAVEn platform users require the ability to not only query information in persistent data stores but also conduct ad-hoc analysis on data they obtain during the course of investigations. The contractor will be required to deliver new tools and utilize tools previously developed by other contractors or teams that enable both the analysis of these two types of data but also the ability to illuminate the inter-connectivity of the information as a whole. Each of the visualization requirements below are expected to enable this functionality.

4.1.2. Data Ingest: The development of user interfaces that utilize previously built capabilities as well as deliver new capabilities as required by project that allows users to upload a variety of documents and media files (pdf, html, word, xlsx, images, videos etc.). A challenge in this area will be handling large files and handling the upload of multiple (dozens to hundreds) files in one event. At the Government's direction, the contractor may be required to participate in the creation of data storage schemas and implement those schemas into their products, however the administration and maintenance of the data storage layer is outside of the scope of this task order. The contractor will be required to ensure that all products they are creating or adapting are compliant with the RAVEn platform when participating in the design and implementation of tools related to data ingestion and storage.

4.1.3. Data Mapping (Flat Files): Provide capability for data in different formats (xls, xlsx, csv, xml, json, word, pdf, etc.) to be mapped (linked) to an expected ontology. For example, a method for mapping columns in a spreadsheet to specific properties of a graph vertex or

edge. This will require a drag and drop style user interface that makes the process as simple as possible. Additionally, the system should be intelligent enough to infer structure based on previous mappings and present that to the user for confirmation.

4.1.4. Data Mapping (Relational Databases): Provide capability to connect to a relational database within RAVEn and when needed elsewhere and map tables and columns to an expected ontology.

4.1.5. Graph Visualization: Central to much of the work conducted by HSI investigators is determining the interconnectivity of people, things and events. Many of the developed UI/UXs will require the delivery of innovative graph visualizations. An example of a tool which RAVEn uses for this purpose is CytoscapeJS.

4.1.6. Geospatial Visualization: Another area of significance to HSI investigators is the ability to understand the geospatial significance of information. RAVEn utilizes the Esri ArcGIS Geospatial platform and intends to utilize the ArcGIS Javascript APIs whenever practical.

4.1.7. Timeline Visualization: It is also very important for HSI investigators to have the ability to rapidly understand the temporal interconnectivity of information. Many of the developed UI/UXs will require the delivery of innovative timeline visualizations and the integration of timelines, time sliders and other time related effects into other visualizations such as graphs and maps.

4.1.8. Intuitive Search: Search will be at the core of the majority of the UI/UXs which will be delivered during this task order. The RAVEn eco system currently incorporates Elastic Search, Cassandra, and Janus Graph as the core storage layer components. All developed UI/UXs will be required to incorporate search and information retrieval that is transparent to the end user. Additionally, search and information retrieval are expected to be accessible from the graphs, tables, maps, timelines, aggregation charts and other visualization not solely from a search bar.

4.1.9. Customized Reports: Often the ability to create repeatable exportable reports in Microsoft Word, PDF, Analyst Notebook, and or other formats is essential. Incorporating a system where report templates are capable of being created by superusers leveraging high level programing languages like Markup.

4.1.10. Mobile Device Accessible: Most UIs within the RAVEn environment must be designed to be accessible from mobile devices.. The RAVEn platform currently uses ReactNative to build JavaScript applications which compile to native device languages for deployment. RAVEn also utilizes iOS Swift to supplement the capabilities of ReactNative.

4.1.11. Export: A requirement of most every UI/UX that will be developed is the ability to export data to spreadsheets, graphs, maps, and other saved files.

4.1.12. Logging and user interaction monitoring: All UI/UXs within the RAVEn environment will be required to log user interaction. This will be done to comply with DHS4300 (System Auditability) requirements and to pave the way for the integration of machine learning strategies such as sentiment analysis and recommendations engines to enhance tool development and overall user experience. It will be required that during development phases, the development team will be responsible for creating hooks into their developed tools so that the RAVEn system can collect useful information from user groups.

4.1.13. Ease of Use: The user interface will be intuitive, affording ease of use by investigators and analysts. The UI/UX should implement functionality that adapts to specific users with the objective of improving overall system productivity.

4.1.14. ICE Security Standards: All systems developed shall conform to ICE Security Standards, to be provided at a later time.

4.1.15. Collaboration and Sharing

4.1.15.1. Facilitate a secure and fully integrated mechanism for users from different components and agencies to work together on investigations and share information without having to be co-located.

4.1.15.2. A fully integrated knowledge transfer system for users to share information concerning constantly evolving criminal typologies. This system must facilitate the use of all available information and incorporate intelligent analytics to test, support, or refute assertions and expose non-obvious trends.

4.1.16. Visualization and Reporting

4.1.16.1. User interfaces which can be accessed via web and mobile devices.

4.1.16.2. User friendly interfaces which are tailored to effectively address the needs of the user and have a consistent appearance and function so as to lower the level of training required for their effective use.

4.1.16.3. Reports and exportable visualizations which can be shared with team members who do not have access to the system and can be used to brief interested parties.

4.2 Program Management and Key Personnel

All Key Personnel shall be required to have an active TS clearance with Defense Counterintelligence and Security Agency (DCSA) prior to on-boarding. ICE is not be able to grant or accept a temporary adjudication for TS clearances.

4.2.1. Program Manager

The Program Manager (PM) will have overall responsibility of the Task Order activities: planning, organizing, directing, controlling, staffing, and reporting status, deliverables, and schedules to the Government. See Section 5.3.1 for additional details.

4.2.2. Lead Architect

The Architect – Lead shall have the same responsibility of an Architect as identified in Section 5.3.2, as well as having the overall responsibility of being the Contractor's primary representative on all architecture matters and the Contractor's leading member of the Architecture Team. Responsibilities include mentoring and directing junior developers of the Contract team related to technical tasks and agile project development practices and ensuring that all development the Contractor performs is aligned with the RAVEN platform and is not duplicative or designed in a way that it is not reusable.

4.2.3. User Interface Designer – Lead

The User Interface Designer – Lead shall have the same responsibility of an User Interface Designer as identified in Section 5.3.2, as well as having the overall responsibility of managing User Interface and Experience tasks and standards.

4.2.4. DHS Certified Section 508 Trusted Tester

The DHS Certified Section 508 Trusted Tester will have the overall responsibility of managing conformance to Section 508 standards. See Section (Key Personnel Description Section, not the normal LCAT section)

4.3 Development

Development focuses on the enhancement of the RAVEN Unclassified environments with some limited work conducted in the Classified environments. The primary customer base for work conducted in this CLIN is HSI personnel.

4.4 Adaptive Maintenance

Adaptive Maintenance focuses on the use of adaptive maintenance to leverage the existing RAVEN platform components to address ever evolving threats posed by criminal networks and support additional workflows which do not require enhancements to the RAVEN platform.

4.5 Optional Surge Support

Provide additional labor for surge DevSecOps support for advancement of HSI Innovation Lab and the RAVEn platform. The contractor shall provide additional staff with the experience and skills necessary to support the administration, configuration, maintenance, and enhancement of the RAVEn Platform as described in Sections 4.1 and 4.2 above to accommodate a surge of DevSecOps requirements.

5. Contractor Personnel Requirements

5.1 Personnel Qualifications

The Contractor shall provide qualified personnel to perform all requirements specified in this PWS. Experience from the private is acceptable; however, purely theoretical or academic experience will not qualify for these requirements. Required Skills/Experience for Contract Personnel:

5.1.1 Program Manager

The Program Manager (PM) will have overall responsibility of the Task Order activities: planning, organizing, directing, controlling, staffing and reporting status, deliverables, and schedules to the Government. The Program Manager is required to meet the following requirements and have the following skills:

5.1.1.1. Be a U.S. Citizen.

5.1.1.2. Five (5) or more years of relevant experience managing a team in an Enterprise IT environment with experience utilizing requirements tools and tracking software (e.g. JIRA)
5.1.1.3. Five (5) or more years of Project Management experience in an Agile Software Development environment, including methodologies related to software lifecycle management
5.1.1.4. Security Clearance Requirement: Top Secret/ Sensitive Compartmentalized Information
5.1.1.5. The Program Manager will be required to supply at least one (1) and no more than three (3) examples of projects managed with a total contract value over $2 million dollars during the past five (5) years where the following desired skills sets were demonstrated:

5.1.1.5.1. Experience leading multiple teams consisting of technical leads, and business analysts to execute tasks with independent release schedules
5.1.1.5.2. Experience defining all project activities and milestones required to meet objectives and deliverables, properly sequencing tasks and estimating effort with project team members doing the work, determining the critical path, and leveling the project schedule
5.1.1.5.3. Experience monitoring program execution to identify obstacles and deviations from plan and takes corrective action as needed
5.1.1.5.4. Experience conducting continuous risk assessment and management including developing measures to reduce risk in program execution
5.1.1.5.5. Experience developing metrics and reports for tracking program execution
5.1.1.5.6. Experience with contract management, budgeting, and resource allocation, including management of subcontractor personnel
5.1.1.5.7. Proficient in development of plans, assigning tasks, monitoring performance, communicating progress, resolving conflicts, and escalating issues
5.1.1.5.8. Experience with all aspects of configuration management planning including configuration identification, change control, configuration status accounting, configuration audits, configuration documentation

5.1.2. Lead Architect

The Architect Lead will have overall responsibility of planning how work within different teams will integrate into one solution. They shall also ensure collaboration and compliance with HSI standards. Required Skills/Experience for Contract Personnel:

5.1.2.1. Be a U.S. Citizen
5.1.2.2. Must meet High Risk, Law Enforcement Sensitive background and have the ability to obtain and maintain a TS-S/CI clearance.
5.1.2.3. Have the ability to work embedded with a HSI Field Office and HSI Headquarters Components. This includes having the ability to operate as a member of team in an often-high stress high tempo office environment.
5.1.2.4. Possess a minimum of eight (8) years of professional experience developing and testing software.
5.1.2.5. Possess a minimum of five (5) years of web-development experience including experience writing web applications using HMTL5, CSS3 and JavaScript.
5.1.2.6. Possess a minimum of six (6) years of experience developing production applications using at least one of the following server-side computer languages:

5.1.2.6.1. Python;
5.1.2.6.2. NodeJS; or
5.1.2.6.3. Java – SpringBoot

5.1.2.7. Possess a minimum of four (4) years of experience conducting analysis and design for medium to large enterprise systems.
5.1.2.8. Possess a minimum of two (2) years of experience developing applications leveraging big data technologies including at least one of the following:
5.1.2.8.1. Elastic Search
5.1.2.8.2. Cassandra
5.1.2.8.3. Janus Graph
5.1.2.9. Possess a minimum of two (2) years of experience developing enterprise level production tools built with:
5.1.2.9.1. ReactJS
5.1.2.10. Possess a minimum of two (2) years of experience leveraging CICD tools such as:
5.1.2.10.1. Jenkins
5.1.2.10.2. SonarCube
5.1.2.11. Possess the ability to demonstrate current and at least advanced skills in front-end and middle tier.
5.1.2.12. Possess the ability to demonstrate current and at least intermediate-advanced skills in back-end development.
5.1.2.13. Demonstrate a strong knowledge of concepts, methodologies, and best practices - especially as they pertain to mitigating development risks, estimating tasks, coding standards and source control procedures.

5.1.3. Senior Web User Interface Developer
The Senior Web User Interface Developer shall be responsible for user interface development and is expected to utilize the required experience and skills to ensure compliance with HSI standards. Required Skills/Experience for Contract Personnel:

5.1.3.1. Be a U.S. Citizen
5.1.3.2. Must meet High Risk, Law Enforcement Sensitive background and have the ability to obtain and maintain a TS-S/CI clearance.
5.1.3.3. Have the ability to work embedded with a HSI Field Office and HSI Headquarters Components. This includes having the ability to operate as a member of team in an often-high stress high tempo office environment.
5.1.3.4. Possess a minimum of four (4) years of professional experience in writing web applications deployed in an enterprise level production environment using HMTL5, CSS3, and JavaScript.
5.1.3.5. Possess a minimum of two (2) years of experience developing enterprise level production tools built with:
5.1.3.5.1. ReactJS; or
5.1.3.5.2. NodeJS
5.1.3.6. Possess a minimum of two (2) years of experience leveraging CICD tools such as:
5.1.3.6.1. Jenkins
5.1.3.6.2. SonarCube
5.1.3.7. Possess the ability to demonstrate current and at least intermediate skills in front-end and middle- tier development.
5.1.3.8. Demonstrate a strong knowledge of concepts, methodologies and best practices especially as they pertain to mitigating development risks, estimating tasks, coding standards and source control procedures.

5.1.4. Journeyman Web User Interface Developer

The Journeyman Web User Interface Developer shall be responsible for user interface development and is expected to utilize their required experience and skills to ensure compliance with HSI standards. Required Skills/Experience for Contract Personnel:

5.1.4.1. Be a U.S. Citizen
5.1.4.2. Must meet High Risk, Law Enforcement Sensitive background and have the ability to obtain and maintain a TS-S/CI clearance.
5.1.4.3. Have the ability to work embedded with a HSI Field Office and HSI Headquarters Components. This includes having the ability to operate as a member of team in an often-high stress high tempo office environment.
5.1.4.4. Possess a minimum of four (4) years of professional experience in writing web applications deployed in an enterprise level production environment using HMTL5, CSS3, and JavaScript.
5.1.4.5. Possess a minimum of two (2) years of experience developing enterprise level production tools built with:
5.1.4.5.1. ReactJS; or
5.1.4.5.2. NodeJS
5.1.4.6. Possess the ability to demonstrate current and at least intermediate skills in front-end and middle- tier development.
5.1.4.7. Demonstrate a strong knowledge of concepts, methodologies and best practices especially as they pertain to mitigating development risks, estimating tasks, coding standards and source control procedures.

5.1.5. Senior Full Stack Developer

The Senior Full Stack Developer (SFSD) shall be responsible for developing and testing software, writing web applications, developing production applications, and is expected to utilize their required experience and skills to ensure compliance with HSI standards. Required Skills/Experience for Contract Personnel:

5.1.5.1. Be a U.S. Citizen
5.1.5.2. Must meet High Risk, Law Enforcement Sensitive background and have the ability to obtain and maintain a TS-S/CI clearance.
5.1.5.3. Have the ability to work embedded with a HSI Field Office and HSI Headquarters Components. This includes having the ability to operate as a member of team in an often-high stress high tempo office environment.
5.1.5.4. Possess a minimum of four (4) years of professional experience developing and testing software.
5.1.5.5. Possess a minimum of two (2) years of web-development experience including experience writing web applications using HMTL5, CSS3 and JavaScript.
5.1.5.6. Possess a minimum of four (4) years of experience developing production applications using at least one of the following server-side computer languages:
5.1.5.6.1. Java – SpringBoot
5.1.5.7. Possess a minimum of two (2) years of experience designing medium to large enterprise systems.

5.1.5.8. Possess a minimum of two (2) years of experience developing applications leveraging big data technologies including at least one of the following:

5.1.5.8.1. Elastic Search

5.1.5.8.2. Cassandra

5.1.5.8.3. Janus Graph

5.1.5.9. Possess a minimum of two (2) years of experience leveraging CICD tools such as:

5.1.5.9.1. Jenkins

5.1.5.9.2. SonarCube

5.1.6. Journeyman Full Stack Developer

The Journeyman Full Stack Developer (JFSD) shall be responsible for developing and testing software, writing web applications, developing production applications, and is expected to utilize their required experience and skills to ensure compliance with HSI standards. Required Skills/Experience for Contract Personnel:

5.1.6.1. Be a U.S. Citizen

5.1.6.2. Must meet High Risk, Law Enforcement Sensitive background and have the ability to obtain and maintain a TS-S/CI clearance.

5.1.6.3. Have the ability to work embedded with a HSI Field Office and HSI Headquarters Components. This includes having the ability to operate as a member of team in an often-high stress high tempo office environment.

5.1.6.4. Possess a minimum of two (2) years of professional experience developing and testing software.

5.1.6.5. Possess a minimum of one (1) year of web-development experience including experience writing web applications using HMTL5, CSS3 and JavaScript.

5.1.6.6. Possess a minimum of two (2) years of experience developing production applications using at least one of the following server-side computer languages:

5.1.6.6.1. Java – SpringBoot

5.1.6.7. Possess a minimum of one (1) year of experience designing medium to large enterprise systems.

5.1.6.8. Possess a minimum of one (1) year of experience developing applications leveraging big data technologies including at least one of the following:

5.1.6.8.1. Elastic Search

5.1.6.8.2. Cassandra

5.1.6.8.3. Janus Graph

5.1.6.9. Possess a minimum of one (1) year of experience leveraging CICD tools such as:

5.1.6.9.1. Jenkins

5.1.6.9.2. SonarCube

5.1.7. Senior User Experience (UX) Designer

The Senior User Experience (UX) Designer shall be responsible for user experience development and is expected to utilize their required experience and skills to ensure compliance with HSI standards. Required Skills/Experience for Contract Personnel:

5.1.7.1. Be a U.S. Citizen

5.1.7.2. Must meet High Risk, Law Enforcement Sensitive background and have the ability to obtain and maintain a TS-S/CI clearance.
5.1.7.3. Have the ability to work embedded with an HSI Field Office and HSI Headquarters Components. This includes having the ability to operate as a member of team in an often-high stress high tempo office environment.
5.1.7.4. Possess a minimum of four (4) years of professional experience designing and testing web user interfaces.
5.1.7.5. Possess a minimum of two (2) years of web-development experience including experience writing web applications using HMTL5, CSS3, and JavaScript.
5.1.7.6. Possess a minimum of two (2) years of experience working with AdobeXD to design web UIs.
5.1.7.7. Possess a minimum of two (2) years of experience building and maintaining a design style guide used by a web development team with more than five (5) developers.
5.1.7.8. Possess a minimum of two (2) years of graphic artist experience, specifically designing icons and visual artifacts for use in web development.
5.1.7.9. Experience developing web tools utilizing the React.js web framework.
5.1.7.10. Experience developing web tools utilizing the Material UI components library for the React.js web framework.
5.1.7.11. Experience implementing Section 508 compliant features into a design style guide.

1.111 *Journeyman User Experience (UX) Designer*

The Journeyman User Experience (UX) Designer shall be responsible for user experience development and is expected to utilize their required experience and skills to ensure compliance with HSI standards. Required Skills/Experience for Contract Personnel:

- Be a U.S. Citizen
- Must meet High Risk, Law Enforcement Sensitive background and have the ability to obtain and maintain a TS-S/CI clearance.
- Have the ability to work embedded with an HSI Field Office and HSI Headquarters Components. This includes having the ability to operate as a member of team in an often-high stress high tempo office environment.
- 4-6 years of professional experience designing and testing web user interfaces.
- Have at least two (2) years of web-development experience including experience writing web applications using HMTL5, CSS3, and JavaScript.
- Have at least two (2) years of experience working with AdobeXD to design web UIs.
- Have at least two (2) years of experience building and maintaining a design style guide used by a web development team with more than five (5) developers.
- Have at least two (2) years of graphic artist experience, specifically designing icons and visual artifacts for use in web development.

1.1111 Desired Skills/Experience for Contract Personnel

- Experience developing web tools utilizing the React.js web framework.
- Experience developing web tools utilizing the Material UI components library for the React.js web framework.

- Experience implementing Section 508 compliant features into a design style guide.

5.1.8. DHS Certified Section 508 Trusted Tester

The DHS Certified Section 508 Trusted Tester shall be responsible for Section 508 compliance and is expected to utilize their required experience and skills to ensure compliance with HSI standards. Required Skills/Experience for Contract Personnel:

5.1.8.1. Be a U.S. Citizen
5.1.8.2. Must meet High Risk, Law Enforcement Sensitive background and have the ability to obtain and maintain a TS-S/CI clearance.
5.1.8.3. Have the ability to work embedded with HSI Field Offices and HSI Headquarters Components. This includes having the ability to operate as a member of team in an often-high stress high tempo office environment.
5.1.8.4. Possess an active version 3 or 4 certification from DHS as a Trusted Section 508 Tester.

5.2 Continuity of Support

The Contractor shall provide qualified personnel with relevant experience and domain knowledge in line with this performance work statement, in terms of necessary skills at the requisite level of knowledge and experience.

Adequate staffing is critical to successful performance of this requirement. The Contractor shall maintain adequate staffing levels while mitigating risks associated with absenteeism, staffing gaps and high turnover. The Contractor's quoted staffing plan is incorporated into the task order as Attachment 3. The Contractor shall ensure that the required level of support is maintained at all times. The Contractor shall ensure that adequate contract support personnel and all critical functions are present during all hours of operation as defined in paragraph 10.6 of this PWS. If for any reason the Contractor staffing levels are not maintained due to vacation, leave, appointments, gaps, turnover etc., the Contractor shall provide e-mail notification to the Contracting Officer's Representative (COR) in advance while otherwise providing a fully qualified replacement.

5.3 Key Personnel

Before replacing any individual designated as Key by the Government, the Contractor shall notify the Contracting Officer no less than 15 business days in advance, submit written justification for replacement, and provide the name and qualifications of any proposed substitute(s). All proposed substitutes shall possess qualifications equal to or superior to those of the Key person being replaced, unless otherwise approved by the Contracting Officer. The Contractor shall not replace Key Contractor personnel without approval from the Contracting Officer. The following Contractor personnel are designated as Key for this requirement. Note: The Government may designate additional Contractor personnel as Key at the time of award.

5.3.1. Program Manager

The Program Manager position has the requirements laid out in Section 5.1.1.

5.3.2. Lead Architect

The Lead Architect position has the requirements laid out in Section 5.1.2. The Architect Lead shall also have a current and active TS/SCI clearance.

5.3.3. Lead Web User Interface Developer

The Lead Web User Interface Developer will be responsible for designing, developing and UI/UX tools as outlined in Section 3. The Lead Web User Interface Developer will also be responsible for mentoring and directing junior developers of the Contract team related to technical tasks and agile project development practices. The Lead Web User Interface Developer will be required to meet all requirements laid out for Web User Interface Developer in **Section 4.2.3** and also meet the requirements listed in this section.

The lead web developer is responsible for being the contract team lead and the primary conduit between the contractor and the government for day to day operations. **The Government will not support a contractor program manager position for this task order.** Required Skills/Experience for Contract Personnel:

5.3.3.1. Have the ability to be onboarded and cleared security screening within two weeks of the contract being awarded. This can be accomplished via:

5.3.3.1.1. An active ICE suitability at a minimum of the Public Trust High level **OR**

5.3.3.1.2. Have an active National Security clearance at a minimum of the Secret level with a background that was adjudicated no more than 42 months prior to the contracts award date. This position is not a national security position however holding an active National Security clearance is a known pathway for rapidly obtaining ICE Public Trust High suitability.

5.3.3.2. Possess a minimum of **five (5) years** of web-development experience including experience writing web applications using HMTL5, CSS3 and JavaScript.

5.3.3.3. Possess a minimum of **five (5) years** of experience with a server-side computer language such as ReactJS, Python, PHP, NodeJS or AngularJS.

5.3.3.4. Possess a minimum of **one (1) year** of experience developing using ReactJS web framework.

5.3.3.5. Possess a minimum of **one (1) year** of experience utilizing containers (i.e. Docker) for the delivery of production web applications.

5.3.3.6. Possess a minimum of **two (2) years** of experience incorporating server-side interaction with microservices and REST API tools into production web applications.

5.3.3.7. Possess a minimum of **two (2) years** of experience incorporating structured code testing practices into their web development projects. An example of experience that would satisfy this requirement would be the incorporation of Selenium web driver tests into development.

5.3.3.8. Possess a minimum of **one (1) year** of experience in a leadership role on a development team consisting of at least three members.

5.3.4. DHS Certified Section 508 Trusted Tester

The DHS Certified Section 508 Trusted Tester position has the requirements laid out in Section 5.1.8.

5.3.5. Substitutions

The identified Key Personnel are critical to performance under this PWS. During the period of performance Key Personnel shall only be replaced with people of comparable skill and experience level. The Contractor shall obtain written approval from the contracting officer (CO), prior to replacement of any Key Personnel. All requests for substitutions shall be submitted in writing to the CO.

No changes in Key Personnel will be made unless the Contractor can demonstrate that the qualifications of prospective replacement personnel are equal to or better than the qualifications of the key personnel being replaced. The CO shall be notified in writing of any proposed substitution fifteen (15) days in advance of the proposed substitution. Such notification shall include:

5.3.5.1. An explanation of the circumstances necessitating the replacement
5.3.5.2. Provide a succession plan for the substitution
5.3.5.3. A complete resume of the proposed substitute
5.3.5.4. As requested by the CO, any other information which will enable them to judge whether or not the Contractor is maintaining the same level of high-quality key personnel

The CO will evaluate Key Personnel substitutions and will promptly notify the Contractor of his/her approval or disapproval in writing. All disapprovals will require re-submission of another substitution to fill key positions within two (2) weeks.

5.4. Key Personnel Limits

Contractor Key personnel shall not be assigned by the Contractor to more than one key position for this requirement.

5.5. Employee Identification

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

Contractor employees working on-site at Government facilities shall wear a Government issued identification badge. All Contractor employees shall identify themselves as Contractors when their status is not readily apparent (in meetings, when answering Government telephones, in e-mail messages, etc.) and display the Government issued badge in plain view above the waist at all times.

5.6. Employee Conduct

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

5.7. Removing Employees For Misconduct Or Security Reasons

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

6 Deliverables and Schedules

The following sections explain the required deliverables for this task order. All deliverables shall be provided in electronic format.

6.1. Transition In and Transition Out

6.1.1. Transition In

The Contractor shall present a Post Award Conference Brief as described in Section 6.2 after contract award and Kick Off Brief held by ICE to include an overview of the project team, scope of work, deliverables, transition activities, communication approach, initial risks, and next steps.

The Contractor shall be responsible for the transition of all technical activities identified in this PWS. The Contractor shall submit a final Transition in Plan within two (2) weeks after contract award reflecting all necessary activities and a project schedule 30 days after award. All Transition In activities must be completed within 30 to 60 days after the Kickoff meeting. The following technical activities must be included as part of the Transition In plan:

6.1.1.1. Inventory and orderly transfer of all Government Furnished Equipment and Property (GFE/GFP), software, licenses and current content and work product if applicable.
6.1.1.2. Transfer of documentation and service tickets currently in process.
6.1.1.3. Transfer of current project activities and user story backlog.
6.1.1.4. Workplace logistics and staffing plan: Identification of the key personnel transition team members by name, position, EOD, clearance, start date, and responsibilities.

6.1.1.5. All contract personnel must receive a Favorable Entrance on Duty (EOD) for all Contractor staff from the ICE Personnel Security Unit (PSU).
6.1.1.6. Coordination of knowledge transfer sessions with the incumbent Contractor.
6.1.1.7. Coordination of transition with the RAVEn Program Management.

The Transition In Plan shall be approved by the COR and ITPM and describe the Contractor's process for transitioning with no disruption in operational services. The Contractor shall commence all operations required by the contract as of the first day of the stated contract period of performance. Therefore, on the initial day of performance, the Contractor shall provide a workforce that is fully qualified and capable of performing all work required under the contract. In the event that the Government determines that sufficient staff is not onboard at any specific moment during performance of the contract, the Contractor shall pro-rate the monthly rate until all resources receive an EOD from PSU. For the purposes of determining a CLIN to be fully staffed on the Contract, the EOD date shall be the effective date. The Government also reserves to exercise this right in the event that staffing falls below what is stated in the SOW at any time during the period of performance.

In order to support transition and major on-boarding efforts, and while establishing the agile team's velocity (i.e., the measure of how much work the agile team can deliver during an average sprint for a given team), the majority of the CLINs in the Base Period of this award will be reimbursed on a Time and Materials basis. Surge requirements will be reimbursed on a Firm Fixed Price basis using monthly rates. Once all onboarding has occurred and the team's velocity has been established, the effort needed to support the requirements to an acceptable measure of performance is substantially predictable to the extent that it would not require significant staffing changes. As a result, the Government expects that all staff will be fully on-boarded and stabilized after the Base Period, and all work will convert to Firm Fixed Price for the remainder of contract performance. Due to the team-based nature of the work under this PWS, the Government expects each position to remain filled and stable throughout performance in order to successfully perform the requirements of this PWS.

6.1.2 Transition Out

The Contractor shall be responsible for the Transition Out of all technical activities identified in this PWS during the final period of performance. The Contractor shall submit the Transition Out Plan two (2) months prior to the contract expiration. The Contractor's Transition Out plan shall be approved by the COR.

The following technical activities must be included as part of the Transition Out Plan:
6.1.2.1. Inventory and orderly transfer of all GFE, software and licenses;
6.1.2.2. Submit all contract deliverables to date, including designs, documents, briefings, reports, spreadsheets, and source code;
6.1.2.3. Technical walkthrough of the application, environment, interfaces, backlog, help desk logs, etc.; and
6.1.2.4. Briefing on all in-progress and committed items.

The table below depicts the deliverables required during the period of performance.

Deliverable Description	Delivery Date / Frequency	Deliver To
Post Award Conference Brief	One (1) week after Task Order award	CO, COR, and Federal PM
Transition Plan (In)	Two (2) weeks after Task Order award	COR and Federal PM
Quality Control Plan (QCP)	30 calendar days after contract award and updated at beginning of every option period	CO, COR, and Federal PM
Quality Assurance Surveillance Plan (QASP)	60 calendar days after award	CO, COR, and Federal PM
Project Plan and Schedule	30 calendar days after Task Order award	COR and Federal PM
Weekly Status Reports	Due by 12:00 PM Eastern Time on Friday during the period of performance	COR and Federal PM
Monthly Status Reports	First 45 calendar days after contract award then monthly during the period of performance	COR and Federal PM
Requirements-Based Project Plans and Architecture documents to be defined upon issuance of project	As requested by the RAVEN PM	COR and Federal PM
Briefing material, correspondence, and other documentation	As requested by the RAVEN PM	COR and Federal PM
Respond to requests for information as needed. These requests may vary in nature and will be defined at time of request	As requested by the RAVEN PM	COR and Federal PM
System Documentation	30 calendar days before the end of the period of performance	COR and Federal PM
Final/revised documentation for all requested deliverables and outputs.	1 week before the end of the period of performance	COR and Federal PM
All items first produced under the Task Order	1 week before the end of the period of performance	COR and Federal PM
Transition Plan (Out)	60 calendar days prior to completion of period of performance	COR and Federal PM
Plan for transitioning analytic solutions and capabilities to the RAVEN Operation and Maintenance (O&M) team. This will include requirements such as code quality and frequency of Tier II and Tier III Help Desk requests consistently remaining below a set threshold for a set period of time.	30 calendar days prior to the end of the period of performance	COR and Federal PM

Deliverable Description	Delivery Date / Frequency	Deliver To
Source Code developed in response to all assigned projects and work	As Developed or Published to an ICE approved Repository.	COR and Federal PM
Any work first produced such as configuration scripts, security scripts, software written, user manuals, data models, interface control documents, technical descriptions of the software and scripts, user operations manuals and anything else first produced under this Task Order if applicable	30 calendar days prior to the end of the period of performance	COR and Federal PM
Standard Operating Procedures (SOPs)	As required	COR and Federal PM
ICE Agile Maturity Model Self-Assessment	Quarterly (Fiscal)	COR and Federal PM
IT Security Plan	30 calendar days after Task Order award	COR and Federal PM

References to "days" within this document, if not otherwise specified, shall be interpreted to mean calendar days.

6.2. Post Award Conference Brief/Progress Meeting

The Contractor agrees to attend any post award conference convened by the contracting activity office in accordance with Federal Acquisition Regulation Subpart 42.5. The contracting officer, Contracting Officers Representative (COR), and other Government personnel, as appropriate, may meet periodically with the Contractor to review the Contractor's performance. At these meetings the Contracting Officer will apprise the Contractor of how the Government views the Contractor's performance and the Contractor will apprise the Government of problems, if any, being experienced. Appropriate action shall be taken to resolve outstanding issues. These meetings shall be at no additional cost to the Government. The Contractor shall present the Post Award Conference briefing one (1) week after award, to include an overview of the project team, scope of work, deliverables, transition activities, communication approach, initial risks, and next steps.

6.3. Quality Control Plan (QCP)

The Quality Control Plan (QCP) is developed by the Contractor and is the driver for service quality. The Contractor is required to develop a comprehensive program of inspections and monitoring actions, to include the QCP. The QCP, in conjunction with the QASP, is intended to verify that the Contractor's quality control program and is intended to provide the measures needed to lead the Contractor to project success. Once the quality control program, to include the QCP, is approved by the Government, careful application of the process and standards presented in the QASP document will ensure a robust quality assurance program. A final QCP will be completed by the Contractor and due 30 calendar days after award of the contract. An updated QCP will be submitted at the beginning of each optional period of performance.

6.4. System Lifecycle Management Deliverables

The Contractor, with significant input from the Government, shall provide SLM deliverables as required for Agile Software Development. The Government anticipates a tailoring plan for each major system release to be in compliance with the SLM Agile design patterns. All appropriate documentation[1] shall be prepared in accordance with the guidelines specified by the SLM and the approved Project Tailoring Plan with appropriate elevation to the DHS Systems Engineering Life Cycle (SELC) as appropriate for major acquisitions.

6.5. Weekly Status Reports

The Contractor shall prepare a weekly status report. The intended audience includes Government Project Managers, Product Owners, and the Scrum Team (including external stakeholders). Weekly status reports are due by 12:00 PM Eastern Time on Friday. The weekly status report will include:

6.5.1. Description of work accomplished.
6.5.2. Work planned for the following week.
6.5.3. Deviations from planned activities (changes in scope).
6.5.4. Open issues and risks (including remediation plan).

6.6. Monthly Status Report

The Contractor shall prepare a monthly status report to include Performance, Financial and Staffing, Inventory, and Technical Status. The initial report is due forty-five calendar days after award and shall cover the first calendar month of performance. Subsequent reports will be provided monthly within thirty days of the end of each calendar month until the last month of performance. The final delivery shall occur ten days before the end of the final option period and shall summarize performance during the period of performance and provide the status of any planned transition activity. The monthly report shall be electronic and in a format agreed to by RAVEN Program Management, to be established after award.

6.6.1. Performance Reports shall include the following:

6.6.1.1. Description of the work
6.6.1.2. Description of work accomplished
6.6.1.3. Analysis of the difference between planned and accomplished
6.6.1.4. Work planned for the following month
6.6.1.5. Open issues
6.6.1.6. Risk Register
6.6.1.7. System Performance metrics
6.6.1.8. Performance Standard Metrics
6.6.1.9 RAVEN Operational Requirements Metrics

6.7.2. Financial and Staffing Reports shall include the following:

The labor burn rate report, other directs, travel, etc., of costs incurred during the reporting period. This report is tracked at the CLIN level and includes the planned budget, actuals, and the variance for each month through Task Order completion. The report shall also provide staffing level metrics.

The Staffing Report shall detail total hours available for work, per month, less the total hours worked per month in accordance with Government provided format after award. The Staffing Report shall identify any credits to the FFP Monthly invoice due to absence.

6.7.3. Technical Status Reports shall include the following:

6.7.3.1. Period being reported.
6.7.3.2. A narrative of all Contractor work performed during the previous month, including.
6.7.3.3. A description and assessment of technical progress.
6.7.3.4. Status of each applicable task with a description and overview of items and activities completed in the reporting period and planned activities for the next reporting period.
6.7.3.5. Identification of any risks and mitigation plans for those risks including any challenges and the Contractor's plans to overcome those challenges.
6.7.3.6. Updated Project Schedule. The Contractor shall provide an updated project schedule clearly depicting any schedule changes from the previous submission.

6.7.4. GFE Inventory Report

The Contractor shall keep an inventory of GFE/GFP, which shall be made available to the COR and ITPM monthly, or upon request. The Contractor shall ensure that all GFE/GFP provided for their use shall be secured. The Contractor shall manage, maintain, and control all GFE/GFP in support of this Task Order. The report shall document the asset tag information, serial number, assigned resource, primary office location, the date issued, and a description of the asset

6.7.5. System Documentation

One month prior to contract expiration, the Contractor shall provide the following:

6.7.5.1. Plan for transitioning analytic solutions and capabilities to the RAVEN Operation and Maintenance (O&M) team. This will include requirements such as code quality and frequency of Tier II and Tier III Help Desk requests consistently remaining below a set threshold for a set period of time. Interface control documents for system components and networks.
6.7.5.2. Documentation required to meet requirements set forth in DHS Management Directive 102–01, Acquisition Management Directive.
6.7.5.3. Additional documentation as identified and required for OMB, FISMA and internal DHS Government IT projects.
6.7.5.4. At the end of the period of performance, the Contractor shall provide any work first produced such as configuration scripts, security scripts, software written, user manuals, data models, interface control documents, user manuals, technical descriptions of the software and scripts, user operations manuals, system maintenance manuals, and anything else first produced under this Task Order.

6.7.5.5. Data required in accordance with FAR clause 52.227-17.

The Contractor shall develop all major systems interfaces based on nonproprietary, widely supported, and consensus-based standards. The Contractor shall provide authorized access, retention, integration, sharing, transfer, and conversion of IP deliverables. The Offeror shall ensure that processes and tools are in place / use the existing tools in place to support product configuration management, data loss prevention, and data sharing and exchange.

6.7.6. Delivery Instructions

The Contractor shall provide electronic copies of each deliverable. Electronic copies shall be delivered via ICE SharePoint and e-mail. E-mail deliverables should be clearly marked in the subject line as a deliverable (requiring review and/or action by the Government). Electronic copies shall be compatible with Microsoft Office or other applications as appropriate and mutually agreed upon by the parties.

6.7.7. Written Acceptance/Rejection by the Government

The Government shall provide written notification of acceptance or rejection of all final deliverables within two (2) weeks of receipt. All notifications of rejection will be accompanied with an explanation of the specific deficiencies causing the rejection. Items must be approved by the COR and/or the appropriate Government authority to be considered "accepted." Deficiencies shall be corrected within 5 business days of the rejection notice. If the deficiencies cannot be corrected within 5 business days, the Contractor shall immediately notify the COR of the reason for the delay and provide a proposed corrective action plan within 5 business days of receiving the non-conforming products or service notification.

Deliverables shall be deemed acceptable if the document adequately covers all required topics, meets general quality measures; and is professionally prepared in terms of format, clarity and readability; and is delivered in electronic copy on time to the designated delivery location. General quality measures, as set forth below, shall be applied to each work product received from the Contractor.

6.7.7.1. **Accuracy:** Work Products shall be accurate in presentation, technical content, and adherence to accepted elements of style.

6.7.7.2. **Clarity:** Work Products shall be clear and concise. Any/All diagrams and graphics shall be easy to understand and be relevant to the supporting narrative.

6.7.7.3. **File Editing:** All text and diagrammatic files shall be editable by the Government.

6.7.7.4. **Format:** Work Products shall be transmitted via e-mail and in media mutually agreed upon prior to submission.

6.7.7.5. **Timeliness:** Work Products shall be submitted on or before the due date specified in this statement of work or submitted in accordance with a later scheduled date determined by the Government.

The documents shall be considered final upon receiving Government approval. Unless otherwise stated, all deliverables shall be delivered via e-mail not later than 4:00 PM ET on the deliverable's due date.

7. Applicable Documents

The Contractor shall abide by all applicable Federal, DHS, and ICE regulations, policies, standards, publications, manuals and procedures. Note that not all laws and regulations are listed below; the guidance listed provides ICE and/or DHS implementation policies and/or procedures for higher level guidance. If newer versions of these documents are officially released, the Contractor shall comply with the updated versions within the timeframe established by the Government.

7.1 ICE Technical Architecture Guidebook
7.2 ICE Technical Reference Model (TRM) (Standards Profile)
7.3. ICE Enterprise Systems Assurance Plan
7.4. Management Instruction (MI) ICE-OCIO-001 for Agile Development, including Appendices
7.5. ICE Agile-DevOps Playbook
7.6. DHS Management Directive (MD) 4300.1, Information Technology Systems Security
7.7. DHS 4300A Sensitive Systems Policy, Version 9.1, July 17, 2012
7.8. DHS 4300B National Security Systems Policy, Version 8.0, December 27, 2010
7.9. DHS Management Directive (MD) 11042.1, Safeguarding Sensitive But Unclassified (For Official Use Only) Information, January 6, 2005
7.10. ICE Management Directive (MD) 4003.1, Safeguarding Law Enforcement Sensitive Information, March 23, 2007
7.11. ICE Management Directive (MD) 4001.1, Electronic and Information Technology and Accessibility, March 12, 2009
7.12. DHS Directive 047-01, Privacy Policy and Compliance, July 7, 2011
7.13. The Government recommends that the Contractor use the Information
7.14. Technology Infrastructure Library (ITIL) framework in the performance of this task
7.15. DHS Memorandum: Class Deviation 15-01 from the Homeland of Security Acquisition Regulation: Safeguarding of Sensitive Information, March 9, 2015

Development Approach: The Contractor shall follow the ICE Agile development methodology described in the ICE-Management-Instruction-001 for Agile Development, ICE-Management-Instruction-001 Appendix, and ICE AgileDevOps Handbook. The Contractor shall be primarily concerned with the implementation cycle, which in the case of Scrum includes sprint planning, application design, development and testing, deployment, sprint review, and sprint retrospective. The HSI Innovation Lab currently implements two-week sprints.

The Contractor shall use the Government-provided virtual non-production and production environments. The Government will provide and support these environments, which are hosted in cloud service provider infrastructure, currently Amazon Web Services (AWS). The Government will provide and support the infrastructure. The Contractor shall use the Government-provided Product Backlog Repository and defect management tool, currently JIRA, to track user story and task progress. The Contractor shall store and manage all system configuration settings, development code and where appropriate documentation in the ICE Approved Software Configuration Management (SCM) system, currently GitHub Enterprise. The Contractor shall document operational tasks and Standard Operating Procedures (SOPs) in an ICE Approved knowledge management portal. The Contractor shall leverage automation tools to reduce the number of manual tasks performed during operations. This may include recurring

tasks, scheduled jobs, monitoring, updates, patching, user maintenance, and other operational tasks.

8. Performance Standards

Performance standards define desired services. The Government performs surveillance to determine if the Contractor exceeds, meets or does not meet these standards.

This section includes performance standards in accordance with the RAVEN User Interface/User Experience Quality Assurance Surveillance Plan (QASP). The Government shall use these standards to determine Contractor performance and shall compare Contractor performance to the Acceptable Quality Level (AQL).

Performance Standards		
TASK/STANDARD DESCRIPTION	**Acceptable Quality Level (i.e., The minimum level of quality that will be accepted by ICE to meet the performance standard.)**	**Incentive/Disincentive**
The Contractor shall maintain adequate staffing levels while mitigating risks associated with absenteeism, staffing gaps and high turnover. The Contractor shall submit security packages for all personnel, as required by the PWS, within 30 days of award.	95% of security packages are submitted within 30 Days Maintains staffing level of 90% at all times during hours of operation.	On a monthly basis, considering total contract staffing levels, the total work hours in a given month vs the total hours actually worked. If the staffing shortfall is corrected within 30 days, then this standard will be satisfied The Contractor will identify their performance metrics for this standard in the Monthly Report. If this standard is not met, it will be documented in the performance reports, and may result in requirements for written corrective action plan, formal documentation in Contract Performance and Evaluation Records (CPARS) and / or impact exercise of future options.
The Contractor shall expeditiously and effectively pre-vet/onboard clearance ready personnel for Public High Trust and TS/SCI investigations throughout performance. Measured on a monthly basis by the number of personnel accepted vs. number of personnel packages not presented on-time or rejected for security reasons.	98% timely submission; two (2) business days late is acceptable; more than two (2) days late is unacceptable. No more than 2% rejection of personnel for security reasons.	The Contractor will identify their performance metrics for this standard in the Monthly Report. On a monthly basis, considering the total staffing position requirements vs the total staffing positions not yet filled, the Government will review personnel security packages for timely submission and rejection rates. If personnel security packages are submitted timely (DEFINE TIMELY) and there are no more that 2% rejection of personnel for security reasons within the same 30-day period, the Government will pay an incentive consistent with the monthly rate identified in the incentive CLIN. If the Contract is fully staffed for the entire month with cleared personnel, this performance measure is determined to have been met and the incentive shall apply.

All deliverables (unless separately identified) shall adequately cover all required topics, meet general quality measures, be professionally prepared in terms of format, clarity and readability; and be delivered in electronic copy on time to the designated delivery location. General quality measures, as set forth herein, shall be applied to each work product received from the Contractor. Measured on a monthly basis by the number of deliverables accepted vs. number not delivered on-time or rejected.	95% timely submission; two (2) business days late is acceptable; more than two (2) days late is unacceptable. No more than 2% error, rework or duplication.	The Contractor will identify their performance metrics for this standard in the Monthly Report. If this standard is not met, it will be documented in the performance reports, and may result in requirements for written corrective action plan, formal documentation in Contract Performance and Evaluation Records (CPARS) and / or impact exercise of future options.
Weekly Status Reports shall adequately cover all required topics, meet general quality measures, be professionally prepared in terms of format, clarity and readability; and be delivered in electronic copy on time to the designated delivery location. General quality measures, as set forth herein, shall be applied to each work product received from the Contractor. Measured on a weekly basis by the number of reports accepted vs. number not delivered on-time or rejected.	95% timely submission; two (2) business days late is acceptable; more than two (2) days late is unacceptable. No more than 2% error, rework or duplication.	The Contractor will identify their performance metrics for this standard in the Monthly Report. If this standard is not met, it will be documented in the performance reports, and may result in requirements for written corrective action plan, formal documentation in Contract Performance and Evaluation Records (CPARS) and / or impact exercise of future options.
Monthly Status Reports shall adequately cover all required topics, meet general quality measures, be professionally prepared in terms of format, clarity and readability; and be delivered in electronic copy on time to the designated delivery location. General quality measures, as set forth herein, shall be applied to each work product received from the Contractor. Measured on a monthly basis by the number of reports accepted vs. number not delivered on-time or rejected.	91% timely submission; two (2) business days late is acceptable; more than two (2) days late is unacceptable. No more than 2% error, rework or duplication.	The Contractor will identify their performance metrics for this standard in the Monthly Report. If this standard is not met, it will be documented in the performance reports, and may result in requirements for written corrective action plan, formal documentation in Contract Performance and Evaluation Records (CPARS) and / or impact exercise of future options.
Requirements-Based Project Plans, Architecture documents, and Code shall adequately cover all required topics, meet general quality measures, be professionally prepared in terms of format, clarity and readability; and be delivered in electronic copy on time to the designated delivery location. General quality measures, as set forth herein, shall be applied to each work product received from the Contractor. Measured as requested by the number of plans and documents accepted vs. number not delivered on-time or rejected.	95% timely submission; two (2) business days late is acceptable; more than two (2) days late is unacceptable. No more than 2% error, rework or duplication.	The Contractor will identify their performance metrics for this standard in the Monthly Report. If this standard is not met, it will be documented in the performance reports, and may result in requirements for written corrective action plan, formal documentation in Contract Performance and Evaluation Records (CPARS) and / or impact exercise of future options.

Operational Requirements Metrics: The Contractor shall work within their solutions development teams to meet all applicable operational requirements as identified in Attachment E – RAVEN Operational Requirements. As the RAVEN program progresses through the agile process, additional operational requirements will be assigned to solutions development teams as performance standards.	Assigned Operational Requirements are met or exceeded 90% of the time.	The Contractor will identify their performance metrics for this standard in the Monthly Report. If this standard is not met, it will be documented in the performance reports, and may result in requirements for written corrective action plan, formal documentation in Contract Performance and Evaluation Records (CPARS) and / or impact exercise of future options.

9. Other General Requirements

9.1. **Government Furnished Resources:** If work at Government-provided facilities is necessary for the services being performed under this PWS, such facilities will be provided at ICE Offices identified above. Parking facilities are not provided. Basic facilities such as workspace and associated operating requirements will be provided to Task Order personnel that are providing support at the designated facilities.

The Government will provide the Contractor with basic equipment and property (e.g., laptops, desktops, thumb drives and mobile smart phones). The Government will also provide access to ICE mandated tools such as JIRA, Remedy, and other applications as needed to support this effort. ICE reserves the right to add, delete, or modify at its discretion any hardware or software at any time during Task Order performance, based upon what, in ICE's judgment, is necessary to most effectively and efficiently perform the mission.

All GFE/GFP provided to the Contractor to perform work under this Call Order shall be returned to the Government at the end of the period of performance. The Contractor shall keep an inventory of GFE/GFP, which shall be made available to the COR or CO upon request. The Contractor shall ensure that all GFE/GFP provided for their use shall be secured. The Contractor shall manage, maintain, and control all GFE/GFP in support of this Task Order.

Within 24 hours after initial request from the COR, the Contractor shall provide a GFE inventory report. The report shall include asset tag information, serial number, assigned resource, primary office location, the date issued, and a description of the asset.

The Contractor shall use Government furnished information, data, and documents only for the performance of work under this contract and shall be responsible for returning all Government furnished information, data and documents to the Government at the end of the performance period. The Contractor shall not release Government furnished information, data and documents to outside parties without the prior and explicit consent of the Contracting Officer. Nothing herein shall be deemed to grant the Contractor any right or title in or to such Government Data, unless and to the extent expressly granted herein. The Contractor shall return all such Government Data to the Contracting Officer by the end of the period of performance or such other data as may be specifically directed by the Contracting Officer in writing.

9.2. **Contractor Furnished Property:** The Contractor shall furnish all materials, equipment, and services necessary to fulfill the requirements of this contract, except for the Government Furnished Resources specified this PWS.

9.3. **Staffing Plan:** The Staffing Plan produced by the Contractor and accepted by the Government can be found in the Contractor's Task Order award.

9.4. **Period Of Performance:** The period of performance for this contract is a one-year base period (inclusive of transition) with four one-year option periods as follows:

Base Period/Transition-In	September 24, 2021 through September 23, 2022
Option Period 1	September 24, 2022 through September 23, 2023
Option Period 2	September 24, 2023 through September 23, 2024
Option Period 3	September 24, 2024 through September 23, 2025
Option Period 4	September 24, 2025 through September 23, 2026
6 Month Extension (Option)	N/A (Will be evaluated at award.)

9.5. **Place of Performance:** Work shall be performed primarily at the Government's facility located at 1901 South Bell Street, Arlington, VA 22202, 4141 N. Sam Houston Pkwy E, Houston, TX 77032 and other domestic locations mutually agreeable to the Government and the Contractor.

The Contractor shall establish a collaborative work environment that is conducive to Agile project execution, allowing for co-location of business sponsors, stakeholders, project sponsors, product owners, and development teams. The Contractor shall establish a daily scrum board that can be easily shared with team members participating virtually. Additionally, on occasion, Contractor personnel may be required to attend meetings/briefings at the following locations:

9.5.1. 801 I Street, NW, Washington, DC 20536
9.5.2. ICE Technical Operations in Lorton, VA
9.5.3. Cyber Crimes Center in Fairfax, VA
9.5.4. National Targeting Center in Reston, VA
9.5.5. Any other on-site locations requested by the Government, within the metro DC area
9.5.6. All Classified work will be performed at a Government Site.

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

9.7. Telework: Telework is authorized under this contract when it is in the best interest of the Government. The Contractor may telework one day per week as coordinated with the Contracting Officer and COR. When the federal Government offices are closed due to inclement weather or other emergency situations, the Contractor will be required to telework. In other extenuating circumstances, such as a pandemic event or when the Office of Personnel

Management (OPM) changes the federal Operating Status, the Contractor may telework more than one day per week based on the guidance provided by the CO and COR in writing.

9.8. Non-Personal Services: DHS retains the authority to make all decisions regarding the DHS mission, and the execution or interpretation of laws of the United States. Contractor services defined are not considered to be inherently Governmental in nature, as defined by FAR Subpart 7.5. This is a non-personal services contract as defined by FAR Subpart 37.101. Contractor personnel rendering services under this requirement are not subject to supervision or control by Government personnel. The Contractor will be responsible for the supervision of the Contractor employees. The Contractor is expected to work independently to accomplish the requirements under this PWS. **Ultimate design strategy and decisions are owned by the Government. The Government may, at times, allow the team to provide design recommendations in order to foster innovation and new ideas, but accountability rests with the Government to ensure that design supports the desired business intent and adheres to agency and Government guidance.**

9.9 Organizational Conflict of Interest (OCI): Pursuant to FAR Subpart 9.5 and Homeland Security Acquisition Regulation (HSAR) 3052.209-72, the Contractor shall manage work distribution to ensure there are no OCIs. The Contractor shall promptly notify the Government when such a situation occurs and provide the CO with the associated mitigation plan.

9.10. Travel: Travel may be required for this Task Order. Additionally, the Contractor may be required to travel to HSI offices throughout the country. The Contractor shall request all travel in writing and provide the names of individuals traveling, dates, destination(s), purpose, and estimated costs. All travel is subject to advance Government approval by the COR prior to incurring costs. The Contractor must submit the request through the Government PM and route it through the COR for approval via the Government PM. Approval shall be provided in writing. Reimbursement for local travel is not authorized. Local travel is defined as within 50 miles of the District of Columbia; Washington D.C. area. Approved travel outside of the defined local area will be reimbursed in accordance with the limits set forth in FAR Part 31.205-46 Travel Costs and the Federal Travel Regulations (FTR). No profit is allowed for travel. Indirect costs may be applied to travel in accordance with the Offeror's established accounting practices consistent with FAR 31.2 Contracts with Commercial Organizations. Travel will be a separate not-to-exceed CLIN on the Task Order. The travel costs will be minimized, to the maximum extent possible, by taking advantage of discounted airfare rates available through advance purchase. The Government will only pay travel expenses in accordance with FTR rates. Required travel within the National Capital Region is considered within scope of this Task Order and will not be reimbursed. Upon completion of travel, all documentation associated with the respective travel shall be submitted with the invoices. Travel shall only be reimbursed to the Contractor based on actual costs incurred.

9.11 Security Requirements: Contractor access to classified information is required under this PWS. The maximum level of classification is Law Enforcement Sensitive. At the time of award, the Contractor shall have the appropriate Top Secret or Secret security clearances for the employees as required by the Work Assignment they will work under on this contract. Affected employees must have a current investigation in place or being processed for a periodic reinvestigation. A Department of Defense Contract Security Classification Specification (DD Form 254) shall be issued by the GCA CO to the Contractor at the time of contract award (FAR 4.403) (c)(1)). The contracting officer shall also provide a copy to the DSS and the GCA

COR. In accordance with DoD Manual 5200.22M, Industrial Security Manual for Safeguarding Classified Information, the Contractor shall have a Facility Clearance issued by DSS.'

The majority of the work conducted on this contract will be at the High Risk, Law Enforcement Sensitive but Unclassified level. There will be the need to develop mechanisms to port information into the HSI Innovation Lab's classified environment and develop tools/processes as outlined throughout this PWS in a classified environment when directed by the Government. As detailed in the PWS, all personnel will be required to pass a T4 National Background Investigation Services (NBIS) investigation to receive a Public Trust High Risk assessment. Approximately 25% of all personnel on this order will require the ability to obtain and maintain an active TS/SCI clearance. ICE will require the Key Personnel (Program Manager, Architect – Lead, UX Designer – Lead, DHS 508 Tester – Lead) and One (1) Architect to have active TS clearances with Defense Counterintelligence and Security Agency (DCSA) prior to on-boarding. ICE is not be able to grant or accept a temporary adjudication for TS clearances.

All work conducted as part of this task is expected to align with ICE privacy and information assurance policies and regulations regarding the creation and maintenance of systems technology.

The attachments to this PWS are incorporated in full force and effect. The Contractor shall adhere to the requirements of each attachment.

9.12 DHS Geospatial Information System Compliance

All implementations including geospatial data, information, and services shall comply with the policies and requirements set forth in the DHS Geospatial Information Infrastructure (Gil), including (but not limited to) the following:

All data built to the GII whether adopted or developed, shall be submitted to the government for review and insertion into the DHS Data Reference Model.
All software built to the GII, whether adopted or developed, shall be submitted to the government for review and insertion into the DHS Technical Reference Model.

A. SECTION 508 REQUIREMENTS

A.1. Section 508 of the Rehabilitation Act, as amended by the Workforce Investment Act of 1998 (P.L. 105-220) (codified at 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.

A.2. 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 & Appendix A, C & D, and available at https://www.gpo.gov/fdsys/pkg/CFR-2017-title36-vol3/pdf/CFR-2017-title36-vol3-part1194.pdf. 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.

A.3. 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.

A.3.1. Section 508 Requirements for Technology Services

A.4. When developing or modifying ICT, the Contractor is required to validate ICT deliverables for conformance to the applicable Section 508 requirements. Validation shall occur on a frequency that ensures Section 508 requirements is evaluated within each iteration and release that contains user interface functionality.

A.5. When modifying, installing, configuring or integrating commercially available or Government-owned ICT, the Contractor shall not reduce the original ICT Item's level of Section 508 conformance.

A.6. When developing or modifying web based and electronic content components, except for electronic documents and non-fillable forms provided in a Microsoft Office or Adobe PDF format, the Contractor shall demonstrate conformance to the applicable Section 508 standards (including WCAG 2.0 Level A and AA Success Criteria) by conducting testing using the DHS Trusted Tester for Web Methodology Version 5.0 or successor versions, and shall ensure testing is conducted by individuals who are certified by DHS on version 5.0 or successor versions (e.g. "DHS Certified Trusted Testers"). The Contractor shall provide the Trusted Tester Certification IDs to DHS upon request. Information on the DHS Trusted Tester for Web Methodology Version 5.0, related test tools, test reporting, training, and tester certification requirements is published at https://www.dhs.gov/trusted-tester.

A.7. When developing or modifying ICT deliverables that contain the ability to automatically generate electronic documents and forms in Microsoft Office and Adobe formats, or when the capability is provided to enable end users to design and author web based electronic content (i.e. surveys, dashboards, charts, data visualizations, etc.), the Contractor shall demonstrate the ability to ensure these outputs conform to the applicable Section 508 standards (including WCAG 2.0 Level A and AA Success Criteria). The Contractor shall demonstrate conformance by conducting testing and reporting test results based on representative sample outputs. For outputs produced as Microsoft Office and Adobe PDF file formats, the Contractor shall use the test methods published under "Accessibility Tests for Documents", which are published at https://www.dhs.gov/compliance-test-processes. For outputs produced as web based electronic content, the Contractor shall use the DHS Trusted Tester for Web Methodology Version 5.0, or successor versions. This methodology is published at https://www.dhs.gov/trusted-tester

A.8. When developing or modifying software functions of ICT, the Contractor shall demonstrate conformance to the applicable Section 508 standards (including the requirements in Chapter 5 and WCAG 2.0 Level A and AA Success Criteria). When the requirements in Chapter 5 do not address one or more software functions, the Contractor shall demonstrate conformance to the Functional Performance Criteria specified in Chapter 3. The Contractor shall use a test process capable of validating conformance to all applicable Section 508 standards for software functionality delivered pursuant to this contract. The Contractor may utilize the DHS Trusted Tester Methodology for Web and Software Version 4.0 as a component of the overall test process used. This version of the test process provides partial test coverage of the Section 508 standards that apply to software. If the Contractor uses this test process, the Contractor shall address the test coverage gaps through additional test procedures. Information on the DHS Trusted Tester Methodology for Web and Software Version 4.0, including coverage against the applicable Section 508 standards for software as well as gaps that need to be addressed through other test methods, related test tools, and training is published at https://www.dhs.gov/trusted-tester.

A.9. Contractor personnel shall possess the knowledge, skills and abilities necessary to address the accessibility requirements in this work statement.

A.9.1. Section 508 Deliverables

A.10. Section 508 Test Plans: When developing or modifying ICT pursuant to this contract, the Contractor shall provide a detailed Section 508 Conformance Test Plan. The Test Plan shall describe the scope of components that will be tested, an explanation of the test process that will be used, when testing will be conducted during the project development life cycle, who will conduct the testing, how test results will be reported, and any key assumptions.

A.11. Section 508 Test Results: When developing or modifying ICT pursuant to this contract, the Contractor shall provide test results in accordance with the Section 508 Requirements for Technology Services provided in this solicitation.

A.12. 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.

A.13. Other Section 508 Documentation: The following documentation shall be provided upon request for ICT items offered through this contract:

A.14. Documentation of features provided to help achieve accessibility and usability for people with disabilities.

A.15. Documentation on how to configure and install the ICT Item to support accessibility.

A.16. Documentation of core functions that cannot be accessed by persons with disabilities.

A.17. Documentation of remediation plans to address non-conformance to the Section 508 standards

Attachment B – Privacy and Security Requirements

B-1. 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 **www.dhs.gov/privacy**. Applicable SORNS of other agencies may be accessed through the agencies' websites or by searching FDsys, the Federal Digital System, available at **http://www.gpo.gov/fdsys/**. 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.

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 PWS 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.

8. 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.

B-2. Required Security Language For Sensitive /But Unclassifed (SBU) Contracts

SECURITY REQUIREMENTS

GENERAL

The United States Immigration and Customs Enforcement (ICE) has determined that performance of the tasks as described in Contract **TBD (at award)** 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 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 preliminary Fitness determination or final Fitness determination by the Office of Professional Responsibility, Personnel Security Unit (OPR-PSU). No employee of the Contractor shall be allowed unescorted access to a Government facility without a favorable preliminary Fitness determination or final Fitness determination by OPR-PSU. Contract employees are processed under DHS Instruction 121-01-007-001 (Personnel Security, Suitability and Fitness Program), 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, temporaries, 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 the Personnel Security Unit. Contractor employees nominated by a Contracting Officer Representative for consideration to support this contract shall submit the following security vetting documentation to OPR-PSU, through the Contracting Officer Representative (COR), within 10 days of notification by OPR-PSU of nomination by the COR and initiation of an Electronic Questionnaire for Investigation Processing (e-QIP) in the Office of Personnel Management (OPM) automated on-line system.

Standard Form 85P (Standard Form 85PS (With supplement to 85P required for armed positions)), "Questionnaire for Public Trust Positions" Form completed on-line and archived by the Contractor employee in their OPM e-QIP account.

Signature Release Forms (Three total) generated by OPM e-QIP upon completion of Questionnaire (e-signature recommended/acceptable – instructions provided to applicant by OPR-PSU). Completed on-line and archived by the Contractor employee in their OPM e-QIP account.

Two (2) SF 87 (Rev. December 2017) Fingerprint Cards. (Two Original Cards sent via COR to OPR-PSU)

Foreign National Relatives or Associates Statement. (This document sent as an attachment in an e-mail to Contractor employee from OPR-PSU – must be signed and archived into Contractor employee's OPM e-QIP account prior to electronic "Release" of data via on-line account)

DHS 11000-9, "Disclosure and Authorization Pertaining to Consumer Reports Pursuant to the Fair Credit Reporting Act" (This document sent as an attachment in an e-mail to Contractor employee from OPR-PSU – must be signed and archived into Contractor employee's OPM e-QIP account prior to electronic "Release" of data via on-line account)

Optional Form 306 Declaration for Federal Employment (This document sent as an attachment in an e-mail to Contractor employee from OPR-PSU – must be signed and archived into Contractor employee's OPM e-QIP account prior to electronic "Release" of data via on-line account)

If occupying PREA designated position: Questionnaire regarding conduct defined under 6 CFR § 115.117 (Sexual Abuse and Assault Prevention Standards) (This document sent as an attachment in an e-mail to Contractor employee from OPR-PSU – must be signed and archived into Contractor employee's OPM e-QIP account prior to electronic "Release" of data via on-line account)

One additional document may be applicable if Contractor employee was born abroad. If applicable, additional form and instructions will be provided to Contractor employee. (If applicable, the document will be sent as an attachment in an e-mail to Contractor employee from OPR-PSU – must be signed and archived into Contractor employee's OPM e-QIP account prior to electronic "Release" of data via on-line 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 7 will be required for positions designated under PREA.

An adequate and current investigation is one where the investigation is not more than five years old, 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-PSU at the time of award of the contract. Only complete packages will be accepted by the OPR-PSU as notified by the COR.

To ensure adequate background investigative coverage, Contractor employees must currently reside in the United States or its Territories. Additionally, Contractor employees are required to have resided within the Unites States or its Territories for three or more years out of the last five (ICE retains the right to deem a Contractor 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.

TRANSFERS FROM OTHER DHS CONTRACTS:

Contractor employees may be eligible for transfer from other DHS Component contracts provided they have an adequate and current investigation meeting the new assignment requirement. If the Contractor employee does not meet the new assignment requirement a DHS 11000-25 with ICE supplemental page will be submitted to OPR-PSU to initiate a new investigation.

Transfers will be accomplished by submitting a DHS 11000-25 with ICE supplemental page indicating "Contract Change." The questionnaire related to 6 CFR § 115.117 listed above in item 7 will be required for positions designated under PREA.

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

REQUIRED REPORTS

The Contractor will notify OPR-PSU, via the COR, of all terminations/resignations of Contractor employees under the contract within five days of occurrence. 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 the OPR-PSU, 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 containing the names of Contractor employees who are active, pending hire, have departed within the quarter or have had a legal name change (Submitted with documentation). 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.

CORs will submit reports to psu-industrial-security@ice.dhs.gov

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 NDA for Contractor access to sensitive information. The NDA will be administered by the COR to the 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 should be reported to ICE.ADSEC@ICE.dhs.gov.

SECURITY MANAGEMENT
The Contractor shall appoint a senior official to act as the Corporate Security Officer. The individual will interface with the OPR-PSU 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 the OPR-PSU 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 in order to effect compliance with such requirements.

INFORMATION TECHNOLOGY SECURITY CLEARANCE
When sensitive Government information is processed on Department telecommunications and automated information systems, the Contractor 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, whether or not the failure results in criminal prosecution. Any person who improperly discloses sensitive information is subject to criminal and civil penalties and sanctions under a variety of laws (e.g., Privacy Act).

INFORMATION TECHNOLOGY SECURITY TRAINING AND OVERSIGHT
In accordance with Chief Information Office 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, Information Assurance Awareness Training (IAAT) will be required upon initial access and annually thereafter. IAAT 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 PALMS or by contacting ICE.ADSEC@ICE.dhs.gov. Department 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).

1.1 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.
- All IT hardware and software shall be compliant with the HLS EA Technical Reference Model (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 Enterprise Data Management Policy Directive 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.

1.2 APPLICATION ARCHITECTURE

ICE Application Architecture Compliance

- The Contractor shall ensure that the application is designed and developed for browser independence, i.e., the application will generally work with any of the major browsers. ICE currently uses Internet Explorer (IE) version 11 configured with numerous Group Policy Objects (GPOs) as well as Chrome for Work, similarly, secured with centrally managed security policies. Browser specific implementations or limitations on browser independence must be approved in writing by ICE OCIO prior to development. Web Applications should be designed utilizing a responsive web design (RWD) approach, to provide an optimal viewing and interaction experience, independent of the particular platform capabilities the end user is utilizing. If ICE OCIO upgrades to a newer version of IE or Chrome for Work, the Contractor shall ensure the application is compatible with the future version.

Open-Source Compliance

- The Contractor shall follow the ICE Open-Source Manifesto when evaluating any technologies, tools, software, and/or application programmable interfaces (API's) to support a system.
- The Contractor shall prioritize the adoption of, and migration to, Open-Source technologies over proprietary or "closed" technologies.

1.3 AGILE/DEVOPSSEC

Lean-Agile-DevOpsSec Compliance

- All systems development and maintenance projects shall be compliant with ICE OCIO Management Instruction (MI) 001 "Applying Lean-Agile-DevOpsSec Principles at ICE."
- The Contractor shall store and manage all system configuration settings and documentation in the ICE Approved Software Configuration Management (SCM) system, currently GitHub Enterprise.
- The Contractor shall document operational tasks and Standard Operating Procedures (SOPs) in an ICE Approved knowledge management portal, currently ELMS and/or Confluence.
- The Contractor shall leverage an ICE provided automation toolchain (currently Jenkins based) to reduce, if not outright eliminate, the number of manual tasks performed during operations. This includes recurring tasks, scheduled jobs, monitoring, updates, patching, user maintenance, and other operational tasks.
- The Contractor shall perform sufficient* static code analysis in the areas of reliability, security, maintainability, test coverage, and duplication has been performed and is available for review in the ICE Approved Quality Assurance Dashboard (currently SonarQube).

* "Sufficient" is a moving metric that is expected to improve with time.

- The Contractor shall leverage automation tools to reduce the number of manual tasks performed during the development life cycle. This includes the test automation (Unit, Functional, Integration, Performance, and Security), build automation, continuous integration, and continuous development.

Attachment C – Cyber Security Contract Requirements

C-1: DOCUMENT REFERENCES

Table 1-1 contains a list of cybersecurity references that are applicable to ICE acquisitions. Several documents listed contain language that can be copied directly into an acquisition document to cover cybersecurity requirements. Others are listed as references in case additional detail on a given requirement is needed. There are three columns in the table:

- **Document Number:** Provides the number assigned to a document or suite of documents (if applicable). Document numbers beginning with "MD" are DHS Management Directives.
- **Document Name:** The name of the publication or program.
- **Reference Link:** Contains a link (if available) to the website containing the publication. Click on the link or copy and paste the link into the browser URL field, to access the publication.

Table 1-1: Contract Language Document References

Document Abbreviation	Document Name	Reference Link
ITAR	Information Technology Acquisition Review (ITAR) Quick Essentials Guide V3.0	http://dhsconnect.dhs.gov/org/comp/mgmt/ocio/bm/Documents/ITAR/ITAR%20Quick%20Essentials%20Guide%20V3_0%202013.pdf
HSAR	Homeland Security Acquisition Regulation (HSAR)	http://www.dhs.gov/sites/default/files/publications/CPO_HSAR_4.pdf http://dhsconnect.dhs.gov/org/comp/mgmt/ocpo/APL/Deviations/HSAR%20Class%20Deviation%2015-01%20Safeguarding%20of%20Sensitive%20Information.pdf#search=HSAR%20special%20clauses
FR	Federal Risk and Authorization Management Program (FedRAMP)	https://www.fedramp.gov/assets/resources/documents/Agency_Standard_Contract_Clauses.pdf https://www.fedramp.gov/assets/resources/documents/Agency_Control_Specific_Contract_Clauses.pdf
BYODTK	White House Digital Government Bring Your Own Device Toolkit	https://obamawhitehouse.archives.gov/digitalgov/bring-your-own-device

In accordance with ITAR 4.5.4.1 – Compliance with DHS Security Policy Terms and Conditions.

CLASSIFIED REQUESTS:

Compliance with DHS Security Policy Terms and Conditions:

All hardware, software, and services provided under this task order must be compliant with *DHS National Security Systems Policy Directive 4300B, Version 10.1, November 21, 2018' for NSS Collateral (Unclassified, Secret or Top-Secret Collateral).*

In accordance with ITAR 4.5.3.1 – Compliance with DHS Security Policy Terms and Conditions.

SBU REQUESTS:

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.*

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.

In accordance with HSAR 3052.204-70 - Security requirements for unclassified IT resources, with ITAR 4.5.3.3 – Access to Unclassified Facilities, IT Resources, and Sensitive Information Requirement Clause Inclusion Instruction, with ITAR 4.5.3.9 – Security Requirements for Unclassified Information Technology Resources Clause, with ITAR 4.5.4.6 – Required Protections for DHS Systems Hosted in Non-DHS Data Centers, and with ITAR 4.5.4.7 – Contractor Employee Access Clause. As prescribed in (HSAR) 48 CFR 3004.470-3 **Contract clauses:**

Security Requirements for Unclassified Information Technology Resources (JUN 2006)

The Contractor shall be responsible for IT security for all systems connected to a DHS network or operated by the Contractor for DHS, regardless of location. This clause applies to all or any part of the contract that includes information technology resources or services for which the Contractor must have physical or electronic access to sensitive information contained in DHS unclassified systems that directly support the agency's mission.

The Contractor shall provide, implement, and maintain an IT Security Plan. This plan shall describe the processes and procedures that will be followed to ensure appropriate security of IT resources that are developed, processed, or used under this contract.

Within 30 days after contract award, the Contractor shall submit for approval its IT Security Plan, which shall be consistent with and further detail the approach contained in the offeror's proposal. The plan, as approved by the Contracting Officer (CO), shall be incorporated into the contract as a compliance document.

The Contractor's IT Security Plan shall comply with Federal laws that include, but are not limited to, the Computer Security Act of 1987 (40 U.S.C. 1441 et seq.); the Government Information Security Reform Act of 2000; and the FISMA of 2002; and with Federal policies and procedures that include, but are not limited to, OMB Circular A-130.

The security plan shall specifically include instructions regarding handling and protecting sensitive information at the Contractor's site (including any information stored, processed, or transmitted using the Contractor's computer systems), and the secure management, operation, maintenance, programming, and system administration of computer systems, networks, and telecommunications systems.

Examples of tasks that require security provisions include:

a) Acquisition, transmission or analysis of data owned by DHS with significant replacement cost should the Contractor's copy be corrupted; and

b) Access to DHS networks or computers at a level beyond that granted the public (e.g., such as bypassing a firewall).

At the expiration of the contract, the Contractor shall return all sensitive DHS information and IT resources provided to the Contractor during the contract and certify that all non-public DHS information has been purged from any Contractor-owned system. Components shall conduct reviews to ensure that the security requirements in the contract are implemented and enforced.

A.6 In accordance with HSAR 3052.204-71 - Contractor Employee Access

Contractor Employee Access (Sep 2012)

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:

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

b) 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).

c) 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

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

e) "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.

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 CO. Upon the CO'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.

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

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 CO. 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.

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.

A.7 In accordance with ITAR 4.5.3.10 – Contractor Employee Access Clause (use language from HSAR 3052.204-70 and alternates at 3052.204-71).

A.7.1 Alternate I

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 Technical Representative (COTR) 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 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.

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.

A.8 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.

A.9 In accordance with White House Digital Government BYODTK – Mobile Information Technology Device Policy

Mobile Information Technology Device Usage

Users who conduct official DHS ICE business on a mobile IT device must:

a) Sign the Remote Access and Mobile IT Device User Agreement Form.

b) Operate the device in compliance with this policy, all applicable federal requirements, and the DHS ICE Remote Access and Mobile Information Technology Guide.

c) Not process or access Classified information on the device.

d) Use only approved and authorized DHS ICE owned devices to physically attach to DHS ICE IT systems.

e) Store only the minimum amount, if any, of Personally Identifiable Information (PII) and electronic Protected Health Information (ePHI) necessary to do one's work, and immediately delete the PII or ePHI when no longer needed. Users shall receive written approval from their supervisor before accessing, processing, transmitting, or storing DHS ICE Sensitive Information such as PII or ePHI.

f) Exercise extra care to preclude the compromise, loss, or theft of the device, especially during travel.

g) Immediately contact the DHS ICE Service Desk and their immediate supervisor if the IT device is lost, stolen, damaged, destroyed, compromised, or non-functional.

h) Abide by all federal and local laws for using the device while operating a motor vehicle (e.g., users are banned from text messaging while driving federally owned vehicles, and text messaging to conduct DHS ICE business while driving non-Government vehicles).

Users who are issued a DHS ICE owned mobile IT device must also:

a. Comply with DHS 4300A Sensitive Systems Handbook Attachment Q.

b. Not disable or alter security features on the device.

c. Only use the DHS ICE owned device for official Government use and limited personal use.

d. Reimburse the OCIO for any personal charges incurred that are above the established fixed cost for the Agency's use of the device (e.g., roaming charges incurred for personal calls).

e. Be required to reimburse DHS ICE if the mobile IT device is lost, stolen, damaged or destroyed as a result of negligence, improper use, or willful action on the employee's part and if determined by ICE.

A.10 In accordance with HSAR Class Deviation 15-01, Special Clause, Safeguarding of Sensitive Information (MAR 2015)

Safeguarding of Sensitive Information (MAR 2015)

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

b) **Definitions**. As used in this clause—

"Personally Identifiable Information (PII)" means information that can be used to distinguish or trace an individual's identity, such as name, social security number, or biometric records, either alone, or when combined with other personal or identifying information that is linked or linkable to a specific individual, such as date and place of birth, or mother's maiden name. The definition of PII is not anchored to any single category of information or technology. Rather, it requires a case-by-case assessment of the specific risk that an individual can be identified. In performing this assessment, it is important for an agency to recognize that non-personally identifiable information can become personally identifiable information whenever additional information is made publicly available—in any medium and from any source—that, combined with other available information, could be used to identify an individual.

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

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

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

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

amended, and any supplementary guidance officially communicated by an authorized official of the Department of Homeland Security (including the Assistant Secretary for the Transportation Security Administration or his/her designee);

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

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

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

"Sensitive Personally Identifiable Information (SPII)" is a subset of PII, which if lost, compromised or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. Some forms of PII are sensitive as stand-alone elements. Examples of such PII include: Social Security numbers (SSN), driver's license or state identification number, Alien Registration Numbers (A-number), financial account number, and biometric identifiers such as fingerprint, voiceprint, or iris scan. Additional examples include any groupings of information that contain an individual's name or other unique
identifier plus one or more of the following elements:
(1) Truncated SSN (such as last 4 digits)
(2) Date of birth (month, day, and year)
(3) Citizenship or immigration status
(4) Ethnic or religious affiliation
(5) Sexual orientation
(6) Criminal History
(7) Medical Information
(8) System authentication information such as mother's maiden name, account passwords or personal identification numbers (PIN)

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

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

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

(2) DHS Sensitive Systems Policy Directive 4300A

(3) DHS 4300A Sensitive Systems Handbook and Attachments

(4) DHS Security Authorization Process Guide

(5) DHS Handbook for Safeguarding Sensitive Personally Identifiable Information

(6) DHS Instruction Handbook 121-01-007 Department of Homeland Security Personnel Suitability and Security Program

(7) DHS Information Security Performance Plan (current fiscal year)

(8) DHS Privacy Incident Handling Guidance

(9) Federal Information Processing Standard (FIPS) 140-2 Security Requirements for Cryptographic Modules accessible at http://csrc.nist.gov/groups/STM/cmvp/standards.html

(10) National Institute of Standards and Technology (NIST) Special Publication 800-53 Security and Privacy Controls for Federal Information Systems and Organizations accessible at http://csrc.nist.gov/publications/PubsSPs.html

(11) NIST Special Publication 800-88 Guidelines for Media Sanitization accessible at http://csrc.nist.gov/publications/PubsSPs.html

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

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

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

(3) All Contractor employees with access to sensitive information shall execute *DHS Form 11000-6, Department of Homeland Security Non-Disclosure Agreement (NDA),* as a condition of access to such information. The Contractor shall maintain signed copies of the NDA for all employees as a record of compliance. The Contractor shall provide copies of the signed NDA to the Contracting Officer's Representative (COR) no later than two (2) days after execution of the form.

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

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

(1) Complete the Security Authorization process. The SA process shall proceed according to the *DHS Sensitive Systems Policy Directive 4300A* (most current version), or any successor

publication, *DHS 4300A Sensitive Systems Handbook* (most current version), or any successor publication, and the *Security Authorization Process Guide* including templates.

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

(ii) Independent Assessment. Contractors shall have an independent third party validate the security and privacy controls in place for the system(s). The independent third party shall review and analyze the SA package, and report on technical, operational, and management level deficiencies as outlined in *NIST Special Publication 800-53 Security and Privacy Controls for Federal Information Systems and Organizations*. The Contractor shall address all deficiencies before submitting the SA package to the Government for acceptance.

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

(2) Renewal of ATO. Unless otherwise specified in the ATO letter, the ATO shall be renewed every three (3) years. The Contractor is required to update its SA package as part of the ATO renewal process. The Contractor shall update its SA package by one of the following methods: (1) Updating the SA documentation in the DHS automated information assurance tool for acceptance by the Headquarters or Component CIO, or designee, at least 90 days before the ATO expiration date for review and verification of security controls; or (2) Submitting an updated SA package directly to the COR for approval by the Headquarters or Component CIO, or designee, at least 90 days before the ATO expiration date for review and verification of

security controls. The 90 day review process is independent of the system production date and therefore it is important that the Contractor build the review into project schedules. The reviews may include onsite visits that involve physical or logical inspection of the Contractor environment to ensure controls are in place.

(3) Security Review. The Government may elect to conduct random periodic reviews to ensure that the security requirements contained in this contract are being implemented and enforced. The Contractor shall afford DHS, the Office of the Inspector General, and other Government organizations access to the Contractor's facilities, installations, operations, documentation, databases and personnel used in the performance of this contract. The Contractor shall, through the Contracting Officer and COR, contact the Headquarters or Component CIO, or designee, to coordinate and participate in review and inspection activity by Government organizations external to the DHS. Access shall be provided, to the extent necessary as determined by the Government, for the Government to carry out a program of inspection, investigation, and audit to safeguard against threats and hazards to the integrity, availability and confidentiality of Government data or the function of computer systems used in performance of this contract and to preserve evidence of computer crime.

(4) Continuous Monitoring. All Contractor-operated systems that input, store, process, output, and/or transmit sensitive information shall meet or exceed the continuous monitoring requirements identified in the *Fiscal Year 2014 DHS Information Security Performance Plan,* or successor publication. The plan is updated on an annual basis. The Contractor shall also store monthly continuous monitoring data at its location for a period not less than one year from the date the data is created. The data shall be encrypted in accordance with *FIPS 140-2 Security Requirements for Cryptographic Modules* and shall not be stored on systems that are shared with other commercial or Government entities. The Government may elect to perform continuous monitoring and IT security scanning of Contractor systems from Government tools and infrastructure.

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

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

f) Sensitive Information Incident Reporting Requirements.

(1) All known or suspected sensitive information incidents shall be reported to the Headquarters or Component Security Operations Center (SOC) within one hour of discovery in accordance with *4300A Sensitive Systems Handbook Incident Response and Reporting* requirements. When notifying the Headquarters or Component SOC, the Contractor shall also notify the Contracting Officer, COR, Headquarters or Component Privacy Officer, and US-

CERT using the contact information identified in the contract. If the incident is reported by phone or the Contracting Officer's email address is not immediately available, the Contractor shall contact the Contracting Officer immediately after reporting the incident to the Headquarters or Component SOC. The Contractor shall not include any sensitive information in the subject or body of any e-mail. To transmit sensitive information, the Contractor shall use *FIPS 140-2 Security Requirements for Cryptographic Modules* compliant encryption methods to protect sensitive information in attachments to email. Passwords shall not be communicated in the same email as the attachment. A sensitive information incident shall not, by itself, be interpreted as evidence that the Contractor has failed to provide adequate information security safeguards for sensitive information, or has otherwise failed to meet the requirements of the contract.

(2) If a sensitive information incident involves PII or SPII, in addition to the reporting requirements in *4300A Sensitive Systems Handbook Incident Response and Reporting*, Contractors shall also provide as many of the following data elements that are available at the time the incident is reported, with any remaining data elements provided within 24 hours of submission of the initial incident report:

(i) Data Universal Numbering System (DUNS);
(ii) Contract numbers affected unless all contracts by the company are affected;
(iii) Facility CAGE code if the location of the event is different than the prime Contractor location;
(iv) Point of contact (POC) if different than the POC recorded in the System for Award Management (address, position, telephone, email);
(v) Contracting Officer POC (address, telephone, email);
(vi) Contract clearance level;
(vii) Name of subcontractor and CAGE code if this was an incident on a subContractor network;
(viii) Government programs, platforms or systems involved;
(ix) Location(s) of incident;
(x) Date and time the incident was discovered;
(xi) Server names where sensitive information resided at the time of the incident, both at the Contractor and subContractor level;
(xii) Description of the Government PII and/or SPII contained within the system;
(xiii) Number of people potentially affected and the estimate or actual number of records exposed and/or contained within the system; and
(xiv) Any additional information relevant to the incident.

g) Sensitive Information Incident Response Requirements.

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

(2) The Contractor shall provide full access and cooperation for all activities determined by the Government to be required to ensure an effective incident response, including providing all requested images, log files, and event information to facilitate rapid resolution of sensitive information incidents.

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

(i) Inspections,
(ii) Investigations,
(iii) Forensic reviews, and
(iv) Data analyses and processing.

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

h) Additional PII and/or SPII Notification Requirements.

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

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

(i) A brief description of the incident;
(ii) A description of the types of PII and SPII involved;
(iii) A statement as to whether the PII or SPII was encrypted or protected by other means;
(iv) Steps individuals may take to protect themselves;
(v) What the Contractor and/or the Government are doing to investigate the incident, to mitigate the incident, and to protect against any future incidents; and
(vi) Information identifying who individuals may contact for additional information.

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

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

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

(i) Triple credit bureau monitoring;
(ii) Daily customer service;

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

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

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

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

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

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

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

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

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

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

A.11 In accordance with HSAR Class Deviation 15-01, Special Clause, Information Technology Security and Privacy Training (MAR 2015)

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.

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.

In accordance with ITAR 4.5.3.2 – Encryption Compliance

Encryption Compliance Terms and Conditions

If encryption is required, the following methods are acceptable for encrypting sensitive information:

a) FIPS 197 (Advanced Encryption Standard (AES)) 256 algorithm and cryptographic modules that have been validated under FIPS 140-2.

b) National Security Agency (NSA) Type 2 or Type 1 encryption.

c) Public Key Infrastructure (PKI) (see paragraph 5.5.2.1 of the *Department of Homeland Security (DHS) IT Security Program Handbook (DHS Management Directive (MD) 4300A) for Sensitive Systems*).

In accordance with ITAR 4.5.3.5 and ITAR 4.5.4.5 – Interconnection Security Agreement (ISA)

ISA Terms and Conditions

Interconnections between DHS/ICE and non-DHS/ICE IT systems shall be established only through controlled interfaces and via approved service providers. The controlled interfaces shall be authorized at the highest security level of information on the network. Connections with other Federal agencies shall be documented based on interagency agreements; memoranda of understanding, service level agreements or interconnection security agreements.

In accordance with ITAR 4.5.3.6 and ITAR 4.5.4.6 – Required Protections for DHS/ICE Systems Hosted in Non-DHS/ICE Data Centers

1) Security Authorization Terms and Conditions

A Security Authorization of any infrastructure directly in support of DHS/ICE information system shall be performed as a general support system (GSS) prior to DHS/ICE occupancy to characterize the network, identify threats, identify vulnerabilities, analyze existing and planned security controls, determine likelihood of threat, analyze impact, determine risk, recommend controls, perform remediation on identified deficiencies, and document the results. The Security Authorization (SA) shall be performed in accordance with DHS/ICE Security Policy and the controls provided by the hosting provider shall be equal to or stronger than the FIPS 199 security categorization of DHS/ICE information system.

At the beginning of the contract, and upon request thereafter (generally at the deployment of a new system or renewal of a System Authority to Operate), the Contractor/Cloud Service Provider (CSP) shall provide the results of an independent assessment and verification of security controls. The independent assessment and verification shall apply the same standards that DHS/ICE applies in the SA process of its information systems. Any deficiencies noted during this assessment shall be provided to the COR for entry into DHS/ICE POA&M Management Process. ICE shall use DHS' POA&M process to document planned remedial actions to address any deficiencies in information security policies, procedures, and practices, and the completion of those activities. Security deficiencies shall be corrected within the timeframes dictated by DHS/ICE POA&M Management Process. CSP procedures shall be subject to periodic, unannounced assessments by DHS/ICE officials. The documented physical aspects associated with CSP activities shall also be subject to such assessments. Inspections of CSP physical facilities will be scheduled in advance and coordinated with the provider in accordance with their facility procedures. On a periodic basis, DHS and its Components, including DHS Office of Inspector General, may choose to evaluate any or all of the security controls implemented by the Contractor under these clauses. Evaluation could include, but is not limited to vulnerability scanning. The DHS and its Components reserve the right to conduct audits at their discretion. With ten working days' notice, at the request of the Government, the CSP and reseller shall fully cooperate and facilitate in a Government-sponsored security control assessment at each location wherein DHS/ICE information is processed or stored, or information systems are developed, operated, maintained, or used on behalf of DHS/ICE, including those initiated by the Office of the Inspector General. The Government may conduct a security control assessment on shorter notice (to include unannounced assessments) determined by DHS/ICE in the event of a security incident.

2) Enterprise Security Architecture Terms and Conditions

The CSP shall utilize and adhere to DHS/ICE Enterprise Security Architecture in accordance with applicable laws and DHS/ICE policies to the satisfaction of DHS/ICE COR.

3) Continuous Monitoring Terms and Conditions

The CSP shall participate in the DHS/ICE Continuous Monitoring methodologies and, shall provide a Continuous Monitoring capability over their resources as required by FedRAMP. The DHS Chief Information Security Officer (CISO) issues annual updates to its Continuous Monitoring requirements via the Annual Information Security Performance Plan. At a minimum, the CSP shall adhere to all ITAR and FedRAMP continuous monitoring requirements and ensure that DHS/ICE can implement and integrate the following processes:

a) Asset Management

b) Vulnerability Management

c) Configuration Management

d) Malware Management

e) Log Integration

f) Security Information Event Management (SIEM) Integration

g) Patch Management

h) Providing near-real-time security status information to DHS/ICE SOC Specific Protections Terms and Conditions

i) Specific protections that shall be provided by the CSP include, but are not limited to the following:

Specific Operations Terms and Conditions

The Contractor shall operate a SOC to provide security for the below mentioned services. The CSP shall support regular reviews with DHS/ICE Information Security Office to coordinate and synchronize the security posture of the CSP hosting facility with that of DHS Data Centers. The SOC personnel shall provide 24x7x365 staff to monitor the network and all of its devices. The CSP staff shall also analyze the information generated by the devices for security events, respond to real-time events, correlate security device events, and perform continuous monitoring. It is recommended that the CSP staff shall also maintain a trouble ticket system in which incidents and outages are recorded. In the event of an incident, the CSP facility SOC shall adhere to the incident response plan.

4) Computer Incident Response Services Terms and Conditions

The CSP shall provide Computer Incident Response Team (CIRT) services. The CSP shall adhere to the standard Incident Reporting process as determined by the Component and is defined by a DHS/ICE-specific incident response plan that adheres to DHS/ICE policy and procedure for reporting incidents. The CSP shall conduct Incident Response Exercises to ensure all personnel are familiar with the plan. The CSP shall notify DHS/ICE SOC of any incident in accordance with the Incident Response Plan and work with DHS/ICE throughout the incident duration.

5) Network Intrusion Detection Systems (NIDS) and Monitoring Terms and Conditions

The Contractor shall provide the design, configuration, implementation, and maintenance of the sensors and hardware that are required to support the NIDS solution. The Contractor is responsible for creating and maintaining the NIDS rule sets for their facility(s). The NIDS solution should provide real-time alerts. These alerts and other relevant information shall be located in a central repository. The NIDS shall operate 24x7x365. A summary of alerts shall be made available to DHS/ICE upon request. If an abnormality or anomaly is identified, the Contractor shall notify the appropriate DHS/ICE point of contact in accordance with the incident response plan.

6) Physical and Information Security and Monitoring Terms and Conditions

The CSP shall provide a facility using appropriate protective measures to provide for physical security. All facilities will be located within the United States. The CSP shall maintain a process to control physical access to all DHS/ICE IT assets. DHS/ICE IT Assets shall be monitored 24x7x365. A summary of unauthorized access attempts shall be reported to the appropriate DHS/ICE security office upon request.

7) **Vulnerability Assessments Terms and Conditions**

The CSP and reseller shall provide all information from any managed device to DHS/ICE, as requested, and shall assist, as needed, to perform periodic vulnerability assessments of the network, operating systems, and applications to identify vulnerabilities and propose mitigations. Vulnerability assessments shall be included as part of compliance with the continuous monitoring of the system.

8) **Anti-malware (e.g., virus, spam) Terms and Conditions**

The CSP shall design, implement, monitor, and manage to provide comprehensive anti-malware service. The CSP shall provide all maintenance for the system providing the anti-malware capabilities to include configuration, definition updates, when changes are required. A summary of alerts shall be reported to DHS/ICE SOC in weekly status report. If an abnormality or anomaly is identified, the CSP shall notify the appropriate DHS/ICE point of contact in accordance with the incident response plan.

9) **Log Retention Terms and Conditions**

Log files for all infrastructure devices, physical access, and anti-malware should be retained online for 180 days and offline for three years.

In accordance with ITAR 4.5.3.8 – Personal Identification Verification (PIV) Credential Compliance

Personal Identification Verification (PIV) Credential Compliance Terms and Conditions

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

b) Procurements for software products or software developments shall be compliant by accepting PIV credentials as the common means of authentication for access for federal employees and Contractors.

c) PIV-enabled information systems must demonstrate that they can correctly work with PIV credentials by responding to the cryptographic challenge in the authentication protocol before granting access.

d) If a system is identified to be non-compliant with HSPD-12 for PIV credential enablement, a remediation plan for achieving HSPD-12 compliance shall be required for review, evaluation, and approval by the CISO.

In accordance with ITAR 4.5.4.2 – Encryption Compliance

CLASSIFIED:

Encryption Compliance Terms and Conditions

National Security Systems, requiring encryption shall comply with the following standards:

a) Products using FIPS 197 AES algorithms with at least 256 bit encryption that has been validated under FIPS 140-2 (**Note:** The use of triple DES [3DES] and FIPS 140-1 is no longer permitted. A waiver or exception is required for systems where AES cannot currently be used.)

b) NSA Type 2 or Type 1 encryption

In accordance with ITAR 4.5.4.3 – Handling or Processing of Classified Information

CLASSIFIED:

Handling or Processing of Classified Information

Contractor access to classified information is required under this procurement. The maximum level of classification is *Top Secret.* Details will be provided in a Department of Defense (DD) Form 254.

Handling or Processing of Classified Information Terms and Conditions

a) Classified information is Government information, which requires protection in accordance with Executive Order 12958, National Security Information (NSI) as amended and supplemental directives. Ifthe Contractor has access to classified information at a DHS/ICE owned or leased facility, it shall comply with the security requirements of DHS/ICE and the facility.

b) Contractor shall comply with all Government facility and security requirements while on Government property, including obtaining and displaying identification badges, obtaining vehicle decals and proper vehicle operation.

c) The Contractor shall have a facility security clearance up to *Top Secret* level. All personnel supporting this procurement shall be required to obtain and maintain a *Top Secret* level clearance. The Government reserves the right to approve or deny suitability of the Contractor's individual employees based on security risks, unsatisfactory performance, or disruptive influence to mission accomplishment.

Requirements for Handling Sensitive Information Terms and Conditions

The Contractor shall abide by the requirements set forth in the DD Form 254, Contract Security Classification Specification, an attachment to the contract, and the National Industrial Security Program Operating Manual (NISPOM) for protection of classified information at its cleared facility, if applicable, as directed by the Defense Counterintelligence Security Agency (DCSA).

As referenced in ITAR 4.5.4.3 and in accordance with FAR 52.204-2 Security Requirements (Aug 1996)

CLASSIFIED:

Security Requirements, FAR 52.204-2

a) This clause applies to the extent that this contract involves access to information classified "Confidential," "Secret," or "Top Secret."

b) The Contractor shall comply with (1) the Security Agreement (DD Form 441), including the NISPOM (DOD 5220.22-M), and (2) any revisions to that manual, notice of which has been furnished to the Contractor.

c) If, subsequent to the date of this contract, the security classification or security requirements under this contract are changed by the Government and if the changes cause an increase or decrease in security costs or otherwise affect any other term or condition of this contract, the contract shall be subject to an equitable adjustment as if the changes were directed under the Changes clause of this contract.

d) The Contractor agrees to insert terms that conform substantially to the language of this clause, including this paragraph (d) but excluding any reference to the Changes clause of this contract, in all subcontracts under this contract that involve access to classified information.

Security Clearances

At the time of award, the Contractor shall have the appropriate Top Secret or Secret security clearances for the employees as required by the Work Assignment they will work under on this contract. Affected employees must have a current investigation in place or being processed for a periodic reinvestigation.

A Department of Defense Contract Security Classification Specification (DD Form 254)

shall be issued by the Government Contracting Agency (GCA) CO to the Contractor at the time of contract award (FAR 4.403(c)(1)). The contracting officer shall also provide a copy to the DCSA and the GCA COR, in accordance with DoD Directive 5200.22-M, National Industrial Security Program Operating Manual.

B.8 In accordance with FedRAMP

1) FedRAMP IT Systems Security Requirements

a) The Federal agency will determine the security category for the cloud system in accordance with Federal Information Processing Standard 199; then, the Contractor/Cloud Service Provider (CSP) shall apply the appropriate set of impact baseline controls as required in the FedRAMP Cloud Computing Security Requirements Baseline document to ensure compliance to security standards. The FedRAMP baseline controls are based on the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations (as amended), and also includes a set of additional controls for use within systems providing cloud services to the federal Government.

b) The CSP shall maintain a security management continuous monitoring environment that meets or exceeds the requirements outlined in the latest edition of FedRAMP Cloud Computing Security Requirements Baseline and FedRAMP Continuous Monitoring Requirements.

2) FedRAMP Privacy Requirements

Contractor shall be responsible for the following privacy and security safeguards:

a) To the extent required to carry out the FedRAMP assessment and authorization process and FedRAMP continuous monitoring, to safeguard against threats and hazards to the security, integrity, and confidentiality of any non-public Government data collected and stored by the Contractor, the Contractor shall afford the Government access to the Contractor's facilities, installations, technical capabilities, operations, documentation, records, and databases.

b) If new or unanticipated threats or hazards are discovered by either the Government or the Contractor, or if existing safeguards have ceased to function, the discoverer shall immediately bring the situation to the attention of the other party.

c) The Contractor shall also comply with any additional FedRAMP privacy requirements.

d) The Government has the right to perform manual or automated audits, scans, reviews, or other inspections of the vendor's IT environment being used to provide or facilitate services for the Government. In accordance with the Federal Acquisitions Regulations (FAR) clause 52.239-1, Contractor shall be responsible for the following privacy and security safeguards:

(i) The Contractor shall not publish or disclose in any manner, without the CO's written consent, the details of any safeguards either designed or developed by the Contractor under this contract or otherwise provided by the Government. Exception—Disclosure to a Consumer Agency for purposes of C&A verification.

(ii) To the extent required to carry out a program of inspection to safeguard against threats and hazards to the security, integrity, and confidentiality of Government data, the Contractor shall afford the Government access to the Contractor's facilities, installations, technical capabilities, operations, documentation, records, and databases within 72 hours. The program of inspection shall include,

but is not limited to: Authenticated and unauthenticated operating system/network vulnerability scans Authenticated and unauthenticated we b application vulnerability scans Authenticated and unauthenticated database application vulnerability scans Automated scans can be performed by Government personnel, or agents acting on behalf of the Government, using Government operated equipment, and Government specified tools.

(iii) If new or unanticipated threats or hazards are discovered by either the Government or the Contractor, or if existing safeguards have ceased to function, the discoverer shall immediately bring the situation to the attention of the other party.

(iv) If the vendor chooses to run its own automated scans or audits, results from these scans may, at the Government's discretion, be accepted in lieu of Government performed vulnerability scans. In these cases, scanning tools and their configuration shall be approved by the Government. In addition, the results of vendor-conducted scans shall be provided, in full, to the Government.

3) Sensitive Information Storage

Sensitive But Unclassified (SBU) information, data, and/or equipment will only be disclosed to authorize personnel on a need-to-know basis. The Contractor shall ensure that appropriate administrative, technical, and physical safeguards are established to ensure the security and confidentiality of this information, data, and/or equipment is properly protected. When no longer required, this information, data, and/or equipment will be returned to Government control, destroyed, or held until otherwise directed. Destruction of items shall be accomplished by following NIST SP 800-88, Guidelines for Media Sanitization.

The disposition of all data will be at the written direction of the COR, this may include documents returned to Government control; destroyed; or held as specified until otherwise directed. Items returned to the Government shall be hand carried or sent by certified mail to the COR.

4) Protection of Information

The Contractor shall be responsible for properly protecting all information used, gathered, or developed because of work under this contract. The Contractor shall also protect all Government data, equipment, etc. by treating the information as sensitive. All information about the systems gathered or created under this contract should be considered as SBU information. It is anticipated that this information will be gathered, created, and stored within the primary work location. If Contractor personnel must remove any information from the primary work area they should protect it to the same extent they would their proprietary data and/or company trade secrets. The use of any information that is subject to the Privacy Act will be utilized in full accordance with all rules of conduct as applicable to Privacy Act Information.

The Government will retain unrestricted rights to Government data. The Government retains ownership of any user created/loaded data and applications hosted on vendor's infrastructure, as well as maintains the right to request full copies of these at any time.

The data that is processed and stored by the various applications within the network infrastructure contains financial data as well as personally identifiable information (PII). This data and PII shall be protected against unauthorized access, disclosure or modification, theft, or destruction. The Contractor shall ensure that the facilities that house the network infrastructure are physically secure.

The Government-owned data must be available to the Government upon request within one business day or within the timeframe specified otherwise, and shall not be used for any other purpose other than that specified herein. The Contractor shall provide requested data at no

additional cost to the Government.

No data shall be released by the Contractor without the consent of the Government in writing. All requests for release must be submitted in writing to the COR/CO.

5) Security Classification

The preparation of the deliverables in this contract will be completed at a Sensitive but Unclassified level unless a higher level is specified.

6) Confidentiality and Nondisclosure

The preliminary and final deliverables and all associated working papers and other material deemed relevant by the agency that have been generated by the Contractor in the performance of this contract, are the property of the U.S. Government, and must be submitted to the COTR at the conclusion of the contract. The U.S. Government has unlimited data rights to all deliverables and associated working papers and materials in accordance with FAR 52.227-17.

All documents produced for this project are the property of the U.S. Government and cannot be reproduced, or retained by the Contractor. All appropriate project documentation will be given to the agency during and at the end of this contract. The Contractor shall not release any information without the written consent of the CO.

Personnel working on any of the described tasks may, at Government request, be required to sign formal non-disclosure and/or conflict of interest agreements to guarantee the protection and integrity of Government information and documents.

7) Disclosure of Information

Any information made available to the Contractor by the Government shall be used only for carrying out the provisions of this contract and shall not be divulged or made known in any manner to any persons except as may be necessary in the performance of the contract. In performance of this contract, the Contractor assumes responsibility for protection of the confidentiality of Government records and shall ensure that all work performed by its subcontractors shall be under the supervision of the Contractor or the Contractor's responsible employees. Each officer or employee of the Contractor or any of its subcontractors to whom any Government record may be made available or disclosed shall be notified in writing by the Contractor that information disclosed to such officer or employee can be used only for that purpose and to the extent authorized herein. Further disclosure of any such information, by any means, for a purpose or to an extent unauthorized herein, may subject the offender to criminal sanctions imposed by 18 U.S.C. §§ 1030.

8) FedRAMP Security Requirements Overview:

a) The minimum requirements for low and moderate impact cloud systems are contained within the FedRAMP Cloud Computing Security Requirements Baseline. The Contractor and Federal Government Agency share responsibility to ensure compliance with security requirements.

b) The implementation of a new Federal Government cloud system requires a formal process, known as Assessment and Authorization, which provides guidelines for performing the assessment.

c) FedRAMP requires cloud service providers to utilize a Third-Party Assessment Organization (3PAO) to perform an assessment of the cloud service provider's security controls to determine the extent to which security controls are implemented correctly, operate as intended, and produce the desired outcome with respect to meeting security requirements.

d) The FedRAMP PMO security staff will be available for consultation during the process. Both the FedRAMP PMO staff and JAB will review the results before issuing a Provisional Authorization decision. The Government reserves the right to verify the infrastructure and security test results before issuing an Authorization decision.

e) Federal agencies will be able to leverage the provisional Authorization granted by FedRAMP and any documentation prepared by the Contractor to issue their own authority to operate.

f) The vendor is advised to review the FedRAMP guidance documents (see References below) to determine the level of effort that will be necessary to complete the requirements. All FedRAMP documents and templates are available at http://FedRAMP.gov.

9) FedRAMP Security Compliance Requirements

The Contractor shall implement the controls contained within the FedRAMP Cloud Computing Security Requirements Baseline and FedRAMP Continuous Monitoring Requirements for low and moderate impact system (as defined in FIPS 199). These documents define requirements for compliance to meet minimum Federal information security and privacy requirements for both low and moderate impact systems. While the FedRAMP baseline controls are based on NIST SP 800-53, Revision 4. The Contractor shall generally, substantially, and in good faith follow FedRAMP guidelines and Security guidance. In situations where there are no procedural guides, the Contractor shall use generally accepted industry best practices for IT security.

10) Required FedRAMP Policies and Regulations

The Contractor shall comply with FedRAMP Security Assessment Framework – describing a general security Assessment Framework for the Federal Risk and Authorization Management Program (FedRAMP). This document details the security assessment process which must be used to achieve FedRAMP compliance. Download here:

https://www.fedramp.gov/assets/resources/documents/FedRAMP_Security_Assessment_Framework.pdf

11) Assessment and Authorization

DHS/ICE may choose to cancel the contract/award and terminate any outstanding orders if the Contractor has its provisional authorization revoked and the deficiencies are greater than agency risk tolerance thresholds.

12) Assessment of the System

a) The Contractor shall comply with FedRAMP requirements as mandated by Federal laws and policies, including making available any documentation, physical access, and logical access needed to support this requirement. The Level of Effort for the A&A is based on the System's NIST Federal Information Processing Standard (FIPS) Publication 199 categorization. The Contractor shall create, maintain and update the following documentation using FedRAMP requirements and templates, which are available at http://FedRAMP.gov :

- Privacy Impact Assessment (PIA)
- FedRAMP Test Procedures and Results
- Security Assessment Report (SAR)
- System Security Plan (SSP)

- IT System Contingency Plan (CP)
- IT System Contingency Plan (CP) Test Results
- POA&M Continuous Monitoring Plan (CMP)
- FedRAMP Control Tailoring Workbook
- Control Implementation Summary Table
- Results of Penetration Testing
- Software Code Review
- Interconnection Agreements/Service Level Agreements/Memorandum of Agreements.

b) Information systems must be assessed by an accredited 3PAO whenever there is a significant change to the system's security posture in accordance with the FedRAMP Continuous Monitoring Plan.

c) The Government reserves the right to perform Penetration Testing. If the Government exercises this right, the Contractor shall allow Government employees (or designated third parties) to conduct Security Assessment activities to include control reviews in accordance with FedRAMP requirements (https://www.fedramp.gov/assets/resources/documents/CSP_Penetration_Test_Guidance.pdf). Review activities include but are not limited to scanning operating systems, web applications, wireless scanning; network device scanning to include routers, switches, and firewall, and IDS/IPS; databases and other applicable systems, including general support structure, that support the processing, transportation, storage, or security of Government information for vulnerabilities.

d) Identified gaps between required FedRAMP Security Control Baselines and Continuous Monitoring controls and the Contractor's implementation as documented in the Security Assessment Report shall be tracked by the Contractor for mitigation in a POA&M document. Depending on the severity of the gaps, the Government may require them to be remediated before a provisional authorization is issued.

e) The Contractor is responsible for mitigating all security risks found during A&A and continuous monitoring activities. All high-risk vulnerabilities must be mitigated within 30 days and all moderate risk vulnerabilities must be mitigated within 30 days from the date vulnerabilities are formally identified. The Government will determine the risk rating of vulnerabilities.

13) Authorization of System

The Contractor shall provide access to the Federal Government, or their designee acting as their agent, when requested, in order to verify compliance with the requirements for an Information Technology security program. The Government reserves the right to conduct onsite inspections. The Contractor shall make appropriate personnel available for interviews and provide all necessary documentation during this review.

14) Reporting and Continuous Monitoring

Maintenance of the FedRAMP Provisional Authorization will be through continuous monitoring and periodic audit of the operational controls within a Contractor's system, environment, and processes to determine if the security controls in the information system continue to be effective over time in light of changes that occur in the system and environment. Through continuous monitoring, security controls and supporting deliverables are updated and submitted to the FedRAMP PMO as required by FedRAMP Requirements. The submitted deliverables (or lack thereof) provide a current understanding of the security

state and risk posture of the information systems. The deliverables will allow the FedRAMP JAB to make credible risk-based decisions regarding the continued operations of the information systems and initiate appropriate responses as needed when changes occur. Contractors will be required to provide updated deliverables and automated data feeds as defined in the FedRAMP Continuous Monitoring Plan.

All deliverables shall be labeled "Controlled Unclassified Information" (CUI), unless otherwise specified. External transmission/dissemination of labeled deliverables to or from a Government computer must be encrypted. Certified encryption modules must be used in accordance with FIPS PUB 140 (as amended), "Security requirements for Cryptographic Modules."

15) Non-Repudiation

The Cloud Service Provider vendor shall provide a system that is capable of implementing NIST SP 800-53 Control AU-10 approved controls, which provides for origin authentication, data integrity, and signer non-repudiation. This binds the identity of the information producer with the information to and provides the means for authorized individuals to determine the identity of the producer of the information.

16) Identification and Authentication (Organizational Users)

The vendor shall support a secure, multi-factor method of remote authentication and authorization to identified Government Administrators that will allow Government designated personnel the ability to perform management duties on the system.

The vendor shall support multi-factor authentication to specified by the Government POC.

17) Identification and Authentication (Non-Organizational Users)

The vendor shall support a secure, dual factor method of remote authentication and authorization to identified Vendor Administrators that will allow vendor-designated personnel the ability to perform management duties on the system.

18) Incident Reporting Timeframes

Cloud Service Providers are required to report all computer security incidents to the United States Computer Emergency Readiness Team (U.S.-CERT) in accordance with U.S.-CERT "Incident Categories and Reporting Timeframes" in , Appendix J, Table J-1 of NIST SP 800-61 (as amended), "Computer Security Incident Handling Guide." Any Category (CAT) 1, CAT 2, or CAT 3 incident, must be reported immediately to their Information Systems Security Officer (ISSO) and the Senior Agency Information Security Officer (SAISO). Any incident that involves compromised Personally Identifiable Information (PII) must be reported to U.S.-CERT within 1 hour of detection regardless of the incident category reporting timeframe.

19) Media Transport

The vendor shall document activities associated with the transport of Federal agency information stored on digital and non-digital media and employ cryptographic mechanisms to protect the confidentiality and integrity of this information during transport outside of controlled areas.

Digital media, containing Federal agency information, that is transported outside of controlled areas must be encrypted using an encryption method to be identified by the Government POC; non-digital media including but not limited to CD-ROM, floppy disks, etc., must be secured using the same policies and procedures as paper.

Media, containing Federal Agency information that is transported outside of controlled areas must ensure accountability. This can be accomplished through appropriate actions such as

logging and a documented chain of custody form.

Federal Agency data that resides on mobile/portable devices (e.g., USB flash drives, external hard 12 drives, and SD cards) must be encrypted using an encryption mode to be identified by the Government POC. All Federal Agency data residing on laptop computing devices must be protected with approved encryption software.

20) Boundary Protection

The CSP/Reseller shall route all external connections through a Trusted Internet Connection (TIC).

21) Protection of Information At Rest

The CSP shall provide security mechanisms for handling data at rest and in transit in accordance with FIPS 140-2.

22) Security Alerts, Advisories, and Directives

The CSP/Reseller shall provide a list of their personnel, identified by name and role, with system 1 administration, monitoring, and/or security responsibilities that are to receive security alerts, two advisories, and directives. This list shall include ICE SOC.

B.9 Patch Management Terms and Conditions

The CSP, or software vendor (for certain Software-as-a-Service (SaaS) offerings), shall perform patch management services to all Platform-as-a-Service (PaaS) and SaaS offerings managed by the CSP, or in cases where the SaaS offering is hosted by an independent third party, the third party will be responsible for providing the patch management services. The CSP shall push patches that are required by vendors and DHS/ICE system owner. This is to ensure that the infrastructure and applications that directly support DHS/ICE information system are current in their release and that all security patches are applied. The CSP and software vendor shall be informed by DHS/ICE which patches are required by DHS/ICE through the Information Security Vulnerability Management bulletins and advisories. Core applications, the ones DHS/ICE utilizes to fulfill their mission, shall be tested by DHS/ICE. However, the CSP and software vendor(s) shall be responsible for deploying patches to their products as directed by DHS/ICE. It is recommended that all other applications (host-based intrusion detection system (HIDS), network intrusion detection system (NIDS), Anti-malware, and Firewall) shall be tested by the CSP prior to deployment in a test environment.

Attachment D - Required Security Language For Contracts Requiring Contractor Employees Access To Classified National Security Information

SECURITY REQUIREMENTS

GENERAL

Performance under this agreement will require access to Classified National Security Information (NSI) by contractor employees. Contract agreement # XXXXXXXX requires that the Contractor, subcontractor(s), vendor(s), etc. (herein known as Contractor) may access Classified National Security Information (herein known as classified information). Classified information is Government information which requires protection in accordance with Executive Order 13526, Classified National Security Information, and supplementing directives.

The Contractor will abide by the requirements set forth in the DD Form 254, Contract Security Classification Specification, included in the contract, and the *National Industrial Security Program Operating Manual (NISPOM)* for the protection of classified information at its cleared facility, if applicable, as directed by the Defense Security Service. If the Contractor has access to classified information at an ICE or other Government Facility, it will abide by the requirements set by the agency.

In conjunction with acquisition XXXXXXXX the contractor shall ensure all investigative, reinvestigate, and adjudicative requirements are met in accordance with National Industrial Security Program Operating Manual (DOD 5220.22-M) Chapter 2-1.

No person shall be allowed to begin work on contract XXXXXXXX and/or access sensitive information related to the contract without ICE receiving clearance verification from the Facility Security Officer (FSO). ICE further retains the right to deem a contractor employee ineligible due to an insufficient background investigation or when derogatory information is received and evaluated under a Continuous Evaluation Program. Any action taken by ICE does not relieve the Contractor from required reporting of derogatory information as outlined under the NISPOM.

The FSO will submit a Visit Authorization Letter (VAL) through the Contracting Officer's Representative (COR) to **psu-industrial-security@ice.dhs.gov** for processing contractor employees onto the contract. The clearance verification process will be provided to the COR during Post-Award conference. Note: *Interim TS is not accepted by DHS for access to Top Secret information. The contract employee will only have access to SECRET level information until DoD CAF has granted a final TS.*

See BACKGROUND INVESTIGATIONS paragraph below for processing of contractor employees who will not require access to Classified NSI in support of this agreement.

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 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 preliminary Fitness determination or final Fitness determination by the Office of Professional Responsibility (OPR) Personnel Security. No employee of the Contractor shall be allowed unescorted access to a Government facility without a favorable preliminary Fitness determination or final Fitness determination by OPR Personnel Security. Contract employees are processed under DHS Instruction 121-01-007-001 (Personnel Security, Suitability and Fitness Program), 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 (Process for personnel not requiring access to classified information):

Contractor employees (to include applicants, temporaries, 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 the Personnel Security Unit. Contractor employees nominated by a Contracting Officer Representative for consideration to support this contract shall submit the following security vetting documentation to OPR Personnel Security, through the Contracting Officer Representative (COR), within 10 days of notification by OPR Personnel Security of nomination by the COR and initiation of an Electronic Questionnaire for Investigation Processing (e-QIP) in the Office of Personnel Management (OPM) automated on-line system.

1. Standard Form 85P (Standard Form 85PS (With supplement to 85P required for armed positions)), "Questionnaire for Public Trust Positions" Form completed on-line and archived by the contractor 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 – instructions provided to applicant by OPR Personnel Security). Completed on-line and archived by the contractor employee in their OPM e-QIP account.

3. Two (2) SF 87 (Rev. December 2017) Fingerprint Cards. **(Two Original Cards sent via COR to OPR Personnel Security)**

4. Foreign National Relatives or Associates Statement. (This document sent as an attachment in an e-mail to contractor employee from OPR Personnel Security – must be signed and archived into contractor employee's OPM e-QIP account prior to electronic "Release" of data via on-line account)

5. DHS 11000-9, "Disclosure and Authorization Pertaining to Consumer Reports Pursuant to the Fair Credit Reporting Act" (This document sent as an attachment in an e-mail to contractor employee from OPR Personnel Security – must be signed and archived into contractor employee's OPM e-QIP account prior to electronic "Release" of data via on-line account)

6. Optional Form 306 Declaration for Federal Employment (This document sent as an attachment in an e-mail to contractor employee from OPR Personnel Security – must be signed and archived into contractor employee's OPM e-QIP account prior to electronic "Release" of data via on-line account)

7. If occupying PREA designated position: Questionnaire regarding conduct defined under 6 CFR § 115.117 (Sexual Abuse and Assault Prevention Standards) (This document sent as an attachment in an e-mail to contractor employee from OPR Personnel Security – must be signed and archived into contractor employee's OPM e-QIP account prior to electronic "Release" of data via on-line account)

8. One additional document may be applicable if contractor employee was born abroad. If applicable, additional form and instructions will be provided to contractor employee. (If applicable, the document will be sent as an attachment in an e-mail to contractor employee from OPR Personnel Security – must be signed and archived into contractor employee's OPM e-QIP account prior to electronic "Release" of data via on-line 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 7 will be required for positions designated under PREA.

An adequate and current investigation is one where the investigation is not more than five years old, 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 Personnel Security at the time of award of the contract. Only complete packages will be accepted by the OPR Personnel Security as notified by the COR.

To ensure adequate background investigative coverage, contractor employees must currently reside in the United States or its Territories. Additionally, contractor employees are required to have resided within the Unites States or its Territories for three or more years out of the last five (ICE retains the right to deem a contractor 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.

TRANSFERS FROM OTHER DHS CONTRACTS (Unclassified support position):

Contractor employees may be eligible for transfer from other DHS Component contracts provided they have an adequate and current investigation meeting the new assignment requirement. If the contractor

employee does not meet the new assignment requirement a DHS 11000-25 with ICE supplemental page will be submitted to OPR Personnel Security to initiate a new investigation.

Transfers will be accomplished by submitting a DHS 11000-25 with ICE supplemental page indicating "Contract Change." The questionnaire related to 6 CFR § 115.117 listed above in item 7 will be required for positions designated under PREA.

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. The OPR Personnel Security will conduct periodic reinvestigations every 5 years, or when derogatory information is received, to evaluate continued Fitness of contractor employees.

REQUIRED REPORTING:

The Contractor will notify OPR Personnel Security, via the COR, of all terminations/resignations of contractor employees under the contract within five days of occurrence. 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 the OPR Personnel Security, 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 containing the names of contractor employees who are active, pending hire, have departed within the quarter or have had a legal name change (Submitted with documentation). 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.

CORs will submit reports to **psu-industrial-security@ice.dhs.gov**

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 NDA for contractor access to sensitive information. The NDA will be administered by the COR to the 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 should be reported to **ICE.ADSEC@ICE.dhs.gov**.

The contractor is required to report certain events that have an impact on the status of the facility clearance (FCL) and/or the status of a contractor employee's personnel security clearance as outlined by National Industrial Security Program Operating Manual (DOD 5220.22-M) Chapter1-3, Reporting Requirements. Contractors shall establish internal procedures as are necessary to ensure that cleared personnel are aware of their responsibilities for reporting pertinent information to the FSO and other federal authorities as required.

SECURITY MANAGEMENT

The Contractor shall appoint a senior official to act as the Corporate Security Officer. The individual will interface with the OPR Personnel Security 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 the OPR Personnel Security 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 in order to effect compliance with such requirements.

Contractors shall provide all employees supporting contract XXXXXXXX proper initial and annual refresher security training and briefings commensurate with their clearance level, to include security awareness, defensive security briefings. (National Industrial Security Program Operating Manual (DOD 5220.22-M) Chapter 3-1. The contractor shall forward a roster of the completed training to the COR on a quarterly basis.

INFORMATION TECHNOLOGY SECURITY CLEARANCE

When sensitive government information is processed on Department telecommunications and automated information systems, the Contractor 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, whether or not the failure results in criminal prosecution. Any person who improperly discloses sensitive information is subject to criminal and civil penalties and sanctions under a variety of laws (e.g., Privacy Act).

INFORMATION TECHNOLOGY SECURITY TRAINING AND OVERSIGHT

In accordance with Chief Information Office 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 PALMS or by contacting **ICE.ADSEC@ICE.dhs.gov**. Department 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).

a. "Gray-Market" Equipment

   i. The Offeror shall provide only new equipment unless otherwise expressly approved, in writing, by the DHS Contracting Officer. Offerors 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.

   ii. The Offeror shall be excused from using new OEM (i.e., "gray market", "previously used") components only with formal Government approval, in writing, from the DHS Contracting Officer. Such components shall be procured from their original source and shipped only from the manufacturer's authorized shipment points.

   iii. All equipment obtained by the Offeror on behalf of the Government will need to be provided to OIG OCIO for review to validate requirements and approved Contractors by DHS.

b. Hardware and Software Requests

   i. The contractors supply the Government hardware and software will provide the manufacturer's name, address, state, and/or domain of registration, and the 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 be provided.

   ii. Subcontractors are subject to the same general requirements and standards as prime contractors. Contractors employing subcontractors will perform due diligence to ensure that these standards are met.

   iii. 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.

      1. For software products, the Offeror shall provide all OEM software updates to correct defects for the life of the product (i.e., until the "End of Life (EoL)"). Software updates and patches shall be either: made available to the government for all products procured under this Contract, replaced upon End of Support (EoS) is reached, or formally waived (in writing) by the DHS Contracting Officer.

c. Supply-Chain Transport

   i. Offerors 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.

   ii. 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.

   iii. This transit process shall minimize the number of times in 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.

   iv. All records pertaining to the transit, storage, and delivery shall be readily available for inspection by any agent designated by the U.S. Government as

having the authority to examine them.

v. The Offeror 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.

vi. The Offeror shall provide a packing slip which shall accompany each container or package with the information identifying this solicitation number, the order number, a description of the hardware/software enclosed (Manufacturer name, model number, serial number), and the customer point of contact.

vii. The Offeror shall send a shipping notification to the intended government recipient; with a copy transmitted via email to the Contracting Officer, or designated representative. This shipping notification shall be sent electronically and will state this solicitation 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.

d. Notifications

i. The Offeror shall notify DHS Contracting Officer, COR and the Office of the Chief Information Officer and the DHS component Chief Information Officer through the Enterprise Security Operations Center (ESOC) directly of any suspected or potential violations of Section 889 of the National Defense Authorization Act (NDAA) for Information Communications Technology (ICT) at NDAA_Incidents@hq.dhs.gov.

e. Foreign Equities

The Offeror shall immediately notify the DHS Contracting Officer, COR that will report to the Office of the Chief Security Officer (OCSO) or cognizant component personnel security office regarding any changes to corporate foreign ownership, control, or influence.

Attachment F – List of Acronyms

Acronym	Definition
AWS	Amazon Web Services
C&A	Certification and Accreditation
CO	Contracting Officer
COR	Contracting Officer's Technical Representative
COTS	Commercial Off-The-Shelf
CSP	Cloud Service Provider
DC	Data Center
DHS	U.S. Department of Homeland Security
EIT	Electronic and information technology
ELMS	Electronic Lifecycle Management System
EOD	Entry of Duty
ETL	Extract, Transform and Load
FISMA	Federal Information Management Security Act
FTR	Federal Travel Regulations
GFE	Government Furnished Equipment
GFI	Government Furnished Information
GFP	Government-furnished Property
GOTS	Government Off-The-Shelf
HDFS	Hadoop File System
HSI	Homeland Security Investigations
ICE	U.S. Immigration & Customs Enforcement
ISSO	Information Systems Security Officer
IT	Information Technology
ITPM	Information Technology Project Manager
NIST	National Institute of Standards and Technology
OCI	Organizational Conflict of Interest
OCIO	Office of the Chief Information Officer
O&M	Operations and Maintenance
PIV	Personal Identity Verification
POC	Point of Contact
PoP	Period of Performance
PSU	Personnel Security Unit
PWS	Performance Work Statement
RAVEN	RAVEn – Repository for Analytics in a Virtualized Environment
RDBMS	Relational Database Management Systems
SBU	Sensitive But Unclassified
SCR	System Change Request
SELC	Systems Engineering Life Cycle
SLM	Systems Lifecycle Management
PWS	Statement of Work
SSO	Single Sign-On
T&E	Test and Evaluation

Attachment G – RAVEN Operational Requirements

High-Level Desired Operating Concept and Operational Requirements

HSI has identified 12 operational requirements (ORs) that are essential to accomplishing the HSI Innovation Lab's mission tasks. As the primary purpose of this requirement is to support for the RAVEN Platform, the Contractor is expected to support HSI in meeting these objectives, where applicable, for the RAVEN Platform. HSI has identified the primary contractor teams, if any, that are responsible for helping HSI achieve its objective for each OR. By supporting these efforts, HSI hopes to have RAVEN reach Full Operational Capability by Fiscal Year 2026. RAVEN has already achieved many of these operations; and continuously seeks to improve throughout its life cycle.

Effectiveness Requirements

The RAVEn Platform will enable HSI to expedite development of information tools and services that address investigative needs. The effectiveness requirements identify criteria for enabling expedited development in different categories of tools and services.

The operational requirements (ORs) below relate to the time required to develop tools and services in response to *qualified* requests to support investigations. Here, a *qualified* request meets the following conditions:

- The request comes from an investigator(s), through a website that ICE will establish. This request will be added to a queue on the website, for further assessment.
- The request is verified in that it is assessed to reflect a genuine need to support an investigation.
- The request is validated in that the resulting tool is assessed as something that would substantially expedite a broad number of investigations, not just one single investigation.
- The request is assessed to be technically feasible; RAVEn Program personnel could create the tool using available resources.
- The request is assessed to be operationally feasible; ICE investigators and partners are assessed as being likely to use the resulting tool in practice.
- The RAVEn Platform program makes a documented decision, captured on the website, to start development of the tool. The request is marked as such in the queue on the website. The time/date stamp of the documented decision is the *start time* for meeting the request.

The RAVEn Platform program will then assign qualified requests into one of two categories: rapid configuration or rapid developing.

- Rapid configuration requests can be addressed through tailoring of existing tools.
- Rapid development requests require novel software development.

Qualified requests have an additional attribute – whether they are for the types of tools specified in Table 1.1 below. These reflecting standing investigative needs for core types of tools that are known to ICE today, and detailed technical planning for the RAVEn platform is preparing to address these standing needs.

There will be qualified requests that are not for the types of tools specified in Table 1.1. These will be to address future, unpredictable changes to the criminal threat or technological developments. The

operational requirements permit more time to develop tools outside of Table 1.1, as the RAVEn Platform infrastructure and user base will not be able to rely on past tools and experience in meeting the request.

Table 1.1. Types of Tools For Which There Are Standing Investigative Needs

Types of Tools for Which There are Standing Investigative Needs
1. Customized interfaces to collect publicly available web data and dark web information. 2. Customized, secure data transfer interfaces to electronically transmit data from external sources into internal stores. 3. Customized ingestion tools that import data into the RAVEn Platform system and translate the data from their original format into a format ready for analytic transformation. 4. Customized data transformation tools that: a. Check data for errors, including duplicate transactions. b. Associate data records with sources. c. Transform the data from to forms and formats needed for downstream analysis and use. 5. Secure partner data sharing portals through which ICE investigators exchange information with operational partners electronically. 6. Entity resolution and linking tools that: a. Identify materially relevant entities from within transformed data, to include names, events, addresses, phone numbers, e-mail addresses, and financial account numbers, and convert them to data elements for further analysis. b. Identify relationships between materially relevant entities and convert these relationships to data elements for further analysis. c. Identify materially relevant attributes about the entities and relationships and convert these relationships to data elements for further analysis. 7. Customized federated search instruments covering multiple law enforcement sources and datasets. 8. Customized network-generating and analysis tools, including the following: a. Tools that fuse data on materially relevant entities, relationships, and attributes into connected networks for further analysis. b. Tools that create network diagrams of subsets of the entities, relationships, and attributes. c. Tools that create timeline charts. d. Tools that create trend charts and analyses. e. Tools that create pattern analyses and charts. f. Tools that that create geospatial charts and analyses. g. Tools that perform lead-generating analyses. 9. Tools to prioritize investigative leads and cases. 10. Tools to review analytic reports and visualizations across multiple platforms, to include web, iOS, and Android platforms. 11. Tools enabling collaborative analyses, including tools that: a. Have multiple users work on, or view, quantitative analyses in support of investigations. b. Have multiple users author, edit, or view, investigative reports. c. Have multiple users work on, or view, high-level dashboards. d. The "multiple users" shall include investigators in DHS components outside ICE. 12. Customized portals for sharing data and supporting collaboration with operational partners, including both domestic law enforcement agencies and partner countries.

13. Tools for tracking and using tips, including tools that:
    a. Track tips and attributes about them, including source offices, recipient offices, priorities, and actions taken.
    b. Share tips and related data with partner offices (note that this can be done through other data sharing portals as described above)).
    c. Ingesting and transforming tip information into entity and relationship data that can be used in analyses.

OR 1. Mean time to complete qualified requests. (Data Analytics, User Interface/User Experience, DevSecOps) The following requirement on mean completion times for tools built on the RAVEN Platform result from the program's consultations with its developers, testers, and outside experts on what will be feasible. These times further align with the HSI Innovation Laboratory's standard development cycle times within its agile development and testing framework; within the framework, one sprint (smallest planning unit) is two weeks, and major planning units are one quarter (three months).
The mean time to complete qualified requests shall be measured as the average difference between completion time and the start time, as defined above. The completion time is the time at which the request meets HSI's technical definition of *complete*, which means:

- The code and user interfaces have been tested through a series of testing gateways starting from initial unit tests (preliminary tests to ensure that major software functions appear to work correctly) to full end-to-end integration testing.
- The sponsoring user group has signed off on the new tool.
- The tool has been deployed and observed in practice.
- The satisfaction of the above conditions has been documented on the website. The time/stamp date of this documentation is the *completion time*.

The following requirement on mean completion times for tools built on the RAVEn Platform result from the program's consultations with its developers, testers, and outside experts on what will be feasible. These times further align with the HSI Innovation Laboratory's standard development cycle times within its agile development and testing framework; within the framework, one sprint (smallest planning unit) is two weeks, and major planning units are one quarter (three months).

The mean time the RAVEN Platform takes to complete qualified requests for tools that address investigative needs shall be:

- OR 1A. Rapid configuration requests for types of tools in Table 1.1: 2 weeks.
- OR 1B. Rapid configuration requests for types of tools not in Table 1.1: 4 weeks.
- OR 1C. Rapid development requests for types of tools in Table 1.1: 3 months.
- OR 1D. Rapid development requests for types of tools not in Table 1.1: 6 months.

OR 2. Increase in Qualified Requests Addressed Through Rapid Configuration. (Data Analytics, User Interface/User Experience, DevSecOps) Between Initial Operating Capability (IOC) and Full

Operating Capability (FOC), the RAVEN Platform shall increase the fraction of qualified requests addressed through rapid configuration.

- *Threshold*: increase by an average of 10% annually, until at least 50% of qualified requests are addressed through rapid configuration.
- *Objective*: increase by an average of 15% annually, until at least 75% of qualified requests are addressed through rapid configuration.

An indicator of the RAVEN Platform's progress is that the fraction of qualified requests that can be handled via rapid configuration in the span of a week (as opposed to months for rapid development) will increase over time, as the investigative toolset enabled by RAVEN Platform increases. HSI's objective is to build processes and tools that will help HSI meet these completion lead times.

The RAVEN Platform will enable HSI to expedite development of information tools and services that address investigative needs. The effectiveness requirements identify criteria for enabling expedited development in different categories of tools and services.

OR 3. Measuring Tool Use (Reference only) The percent of tools and qualified requests on the RAVEN platform that are associated with sets of identifiers for the investigations using that tool (or making that request) shall be: Threshold: 75%. Objective: 100%.

The following requirements are necessary conditions for the RAVEN Platform to enable expedited tool delivery.

For planning purposes, the RAVEN Platform shall associate specific uses of information and analysis tools, as well as qualified requests, with specific case investigations. The RAVEN Platform shall provide a dashboard-like functionality to assess which tools are most used in investigations, and what types of information and analysis are being requested.

OR 4. Integrated and Isolated Environment for Development, Testing, and Training. (DevSecOps) The percent of tools developed and fielded through the RAVEN Platform that are fielded without completing development and testing through the integrated and isolated environment, without a documented waiver from the RAVEN Platform program, shall be: *Threshold / Objective*: 0%.
For development, testing, and training purposes, the RAVEN Platform shall provide an integrated and isolated environment.2 All development and testing shall be done through this environment.

Availability Requirements

The following terms have significant meaning for the calculation of availability:

[2] Here, "environment" can include multiple isolated servers or sites.

- Maintenance Window: The sixteen hours between 5:00am Eastern and 9:00pm Eastern time have been identified as the primary period of system usage. Contractors are advised that the RAVEN Platform supports global operations and spans multiple time zones. The remaining eight hours are designated as low impact hours where scheduled maintenance may be performed without impacting observed Reliability, Maintainability and Availability (RMA).
- Failure: Any loss of service of a user impacting RAVEN Platform production application which lasts longer than five (5) minutes AND is (1) unscheduled OR (2) scheduled and occurs or persists outside of the Maintenance Window. For the purpose of this these calculations, a failure occurs only if it is the result of a component within the RAVEN system boundary. For instance, network outages between the RAVEN Platform environment and a field office would not constitute a failure.
- Mean Time Between Failures (MTBF): The MTBF is calculated based upon the time between failures, as defined above.
- Mean Time To Repair (MTTR): The MTTR is calculated based upon the duration of time which the RAVEN system is in a failure state.

Operational Availability is equal to the MTBF divided by the MTBF plus the MTTR.

Operational Availability = MTBF/(MTBF+MTTR)

OR 6A. Mean Time Between Failures. (DevSecOps) The MTBF for the RAVEN Platform shall be greater than: *Threshold*: 160 hours. *Objective*: 320 hours.

OR 6B. Operational Availability. (DevSecOps) The RAVEN Platform shall have an operational availability of: *Threshold*: 95%. *Objective*: 98%.

Materiel availability is not applicable to the RAVEN Platform solution due to its use of cloud solution services. RAVEN Platform components will be hosted on cloud services compliant with FedRAMP high requirements, which includes its own materiel availability requirements.

Reliability and Maintainability Requirements

Software Reliability is meant to capture the probability that the developed software will not cause a failure for a specified period. The following terms have significant meaning for the calculation of Software Reliability:

- Emergency Break-Fix: A software release which requires immediate remedial action to resolve a system outage or unacceptable performance degradation that is occurring or is predicted to occur imminently in a production system.
- Emergency Change Request (ECR): All Emergency Break-Fixes require the filing of an Emergency Change Request (ECR) with the ICE Change Control Board.[3]

OR 7. Software Reliability (Data Analytics, User Interface/User Experience, DevSecOps) RAVEN Platform shall have a Software Reliability Coefficient of: *Threshold*: 90%, *Objective*: 95%.

Software Reliability will be measured by subtracting the number of ECRs from the total number of services successfully deployed to production and then divided by the total number of services deployed to production.

Software Reliability Coefficient = (Number of services deployed to production – Number of ECRs) / Number of services deployed to production)

[3] ICE Change Management Process and Procedure updated 6/1/2020

OR 8. Maintainability. (DevSecOps) *Threshold*: 90%. *Objective*: 95%. Of RAVEN Platform corrective maintenance shall be completed within 8 hours.
Maintainability will be measured by the Maximum Active Corrective Maintenance Time(M_{max}). M_{max} is defined as the value of maintenance downtime below which one can expect a specified percent of all corrective maintenance actions to be completed. For the RAVEN Platform specifically, M_{max} is defined as the maximum corrective maintenance downtime for any actions performed by the RAVEN program and excludes corrective maintenance on (Amazon Web Services) AWS and other infrastructure.
The RAVEN Platform will provide interfaces to a series of systems that provide data to HSI, as described in the following operational requirement.
OR 9. Systems Interfaces. (DevSecOps) The RAVEN Platform shall provide interfaces for exchanging data with the following systems with exceptions when these systems are inoperable for reasons outside of ICE's control.

- Tier 1
    - HSI Data Warehouse
    - ICE/HSI Investigative Case Management (ICM)
    - USCIS Person Centric Query System (PCQS)
    - CBP Passenger Lookout
    - CBP Passenger TECS Screening Services (TSSV)
    - CBP Import/Export
    - National Crime Information Center (NCIC; FBI)
    - National Law Enforcement Telecommunications System (NLETS; private nonprofit corporation owned by States)
    -
- Tier 2:
    - ICE Enforcement Integrated Database (EID)
    - ICE Student and Exchange Visitor Information System
    - ICE Subpoena System (ISS)
    - ICE Significant Event Notification System (SEN)
    - ICE Exodus Accountability Referral System (EARS; ICE Office of Investigations)
    - ICE/ERO Detainee Telephone Services (DTS)
    - DHS Office of Biometric Identity Management (OBIM) Automatic Biometric System (IDENT) OR
    - DHS Office of Biometric Identity Management (OBIM) Homeland Advanced Recognition Technology (HART)
    - HSI PLX Program

Threshold: The RAVEN Platform provides interfaces to 75% of the above systems, including not less than 7 of the Tier 1. Objective: The RAVEN Platform provides interfaces to 87% including all Tier 1 interfaces.
Platform will connect with a variety of data resources held and/or managed by a variety of organizations, beginning within ICE and extending to the private sector. Interoperability begins with assuring ease of use and of fusion of data from these and other sources through the RAVEn Platform. Compliance with the National Information Exchange Model will help in overcoming issues that could arise from differences in terminology or nomenclature across information sources.[4]
Standards will help to assure interoperability, beginning with the Open API specification for vendor-neutral characterization of application programming interfaces.[5] The RAVEn Platform will use standards to guide data collection, storage, access, and analysis. In particular, it will rely on Avro[6] for data

---

[4] "The National Information Exchange Model (NIEM) is a common vocabulary that enables efficient information exchange across diverse public and private organizations. NIEM connects communities of people who share a common need to exchange information in order to advance their mission." See National Information Exchange Model, "NIEM Governance," undated. As of February 23, 2021: https://www.niem.gov/about-niem
[5] The Linux Foundation, "OpenAPI Initiative," undated. As of February 23, 2021: https://www.openapis.org/
[6] The Apache Software Foundation, "Apache Avro 1.10.1 Documentation," December 3, 2020. As of February 23, 2021: https://avro.apache.org/docs/current/

structuring and formatting. Reusable data normalizer and enrichers will enable data from different sources using different formatting to supply common elements, such as E164-compliant phone numbers.
The RAVEn Platform will draw from standards arising from the Immigration Data Integration Initiative (IDII; supporting consistency in data definitions and formatting and the development of standards[7]), the ICE Office of Information Governance and Privacy (OIGP), as well as the establishment of the DHS Data Governance Council and the Data Stewardship Tactical Working Group.

OR 10. User Training. (Reference only) The RAVEN Platform shall have a TMPC of: *Threshold*: 90%, *Objective*: 95%.

In addition to the operator training, RAVEN team members will receive specialized training on the platform's architecture and development philosophy. This training will occur through the same avenues as operator training: a combination of video-based, in-person, and user guides. RAVEN team members will be required to complete this onboarding training within the first 30 days of being assigned to the RAVEN team.

The following terms have significant meaning for the calculation of effective training material production:

User Significant Release (USR): A production releases with significant user impacting changes, this will include releases which introduce or change user interaction in a significant way. This does not include minor user interface changes such as button colors or minor feature additions. Also, it does not include production releases only effecting back-end components which are not visible to the users.

The RAVEN Platform will measure the rate of training material production via the Training Material Production Coefficient (TMPC). The TMPC is calculated by dividing the USRs with accompanying training material from the total number USRs.

TMPC = USRs with accompanying training material/USRs

OR 11. RAVEN Team Member Training. (Data Analytics, User Interface/User Experience, DevSecOps) The RAVEN Platform shall have a TCC of: *Threshold*: 80%, *Objective*: 90%

During its design phase, the RAVEN Platform will comply with User Interface (UI) design standards and incorporate user acceptance testing, to make it easy to interact with the platform, lower training needs, and increase efficiency. Once deployed, a feedback mechanism will be incorporated into the program, allowing end users to provide feedback and requests for enhanced functionality. Requests for changes to the user interface will occur through the data sharing portals. Developers will evaluate and incorporate these requests and feedback into system design and updates.

The RAVEN Platform will measure the completion of this task using the Training Completion Coefficient (TCC). The TCC is calculated by dividing the number of new RAVEN team members who complete the required onboarding training within 30 days of joining the team by the total number of team members who onboarded to the RAVEN team.

TCC = Team members who complete onboarding training on time/ Total number of development team members

OR 12. Section 508 Compliance. (User Interface/User Experience) *Threshold/Objective*: The RAVEN Platform will comply with all applicable Section 508 requirements.

The RAVEn Platform must operate with no special operating factors or considerations. There are no unique personnel, safety, human factors, or environmental considerations for the RAVEn Platform. Training will be developed in accordance with the training task and will include these considerations as required.

During its design phase, the RAVEn Platform will comply with User Interface (UI) design standards and incorporate user acceptance testing, to make it easy to interact with the platform, lower training needs, and increase efficiency. Once deployed, a feedback mechanism will be incorporated into the program, allowing end users to provide feedback and requests for enhanced functionality. Requests for changes to

[7] See U.S. Immigration and Custom Enforcement, *Comprehensive Plan for immigration Data Improvement: Fiscal Year 2017 Report to Congress*, July 26, 2018. https://www.dhs.gov/sites/default/files/publications/ICE%20-%20Comprehensive%20Plan%20for%20Immigration%20Data%20Improvement.pdf

the user interface will occur through the portal described in OR 17. Developers will evaluate and incorporate these requests and feedback into system design and updates.