Performance Work Statement

# Joint Engineering Teams – Sustainment (JETS)

---

## 1. OVERVIEW

Joint Engineering Teams - Sustainment (JETS) will provide USCIS with Agile development and maintenance capability to sustain IT systems for the agency's four mission-focused portfolios: Records, Benefits, Customer Service, and Biometrics. Each portfolio is issued as a separate task order. JETS will supply Agile development teams to participate in IT maintenance efforts using Scrum and other Agile processes, to include other activities necessary for sustaining previously developed systems and applications using Lean processes. The Contractor will be part of an ecosystem participating with federal employees and other contractors in a team-based scaled Agile approach to deliver mission value frequently, cost-effectively, responsively, and with high quality.

The Government will oversee the architecture and design of systems, the Agile methodologies to be used, product planning, and the prioritization of requirements; the JETS Contractors will be responsible for maintaining IT systems with quality and applications to work within those architectures and processes to meet the business requirements; code integration and deployment will be addressed as an entire team, JETS contractors, other contractors, and government staff

## 2. AGENCY MISSION AND GOALS

The Department of Homeland Security (DHS), U.S. Citizenship and Immigration Services (USCIS) is responsible for lawful immigration to the United States. USCIS secures America's promise as a nation of immigrants by providing accurate and useful information to our customers, granting immigration and citizenship benefits, promoting an awareness and understanding of citizenship, and ensuring the integrity of our immigration system.

USCIS has 18,000 Government employees and Contractors working at 250 offices worldwide. USCIS' strategic goals include:

- Strengthening the security and integrity of the immigration system.
- Providing effective customer-oriented immigration benefit and information services.
- Supporting immigrants' integration and participation in American civic culture.
- Promoting flexible and sound immigration policies and programs.
- Strengthening the infrastructure supporting the USCIS mission.
- Operating as a high-performance organization that promotes a highly talented workforce and a dynamic work culture.

## 3. JETS VISION

JETS will provide high-productivity Agile development services and Lean processes focused on IT sustainment of applications that support core business areas in order to effectively and efficiently maintain these systems and applications that are in production at USCIS.

USCIS is a leader in the federal movement toward the adoption of Agile approaches, such as Scrum, Kanban, and DevOps, and use of cloud services to support the IT development pipeline, and is a leader in the DHS movement toward open source frameworks for application development and production. JETS Contractors will participate in a team-based Agile environment. They will work alongside other teams of Government Contractors and federal employees to accomplish projects as assigned by the agency, most notably development efforts. There will be a number of Agile teams from several Contractors working in parallel in a collaborative environment where new development and sustainment of existing systems takes place. These development and sustainment teams will work with Contractor-supported teams responsible for architecture and design, processes and practices (methodology), continuous integration and continuous delivery, testing, quality assurance and training development for fielded capability.

The JETS Contractors will be expected to work with a technical architecture and design specified by the Government, and to work within the Agile process and SELC frameworks defined by the Government. Individual sustainment teams will include Government employees functioning as product owners, business area subject matter experts (SME), and so on, as well as other Contractors with roles in infrastructure, continuous integration, quality assurance, and Independent Verification and Validation (IV&V). JETS Contractors are expected to work well in these team environments and demonstrate a highly collaborative and cooperative attitude.

## 4. SCOPE

USCIS will create and maintain system roadmaps, project plans, and product and release backlogs that will be the basis for the JETS Contractors' work. The USCIS product owner will specify high-level requirements to the Agile teams. As in typical Scrum-based Agile processes, the USCIS product owners will work together with the JETS teams (Government and Contractors) to develop and estimate user stories and establish acceptance criteria. These acceptance criteria will specify expected functionality for a user story, as well as any non-functional requirements that must be met in the development of the story. The USCIS product owners, supported by business SMEs will determine whether or not acceptance criteria have been satisfied. USCIS may adopt other Agile processes such as but not limited to Kanban and Lean, and the Contractors will be expected to conform its processes to these approaches.

As part of the sustainment effort, JETS Contractors will include in its Agile teams members who can provide tier 2/3 service desk support, resources who are able to create and update ad hoc and recurring reports, system administrators, and persons who are able to maintain the development environment(s) used to support the named systems and applications. The intent is to create DevOps teams that can support the application. Additional specialty engineering resources will be required that are outside of the agile teams themselves. These include resources who are capable of providing Information Systems Security Officials (ISSO) for the named systems and applications and others who are user interface designers.

JETS Contractors are expected to provide high-performing, skilled sustainment teams. Critical elements will be:

- High productivity
- High quality work
- Collaboration and cooperation with other teams and participants
- Technical skills and expertise as necessary (see below)
- Estimation and planning skills
- Innovation and creativity in problem solving
- Efficient use of team resources to maximize productivity in named tasks

The providers of JETS services shall adopt evolving USCIS design and coding standards in the course of their application development. The Contractors shall provide technical methods, techniques, and concepts that are innovative, practical, cost-effective, and conducive to Agile application development and Lean sustainment. The Contractors shall maintain applications based on requirements that are evolving and emerge as the business climate shifts. JETS developers will be required to develop high quality code and are responsible for any technical debt that is incurred as a result of their sustainment-related development activities.

Services in support of JETS shall be provided by teams of experts with demonstrated experience with USCIS specified tools and technologies as described in *Appendix A-D.* Agile development work involves some degree of analysis, requirements collection, design, development, and test, in addition to the support functions of configuration management, planning, project management, infrastructure, service desk support, reporting, security, and system administration.

JETS consists of four portfolios: Records, Benefits, Customer Services, and Biometrics. The PWS describes the technical landscape and level of effort required for each portfolio separately (Appendix A, B, C, and D respectively).

## 5. TEAM TASKS

The tasks identified in the following sections describe the work that will occur in order to accomplish the vision, as identified in *Section 3 JETS VISION.*

It is expected that the Contractors, in the spirit of Agile development, will provide multidisciplinary teams composed of members who have two or more of the capabilities required to perform the tasks stated in this PWS, and that the teams will be capable of supporting more than one application. This is necessary because the work is episodic. The Contractors must be able to shift workload among the teams and shift workload between team members as it is needed. Each team should be able to handle all required tasks for a portfolio. Further definition of the teams and the technical proficiencies required are included in the appendices.

The Contractors shall provide Agile teams for the purpose of maintaining each Portfolio and responding to specific application sustainment requirements USCIS identifies. The Contractors' work shall conform to the architecture and design provided by the USCIS Architecture and Design team and the Agile processes set up by the USCIS Processes and Practices team (which also include Kanban processes) and/or other processes as directed by the Change Control and Release

Management (CCRM) team. The Contractors shall accredit a member of each team as a DHS trusted Section 508 tester within 6 months of contract award.

The Contractors shall maintain, manage, operate, and sustain supporting services and architectural solutions as part of agile sustainment. This includes adjusting to and meeting changing requirements and expectations. The solution should be flexible and open to allow for such inevitable enhancement requests. The Agile teams will follow the Agile software development methods based on iterative and incremental development, where requirements and solutions evolve through collaboration between self-organizing, cross-functional teams. It promotes adaptive planning, evolutionary development and delivery, a time-boxed iterative approach, and encourages rapid and flexible response to change. It is a conceptual framework that promotes foreseen interactions throughout the development cycle.

The Contractors shall coordinate efforts with the Government team that is assigned technical and management responsibilities for portfolios. The Contractors shall organize, direct and coordinate planning and execution of all task activities. The Contractors shall manage all Contractor resources and supervise all Contractor staff in the performance of work on this task order. Each of the Contractors' teams shall include a scrum master. The Contractors shall manage and coordinate its team(s) on a day-to-day basis and ensure plans are communicated to team members. Likewise, the Contractors must ensure that the health and progress against those plans are adequately reported.

Vehicles for transparency, such as the agency-provided Agile Application Lifecycle Management (ALM) tool, shall be maintained with data so that reports and charts can be generated as needed, and so that user stories, defects, and tasks and their status are available to stakeholders. As an example, tools that are currently in use include LeanKit, Rally, JIRA, and team Foundation Server. Task boards and SharePoint sites, meetings, and demos can be used to share information and report progress. Contractors and Government employees will utilize and have access to the same ALM tool. The Contractors shall refrain from using proprietary tools that a product owner, who is a federal employee, cannot access.

## 5.1 Code Maintenance

Code maintenance tasks involve changes to software code, whether the code is modified by the Contractors directly or through third party vendors, such as for COTS upgrades. Maintenance may arise based on needs of OIT and business stakeholders. Code maintenance activities are categorized as *corrective, adaptive, or relevance*, as described below:

- **Corrective Maintenance:** Correct software failures, performance failures, and implementation failures that result from design errors, logic errors, and coding errors.
- **The Adaptive Maintenance:** Upgrade or convert the application as a result of changes in the operating environment. The term environment refers to all of the conditions and influences which act from outside upon the application, such as business rule, Government policies, legislative changes, work patterns, or software and hardware platform changes.
- **Relevance Maintenance:** Accommodate new or changed user requirements or to increase the application performance or enhance its user interface.

The Contractors shall submit artifact deliverable items required by USCIS as specified by USCIS to the USCIS electronic document library and/or to other recipients as directed. The Contractors shall comply with a standard and accessible change control process in accordance with USCIS OIT

CCRM policy. A change is an addition, modification, or removal of approved, supported, or baseline hardware, network, software, application, system, image, or associated documentation. The Contractors shall:

- Perform the full suite of code maintenance tasks using Agile methodologies, including, but not limited to: participating in creating user stories for both business functionality, technical requirements and defining acceptance criteria; estimating the size of stories; solution design; development; and testing.
- Collaborate with stakeholders, support Contractors, and third party vendors throughout system integration, performance, security, Section 508, system acceptance, user acceptance, usability, and test and evaluation reporting.
- Document each aspect of the development process, report outcomes and forecasts, document developing epics, user story features, release trains and other agile artifacts.
- Work with stakeholders to analyze data, complexity, and risks to ensure identification during the planning process. The Contractors will gather project requirements and will meet stakeholder expectations and present task risk assessments associated with each project.
- Create change requests as required and submit them to the Government for approval.
- Develop fully commented executable code and other artifacts against the user stories documented in this task or as assigned by the Government.
- Develop code that does not add new technical debt to a release; the Contractors shall correct any defects identified by testers, code reviewers, automated tools, or as part of the CI/CD activities etc.
- Deliver fully commented executable code and code revisions that follow Agile industry best practices, to include: version control, automated builds, automated testing, and continuous integration.
- Produce output that conforms to the architecture and standards provided by the Government and the Agile processes set up by the USCIS Processes and Practices team. This will include providing input to any documentation required to maintain compliance with DHS and USCIS standards, as specified by USCIS.
- Produce code that meets the functional and non-functional requirements, meets database development requirements, and is deployable and fully tested in preparation for USCIS OIT Independent Validation & Verification (IV&V) review.
- Perform database and application software upgrades and migrations.

For code maintenance test and integration, the Contractors shall:

- Create test cases and automated test scripts to support test automation activities.
- Collaborate with other teams to support continuous code integration.
- Share test scripts (manual and automated) as needed with other testing entities.
- Assist with crafting validation steps (both positive and negative testing) for user acceptance testing on an as needed basis.

- Support the activities of the integration and configuration team to ensure the automatic build and deployment process works effectively across all environments, including the Contractors' dev/test enclave. Deployment and testing in the dev/test environment should mimic closely the actions performed for deployment and testing in staging and production.
- Perform development testing before the commit stage in the continuous integration pipeline
- Participate in the deployment pipeline, which will be managed by different Contractors and USCIS teams.

## 5.2 Operational Maintenance

The objective of operational maintenance is to ensure the Portfolios maintain operational readiness. Although the Contractors share responsibility for operational tasks with other vendors who support the production/operations environments, the Contractors shall monitor and perform routine and corrective actions on applications that are in production while following established change and release management processes and procedures. As the Contractors monitor the operational posture of applications, further evaluation and analysis may be authorized to ensure the continued sustainability of the applications. Monitoring and early warning will allow OIT to pro-actively plan and carry out maintenance activities.

The Contractors must have the technical skills for performing administrative, application, and database actions. System administrators must be knowledgeable in Windows 2003/2008 and z/OS operating system maintenance. Database administrators (DBAs) must be knowledgeable in the maintenance of Oracle, CA-IDMS, MS SQL Server, Pervasive and My SQL database management systems. The development languages predominantly used by the JETS applications include: Visual Basic, C#, C/C++, Java, and, COBOL. Lesser used development languages include: XML, ADSO, ASP.NET, ASP/JSP, HTML/CSS, JavaScript, JCL and PHP. Contractor personnel performing application administration tasks must be knowledgeable in these languages. Administrators of JETS applications must also have experience with COTS products including but not limited to: Captiva InputAccel, Global360, Documentum, Crystal Reports, Siebel CRM, OBIEE, Informatica, Oracle Secure Enterprise Search (OSES), and Oracle Business Intelligence (BI) Publisher.

For operational maintenance tasks, the Contractors will estimate the size of tasks in terms of user stories, assigning story points and inserting them into the product backlog along with technical requirements so that operational tasks can be resourced given team size and other priorities. These activities occur within the development team and not as a separate team. This allows the USCIS product owner and other stakeholders to have visibility into all activities and resources. The Contractors shall:

- Provide teams responsible for performing the full suite of operational maintenance tasks using Agile methodologies, including, but not limited to: participating in creating user stories for operational maintenance requirements and defining acceptance criteria; estimating the size of stories; determining solution approach; and executing.
- Assist in the documentation of user stories, acceptance criteria, and tasks to be completed to fulfill the definition of done for a story.
- Produce scheduled and unscheduled reports derived from data contained in Portfolio applications. This will involve obtaining report requirements, reviewing and researching

applicable available documentation, extracting applicable database information required to assemble the report, and displaying the extracted information as required by the Government.

- Produce studies, analysis, and white papers, as directed by the Government, which are typically assigned in order to identify potential improvements and problem or issue resolution. The output of this activity shall be a written deliverable that addresses the problem area and recommends solutions and estimates for the LOE needed for execution. The Contractors shall stand up tiger teams as needed to address critical and/or complex problems.
- Respond to user-initiated service-desk requests that are referred to Tier 2 and/or Tier 3 support for application-related problems. Key application support personnel or qualified designated backup must be accessible (via e-mail/voice after normal business hours) in the event of a critical emergency. The Contractors shall respond to service requests appearing in the Contractors' queue. After proper diagnosis of the service request, the team shall be required to indicate resolution in Remedy (or any other Government-supplied incident management tool), or assign the ticket to the appropriate queue for further action, as appropriate, and describe in Remedy the Contractors' course of action. The Contractors shall follow the service desk resolution workflow proscribed by the Government.

For system and database administration the Contractors shall:

- Provide system and database administrators for the engineering/development environments.
- Support the execution of emergency backups in coordination with other infrastructure operational components and/or DHS data center specific requirements; support the development of contingency plans, including disaster recovery and COOP testing, and operation failover testing consisting of documented contingency plans; develop contingency plans for supported applications.
- Routinely evaluate the need to upgrade database servers and application software while determining compatibility with current application versions.
- Configure database environments, or support other parties who will configure those environments, for Functional Qualification Testing (FQT), regression testing, Independent Test & Evaluation (IT&E), user acceptance testing, integration testing, database security testing, installation/migration testing, configuration/compatibility testing, and performance, load, and stress testing, as requested.
- Support the migration of databases from the non-production to the production environment, as well as migrations of applications and databases between data centers, as requested.
- Provide technical assistance to infrastructure stakeholders to resolve failures or address network related issues, and support incident management and problem management activities.
- Coordinate OS upgrades, patches, fixes, and testing with data center staff.
- Monitor application usage and storage, and provide advance warning when thresholds are reached. Provide advice and implementation support to address application high availability issues and requirements.

- Perform periodic database clean-up and maintenance of training environments in support of end-user training classes.

Each application's administrative requirements are different, and specific activities are described in the portfolio appendices for illustrative purposes (administrative actions needed will change with time as the application and organization change). *Table 1: Typical Administrative Functions* describes application and database administration functions at a general level.

| Function | Frequency | Description |
|---|---|---|
| Account management | As required | Complete and process access requests (e.g., user profiles/preferences, password reset) for systems and applications. |
| Monitor logs and alerts | Daily | Monitor system event logs, application event logs, and monitoring tool alerts. |
| System Performance Monitoring | Daily | Monitor systems CPU, memory, disk, network utilization, and other key performance indicators prescribed by the application. |
| System maintenance activities | Daily | Move or clear logs, daily backups, or other activities required to continue daily operations. |
| Patch management | Monthly | Identify required patches, download and test, coordinate installation. |
| System updates, configuration changes, deployments | As required | Identify and recommend required updates, plan and schedule update activities, test updates, coordinate installation. |
| Troubleshooting support | As required | Provide research and corrective actions for event logs, alerts, or incidents that indicate a system loss or degradation of function. |
| User account and organization hierarchy management | As required | Add new user meta-data, update existing users' meta-data, create/update USCIS locations/sites, create/update user positions, update user responsibilities, etc. |

**Table 1: Typical Administrative Functions**

JETS applications are located at multiple locations. The system locations, which are subject to change, are defined below in *Table 2: Application Locations.* Each location has unique support staff and operating environments that are important to understand. Additional information about the locations is described in the portfolio appendices. All applications currently in TECC will be moving to DC1.

| Location | Applications |
|---|---|
| DC1 | APSS, AR-11, BBSS, CIS, CLAIMS 3 MF, CLAIMS 4, CMIS 3.0, CRIS, E-Filing, FD-258 MF, ICPS, MiDAS, NFTS, RAPS, Remedy |
| TECC | CMIS 2.0, EDMS, FIPS, InfoPass |
| Service Centers | • CLAIMS 3 - Administrative Appeals Office (AAO)<br>• CLAIMS 3 - Baltimore District Office (BDO)<br>• ICPS-NPS - Corbin Card Production Facility (CCPF)<br>• CLAIMS 3, ICPS-NPS, BBSS - California Service Center (CSC)<br>• CLAIMS 3, ICPS-NPS, ICMS - National Benefits Center (NBC)<br>• BBSS, CLAIMS 3, ICMS, ICPS-NPS -Nebraska Service Center (NSC)<br>• BBSS, CLAIMS 3, ICPS-NPS - Texas Service Center (TSC)<br>• BBSS, CLAIMS 3, ICPS-NPS - Vermont Service Center (VSC)<br>• SODA - National Records Center (NRC)<br>CLAIMS 3 also includes the interfacing systems: Biometric Retrieval Utility (BRU) and Family-Based Adjustment of Status Interface (FBASI). |
| DHS CGI Public Cloud | CSWP |
| 1001 G St., NW | CLAIMS 4 National Server, CLAIMS 4 NFTS Interface Server |
| NY MDC | NCSC Siebel |

**Table 2: Application Locations**

The primary tools currently used to support the administrative functions described above are Remote Desktop Connection and Windows Server Performance Monitor which are standard with Windows Server and the Windows XP and Windows 7 desktops. Standard USCIS software image are used by systems administrators. Other administration tools are provided below in *Table 3: Administrative Tools.* Tools and hardware may change or evolve to meet changing needs.

| Manufacturer | Product/Version | Quantity and Type of Licenses | Gov't Owned? (yes/no) POC |
|---|---|---|---|
| Microsoft | System Center Operation Manager Console | 4 / Enterprise License | Yes |
| Open Source | PuTTy 0.62 | 4 /Free | Yes |
| Siebel | Customer Relationship Management (CRM) 8.1.11 | Enterprise | Yes |
| Oracle | Oracle Business Intelligence Enterprise Edition suite (OBIEE) 9.2.0.8.0 | Enterprise | Yes |

**Table 3: Administrative Tools**

# 6. SPECIALTY ENGINEERING TASKS

## 6.1 User Interface Services

The Contractors shall provide **Usability or Human Factors IT Design experts** to provide User Interface services across the applications within each of the portfolios. The Contractors shall provide **1 Usability or Human Factors IT Design expert for each portfolio.** These Usability or Human Factors IT Design experts are not included in the team count provided in each of the Appendices and will be included in the Specialty Engineering CLIN. The quantity of Usability or Human Factor IT Design effort required for each portfolio is as follows:

- **Records: 1** (1860 hours per 12 months)
- **Benefits: 1** (1860 hours per 12 months)
- **Customer Service: 1** (1860 hours per 12 months)
- **Biometrics: 1** (1860 hours per 12 months)

The Contractors shall provide user interfaces (UI) that are highly usable and sufficiently accessible. The final arbiter for accessibility (conforms with Section 508 of the Rehabilitation Act) rests with Government-provided inspection and acceptance bodies. The usability of an application is a measure of the overall effectiveness, efficiency, and satisfaction with which a typical user population can perform specific tasks/actions and achieve specific goals in a particular environment with the UI provided. The primary goals of user interface services are:

- Increase user success rates: Eliminating application and UI design problems to prevent errors (of commission or omission) while enabling users to correctly request, locate, navigate, and interpret critical transaction data and to accurately understand the purpose and use of the system presented to them.
- Reduce training requirements and performance support intervention costs: Building clear and effective UIs to enable end users to perform their required system functions with minimal learning curves.
- Reduce job-related stress, operator down time, and staff turn-over: providing ergonomically sound design to increase user productivity and job satisfaction.
- Reduce development costs: identifying usability problems and inefficient, error-prone designs early in the project lifecycle reduces costs of re-work.

The Contractors shall employ Lean User Experience (UX) practices and apply visual design expertise on applications within the scope of this PWS in order to achieve the goals referenced above. The Contractors shall:

- Design and conduct usability tests to determine deliverables' accuracy to functional requirements (the Government will identify and provide access to the individuals who will serve as usability test participants - "users").
- Create Lean prototypes and interaction models (affordable low-tech models, such as wireframes, are acceptable), and validate them by gathering feedback and testing (qualitative and quantitative) with users.

- Design develop, test, and implement intuitive navigation structures, information architectures, and user interfaces using user-centered or task/goal-directed design principles and UI best practices.
- Conduct usability and content analysis.
- Maintain design consistency throughout applications, and where feasible among portfolios of applications, and if possible between portfolios.
- Conform with USCIS and DHS graphical design styles that appeal to users to the extent possible and feasible given rapidly evolving platforms

## 6.2 Security

The Contractors shall provide **Security Specialists** who will be used across the applications within each portfolio as Information Systems Security Officials (ISSO). These Security Specialists/ISSOs are not included in the team count provided in each of the Appendices and will be included in the Specialty Engineering CLIN. The quantity of Security Specialist effort required for each portfolio is as follows:

- **Records: 2** (1860 hours per 12 months)
- **Benefits: 3** (1860 hours per 12 months)
- **Customer Service: 2** (1860 hours per 12 months)
- **Biometrics: 1** (1860 hours per 12 months)

The objective of the Security task is to ensure all of the applications within scope of this PWS receive security Certification & Accreditation (CA) if not achieved previously, and to maintain an acceptable C&A status throughout the duration of the PWS for those applications that receive or have C&A. The Department of Homeland Security 4300A requires that an Authority to Operate (ATO) is granted every three years, with an annual refresh. USCIS has moved many applications to an Ongoing Authorization model where there are monthly reviews of any new risks and security concerns. The Security Specialist must support the Ongoing Authorization process.

Contractor-provided ISSO support shall interface with USCIS OIT representatives to ensure that the requirements identified in DHS 4300A, description of ISSO responsibilities are fulfilled. The Contractor ISSOs shall:

- Prepare required documentation to support the USCIS C&A process as required by the Government.
- Provide localized security training as directed by the Chief Information Security Officer (CISO) or Information System Security Manager (ISSM).
- Provide monthly status reports of all Plan of Action and Milestones (POA&M) related to each application (security section of Performance and Expenditure Report).
- Provide monthly status report of annual assessments performed (security section of Performance and Expenditure Report).
- Report all Information Security and Privacy Data incidents, as required (security section of Performance and Expenditure Report).

- Perform duties as described in the ISSO designation letter.

The Contractors shall provide support to the OIT Information Systems Security Manager (ISSM) in meeting the information security requirements for USCIS data processing installations. The Contractors shall assist the ISSM with the management and administration of USCIS IT application systems operations and ensuring compliance with Federal security regulations, policies, guidelines, and applicable National Institute of Standards and Technology (NIST) standards.

As part of this task, the Contractors shall maintain USCIS JETS hardware and software tracking data sets. The production hardware and software of JETS applications is maintained primarily for the ISSO's C&A use. Since third-party entities are the custodians of the production environment, system information is not always readily available, especially when virtualized. Where possible, data tracked includes, but is not limited to, project owner, product name, manufacturer, version, quantity, location, and description. This data currently resides in an Excel spreadsheet.

The data set of software used by JETS developers is much more robust. It currently resides in an Excel spreadsheet and includes all pertinent data with regard to licenses that are provided to JETS developers for use while performing tasks in support of this PWS. Examples of the type of data tracked include user, license key, serial number, vendor, manufacturer, purpose, project owner, quantity, physical media location, format, special instructions. A list of freeware is also maintained for each of the JETS applications.

## 7. KEY PERSONNEL

The Contractors shall identify key personnel and provide statements of qualifications for these individuals. Key personnel shall be full time employees of the prime contractor. The Government requires two key personnel for each portfolio: a **management lead** and a **technical lead**. Key personnel may be members of the portfolio teams or they may be members associated with the Program Management CLIN. These individuals must have expertise in the Agile development methodology and the technical leads must have experience with many of the technologies in *Appendices A-D* as it relates to the portfolio assigned.

The management lead shall ensure that all work on this contract complies with contract terms and conditions and shall have access to Contractor corporate senior leadership when necessary. The Contractors' management leads shall be the primary interface with the USCIS Contracting Officer's Representative (COR) and Contracting Officer (CO) and shall attend status meetings and ad hoc meetings with stakeholders in person as required, accompanied by the technical lead when necessary.

| Title | Education/ Certification | Experience | Knowledge/Skills |
|---|---|---|---|
| Management Lead | Master's Degree or higher from an accredited University; Certified Project Management | 10 or more yrs. of exp. in the technology sector; with at least 8 yrs. of project and/or program management exp.; and with at least 3 years managing programs or projects | Organizes, directs, and manages contract operation functions, involving multiple, complex and inter-related project tasks that use agile development methodologies. Manages teams of contract support personnel at multiple locations so that that delivery is on time, within budget, and meets the specifications and requirements. Maintains and manages the client interface at the senior levels of |

| Title | Education/ Certification | Experience | Knowledge/Skills |
|---|---|---|---|
| | Institute Project Management Professional (PMI-PMP) or Project Management Institute Agile Certified Practitioner (PMI-ACP) | that use agile methodologies<br><br>Substitute Bachelor's degree in lieu of Master's and 15 or more yrs. of exp. in the technology sector; with at least 10 yrs. of project and/or program management exp.; and with at least 4 years managing programs or projects that use agile methodologies | the client organization. Meets with customer and contractor personnel to formulate and review task plans and deliverable items. Establishes and maintains technical and financial reports to track project progress to management and customers. Organizes and delegates responsibilities to subordinates and oversees the successful completion of all assigned tasks. |
| Technical Lead | Master's Degree or higher from an accredited University; engineering, science, or technical degree at either the Bachelor's or Master's level | 10 or more yrs. of exp. in the technology sector; with at least 8 yrs. of IT leadership exp.; and with at least 3 years leading engineering activities that use agile methodologies; application development and design experience for two or more major technologies employed by the applicable portfolio<br><br>Substitute Bachelor's degree in lieu of Master's and 15 or more yrs. of exp. in the technology sector; with at least 10 yrs. yrs. of IT leadership exp.; and with at least 4 years leading engineering activities that use agile methodologies | Develops technical solutions to meet a wide range of business needs. Evaluates technical trends and provides recommendations for technology and architecture to meet business objectives. Prepares cost-benefit and return-on-investment analyses for management decision-making purposes. Devises or modifies procedures to solve complex problems considering computer equipment capacity and limitations, operating time, and form of desired results. Leads the requirements, design, development, testing, implementation, and documentation of new software and enhancements of existing applications. Works with program managers, project managers, developers, and end users to ensure application designs meet business requirements, and delivers capability using agile methodologies. Formulates/defines specifications for complex operating software programming applications and modifies/maintains complex existing applications using engineering releases and utilities from the manufacturer. Leads all phases of software systems programming of new applications and enhancing, correcting, refreshing, and modifying existing software applications. |

# 8. TRANSITION-IN SUPPORT

Transition is a set of activities that occur when an existing application is added to a JETS portfolio (such as resulting from contract award, as well as after contract award) or when an application within the scope of this PWS transitions out of this PWS (such as resulting from decommissioning, or continuation of efforts by another third party or Government entity). At the completion of

performance of this contract, and/or as otherwise directed by the Government, the Contractors shall fully support the transition of their work that is turned over to another entity.

A Transition Plan shall be completed and agreed to by the Government prior to the transition of an application(s) onto or off of a JETS portfolio. The JETS Contractors shall play a key role in the planning of transitions and the creation of JETS application Transition Plans, and shall comply with transition milestones and schedules of events.

The Contractors shall be responsible for the implementation of the transition and application cutover activities. The transition shall cause no disruption in development services. To ensure the necessary continuity of services and to maintain the current level of support, USCIS may retain services of the incumbent Contractors for some, or all of, the transition period, as may be required.

The Contractors shall be responsible for the transition of all technical activities identified in this task order, and engage in transition planning at the direction of the Government. As part of the transition, the Contractor shall be responsible for:

- Inventory and orderly transfer of all GFP, to include hardware, software, and licenses, Contractor Acquired Government Property, and Government Furnished Information (GFI)
- Transfer of documentation currently in process
- Transfer of all software code in process
- Certification that all non-public DHS information has been purged from any Contractor-owned system
- Exchange of accounts to access software and hosted infrastructure components
- Participate in knowledge transfer activities in accordance with the transition plan
- Provide members to and participate in transition management team

The Government will provide a Transition Plan template, the Contractors shall complete it as assigned. The Transition Plan shall include support activities for all transition efforts for follow-on requirements to minimize disruption of services. The Transition Plan shall:

- Document the strategic approach
- Identify equipment, hardware, software, documents and other artifacts that are included in the transition
- Establish milestones and schedules
- Establish activities
- Identify transition risks and risk mitigation
- Define roles and responsibilities
- Define transition approval authorities and lines of communication
- Define a knowledge transfer approach
- Define a property inventory and transition approach
- Create bi-party or tri-party agreements

- Provide checklists

A Transition Plan shall be delivered 90 calendar days prior to the task order expiration date or, if directed by the Government, 90 days prior to the end of each option period, or as otherwise directed by the Government.

Transition support shall commence upon direction of the Government. The incumbent Contractor will work with the new Contractors to provide knowledge transfer and transition support, as required by the COR and PM.

## 8.1 Transition Phases

The transition phases are intended to help organize the transition activities and to make transition status assessment easier. The transition phases are: Planning, Due Diligence, Knowledge Transfer, and Cutover, each lasting approximately one month. The total transition period is 4 months and the four transition phases apply to the initial transition after task order award, as well as to application transitions that may occur during task order performance.

## 8.2 Planning Phase

The Transition Planning phase lays the groundwork for the transition and prepares participants, so that the transition will proceed as smoothly as possible. Planning activities include finalizing the transition MOUs and Due Diligence checklists, defining specific work elements required by the task, developing or revising the task plans necessary to perform the work, and completing staffing efforts.

Work activities performed during this phase include:

- Convene meetings with the originating organization and the receiving organization to determine the application state and status, and to jointly define specific work activities and the products, systems, and services that should be addressed during transition
- Identify critical operational and maintenance issues that must be resolved
- Review open system discrepancies or problems
- Provide information requested in Due Diligence checklists to receiving organization personnel to prepare for debriefing
- Support facility tours and training sessions for the Knowledge Transfer phase as required

As part of the planning process the team identifies the transition-related activities that are completed by the JETS Contractor and those completed by the originating organization throughout the transition period. Likewise, ensure identification of those activities that the JETS Contractor and the originating organization will complete in order to ensure continuity of services and mission-performance of the application throughout the transition phase. New development should not occur during the transition period and in-process release-related activities should finalize or prepare for a code-cutover. All planning is performed to the level required by task complexity.

## 8.3 Due Diligence Phase

The purpose of the Due Diligence Phase is to discover and provide all available information needed to transition task activities from transitioning-out team to the receiving team without interrupting or degrading service. One of the first activities in this phase is to review the documents stored in the Information Technology Document Library (ITDL).

Working through a Transition Management Team (TMT), the JETS Contractor establishes contact with the transitioning-out Contractor, field offices, end users, and other stakeholders as necessary to develop a sound understanding of the systems and related business processes. Checklists are used to collect relevant contract documentation such as the following:

- Technical environment descriptions
- Field office personnel, call lists, contact points
- Production status and priorities
- System and application software documentation
- Development status and documentation
- Source code
- Status of in-process procurements
- Test documentation, status, and deployment plans
- Operations logs and problem logs
- Security levels and access requirements for environments, applications, and databases
- Tools and tool documentation
- Concepts of operations and functional descriptions
- Operational procedures

The checklists can be improved and tailored by the TMTs and the JETS Contractor. Persons conducting due diligence activities complete the checklists and share them with the TMT prior to the conclusion of Due Diligence Phase.

During this phase the transitioning-out Contractor also provides and validates:

- Existing operations and maintenance (O&M) procedures
- Critical Operation Policy and Procedure (COPP) documents
- Detailed operational work instructions
- Various technical and white papers written and/or acquired that support communication within the task team
- In-process code and associated documentation, and other artifacts

Due diligence information is used to perform a gap analysis to identify missing, incomplete, or out-of-date due diligence items, such as documentation, products, and configuration status reports. For each missing, incomplete, or out-of-date item, the analysis will include an action item assigned to a specific person responsible for resolving the issue during the transition effort. Any gaps that remain at Task Cutover time are presented at the Task Cutover Readiness Review.

In order to resolve gaps, handle issues and risks, follow-up on action items, and update the schedule, meetings will occur twice-weekly throughout the transition period. These meetings may increase or decrease in frequency depending on need. Additional sub-group meetings may spin off to meet specific transition requirements.

During the Due Diligence Phase, the transitioning-out team and JETS team also begin activities associated with the transfer of software, hardware, and other computer resources. The receiving Contractor will start to develop an environment capable of receiving and performing maintenance on the source code as specified in the transitioning-in contract.

## 8.4 Knowledge Transfer Phase

During the Due Diligence and Knowledge Transfer Phases the transitioning-out Contractor will provide the JETS Contractor with honest, accurate assessments of the state of the formal documentation. Where informal working papers are available those will be provided at Knowledge Transfer sessions where the receiving Contractor can ask questions of USCIS and transitioning-out Subject Matter Experts.

The transitioning-out Contractor provides members of the JETS team with system demonstrations and descriptions, to include:

- Overview/orientation training
- USCIS environments and business processes and rules
- Workflow processes
- External interfaces
- System functionality and architecture

Government personnel facilitate knowledge transfer by providing the following:

- Facility tours, as required
- Feedback on transition products
- Big-picture views

## 8.5 Task Cutover Preparation Phase

During Task Cutover Preparation, JETS staff focuses on *doing*, rather than studying. Team members practice the functions they will be performing after cutover, continue attending training and demonstrations, and validate software and procedures. This phase ends with an Application Cutover Readiness Review, in which the TMT provides to the JETS COR, the JETS PM, and to other Government leadership evidence of the JETS team's readiness to assume responsibility for the application.

The JETS Contractor participates in practice sessions (using development and test environments) with the assistance of the out-going Contractor. These practice sessions include the following:

- Development and maintenance teams practice modifying and testing software, improving their proficiency and knowledge of the systems
- Test and evaluation teams rebuild and regression test software, validating procedures and improving proficiencies in and knowledge of the systems

The support teams will perform the following transition activities:

- Update and generate O&M procedures as needed
- Validate CM baselines
- Validate that appropriate development and test environments are transitioned to the JETS Contractor
- Validate complete transfer of government-furnished property (GFP) and relocation of equipment as needed
- Validate the removal of the transitioning-out Contractor access and permissions to software that is transitioned to the receiving contract

- Change service desk POCs and knowledgebase as appropriate

An essential part of the transition is ensuring that all USCIS GFP is inventoried, handed over, and logged in the Government asset management tools. The outgoing Contractor's property manager, the JETS Contractor property manager and the Government property and asset manager work with the TMT in the transition, receipt, identification, control, accounting, and disposition of GFP as appropriate during the transition. The JETS Contractor property manager verifies the receipt of all required property elements, including licenses, supplies, and equipment. The TMT approves the final list of transitioned GFP. The JETS Contractor supports the TMT in accomplishing the following activities for transferring GFP:

- Inventory the GFP
- Prepare USCIS transfer documents
- Obtain all required signatures
- Relinquish custody of the GFP and relocate as required
- Update the USCIS Asset Management tool
- Enter GFP information into the Government Property Management System
- Tag GFP in accordance with approved government property management procedures

## 8.6 Task Cutover

As the transition activities near completion, the TMT will schedule an Application Cutover Readiness Review with the COR, PMs and leadership teams of the outgoing and JETS Contractor. Receiving leadership team includes the JETS COR, the JETS PM and Government leadership. The transitioning-out leadership team includes their contract COR and PM, and Government owner. The Transition Manager is responsible for identifying the appropriate personnel required at the Application Cutover Readiness Review.

At the Application Cutover Readiness Review, the TMT will present a memorandum to all stakeholders stating that the application is phasing over to the JETS contract and informing the stakeholders of the application cutover to the incoming Contractor's responsibility. Memorandum stakeholders sign the MOU indicating that the application is ready for cutover. The memorandum includes information essential or important to the stakeholders, such as key contact names, names of backup responsible personnel, and may identify specific processes or procedures to be followed under the JETS contract. When the memorandum is signed, the transition activities are considered complete, and the JETS Contractor and OIT will assume responsibility for the O&M readiness of the application.

# 9 Reserved

# 10 DELIVERABLES

The primary deliverable of this task order is deployable application code. The Contractors shall deliver this code (in conformance with procedures established by the Integration and Configuration team) throughout the period of performance for integration with an existing codebase in preparation for deployment.

The Contractors shall submit electronic copies of document deliverables that are indicated in the table below to the CO and COR (and other cc's as may be specified by the CO and/or COR) via e-mail in the format specified. All document deliverables shall be made by close of business (COB) 4:30pm local time Monday through Friday, unless stated otherwise.

All deliverables submitted in electronic format shall be free of any known computer virus or defects. If a virus or defect is found, the deliverable will not be accepted. The replacement file shall be provided within two (2) business days after notification of the presence of a virus or defect.

## 10.1 Task Order Management Artifacts

The Contractors shall provide standard and ad hoc reports that support task order management. Standard reports are described below:

- Performance and Expenditure Report (PER)

  The PER, delivered monthly, shall contain a narrative of the month's activities and resource expenditures, as described below:

  - Performance Summary

    The Performance Summary includes documenting any major risks and/or issues and any significant progress and events. Progress and events includes the delivery of documents, artifacts, and code. The summary should provide enough detail for the reader with some but not detailed familiarity with the task order to comprehend the value that the Contractors are providing to the overall application development effort at USCIS.

    Included with this summary shall be burn-down and burn-up charts for those releases and iterations that ended within the month, and a snapshot of the burn-charts for all releases and iterations in progress on the last day of the PER reporting period. Cumulative flow diagrams shall be provided for those releases using kanban.

  - Resource Expenditures

    Resource expenditures track funds expended during the reporting period and their purpose in order to understand the burn rate and provide fiscal accountability to external stakeholders. For firm fixed price contracts the resource expenditures are used for Internal Use Software reporting purposes and in order to measure hours expended. For Firm Fixed Priced efforts within the contract, supply a rationale for how the costs are determined for resources that participate in releases. Reporting of resource expenditures shall conform to the format provided in section 11.5.

  - Service Desk Report

    The Service Desk Report describes the Tier 2 and 3 service-desk tickets that the Contractors received (along with tracking number) for each JETS application and classifies the defects into useful categories, such as defect or error, user knowledge or skills deficit, or an application usability issue. The Report also recommends System Change Requests (SCR) in response to defects or other items as appropriate. The report shall show trends in the classification areas, and summarize cumulative

report data each month, as well as provide more detailed reporting of new items each month.

- Software Inventory Status Report

  The Software Inventory Status Report provides an early warning when software maintenance agreements will expire. The intent of this report is to alert the Government 90 days prior to expiration so that extensions and renewals of agreements can occur. The report will also track the progress of the extensions and renewals. This will require coordination with Government stakeholders involved in the software renewal processes. The Contractors will be provided a software inventory with current data during the transition-in process.

- Security Report

  The Security Report documents the C&A status of all applications within the scope of this PWS; provides status of all Plan of Action and Milestones (POA&M) related to each application; provides status of annual assessments performed; and documents any security or privacy incidents.

- Schedules

  Schedules shall be maintained, updated, and kept current in a Government-furnished tool, such as MS Project Server. Schedules that are of interest to the Government are portfolio-based, and include schedules of applications and their releases along with milestones. Constraints and predecessors that are external to the application and impact milestones must be annotated.

- Status Briefings

  As required by the COR, the Contractors shall attend meetings with the COR and/or other USCIS stakeholders in order to review work accomplished, work in progress, plans for future work, transition plans and status, and issues pertinent to the performance of work tasks that require USCIS attention. The meetings may be scheduled regularly or may be ad hoc.

  In the event the Government requires additional information related to contract technical, cost, or schedule performance, risks, resources, or any contract-related data, the Contractors shall provide this report information in the format requested by the Government. Requests for ad-hoc reporting may vary in scope and complexity and may require the Contractors to attend OIT meetings to obtain required information, review and research applicable documentation, and extract applicable database information required to assemble the ad-hoc report.

## 10.2 Deliverables Schedule

The deliverables that apply to this task order, and that the Contractors shall provide are outlined in *Table 5: Deliverables Schedule.*

| Item | Frequency of Delivery | Acceptable Formats |
|---|---|---|
| Shippable application code | Continuously, with each deployment | Application source code and compiled code |
| Agile development lifecycle documents, such as System Design Document (SDD), etc. | Each release | MS Word 2010 or electronic format such as wiki or SharePoint |
| Software inventory updates | Monthly | MS Excel |
| Status Briefings, presentations, database extractions, reports, white papers and analysis, schedules, etc. | As directed | MS Word 2010, Excel, Visio, or PowerPoint |
| Program and Expenditure Report (PER) | 10th calendar day of each month | MS Word 2010, Excel |
| Task Order Status Report (per F.8.2.1 of the EAGLE II Contract) | 10th calendar day of each month | MS Word 2010, Excel |
| Transition Plan | As directed | MS Word 2010 |
| Security Plan | 30 days ARO | MS Word 2010 |

**Table 4: Deliverables Schedule**

## 10.3 Inspection and Acceptance

Various Government stakeholders will inspect Contractor services and deliverables. The CO will provide official notification of rejection of deliverables. Inspection and acceptance of deliverables will use the following procedures:

- The Government will provide written acceptance, comments and/or change requests, if any, within fifteen (15) calendar days of receipt of task order deliverables. For periods exceeding fifteen (15) days, it is the responsibility of the contractors to confirm receipt and acceptance of the deliverable(s).
- Upon receipt of the Government comments, the Contractors shall have fifteen (15) calendar days to incorporate the Government's comments and/or change requests and to resubmit.
- If written acceptance, comments and/or change requests are not issued by the Government within thirty (30) calendar days of submission, or as specified in individual task order, it is the responsibility of the contractors to confirm receipt and acceptance of the deliverable(s).
- The Government will provide written notification of acceptance or rejection of all final deliverables within thirty (30) calendar days, or as specified in individual task order. Absent written notification, for periods exceeding thirty (30) days, it is the responsibility of the contractors to confirm receipt and acceptance of the deliverable(s). All notifications of rejection will be accompanied with an explanation of the specific deficiencies causing the rejection.

# 11 TASK ORDER ADMINISTRATION DATA

## 11.1 Place of Performance

The principal place of performance shall be at the Contractors' provided work site. The Contractors' facility shall be in close proximity to the USCIS facility at 111 Massachusetts Ave NW, Washington D.C., not to exceed a distance of 15 miles. Meetings will usually take place at USCIS offices in the Washington, D.C. Metropolitan Area, including, but not limited to 20 Massachusetts Avenue, N.W., and 111 Massachusetts Avenue, N.W., Washington DC. Meetings may also occur at the Contractor's work site, especially when close collaboration between stakeholders and the development team is needed. The Contractors shall provide workspace, such as a team room, to accommodate up to five Government representatives per portfolio. Further, the Contractors should provide workspace to accommodate one USCIS IV&V/continuous integration tester Contractor per development team. The Contractors shall provide meeting space for periodic hosting of meetings with both USCIS federal and Contractor personnel.

Because significant collaboration amongst Federal and multiple-vendor teams is required telecommuting is generally discouraged. However, in extenuating circumstances, such as inclement weather, when the Office of Personnel Management (OPM) changes the federal Operating Status in the National Capital Region Contractors are permitted to allow their employees to telework based on the Contractors' telework guidance. Notice shall be given to the COR.

## 11.2 Hours of Operation

Normal duty hours for the Government are from 8am to 5pm, Monday through Friday, excluding Federal Government holidays. The Contractors shall be available during this time period. Deployments almost always occur on the weekends, and the Contractors shall be available to support these. The Government encourages the Contractors to manage the hours in which staff operates so that service is provided when required.

## 11.3 Government Furnished Property (GFP)

Only GFP laptops and Virtual Private Network (VPN) tokens will be issued and used in performing work on this contract. No personal or company owned storage devices, (thumb drives, DVDs, or CDs) will be used with the GFP. A webinar account, such as AT&T Connect, will be provided to the contractor to facilitate virtual demos and other meetings with stakeholders at various physical locations. Handheld devices may be provided as identified by the COR or Government Program Manager if the parties mutually agree and those devices are added to the table in the Government-Furnished Equipment clause.

## 11.4 Travel

Government directed travel within the local commuting area will not be reimbursed. For the purpose of this Task Order the local commuting area is defined as a fifty (50) mile radius from USCIS offices located at 111 Massachusetts Ave NW, Washington D.C.

If the Government specifically and in writing requires the Contractor to travel during the period of this task order to location more than fifty (50) miles from any of the locations listed in Section 11.1 above for the convenience of the Government, costs for transportation, lodging, meals, and incidental expenses incurred by the Contractor will be treated as a direct reimbursable under this the Task Order's Travel CLIN amenable to paragraph H.6.1 of the EAGLE II contract..

## 11.5 Backup Documentation for Invoices

The invoice shall include backup documentation in a format supplied by the Government. The Resource Expenditure Report and its associated Resource Expenditure Format constitute the invoice backup data that the Government requires. The invoice's Resource Expenditure Report shall follow the format provided in *Figure 1: Resources expenditure Report.* The Contractors shall provide this in MS Excel format. A description of the data items in the report are provided in *Table 6: Resource Expenditure Format.* The report data shall represent the labor resources billed in the invoice. In other words, the amount billed shall be consistent with the resource expenditures documented for that reporting period. The Resource Expenditure Report reporting period shall be consistent with the invoice's.

The Resource Expenditure Report requires three types of performance data:

- Aggregate Performance Data. Section 7 of the report requires cost and level of effort data about each of the CLINs. The Portfolio CLINs are further described by the cost and level of effort of each team in the CLIN or portfolio. Each team is further detailed with the cost and level of effort of the individuals that make up the team. The individuals shall be identified by both names and roles.
- IUS Performance Data. Section 8 of the report requires cost and level of effort data about each of the applications/system releases that the Contractors work on. The releases are categorized by portfolio, applications/system, release number, and sprint. Each sprint is further detailed with the cost and level of effort of the individuals that make up the sprint team. The individuals shall be identified by both names and roles.
- Split Team Performance Data. Section 9 of the report requires cost and level of effort data about each of the applications/system in a team only when a given team supports more than one application/system. This is needed to track cost and level of effort on an application by application basis.

| Item No. | Item | Description |
|---|---|---|
| 1 | Contractor | Enter the Contractor's company name in (a) and the Contractor's location of record (for the contract) address and mailing location in (b) |
| 2 | Contract | Enter the contract name in (a), the contract number in (b), and the contract type, such as T&M (c) |
| 3 | Contract Period | Enter the contract period of performance start and end dates |
| 4 | Reporting Period | Enter the start and end dates for the period covering the report, the reporting period shall be consistent with the invoice's |
| 5a | Negotiated Cost | The dollar value (excluding fee or profit unless Firm Fixed Price) on which the contractual agreement has been reached as of the cutoff date of the report. Amounts for changes shall not be included in this item until they have been priced and incorporated in the contract through contract change order or supplemental agreement. |

| | | |
|---|---|---|
| 5b | Estimated Cost of Authorized Unpriced Work | The amount (excluding fee or profit) estimated for that work for which written authorization has been received, but for which definitized contract prices have not been incorporated in the contract through contract change order or supplemental agreement. |
| 5c | Estimated Price | Based on the most likely estimate of cost at completion for all authorized contract work and the appropriate profit/fee, incentive, and cost sharing provisions. Enter the estimated final contract price (total estimated cost to the Government). This number shall be based on the most likely management estimate at complete and normally will change whenever the management estimate or the contract is revised. This does not include Authorized Unpriced Work as referenced above. |
| 5d | Contract Ceiling | Contract ceiling price applicable to the definitized effort as incorporated in the current contract including authorized change orders or supplemental agreements. |
| 5e | Estimated Contract Ceiling | The estimated ceiling price applicable to all authorized contract effort including both definitized and undefinitized effort. |
| 5f | Contract Budget Base | Enter the total of negotiated cost (5.a) and estimated cost of authorized, unpriced work (5.b). |
| 6 | Authorized Contractor Representative | Enter the name of the authorized person (program manager or designee) signing the report in (a), enter that person's title in (b), and enter the date signed in (d). The authorized person shall sign in (c). Electronic signatures are encouraged. |
| 7(1) | Item | Create rows and sub-rows of data that represent the following items in nested order:<br><br>Program Management – All data in this row will reflect planned and actual costs of this CLIN on a monthly basis.<br><br>Portfolio – The name of the portfolio. All data in this row will be a roll-up of all costs and hours associated with this portfolio.<br><br>Team X - All data in this row will reflect planned and actual costs and actual hours of each team assigned to this portfolio, as well as the T&M costs and hours of each T&M resource assigned to this portfolio.<br><br>Resource X – All data in this row will reflect planned and actual costs and actual hours of each resource (name and role) assigned to this Team. |
| 7(2) | Current Period Planned Cost | For the reporting time period, indicate the planned cost of all resources used. |
| 7(3) | Current Period Actual Cost | For the reporting time period, indicate the actual costs of all resources used. Actual costs shall represent what is billed to the various CLINs. |
| 7(4) | Current Period Actual Hours | For the reporting time period, indicate the actual hours expended for all resources used. |
| 7(5) | Cumulative Planned Cost | For the contract time period, indicate the cumulative cost of budgeted resources from the start of the contract to the end of the reporting period. |

| | | |
|---|---|---|
| 7(6) | Cumulative Actual Cost | For the contract time period, indicate the cumulative actual costs of all resources used. |
| 7(7) | Cumulative Actual Hours | For the reporting time period, indicate the cumulative actual hours expended for all resources used. |
| 7(8) | Contract at Completion Planned Cost | Enter the planned cost at completion for the items listed in Column (1). This entry shall consist of the sum of the original budgets. |
| 7(9) | Contract at Completion Estimated Cost | Enter the latest revised estimate of cost at completion including estimated overrun/underrun for all authorized work. |
| 7(10) | Contract at Completion Variance | Enter the difference between the Budgeted - At Completion in Column 7(8) and the Estimated – At Completion in Column 7(9). |
| 7(11) | Contract at Completion Planned Hours | Enter the planned hours at completion for the items listed in Column (1). This entry shall consist of the sum of the original budgets. |
| 7(12) | Contract at Completion Estimated Hours | Enter the latest revised estimate of hours at completion including estimated overrun/underrun for all authorized work. |
| 7(13) | Contract at Completion Variance | Enter the difference between the Budgeted - At Completion in Column 7(11) and the Estimated – At Completion in Column 7(12). |
| 7.a | Total | Enter the sum of the planned cost, actual costs, actual hours, and variances. |
| 8(1) | Item | Create rows and sub-rows of data that represent the following items in nested order:<br>Portfolio – The name of the portfolio. All data in this row will be a roll-up of all costs and hours associated with this portfolio.<br>Application - The name of each of the applications the Contractor supports, such as "ELIS". All data in this row will be a roll-up of all costs and hours associated with this application.<br>Release - The nomenclature of each of the releases the Contractor supports that is associated with the named application, such as "A2.1". All data in this row will be a roll-up of all costs and hours associated with this release.<br>Iteration - The nomenclature that identifies each of the iterations the Contractor is supporting as part of the named release, such as "Sprint 4", "Sprint 5", etc. All data in these rows will be a roll-up of all costs and hours associated with the named iteration.<br>Individual – The names of all of the individuals who charged or planning to charge to the contract during the named sprint, followed by their labor category, and agile team designation, such as "Sean O'Rally /Functional Analyst/Team A". All data in these rows |

| | | |
|---|---|---|
| | | will be itemized costs and hours associated with the named resources for the given iteration. Resources may be placed in planning packages for future releases and iterations that have yet to be identified during the contract period of performance. |
| 8(2) | Current Period Planned Cost | For the reporting time period, indicate the planned cost of resources used. |
| 8(3) | Current Period Actual Cost | For the reporting time period, indicate the actual costs of resources used. |
| 8(4) | Current Period Actual Hours | For the reporting time period, indicate the actual hours expended for resources used. |
| 8(5) | Cumulative Planned Cost | For the contract time period, indicate the cumulative cost of budgeted resources from the start of the contract to the end of the reporting period. |
| 8(6) | Cumulative Actual Cost | For the contract time period, indicate the cumulative actual costs of all resources used. |
| 8(7) | Cumulative Actual Hours | For the reporting time period, indicate the cumulative actual hours expended for all resources used. |
| For each month of the contract Period of Performance, indicate the Planned Cost 7 and 8 (14), Actual Cost 7 and 8 (15), and Actual Hours 7 and 8 (16). Repeat for each month. | | |
| 7 and 8 (14) | Month *x* Planned Cost | The data in Column (14) is maintained for each month during the contract period of performance. |
| 7 and 8 (15) | Month *x* Actual Cost | The data in Column (15) is maintained for each month during the contract period of performance. For the month represented, indicate the actual costs of all resources used. |
| 7 and 8 (16) | Month *x* Actual Hours | The data in Column (16) is maintained for each month during the contract period of performance. For the month represented, indicate the actual hours expended of all resources used. |
| 8 (17) | Fiscal Year and Quarter Budgeted Cost | For the Government fiscal year (Oct 1 to Sept 30) and for each of the 4 quarters in the fiscal year indicate the cumulative (sum) cost of budgeted resources. This will be cumulative costs of the relevant monthly costs (Column 14) in the fiscal year and the fiscal quarters that fall within the contract period of performance. If the contract period of performance ends prior to the conclusion of a fiscal year (Sept. 30), then the Contractor shall estimate all of the available months within the fiscal year, recognizing that no work is scheduled to be performed during some of those months. |
| 8 (18) | Fiscal Year and Quarter Actual Cost | For the fiscal year and for each of the 4 quarters in the fiscal year, indicate the cumulative actual cost of resources. This will be cumulative (sum) costs of the relevant monthly costs (Column 15) in the fiscal year and the fiscal quarters that fall within the contract period of performance. If the contract period of performance ends prior to the conclusion of a fiscal year (Sept. 30), then the Contractor shall estimate all of the available months within the fiscal year, recognizing that no |

| | | |
|---|---|---|
| | | work is scheduled to be performed during some of those months. |
| 8.a | Total | Enter the sum of the planned cost, actual costs, and actual hours. |
| 9 (1) | Item | Create rows and sub-rows of data that represent the following items in nested order:<br>Portfolio – The name of the portfolio.<br>Team X - All data in this row will reflect actual costs and actual hours of the team assigned to this portfolio, when a team supports more than one application. All data in this row will be a roll-up of all costs and hours associated with this team.<br>Application - The name of each of the applications the Contractor supports, such as "CPMS". All data in this row will reflect actual costs and actual hours that the team expended in support of the application. |
| 9(2) | Current Period Actual Cost | For the reporting time period, indicate the actual costs of resources used. |
| 9(3) | Current Period Actual Hours | For the reporting time period, indicate the actual hours expended for resources used. |
| 9(4) | Cumulative Actual Cost | For the contract time period, indicate the cumulative actual costs of resources used. |
| 9(5) | Cumulative Actual Hours | For the reporting time period, indicate the cumulative actual hours expended for resources used. |
| 9(6) | Month *x* Actual Cost | The data in Column (6) is maintained for each month during the contract period of performance. For the month represented, indicate the actual costs of resources used. |
| 9(7) | Month *x* Actual Hours | The data in Column (7) is maintained for each month during the contract period of performance. For the month represented, indicate the actual hours expended of resources used. |

**Table 5: Resource Expenditure Format**

| RESOURCE EXPENDITURE REPORT | | | |
|---|---|---|---|
| DOLLARS IN _____ | | | |
| 1. CONTRACTOR | 2. CONTRACT | 3. CONTRACT PERIOD | 5. CONTRACT COST DATA |
| a. NAME | a. NAME | (YYYYMMDD)<br>a. FROM | a. NEGOTIATED COST |
| b. LOCATION (Address and ZIP Code) | b. NUMBER | b. TO<br>4. REPORTING PERIOD | b. EST COST OF AUTHORIZED UNPRICED WOR |
| | c. TYPE | a. FROM<br>b. TO | c. ESTIMATED PRICE |
| 6. AUTHORIZED CONTRACTOR REPRESENTATIVE | | | d. CONTRACT CEILING |
| a. NAME (Last, First, Middle Initial) | b. TITLE | | e. ESTIMATED CONTRACT CEILING |
| c. SIGNATURE | d. DATE<br>(YYYYMMDD) | | f. CONTRACT BUDGET BASE |

7. AGGREGATE PERFORMANCE DATA

| ITEM | CURRENT PERIOD | | | CUMULATIVE TO DATE | | | CONTRACT AT COMPLETION/COST | | | CONTRACT AT COMPLETION/HOURS | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| (1) | PLANNED COST (2) | ACTUAL COST (3) | ACTUAL HOURS (4) | PLANNED COST (5) | ACTUAL COST (6) | ACTUAL HOURS (7) | PLANNED COST (8) | ESTIMATED COST (9) | CONTRACT AT COMPLETE VARIANCE (10) | PLANNED HOURS (11) | ESTIMATED HOURS (12) | CONTRACT AT COMPLETE VARIANCE (13) |
| **Program Management** | | | N/A | | | N/A | | | | N/A | N/A | N/A |
| **Benefits and Biometrics** | | | | | | | | | | | | |
| Team A | | | | | | | | | | | | |
| Team B | | | | | | | | | | | | |
| Team C | | | | | | | | | | | | |
| Specialty Engineering | | | | | | | | | | | | |
| ISSO | | | | | | | | | | | | |
| UI Designer/User Experience | | | | | | | | | | | | |
| **Customer Service** | | | | | | | | | | | | |
| Team A | | | | | | | | | | | | |
| Team B | | | | | | | | | | | | |
| Team C | | | | | | | | | | | | |
| Surge Team 1 | | | | | | | | | | | | |
| **Records** | | | | | | | | | | | | |
| Team A | | | | | | | | | | | | |
| Team B | | | | | | | | | | | | |
| Team C | | | | | | | | | | | | |
| T&M John Smith | | | | | | | | | | | | |
| T&M Jane Doe | | | | | | | | | | | | |
| 7 a. TOTAL | | | | | | | | | | | | |

| Aug-12 | | | Sep-12 | | | Oct-12 | | | Nov-12 | | | Dec-12 | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| PLANNED COST (14) | ACTUAL COST (15) | ACTUAL HOURS (16) | PLANNED COST (14) | ACTUAL COST (15) | ACTUAL HOURS (16) | PLANNED COST (14) | ACTUAL COST (15) | ACTUAL HOURS (16) | PLANNED COST (14) | ACTUAL COST (15) | ACTUAL HOURS (16) | PLANNED COST (14) | ACTUAL COST (15) | ACTUAL HOURS (16) |
| | | N/A | | | N/A | | | N/A | | | N/A | | | N/A |
| | | N/A | | | N/A | | | N/A | | | N/A | | | N/A |
| | | | | | | | | | | | | | | |

8. IUS PERFORMANCE DATA

| ITEM (1) | CURRENT PERIOD PLANNED COST (2) | CURRENT PERIOD ACTUAL COST (3) | CURRENT PERIOD ACTUAL HOURS (4) | CUMULATIVE TO DATE PLANNED COST (5) | CUMULATIVE TO DATE ACTUAL COST (6) | CUMULATIVE TO DATE ACTUAL HOURS (7) | Aug-12 PLANNED COST (14) | Aug-12 ACTUAL COST (15) | Aug-12 ACTUAL HOURS (16) | Sep-12 PLANNED COST (14) | Sep-12 ACTUAL COST (15) | Sep-12 ACTUAL HOURS (16) | FISCAL YEAR 2012 PLANNED COST (17) | FISCAL YEAR 2012 ACTUAL COST (18) |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Benefits and Biometrics Portfolio | 38 | | | | | | | | | | | | | |
| CLAIMS 4 (example) | 28 | | | | | | | | | | | | | |
| Release 3C | 12 | | | | | | | | | | | | | |
| Sprint 0 | 2 | | | | | | | | | | | | | |
| Sprint 1 | 2 | | | | | | | | | | | | | |
| Sprint 2 | 4 | | | | | | | | | | | | | |
| Sprint 3 | 4 | | | | | | | | | | | | | |
| John Smyth/Functional Analyst/Team A | 1 | | | | | | | | | | | | | |
| Jon Smith/Sr. Developer/Team A | 1 | | | | | | | | | | | | | |
| Jaine Doe/S/W Tester/Team A | 1 | | | | | | | | | | | | | |
| Jain Doe/Config Manager/T&M | 1 | | | | | | | | | | | | | |
| Release 3D | 20 | | | | | | | | | | | | | |
| Sprint 0 | 4 | | | | | | | | | | | | | |
| Sprint 1 | 4 | | | | | | | | | | | | | |
| Sprint 2 | 4 | | | | | | | | | | | | | |
| Sprint 3 | 4 | | | | | | | | | | | | | |
| Sprint 4 | 4 | | | | | | | | | | | | | |
| CPMS | 10 | | | | | | | | | | | | | |
| 8.a. TOTAL | | | | | | | | | | | | | | |

| Oct-12 PLANNED COST (14) | Oct-12 ACTUAL COST (15) | Oct-12 ACTUAL HOURS (16) | Nov-12 PLANNED COST (14) | Nov-12 ACTUAL COST (15) | Nov-12 ACTUAL HOURS (16) | Dec-12 PLANNED COST (14) | Dec-12 ACTUAL COST (15) | Dec-12 ACTUAL HOURS (16) | FY 2013 QUARTER 1 PLANNED COST (17) | FY 2013 QUARTER 1 ACTUAL COST (18) | FISCAL YEAR 2013 PLANNED COST (17) | FISCAL YEAR 2013 ACTUAL COST (18) |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | | | | |

9. SPLIT TEAM PERFORMANCE DATA

| ITEM (1) | CURRENT PERIOD ACTUAL COST (2) | CURRENT PERIOD ACTUAL HOURS (3) | CUMULATIVE TO DATE ACTUAL COST (4) | CUMULATIVE TO DATE ACTUAL HOURS (5) | Aug-12 ACTUAL COST (6) | Aug-12 ACTUAL HOURS (7) | Sep-12 ACTUAL COST (6) | Sep-12 ACTUAL HOURS (7) | Oct-12 ACTUAL COST (6) | Oct-12 ACTUAL HOURS (7) | Nov-12 ACTUAL COST (6) | Nov-12 ACTUAL HOURS (7) |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Benefits and Biometrics | | | | | | | | | | | | |
| Team A | | | | | | | | | | | | |
| APSS | | | | | | | | | | | | |
| C3 MF | | | | | | | | | | | | |
| FD258 MF | | | | | | | | | | | | |
| RAPS | | | | | | | | | | | | |
| Team B | | | | | | | | | | | | |
| BBSS | | | | | | | | | | | | |
| CPMS | | | | | | | | | | | | |
| 9.a. TOTAL | | | | | | | | | | | | |

**Figure 1: Sample Resource Expenditure Reports (Contractor will tailor to fit the task order)**

# 12 Optional Contract Line Item Numbers (CLIN)

The optional Contract Line Item Numbers (CLIN) in this PWS are of two types: Firm Fixed Price (FFP) and Time and Materials (T&M). The purpose of the CLINs is to have the option to scale services upwards in order to meet unanticipated demand. Unanticipated demand may be of one or more of the following type:

- Additional JETS team(s) to support applications named in this PWS because the services required outweigh the current capacity specified in the PWS.
- Additional JETS team(s) to support applications not named in this PWS but require transition to the JETS scope so that sustainment activities may be performed.
- Additional JETS team(s) to support applications not named in this PWS but require creation using agile methodologies and quick turn-around to production, with continued development and sustainment activities performed by JETS teams.

The Contractors shall pre-price the optional CLINs based on teams of ten and 1860 hours of labor per team member per year. If the Government chooses to exercise an optional CLIN, the technology stack that will apply to the CLIN will be provided to the Contractors so that the appropriate skills can be staffed. The T&M surge CLINS may be exercised from time to time up to the Not to Exceed (NTE) amount and are intended to be used to acquire any labor category available in the EAGLE II contract for work with the general scope of the task order but above and beyond the services acquired by the CLINS for teams. The T&M CLINs shall be used to perform functions in *Section 5, TEAM TASKS* or *Section 6, SPECIALTY ENGINEERING,* and can be used for work on weekends for deployments and other temporary surges. Resources applied to the T&M CLIN can be de-scoped at the Government's discretion or rolled onto another FFP team (either optional CLIN or not) if a level of effort and skills deficit warrants the transfer. Such a transfer requires prior approval of the COR and Contracting Officer.

# Performance Work Statement

## Appendix D

# Biometrics Portfolio

---

## 1. WORK REQUIREMENT

The JETS contractor shall provide **4.5 teams, with 4 made up of 10 persons and 1 made up of 5 persons (Team A: BBSS and FD-258 MF),** who are able to perform the tasks as described in Performance Work Statement (PWS) *Section 5 TEAM TASKS,* while conforming to the expectations outlined in the PWS and with expert level ability in the technologies stated in *Appendix D Section 2 TECHNICAL LANDSCAPE.* Members of these teams shall support the JETS Biometrics Portfolio. The technical landscape may change in the course of performing the tasks outlined in this PWS. As applications evolve, so must the technical expertise of the teams' makeup. Applications may be decommissioned, and if so, it is expected that the associated teams shall transition to support different applications (either existing applications within this portfolio or new applications transitioned onto this portfolio). The Contractor may be required to reorganize teams in order to support different applications and portfolio needs.

The contractor shall provide agile teams that perform code maintenance and operational maintenance. Descriptions of these tasks are provided in PWS *Section 5*. In order to plan the team make up, estimates of the proportion of effort each task is likely to consume is provided in *Table B-1: Estimated Proportion of Work* and definition of the code base the teams must have knowledge of are summarized in *Table B-2: Team Structure by Competency*. Further descriptions of technical competences are included in the application descriptions in this appendix. Note that this is only an estimate based on averages of previous work. Actual work will vary depending on the nature of the user stories and priorities assigned. Each member of the contractor's team shall provide **1860 hours** of effort each 12 month period of performance. In other words, each team of ten shall be able to provide 18,600 hours of service per year. Effort will be expressed in terms of user stories and efficiency of teams shall be measured.

Based on past experience, there is not a one-to-one match between the work an application consumes and a team of 10 persons. It is expected, however, that the JETS Biometrics teams shall primarily support assigned applications as noted in *Table B-1: Estimated Proportion of Work*. The contractor's teams shall be versed in multiple technologies. It is also expected that if a surge in capacity is necessary, but likely to be temporary, teams may be assigned backlog items for applications that they do not normally support.

| Application | Code Maint-enance | Operational Maint-enance | Total | Persons | Proportion of Total Work | JETS Team |
|---|---|---|---|---|---|---|
| BBSS | 3,720 | 1,860 | **5,580** | 3 | 7% | A |
| CPMS | 33,480 | 3,720 | **37,200** | 20 | 49% | B, C |
| FD-258 MF | 930 | 930 | **1,860** | 1 | 2% | A |
| NASS | 27,900 | 3,720 | **31,620** | 17 | 42% | D, E |
| **Total** | **66,030** | **10,230** | **76,260** | **41** | 100.00% | |
| **Proportion of total hours** | 87% | 13% | 100% | | | |

Table B-1: Estimated Proportion of Work

| Team | Microsoft VB/.NET | Mainframe/ Cobol | JAVA | Oracle | JavaScript | MS SQL Server |
|---|---|---|---|---|---|---|
| A | X | X | | | X | X |
| B, C | X | | | X | | |
| D, E | | | X | X | | |

Table B-2: Team Structure by Competency

It is presumed that the contractor shall require program management and support activities in order to perform on this PWS. Those resources are at the contractor's discretion and are in addition to the agile teams and specialty engineers described in PWS *Section 5 TEAM TASKS* and *Section 6 SPECIALTY ENGINEERING TASKS.*

## 2. Technical Landscape

The JETS Biometrics Portfolio includes the following legacy applications:

- BBSS
- CPMS
- FD-258 MF
- National Scheduler (NASS)

Each of the legacy Biometrics Portfolio applications is different. A description of the existing landscape for each application is described in the sections below. The contractor shall accomplish the tasks in PWS *Section 5 TEAM TASKS* and *Section 6 SPECIALTY ENGINEERING TASKS* with team members who have expertise in the technologies and tools described herein. Technologies, tools, data center locations, interfaces, and the state of the application are not static and the data in this section is meant to provide illustrative and planning information relative to the start of the contract. Any or all of these elements may evolve during the course of the contract's period of performance in order to adapt to changing contexts.

The Technical Landscape also includes a description of the operational maintenance tasks associated with system, application, and database administration.

## 2.1 Biometrics Benefits Support System (BBSS)

The Biometrics program consists of a group of systems responsible for the capture and storage of biometric information of USCIS applicants. These systems support background investigation, case adjudication, card production, and identity verification activities in USCIS and other agencies.

BBSS receives transactions from the Livescan devices at each ASC, Service Center, and International Mobiles, and then routes the transactions based on the biometrics collected. Ten-print transactions are sent to the FBI for background checks and the results are stored. Photos, press-prints, and signatures are sent to the C3/C4 BRUs and eventually used for card production.

| Biometrics Benefits Support System (BBSS) | | | | |
|---|---|---|---|---|
| COTS | N/A | | | |
| Code Base | - Web pages based on HTML with VBScript and JavaScript<br>- IIS (ASP), VB 6.0 , SMTP<br>- SQL Server 2008<br>- VB 6.0, VBA, ASP, VBScript and JavaScript | | | |
| Interfaces | ESB, FBI, Claims 3, Claims 4, CPMS, SNAP (soon to be decommissioned) | | | |
| Development and Test Environments | Virtual servers at the TECC running Windows Server supporting application in a 3-tier configuration | | | |
| Production Environment | Virtual servers at the TECC running Windows Server supporting application in a 3-tier configuration | | | |
| Development Tools and Functions | VB 6.0, VBA, ASP, VBScript, JavaScript, SQL Server | | | |
| Section 508 Compliance | No | | | |
| W7 and IE9 Compliance | Yes | | | |
| Security/ATO Expiration | 8/20/14 | | | |
| Production Write Access | | **Task** | **Frequency** | **Description** |
| | Systems Admin | Modify Registry | As required | Make registry modifications to support application release in Service Centers. |
| | | Modify Windows and application configuration | As required | Make Windows and application configuration file modifications for application releases, troubleshooting system issues/outages in Service Centers. Access registry, Windows, and administrative tools supporting application and |

| | | | | |
|---|---|---|---|---|
| | | | | environment troubleshooting; modification of host file entries and registry entries are required to support the continued operation of EASS as a store-and-forward system. |
| | Application & Dev. Admin | Support software releases | As required | Support software release with modifications to data, procedures, and view of database in Service Centers. |
| | | Access database and network share | As required | Support fingerprint resubmissions and biometric cloning and transfers in Service Centers. |
| | | Access database | As required | Support transaction edit/repair process in Service Centers. |

## 2.2 Customer Profile Management System (CPMS)

CPMS is the planned repository of all biometric data in United States Citizenship and Immigration Services (USCIS). The primary function of CPMS is to provide the USCIS with the capability to store and reuse biometric images and biographic information and provide access to background check responses from the FBI, DOD, and DHS.

| Customer Profile Management System (CPMS) | |
|---|---|
| COTS | N/A |
| Code Base | Software is developed and maintained using the Oracle relational database system, ASP.NET, utilizing Aware software to render fingerprints. |
| Interfaces | ESB, BBSS, FBI, IDENT, NASS, SMART /eCISCOR |
| Development and Test Environments | Data Center 1 (DC1), Virtual Server 3 tier environment on Windows 2008 server with an Oracle 11g RAC database |
| Production Environment | Data Center 1 (DC1), Virtual Server 3 tier environment on Windows 2008 server with an Oracle 11g RAC database |
| Development Tools and Functions | ASP.NET, Oracle PL/SQL, utilizing a Service Oriented Architecture |
| Section 508 Compliance | Yes |
| W7 and IE9 Compliance | Yes |
| Security/ATO Expiration | 10/31/2014 |

## 2.3 FD-258 MF

The FD 258 Mainframe (FD 258 MF) Fingerprint Tracking System was established to meet the need of the Department of Homeland Security (DHS) to track fingerprint information, to and from, the Federal Bureau of Investigation (FBI). FD 258 MF maintains information on individual applicants fingerprint status. Each record contains applicant information that was sent to the FBI, such as name, birth date and other genetic biometric/biological data, as well as date fingerprinted and date sent to FBI. The records also contain information received from the FBI such as, FBI process date, FBI search result and other information. FD 258 MF processes about 7,000 "send" record transactions per day and about 7,000 "response" record transactions per day. Historical transactional numbers are subject to change.

FD 258 MF has two primary components: an online data inquiry system, and a system of batch runs. The batch system accepts and processes data from the Next Generation Information System via the FD 258 Enterprise Edition system, as well as produces reports and provides interfaces with other systems.

The FD 258 MF was created in order to:

- Effectively serve the adjudication needs of USCIS personnel tracking applicant fingerprint status and results.
- Effectively serve the management needs of USCIS Headquarters personnel concerned with database statistical information.
- Provide the capability of satisfying the DHS National Quality Procedures (NQP) via Control Number display.
- Provide daily reports to USCIS field office personnel via Remote Online Print Executive System (ROPES), on all daily database activity

| FD-258 | |
|---|---|
| COTS | N/A |
| Code Base | COBOL, ADSO |
| Interfaces | ESB, FBI, C4, C3MF, RAPS |
| Development and Test Environments | DC1 - IDMS / COBOL copy tailored to support Development testing. |
| Production Environment | – FD258 operates on a hierarchical database run on an IBM Z/OS host computer that resides at the DHS Data Center 1. It is operational seven days a week, approximately 23 1/2 hours a day. Routine maintenance may periodically result in a brief period of unavailability. Typically, this maintenance occurs during off-peak periods.<br>– The FD258 development team has access to the production environment to create, modify and delete Mainframe flat files with production data, to execute the jobs that update the FD258 database and to maintain database records and indices. Access is in a support and maintenance capacity only. The FD258 development team has access to the production environment to create, modify and delete Mainframe flat files with production data, to execute the jobs that update the FD258 database and to maintain database records and indices. Access is in a support and maintenance capacity only. |
| Development Tools and Functions | ENDEVOR, TSO, IBM COMPILER, IDMS, INSYNC |

| | | | | |
|---|---|---|---|---|
| Section 508 Compliance | N/A | | | |
| W7 and IE9 Compliance | N/A | | | |
| Security/ATO Expiration | 9/23/2014 | | | |
| Production Write Access | | **Task** | **Frequency** | **Description** |
| | Application & Dev. Admin | | As required | Restart failed jobs and submit jobs that require manual updates to input parameters to run the job, including running/restarting manual interfaces to other systems. |
| | | Maintain datasets and JCL | | |

## 2.4 National Appointment Scheduling System (NASS)

The National Appointment Scheduling System (NASS) will provide USCIS with a centralized, scalable national appointment scheduling system replacing the following scheduling systems: Scheduling and Notification for Applications for Processing (SNAP), CLAIMS 4 Scheduling Component, Adjustment of Status (AOS) Scheduler component, Scheduler component of CLAIMS 3, InfoPass, Site Profile System (SPS), and Refugee Asylum and Parole System (RAPS) Scheduler. NASS shall include, but not be limited to the following capabilities:

- Enable USCIS to manage/allocate resources and manage nationwide appointment demands
- Allow a multiple channel approach to scheduling appointments such as the internet, phones and batch scheduling
- Allow customers to schedule and reschedule specified appointment types
- Provide USCIS users the ability to manage scheduling and rescheduling of specific appointment types
- Provide appointment scheduling services to other USCIS applications including ELIS and legacy applications leveraging ESB.
- Manage capabilities and biometric reuse logic.

| National Appointment Scheduling System (NASS) | |
|---|---|
| COTS | N/A |
| Code Base | JAVA, Spring Toolset, Oracle 11g |
| Interfaces | CPMS, ESB, ELIS2, EPMS, ICAM |
| Development and | DC1 Cloud |

| | | | | |
|---|---|---|---|---|
| **Test Environments** | | | | |
| **Production Environment** | DC1 Cloud | | | |
| **Development Tools and Functions** | Java, Spring Toolset, Oracle 11g, Jenkins, subversion | | | |
| **Section 508 Compliance** | Yes | | | |
| **W7 and IE9 Compliance** | Yes | | | |
| **Security/ATO Expiration** | 4/10/2017 | | | |
| **Production Write Access** | | **Task** | **Frequency** | **Description** |
| | Systems Admin | N/A | N/A | N/A |
| | Application & Dev. Admin | N/A | N/A | N/A |

# SECURITY REQUIREMENTS

**GENERAL**

U.S. Citizenship and Immigration Services (USCIS) has determined that performance of this contract requires that the Contractor, subcontractor(s), vendor(s), etc. (herein known as Contractor), requires access to sensitive but unclassified information, and that the Contractor will adhere to the following.

**SUITABILITY DETERMINATION**

USCIS shall have and exercise full control over granting, denying, withholding or terminating access of unescorted Contractor employees to government facilities and/or access of Contractor employees to sensitive but unclassified information based upon the results of a background investigation. USCIS may, as it deems appropriate, authorize and make a favorable entry on duty (EOD) decision based on preliminary security checks. The favorable EOD decision would allow the employees to commence work temporarily prior to the completion of the full investigation. The granting of a favorable EOD decision shall not be considered as assurance that a full employment suitability authorization will follow as a result thereof. The granting of a favorable EOD decision or a full employment suitability determination shall in no way prevent, preclude, or bar the withdrawal or termination of any such access by USCIS, at any time during the term of the contract. No Contractor employee shall be allowed unescorted access to a Government facility without a favorable EOD decision or suitability determination by the Office of Security & Integrity Personnel Security Division (OSI PSD).

**BACKGROUND INVESTIGATIONS**

Contractor employees (to include applicants, temporaries, part-time and replacement employees) under the contract, needing access to sensitive but unclassified information shall undergo a position sensitivity analysis based on the duties each individual will perform on the contract as outlined in the Position Designation Determination (PDD) for Contractor Personnel. The results of the position sensitivity analysis shall identify the appropriate background investigation to be conducted. All background investigations will be processed through OSI PSD.

To the extent the Position Designation Determination form reveals that the Contractor will not require access to sensitive but unclassified information or access to USCIS IT systems, OSI PSD may determine that preliminary security screening and or a complete background investigation is not required for performance on this contract.

Completed packages must be submitted to OSI PSD for prospective Contractor employees no less than 30 days before the starting date of the contract or 30 days prior to EOD of any employees, whether a replacement, addition, subcontractor employee, or vendor. The Contractor shall follow guidelines for package submission as set forth by OSI PSD. A complete package will include the following forms, in conjunction with security questionnaire submission of the SF-85P, "Security Questionnaire for Public Trust Positions" via e-QIP:

1. DHS Form 11000-6, "Conditional Access to Sensitive But Unclassified Information Non-Disclosure Agreement"
2. FD Form 258, "Fingerprint Card" **(2 copies)**
3. Form DHS 11000-9, "Disclosure and Authorization Pertaining to Consumer Reports Pursuant to the Fair Credit Reporting Act"
4. Position Designation Determination for Contract Personnel Form
5. Foreign National Relatives or Associates Statement
6. OF 306, Declaration for Federal Employment (approved use for Federal Contract Employment)
7. ER-856, "Contract Employee Code Sheet"

**EMPLOYMENT ELIGIBILITY**

Be advised that unless an applicant requiring access to sensitive but unclassified information has resided in the U.S. for three of the past five years, OSI PSD may not be able to complete a satisfactory background investigation. In such cases, USCIS retains the right to deem an applicant as ineligible due to insufficient background information.

Only U.S. citizens are eligible for employment on contracts requiring access to Department of Homeland Security (DHS) Information Technology (IT) systems or involvement in the development, operation, management, or maintenance of DHS IT systems, unless a waiver has been granted by the Director of USCIS, or designee, with the concurrence of both the DHS Chief Security Officer and the Chief Information Officer or their designees. In instances where non-IT requirements contained in the contract can be met by using Legal Permanent Residents, those requirements shall be clearly described.

The Contractor must agree that each employee working on this contract will have a Social Security Card issued by the Social Security Administration.

**CONTINUED ELIGIBILITY**

If a prospective employee is found to be ineligible for access to USCIS facilities or information, the Contracting Officer's Representative (COR) will advise the Contractor that the employee shall not continue to work or to be assigned to work under the contract.

In accordance with USCIS policy, contractors are required to undergo a periodic reinvestigation every five years. Security documents will be submitted to OSI PSD within ten business days following notification of a contractor's reinvestigation requirement.

In support of the overall USCIS mission, Contractor employees are required to complete one-time or annual DHS/USCIS mandatory trainings. The Contractor shall certify annually, but no later than December 31st each year, that required trainings have been completed. The certification of the completion of the trainings by all contractors shall be provided to both the COR and Contracting Officer.

- **USCIS Security Awareness Training** (required within 30 days of entry on duty for new contractors, and annually thereafter)
- **USCIS Integrity Training** (Annually)
- **DHS Continuity of Operations Awareness Training** (one-time training for contractors identified as providing an essential service)
- **USCIS Office Safety Training** (one-time training for contractors working within USCIS facilities; contractor companies may substitute their own training)
- **USCIS Fire Prevention and Safety Training** (one-time training for contractors working within USCIS facilities; contractor companies may substitute their own training)

USCIS reserves the right and prerogative to deny and/or restrict the facility and information access of any Contractor employee whose actions are in conflict with the standards of conduct or whom USCIS determines to present a risk of compromising sensitive but unclassified information and/or classified information.

Contract employees will report any adverse information concerning their personal conduct to OSI PSD. The report shall include the contractor's name along with the adverse information being reported. Required reportable adverse information includes, but is not limited to, criminal charges and or arrests, negative change in financial circumstances, and any additional information that requires admission on the SF-85P security questionnaire.

OSI PSD must be notified of all terminations/ resignations within five days of occurrence. The Contractor will return any expired USCIS issued identification cards and HSPD-12 card, or those of terminated employees to the COR. If an identification card or HSPD-12 card is not available to be returned, a report must be submitted to the COR, referencing the card number, name of individual to whom issued, the last known location and disposition of the card.

**SECURITY MANAGEMENT**

The Contractor shall appoint a senior official to act as the Corporate Security Officer. The individual will interface with OSI 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 OSI 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 COTR 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.

The Contractor shall be responsible for all damage or injuries resulting from the acts or omissions of their employees and/or any subcontractor(s) and their employees to include financial responsibility.

## COMPUTER AND TELECOMMUNICATIONS SECURITY REQUIREMENTS

### Security Program Background

The DHS has established a department wide IT security program based on the following Executive Orders (EO), public laws, and national policy:

- Public Law 107-296, Homeland Security Act of 2002.
- Federal Information Security Management Act (FISMA) of 2002, November 25, 2002.
- Public Law 104-106, Clinger-Cohen Act of 1996 [formerly, Information Technology Management Reform Act (ITMRA)], February 10, 1996.
- Privacy Act of 1974, As Amended. 5 United States Code (U.S.C.) 552a, Public Law 93-579, Washington, D.C., July 14, 1987.
- Executive Order 12829, *National Industrial Security Program*, January 6, 1993.
- Executive Order 12958, *Classified National Security Information*, as amended.
- Executive Order 12968, *Access to Classified Information,* August 2, 1995.
- Executive Order 13231, *Critical Infrastructure Protection in the Information Age*, October 16, 2001.• National Industrial Security Program Operating Manual (NISPOM), February 2001.

DHS *Sensitive Systems Policy Publication 4300A* v2.1, July 26, 2004
DHS *National Security Systems Policy Publication 4300B* v2.1, July 26, 2004

- Homeland Security Presidential Directive 7, *Critical Infrastructure Identification, Prioritization, and Protection*, December 17, 2003.
- Office of Management and Budget (OMB) Circular A-130, *Management of Federal Information Resources.*
- National Security Directive (NSD) 42, *National Policy for the Security of National Security Telecommunications and Information Systems* (U), July 5, 1990, CONFIDENTIAL.
- 5 Code of Federal Regulations (CFR) §2635, Office of Government Ethics, *Standards of Ethical Conduct for Employees of the Executive Branch.*
- DHS SCG OS-002 (IT), National Security IT Systems Certification & Accreditation, March 2004.
- Department of State 12 Foreign Affairs Manual (FAM) 600, *Information Security Technology*, June 22, 2000.
- Department of State 12 FAM 500, *Information Security*, October 1, 1999.
- Executive Order 12472, *Assignment of National Security and Emergency Preparedness Telecommunications Functions*, dated April 3, 1984.
- Presidential Decision Directive 67, *Enduring Constitutional Government and Continuity of Government Operations*, dated October 21, 1998.
- FEMA Federal Preparedness Circular 65, *Federal Executive Branch Continuity of Operations (COOP)*, dated July 26, 1999.
- FEMA Federal Preparedness Circular 66, *Test, Training and Exercise (TT&E) for Continuity of Operations (COOP)*, dated April 30, 2001.
- FEMA Federal Preparedness Circular 67, *Acquisition of Alternate Facilities for Continuity of Operations*, dated April 30, 2001.
- Title 36 Code of Federal Regulations 1236, Management of Vital Records, revised as of July 1, 2000.
- National Institute of Standards and Technology (NIST) Special Publications for computer security and FISMA compliance.

## GENERAL

Due to the sensitive nature of USCIS information, the contractor is required to develop and maintain a comprehensive Computer and Telecommunications Security Program to address the integrity, confidentiality, and availability of sensitive but unclassified (SBU) information during collection, storage, transmission, and disposal. The contractor's security program shall adhere to the requirements set forth in the DHS Management Directive 4300 IT Systems Security Pub Volume 1 Part A and DHS Management Directive 4300 IT Systems Security Pub Volume I Part B. This shall include conformance with the DHS Sensitive Systems Handbook, DHS Management Directive 11042 Safeguarding Sensitive but Unclassified (For Official Use Only) Information and other DHS or USCIS guidelines and directives regarding information security requirements. The contractor shall establish a working relationship with the USCIS IT Security Office, headed by the Information Systems Security Program Manager (ISSM).

## IT SYSTEMS SECURITY

In accordance with DHS Management Directive 4300.1 "Information Technology Systems Security", USCIS Contractors shall ensure that all employees with access to USCIS IT Systems are in compliance with the requirement of this Management Directive. Specifically, all contractor employees with access to USCIS IT Systems meet the requirement for successfully completing the annual "Computer Security Awareness Training (CSAT)." All contractor employees are required to complete the training within 60-days from the date of entry on duty (EOD) and are required to complete the training yearly thereafter.

CSAT can be accessed at the following: http://otcd.uscis.dhs.gov/EDvantage.Default.asp or via remote access from a CD which can be obtained by contacting uscisitsecurity@dhs.gov.

## IT SECURITY IN THE SYSTEMS DEVELOPMENT LIFE CYCLE (SDLC)

The USCIS SDLC Manual documents all system activities required for the development, operation, and disposition of IT security systems. Required systems analysis, deliverables, and security activities are identified in the SDLC manual by lifecycle phase. The contractor shall assist the appropriate USCIS ISSO with development and completion of all SDLC activities and deliverables contained in the SDLC. The SDLC is supplemented with information from DHS and USCIS Policies and procedures as well as the National Institute of Standards Special Procedures related to computer security and FISMA compliance. These activities include development of the following documents:

- *Sensitive System Security Plan (SSSP)*: This is the primary reference that describes system sensitivity, criticality, security controls, policies, and procedures. The SSSP shall be based upon the completion of the DHS FIPS 199 workbook to categorize the system of application and completion of the RMS

Questionnaire. The SSSP shall be completed as part of the System or Release Definition Process in the SDLC and shall not be waived or tailored.

- *Privacy Impact Assessment (PIA) and System of Records Notification (SORN).* For each new development activity, each incremental system update, or system recertification, a PIA and SORN shall be evaluated. If the system (or modification) triggers a PIA the contractor shall support the development of PIA and SORN as required. The Privacy Act of 1974 requires the PIA and shall be part of the SDLC process performed at either System or Release Definition.
- *Contingency Plan (CP)*: This plan describes the steps to be taken to ensure that an automated system or facility can be recovered from service disruptions in the event of emergencies and/or disasters. The Contractor shall support annual contingency plan testing and shall provide a Contingency Plan Test Results Report.
- *Security Test and Evaluation (ST&E)*: This document evaluates each security control and countermeasure to verify operation in the manner intended. Test parameters are established based on results of the RA. An ST&E shall be conducted for each Major Application and each General Support System as part of the certification process. The Contractor shall support this process.
- *Risk Assessment (RA):* This document identifies threats and vulnerabilities, assesses the impacts of the threats, evaluates in-place countermeasures, and identifies additional countermeasures necessary to ensure an acceptable level of security. The RA shall be completed after completing the NIST 800-53 evaluation, Contingency Plan Testing, and the ST&E. Identified weakness shall be documented in a Plan of Action and Milestone (POA&M) in the USCIS Trusted Agent FISMA (TAF) tool. Each POA&M entry shall identify the cost of mitigating the weakness and the schedule for mitigating the weakness, as well as a POC for the mitigation efforts.
- *Certification and Accreditation (C&A):* This program establishes the extent to which a particular design and implementation of an automated system and the facilities housing that system meet a specified set of security requirements, based on the RA of security features and other technical requirements (certification), and the management authorization and approval of a system to process sensitive but unclassified information (accreditation). As appropriate the Contractor shall be granted access to the USCIS TAF and Risk Management System (RMS) tools to support C&A and its annual assessment requirements. Annual assessment activities shall include completion of the NIST 800-26 Self Assessment in TAF, annual review of user accounts, and annual review of the FIPS categorization. C&A status shall be reviewed for each incremental system update and a new full C&A process completed when a major system revision is anticipated.

## SECURITY ASSURANCES

DHS Management Directives 4300 requires compliance with standards set forth by NIST, for evaluating computer systems used for processing SBU information. The Contractor shall ensure that requirements are allocated in the functional requirements and system design documents to security requirements are based on the DHS policy, NIST standards

and applicable legislation and regulatory requirements. Systems shall offer the following visible security features:

- *User Identification and Authentication (I&A)* – I&A is the process of telling a system the identity of a subject (for example, a user) (*I*) and providing that the subject is who it claims to be (*A*). Systems shall be designed so that the identity of each user shall be established prior to authorizing system access, each system user shall have his/her own user ID and password, and each user is authenticated before access is permitted. All system and database administrative users shall have strong authentication, with passwords that shall conform to established DHS standards. All USCIS Identification and Authentication shall be done using the Password Issuance Control System (PICS) or its successor. Under no circumstances will Identification and Authentication be performed by other than the USCIS standard system in use at the time of a systems development.
- *Discretionary Access Control (DAC)* – DAC is a DHS access policy that restricts access to system objects (for example, files, directories, devices) based on the identity of the users and/or groups to which they belong. All system files shall be protected by a secondary access control measure.
- *Object Reuse* – Object Reuse is the reassignment to a subject (for example, user) of a medium that previously contained an object (for example, file). Systems that use memory to temporarily store user I&A information and any other SBU information shall be cleared before reallocation.
- *Audit* – DHS systems shall provide facilities for transaction auditing, which is the examination of a set of chronological records that provide evidence of system and user activity. Evidence of active review of audit logs shall be provided to the USCIS IT Security Office on a monthly basis, identifying all security findings including failed log in attempts, attempts to access restricted information, and password change activity.
- *Banner Pages* – DHS systems shall provide appropriate security banners at start up identifying the system or application as being a Government asset and subject to government laws and regulations. This requirement does not apply to public facing internet pages, but shall apply to intranet applications.

## DATA SECURITY

SBU systems shall be protected from unauthorized access, modification, and denial of service. The Contractor shall ensure that all aspects of data security requirements (i.e., confidentiality, integrity, and availability) are included in the functional requirements and system design, and ensure that they meet the minimum requirements as set forth in the DHS Sensitive Systems Handbook and USCIS policies and procedures. These requirements include:

- *Integrity* – The computer systems used for processing SBU shall have data integrity controls to ensure that data is not modified (intentionally or unintentionally) or repudiated by either the sender or the receiver of the

information. A risk analysis and vulnerability assessment shall be performed to determine what type of data integrity controls (e.g., cyclical redundancy checks, message authentication codes, security hash functions, and digital signatures, etc.) shall be used.

- *Confidentiality* – Controls shall be included to ensure that SBU information collected, stored, and transmitted by the system is protected against compromise. A risk analysis and vulnerability assessment shall be performed to determine if threats to the SBU exist. If it exists, data encryption shall be used to mitigate such threats.
- *Availability* – Controls shall be included to ensure that the system is continuously working and all services are fully available within a timeframe commensurate with the availability needs of the user community and the criticality of the information processed.
- *Data Labeling.* – The contractor shall ensure that documents and media are labeled consistent with the DHS *Sensitive Systems Handbook.*

# *SECURITY OF SYSTEMS HANDLING PERSONALLY IDENTIFIABLE INFORMATION AND PRIVACY INCIDENT RESPONSE*

**Privacy Clause Requirements.**

## GENERAL

U.S. Citizenship and Immigration Services (USCIS) has determined that performance of this contract requires the Contractor, subcontractor(s), vendor(s), etc. (herein known as Contractor), to access information that meet the definition of Personally Identifiable Information (PII) and/or Sensitive PII, set forth below. Accordingly, the Contractor will adhere to the following:

### *(a) Definitions.*

"Breach" (may be used interchangeably with "Privacy Incident') as used in this clause means the loss of control, compromise, unauthorized disclosure, acquisition, and/or access, or any similar situation where persons other than authorized users, and for other than authorized purpose, have access or potential access to Personally Identifiable Information, in usable form whether physical or electronic.

"Personally Identifiable Information (PII)" as used in this clause means any information that permits the identity of an individual to be directly or indirectly inferred, including any other information that is linked or linkable to that individual regardless of whether the individual is a citizen of the United States, legal permanent resident, or a visitor to the United States. Sensitive PII is a subset of PII which requires additional precautions to prevent exposure or compromise.

Examples of PII include: 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), Internet protocol addresses, biometric identifiers (e.g., fingerprints), 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 Personally Identifiable Information (Sensitive PII)" as used in this clause is a subset of Personally Identifiable Information, which if lost, compromised or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. Complete social security numbers (SSN), alien registration numbers (A-number) and biometric identifiers (such as fingerprint, voiceprint, or iris scan) are considered Sensitive PII even if they are not coupled with additional PII. Additional examples include any groupings of information that contains an individual's name or other unique identifier plus one or more of the following elements:

(1) Driver's license number, passport number, or truncated SSN (such as last 4 digits)
(2) Date of birth (month, day, and year)
(3) Citizenship or immigration status

(4) Financial information such as account numbers or Electronic Funds Transfer Information
(5) Medical Information
(6) System authentication information such as mother's maiden name, account passwords or personal identification numbers (PIN)

Other Personally Identifiable information may be "sensitive" depending on its context, such as a list of employees with less than satisfactory 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 it is not sensitive.

***(b) Systems Access.*** Work to be performed under this contract requires the handling of PII and/or Sensitive PII. The contractor shall provide USCIS access to, and information regarding systems the contractor operates on behalf of USCIS under this contract, when requested by USCIS, as part of its responsibility to ensure compliance with security requirements, and shall otherwise cooperate with USCIS in assuring compliance with such requirements. USCIS access shall include independent validation testing of controls, system penetration testing by USCIS, Federal Information Security Management Act (FISMA) data reviews, and access by agency Inspectors General for its reviews.

***(c) Systems Security.*** In performing its duties related to management, operation, and/or access of systems, owned and or operated by USCIS as well as by the contractor, containing PII and/or Sensitive PII under this contract, the contractor, its employees and subcontractors shall comply with applicable security requirements described in Department of Homeland Security (DHS) Sensitive System Publication 4300A or any superseding publication, and Rules of Behavior.

In addition, use of contractor-owned laptops or other mobile media storage devices to include external hard drives and memory sticks to process or store PII/Sensitive PII is prohibited under this contract unless the Contracting Officer (CO) in coordination with the USCIS Chief Information Security Officer (CISO) approves. If approval is granted the contractor shall provide written certification that the following minimum requirements are met:

(1) Laptops shall employ full disk encryption using NIST Federal Information Processing Standard (FIPS) 140-2 or successor approved product;

(2) Mobile computing devices use anti-viral software and a host-based firewall mechanism;

(3) When no longer needed, all mobile media and laptop hard drives shall be processed (i.e., sanitized, degaussed, and/or destroyed) in accordance with DHS security requirements set forth in DHS Sensitive System Publication 4300A. The USCIS reserves the right to audit random media for effectiveness of sanitization or degaussing. The contractor shall provide the requested equipment to USCIS no later than 15 days from the date of the request.

(4) The contractor shall maintain an accurate inventory of devices used in the performance of this contract and be made available upon request from USCIS;

(5) All Sensitive PII obtained under this contract shall be removed from contractor-owned information technology assets upon termination or expiration of contractor work. Removal must be accomplished in accordance with DHS Sensitive System Publication 4300A, which the Contracting Officer will provide upon request. Certification of data removal will be performed by the contractor's Project Manager and written notification confirming certification will be delivered to the contracting officer within 15 days of termination/expiration of contractor work.

***(d) Data Security.*** Contractor shall limit access to the data covered by this clause to those employees and subcontractors who require the information in order to perform their official duties under this contract. The contractor, contractor employees, and subcontractors must physically secure PII/Sensitive PII when not in use and/or under the control of an authorized individual, and when in transit to prevent unauthorized access or loss. When PII/Sensitive PII is no longer needed or required to be retained under applicable Government records retention policies, it must be destroyed through means that will make the PII/Sensitive PII irretrievable.

The contractor shall only use PII/Sensitive PII obtained under this contract for purposes of the contract, and shall not collect or use such information for any other purpose without the prior written approval of the Contracting Officer. At expiration or termination of this contract, the contractor shall turn over all PII/Sensitive PII obtained under the contract that is in its possession to USCIS.

***(e) Breach Response.*** The contractor agrees that in the event of any actual or suspected breach of PII/Sensitive PII (i.e., loss of control, compromise, unauthorized disclosure, access for an unauthorized purpose, or other unauthorized access, whether physical or electronic), it shall immediately, and in no event later than one hour of discovery, report the breach to the Contracting Officer , the Contracting Officer's Representative (COR), and the USCIS Service Desk and complete an Incident Report with the Service Desk Representative. The contractor is responsible for positively verifying that notification is received and acknowledged by at least one of the foregoing Government parties. Email notification shall be used to document all telephonic notifications.

***(f) Personally Identifiable Information Notification Requirement.*** The contractor will have in place procedures and the capability to promptly notify any individual whose PII/Sensitive PII was, or is reasonably believed to have been, breached, as determined appropriate by USCIS. The method and content of any notification by the contractor shall be coordinated with, and subject to the prior approval of USCIS, based upon a risk-based analysis conducted by USCIS in accordance with DHS Privacy incident Handling Guidance and USCIS Privacy Incident Standard Operating Procedures. Notification shall not proceed unless USCIS has determined that: (1) notification is appropriate; and (2) would not impede a law enforcement investigation or jeopardize national security.

Subject to USCIS analysis of the breach and the terms of its instructions to the contractor regarding any resulting breach notification, a method of notification may include letters to affected individuals sent by first class mail, electronic means, or general public notice, as approved by USCIS. At minimum, a notification should include: (1) a brief description of how the breach occurred; (2) a description of the types of personal information involved in the breach; (3) a statement as to whether the information was encrypted or protected by other means; (4) steps an individual may take to protect themselves; (5) what the agency is doing, if anything, to investigate the breach, to mitigate losses, and to protect against any further breaches; and (6) point of contact information identifying who affected individuals may contact for further information.

The contractor agrees to assist in and comply with PII/Sensitive PII incident remediation and/or mitigation efforts and instructions, including those breaches that are not a result of the contractor or employee actions, but the contractor is an unintentional recipient of privacy data. Actions may include allowing USCIS incident response personnel to have access to computing equipment or storage devices, complying with instructions to remove emails or files from local or network drives, mobile devices (BlackBerry, Smart Phone, iPad, USB thumbdrives, etc…).

In the event that a PII/Sensitive PII breach occurs as a result of the violation of a term of this contract by the contractor or its employees, the contractor shall, as directed by the contracting officer and at no cost to USCIS, take timely action to correct or mitigate the violation, which may include providing notification and/or other identity protection services to affected individuals for a period not to exceed 12 months from discovery of the breach. Should USCIS elect to provide and/or procure notification or identity protection services in response to a breach, the contractor will be responsible for reimbursing USCIS for those expenses. To ensure continuity with existing government identity protection and credit monitoring efforts, the contractor shall use the identity protection service provider specified by USCIS.

***(g) Privacy Training Requirement.*** The performance of this contract has been determined to have the potential of allowing access, by Offeror employees, to Personally Identifiable Information (PII) and/or Sensitive PII, which is protected under the Privacy Act of 1974, as amended at 5 USC §552a. The Offeror is responsible for ensuring all employees who have access to information protected under the Privacy Act complete annual mandatory USCIS Privacy Awareness Training. New Offeror employees shall complete PII training within 30 days of entry on duty. The Offeror shall use the USCIS provided web-based Privacy Training which is available through the USCIS LearningEdge training system http://learningedge.uscis.dhs.gov to satisfy this requirement. Any employees who do not have access to the online LearningEdge training system shall take Privacy training via a USCIS provided DVD. The Offeror shall certify as soon as this training is completed by its employees and annually thereafter on September 30th. The certification of the completion of the training by all employees shall be provided to both the COR and CO; within 60 days of contract award, within 45 days of new employee accession and no later than September 30th for the annual recertification.

***(h) Pass-Through of Security Requirements to Subcontractors.*** The contractor agrees to incorporate the substance of this clause, its terms and requirements, in all subcontracts under this

contract, and to require written subcontractor acknowledgement of same. Violation by a subcontractor of any provision set forth in this clause will be attributed to the contractor.

***(i) Ability to Restrict Access to Information***. USCIS reserves the right and prerogative to deny and/or restrict the facility and information access of any Contractor employee whose actions are in conflict with the standards of conduct or whom USCIS determines to present a risk of compromising Personally Identifiable Information (PII), Sensitive PII (SPII), Sensitive But Unclassified (SBU) information and/or classified information.