AMENDMENT OF SOLICITATION/MODIFICATION OF CONTRACT

1. CONTRACT ID CODE	PAGE OF PAGES
	1 94

2. AMENDMENT/MODIFICATION NO.	3. EFFECTIVE DATE	4. REQUISITION/PURCHASE REQ. NO.	5. PROJECT NO. *(If applicable)*
000001	11/03/2017		

6. ISSUED BY	CODE	7. ADMINISTERED BY *(If other than Item 6)*	CODE
DHS/OPO/DEPT.OPS		DHS/OPO/DEPT.OPS	

U.S. Dept. of Homeland Security
Office of Procurement Operations
Dept. Operations Acquisition Div.
245 Murray Lane, SW, #0115
Washington DC 20528-0115

U.S. Dept. of Homeland Security
Office of Procurement Operations
Dept. Operations Acquisition Div.
245 Murray Lane SW, #0115
Washington DC 20528-0115

8. NAME AND ADDRESS OF CONTRACTOR *(No., street, county, State and ZIP Code)*

CODE | FACILITY CODE

(x) 9A. AMENDMENT OF SOLICITATION NO.
70RDAD18R00000001

x 9B. DATED *(SEE ITEM 11)*
10/31/2017

10A. MODIFICATION OF CONTRACT/ORDER NO.

10B. DATED *(SEE ITEM 13)*

11. THIS ITEM ONLY APPLIES TO AMENDMENTS OF SOLICITATIONS

☒ The above numbered solicitation is amended as set forth in Item 14. The hour and date specified for receipt of Offers ☐ is extended, ☒ is not extended.
Offers must acknowledge receipt of this amendment prior to the hour and date specified in the solicitation or as amended , by one of the following methods: (a) By completing Items 8 and 15, and returning _____ copies of the amendment; (b) By acknowledging receipt of this amendment on each copy of the offer submitted ; or (c) By separate letter or telegram which includes a reference to the solicitation and amendment numbers. FAILURE OF YOUR ACKNOWLEDGEMENT TO BE RECEIVED AT THE PLACE DESIGNATED FOR THE RECEIPT OF OFFERS PRIOR TO THE HOUR AND DATE SPECIFIED MAY RESULT IN REJECTION OF YOUR OFFER. If by virtue of this amendment you desire to change an offer already submitted , such change may be made by telegram or letter, provided each telegram or letter makes reference to the solicitation and this amendment, and is received prior to the opening hour and date specified.

12. ACCOUNTING AND APPROPRIATION DATA *(If required)*

13. THIS ITEM ONLY APPLIES TO MODIFICATION OF CONTRACTS/ORDERS. IT MODIFIES THE CONTRACT/ORDER NO. AS DESCRIBED IN ITEM 14.

CHECK ONE	
	A. THIS CHANGE ORDER IS ISSUED PURSUANT TO: *(Specify authority)* THE CHANGES SET FORTH IN ITEM 14 ARE MADE IN THE CONTRACT ORDER NO. IN ITEM 10A.
	B. THE ABOVE NUMBERED CONTRACT/ORDER IS MODIFIED TO REFLECT THE ADMINISTRATIVE CHANGES *(such as changes in paying office, appropriation date, etc.)* SET FORTH IN ITEM 14, PURSUANT TO THE AUTHORITY OF FAR 43.103(b).
	C. THIS SUPPLEMENTAL AGREEMENT IS ENTERED INTO PURSUANT TO AUTHORITY OF:
	D. OTHER *(Specify type of modification and authority)*

E. IMPORTANT: Contractor ☐ is not. ☐ is required to sign this document and return _____ copies to the issuing office.

14. DESCRIPTION OF AMENDMENT/MODIFICATION *(Organized by UCF section headings, including solicitation/contract subject matter where feasible.)*

The purpose of this Amendment is as follows:

1)To provide the Government's response to questions received on the RFP, provided as Attachment A000001;

2)To provide revised Attachment A, DHS Hosting;

3)To provide a revised Schedule B Attachment – Pricing Model; and

4)To provide a revised RFP.

DO/DPAS Rating: NONE

Except as provided herein, all terms and conditions of the document referenced in Item 9 A or 10A, as heretofore changed, remains unchanged and in full force and effect.

15A. NAME AND TITLE OF SIGNER *(Type or print)*		16A. NAME AND TITLE OF CONTRACTING OFFICER *(Type or print)*	
		Cynthia Aki	
15B. CONTRACTOR/OFFEROR	15C. DATE SIGNED	16B. UNITED STATES OF AMERICA	16C. DATE SIGNED
_____ *(Signature of person authorized to sign)*		_____ *(Signature of Contracting Officer)*	

SECTION I - SUPPLIES OR SERVICES AND PRICE/COSTS

1 TASK ORDER TYPE

The Government anticipates this task order will be a Hybrid type, which may include a combination of Labor Hour (LH), Time and Materials (T&M), and Firm-Fixed Price (FFP) type CLINs, as proposed by the Contractor. This task order is established under the contractor's Enterprise Acquisition Gateway for Leading-Edge Solutions II (EAGLE II) - IT Solutions contract. All terms and conditions of the Offeror's EAGLE II contract remain unchanged and in full force and effect, unless specifically stated otherwise herein.

2 SCHEDULE B

See Schedule B Attachment–Pricing Model

SECTION II - STATEMENT OF WORK

1 GENERAL

The Department of Homeland Security (DHS) has a need for program management, change management, and software engineering services to support the continuation of the Financial Systems Modernization (FSM) program in support of the Domestic Nuclear Detection Office (DNDO), Transportation Security Administration (TSA) and the United States Coast Guard (USCG), also known as the TRIO. These services shall include resources to support program and change management, Business Process Re-engineering (BPR) support, requirements, refinement, rework/deployment/implementation, perform testing, provide training, complete configuration and integration, migration of service and data, operations and maintenance (O&M), and critical infrastructure services for full lifecycle support in accordance with the DHS System Engineering Life Cycle (DHS SELC) policy (as detailed in DHS Acquisition Directive 102-01) and USCG System Development Life Cycle (USCG SDLC) and all applicable TRIO policies, plans, procedures and standards, as follows:

- DHS Enterprise Architecture (EA) framework;
- DHS System Engineering Life Cycle (SELC);
- USCG System Development Life Cycle (SDLC);
- Federal Information Security Management Act (FISMA);
- Federal Information Technology Acquisition Reform Act (FITARA);
- Clinger-Cohen Act of 1996, Federal Managers' Financial Integrity Act (FMFIA);
- DHS Financial Accountability Act;
- National Institute of Standards and Technology's (NIST) Special Publication (SP) 800-171;
- DHS IT Security 4300A;
- Defense Information Security Agency (DISA) Security Technical Implementation Guide (STIG);
- DHS Test and Evaluation Directive 026-06-001; and
- DHS Test and Evaluation Master Plan (TEMP) Instruction Guide 0026-06-001-01.

DISA STIG Guidance can be found on the DoD/DISA Information Assurance Support Environment (IASE) websites: http://iase.disa.mil/policy-guidance/Pages/index.aspx, http://iase.disa.mil and http://iase.disa.mil/stigs/index.html.

2 BACKGROUND

In August of 2014, DHS entered into an Interagency Agreement (IAA) with the Department of the Interior (DOI)/ Interior Business Center (IBC) as its shared service provider for a FSM Program and Solution to obtain an integrated finance, procurement and asset management business solution. In February 2017, DHS and DOI/IBC mutually agreed to transition FSM efforts from DOI/IBC to DHS.

The solution included the deployment of the integrated Oracle Federal Financials, Oracle Business Intelligence Enterprise Edition (OBIEE), Oracle Business Intelligence Application (OBIA), Oracle Contract Lifecycle Management (CLM), Kofax's Markview, and Sunflower for three of its Component organizations: DNDO, TSA, and USCG. DNDO became operational for the full user base on November 2, 2015. TSA and USCG remain on the legacy DHS financial system pending remaining implementation activities, included here within. Under this task order, the Government has defined the high-level notional schedule as: Global and DNDO capabilities fully functional in DHS Data Center #2 no later than FY19Q1, TSA capabilities and CG-LIMS fully functional in DHS Data Center #2 no later than FY20Q1, and USCG capabilities fully functional in DHS Data Center #2 no later than FY21Q1. This Statement of Work (SOW) uses the term "FSM Solution" to refer to the full set of application systems and modules being deployed to support the TRIO.

The TRIO's implementation is running on a single instance of Oracle 12.2.4 with multiple sets of books. DHS agreed to two customizations of the Oracle product that are specific to USCG's Oil Spill Liability Trust Fund; however, they will not be deployed until USCG's go live on the new solution.

The Oracle applications (OFF, OBIA/OBIEE, and CLM), Kofax's Markview, and Sunflower are the base systems being deployed. The current FSM Solution utilizes the Oracle SPARC T5-8. The SPARC server runs the Oracle Solaris operating system at the legacy data center with network connectivity via a two DS3 circuits provided by DHS. DHS anticipates the new hosting environment at the hosting provider facility will include the Oracle M8 SuperCluster and/or a "like for like" hardware to support production, sustainment, and disaster recovery. Additional, there will be RHEL Linux servers running under x86 processors provided at the data center facility to support applications not deployed on the M8 platform. Storage/SAN devices being provided and hosted at the data center include the Oracle ZFS 5-2 Storage appliance.

2.1 FSM Solution Hosting Collaboration

Under this requirement, the Contractor shall be required to work collaboratively with the hosting provider to support migration of the Application from DOI/IBC to the new hosting environment in order to assume the operations and sustainment for the FSM Solution. The migration/transition of the system from DOI/IBC to DHS must be completed in accordance with the Government's transition schedule. The Contractor shall build out their portion of the transition plan/schedule that shows the tasks the Contractor will need to complete to assume implementation and operations and maintenance responsibility for the FSM Solution.

The hosting provider has documented their ITIL processes and employs approved IT service management tools that as referenced in the DHS Technical Reference Manual (TRM). The hosting provider will build out their portion of the migration transition plan/schedule, propose migration options to transition the FSM Solution from DOI/IBC to DHS, establish the infrastructure as a service (IaaS) capability to receive the FSM Solution, provide security documentation and/or input to the DHS ISSO supporting the DHS JPMO to obtain the FSM Solution ATO and assume hosting O&M for the IaaS capability up to the operating system after transition of the FSM Solution. Each application identified in Attachment A will be migrated

using one of the migration options listed below. The Government and hosting provider are still finalizing the appropriate option for each application; however, at a minimum Control M, Black Box, and GRC will require re-installation. The data center hosting provider infrastructure monitoring tools include the following:

- Inside the SDN environment is satellite to BMC Operations Manager.
- Outside SDN in the hosting provider's managed network will be standard monitoring tools, Oracle Enterprise Manager and Oracle Ops-Center.

Migration Options:

1. Cloning: Creates an identical copy of an existing Oracle system using Oracle cloning tools, works best when cloning between machines that are running identical versions of an operating system.

2. Re-Installation: Applications are installed on OS from Oracle images, patches applied, network settings assigned and configured for application, data synchronized from source application, and applications are setup in pristine environment according to DHS data center standards.

3. Backup and Restore: Create backup copy of entire application and data environments, transfer to target.

The Contractor shall ensure all components documentation, testing, system components, source code, etc. are successfully transitioned during migration to ensure the Contractor can assume O&M responsibility for the FSM Solution. The Contractor shall create missing support documents such as standard operating procedures, installation guides, O&M support documentation, etc. The Contractor shall be responsible for the migration of the FSM Solution including the re-installation of the application if required. While cloning and backup/restore will bring over the application and the database, the Contractor shall be responsible for ensuring the complete FSM Solution was transitioned. The Government anticipates there will be multiple "shakeout" migrations that will allow all support teams an opportunity to test, shakeout, create step by step procedures for the final cutover, and inspect, etc. the FSM Solution. The initial shakeout/mock migration will provide the teams with a copy of production, TSA development, and USCG development environments with the list of all environments needed for final cutover being identified during the discovery meetings and included in the final cutover over procedures document.

Financial applications will be migrated to a Private Cloud solution in DHS Data Centers, DC1 and DC2. DHS specific customized requirements will be maintained in the target environment. The support includes managing the Platform including Hardware through operating system (OS) and supporting environment (LDOMs and Zones) and databases. Oracle M7 hardware with Solaris operating system will be used at both locations. DHS Data Center #2 will support this effort in a Private Cloud environment with DHS Data Center #1 providing the Disaster Recovery capability.

Additional information regarding the DHS FSM Hosting environments, applications, number of users/concurrent users is provided as Attachment A to this RFP. The list of environments is an estimate that the Contractor should review with updates being driven based upon their proposed configuration management processes.

2.2 DHS Joint Program Management Office (JPMO)

The DHS Office of Financial Management (OFM) Financial Systems Modernization (FSM) Program established a Joint Program Management Office (JPMO) responsible for coordinating all efforts to support the FSM Solution. JPMO functions include program management, information technology management, and business transformation. The JPMO will work with the DHS component agencies, DHS leadership, and external stakeholders from the Office of Management and Budget (OMB), the General Services Administration (GSA), and the Unified Shared Services Management (USSM).

2.3 U.S. Coast Guard Finance Center Business Operations

The USCG Finance Center (FINCEN) provides the business operations and functional operations and maintenance support for the TRIO. A draft responsible, accountable, consulted, informed (RACI) matrix, identifying the roles and responsibilities is provided as Attachment C to this RFP. Attachment C is broken into two sections; Functional O&M with a RACI and Technical O&M with a TRACI. The RACI provides the tasks required for Functional O&M support and identifies who is responsible, accountable, consulted and informed. The TRACI provides the tasks required for Technical O&M support and identifies who is technical, responsible, accountable, consulted, and informed. Since the RACI is specific to Functional O&M, this section only speaks to the RACI tasks identified in Attachment C. Section 5.3 references the TRACI in more detail. The Contractor shall collaborate with the USCG FINCEN to update and finalize the RACI matrix for Functional O&M support items during the transition. These are some of the USCG FINCEN support tasks:

- Tier 1 and Tier 2 Help Desk support;
- Manual data pulls for interfaces from external sources;
- Print jobs;
- Error correction for interfaces;
- Period closing;
- TSA and DNDO liaison support; and
- Execute concurrent processes.

2.4 Component Trio Project Management Offices and Support Contractors

Each Trio Component utilizing or migrating to the solution has established a team that will coordinate with the JPMO to support implementation/migration and sustainment activities. In support of O&M, the following functions will be provided by Component PMO:

- TIER 0 Support – initial triage of user issue;

- Submitting Change Requests to the Program Change Management Board (P-CCB); and
- Participating in the P-CCB as a voting member.

In support of implementations, the following functions will be provided by Component PMO:

- Data cleansing and data preparation for migration;
- Change Management, component specific;
- Attending Discovery Meetings;
- Providing requirements for the Joint Concept of Operations (ConOps) and Operational Requirements Document (ORD);
- Attending Configuration/Setup Meetings, Testing Events, Contractor provided training, etc.;
- Reviewing, providing comments and accepting DHS SELC documents provided by the Contractor that support implementation; and
- Providing SMEs for meetings, training, testing, etc..

3 OBJECTIVES

The FSM Solution has been put into operation to meet general DHS goals including improve data quality and timeliness; provide useful and reliable information; provide accurate and timely information to OMB, Congress, Government Accountability Office (GAO), Office of Inspector General (OIG), and the public; and to support unqualified audit opinions on DHS financial statements. In the end state, all TRIO components will be transitioned to the TRIO FSM Solution, supported by the Contractor and maintained in the DHS hosting environment. DNDO will transition from DOI/IBC first to the DHS-led hosted and managed solution, and TSA will cut-over to the FSM Solution next, followed by USCG. The TSA and USCG cut-over (i.e. "go-live") will occur at the beginning at the start of a fiscal year. The key success factors of the FSM Solution include:

- Global and DNDO capabilities fully functional in DHS Data Center #2 no later than FY19Q1; TSA capabilities and USCG's CG-LIMS integration fully functional in DHS Data Center #2 no later than FY20Q1; and USCG capabilities fully functional in DHS Data Center #2 no later than FY21Q1;
- The capability to produce an unqualified audit and accurately report the use of resources is provided by the FSM Solution;
- Information Technology Infrastructure Library (ITIL) Service Design for Information Technology Service, Business, and Operations Management and FSM Solution IT Governance are established, implemented, and successfully support the JPMO and customers;
- All Documentation required supporting DHS SELC stages and reviews as required in DHS Directive Number: 102-01-001 and USCG SDLC are created and maintained;
- Successful coordination with the Infrastructure hosting provider and the Functional O&M provider that ensures customer service level agreement (SLA) requirements are met;

- Successful transition of the FSM Solution environments (DNDO production, DNDO development, TSA development, USCG development, test, sandbox, training, etc.) (See Attachment A) from the DOI/IBC shared service environments into the DHS designated infrastructure hosting provider's established environments;
- Environments are available for rework, implementation, development, production, testing, training, and help desk tiers 1, 2, 3, and 4 to support all three TRIO components;
- FSM Solution O&M support is in place for the TRIO components with a signed off operational familiarization demonstration(OFD) by the contractor accepting responsibility for the FSM Solution (see Attachment I);
- All rework needed to assume responsibility for the FSM Solution is completed and is evidenced when DNDO and FINCEN Business Operations support for DNDO users can perform their business in the system;
- Customer service level agreements are in place and a mechanism to measure satisfaction, product delivery quality, and SLA metrics implemented, tracked, reported, maintained, and attained;
- TSA and USCG development environments are available to begin the work needed to complete the TSA and USCG implementation;
- Successful completion of software configuration, development and implementation, which includes but is not limited to reports, interfaces, extensions and workflows, to meet any remaining unmet requirements necessary to stabilize DNDO and complete the TSA and USCG implementations, data migration, data migration testing event, cut over and "go-live"; and
- Comprehensive training strategies and user guides are planned, deployed, delivered and maintained that enable DNDO, TSA and USCG users to effectively utilize the FSM Solution over the life of the solution to meet their Component's operational requirements.

4 SCOPE

The scope of this task order is to support the three DHS TRIO agencies (DNDO, TSA, and USCG) and incorporates the software engineering tasking required to provide full lifecycle support for the FSM Program and Solution. Support services required under this task order include all solutions, processes, and procedures necessary to sustain business applications at the highest levels of service and availability consistent with cost, schedule, and performance objectives.

This task order will provide the System Deployment Agent/System Support Agent (SDA/SSA) roles that are required for implementation and sustainment of the TRIO Financial System Modernization (FSM) Solution. The Contractor shall show how they intend to segregate the duties between the SDA and SSA and how they will maintain that segregation to ensure future audits of the Contractor's methodology/processes/procedures provide that evidence.

The Contractor shall provide documentation, tools, solutions and engineering life cycle tasks required to establish the FSM Solution IT Service Management and IT governance and support structures, change approach and processes, and implement engineering life cycle support. The list of business applications and systems that encompass the FSM Solution will be detailed in the

documentation provided in OMB Max as Government Furnished Information (GFI) after task order award.

5 REQUIREMENTS

5.1 Functional Requirements & System Requirements Documentation

The Contractor shall maintain, refine and periodically deliver Functional Requirement Document(s) and System Requirement Specification(s). Functional Requirements are derived from the Business Processes. System Requirements are derived from the Functional Requirements. The Contractor shall review draft documents, capture change requests, capture final review comments, and include them in the final technical documentation deliverables.

The Contractor shall review, evaluate, and propose modification to the Requirements Traceability Matrix (RTM) to ensure derived requirements essential to support the business and operational requirements are captured and identify any that may be missing. For example, if the RTM states the system shall allow a user to create an award to procure commercial items, and shall allow the user to create optional CLINS, but does not have another requirement defined in the RTM to exercise the optional CLIN and associate funding, then the requirement(s) would be considered incomplete and will most likely cause confusion for the user when no test scripts were developed to execute an optional CLIN with funding. If during the review of the RTM, the Contractor noted the requirement to exercise the CLIN and associate funding to the CLIN did not exist, then the Contractor shall include their findings in the Discovery Report. The Government shall review the report and determine how the RTM is updated. The Contractor shall evaluate the RTM and provide feedback including a request for additional information when requirements are not clear, may not be valid, and do not appear testable or otherwise able to be evaluated as written. The maintenance for the RTM shall be collaborative between the Contractor and the Government to ensure business and operational requirements are met.

5.2 Application Configuraiton, Implementation, and Deployment

The Contractor shall establish architectures for development activities, for developmental integration and test activities and for software build activities. The Contractor shall perform technology assessments, system upgrade analysis and testing, concept prototyping, product evaluations, and human/computer interface evaluations. The Contractor shall perform and/or coordinate system activities with other business applications where an interface has been or needs to be established to maintain/create the exchange of information between the business applications. The Contractor shall demonstrate the product(s) being proposed to meet the solution, both pre- and post- design. The Contractor shall design, develop, implement/deploy, configure, conduct risk analysis and life cycle analysis for new software application deployment/development.

All solutions and services shall meet DHS Enterprise Architecture policies, standards, and procedures. Specifically, the contractor shall comply with the following HLS EA requirements:

- All developed solutions and requirements shall be compliant with the HLS EA

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

5.3 Software Maintenance & Upgrades

The Contractor shall perform preventive, corrective, perfective and adaptive sustainment engineering, and corrective maintenance for all business applications and associated databases. The Contractor shall perform obsolescence management. Regular system maintenance is required to support the FSM Solution production instances. The maintenance for the FSM Solution should be proposed by the Contractor. For information purposes only, DHS is providing the DOI/IBC scheduled maintenance windows.

- Weekly Maintenance Windows: DOI/IBC schedules weekly maintenance windows during which routine system and infrastructure maintenance occurs.
- Monthly Maintenance Windows: Used to push patches to the FSM Solution. The Contractor shall coordinate all downtime with the other support teams (FINCEN and the DHS hosting provider) to ensure there are no conflicts.

Upgrades, patches, and/or updates to the FSM Solution should be coordinated and put in place during agreed to maintenance windows or downtime. Commercial off the shelf (COTS) applications shall be updated to the latest version, either major or minor, within three (3) months of the update being received unless cyber security requirements state the update must be sooner.

The Contractor shall work with the DHS JPMO, Stakeholders, and other support teams to determine the maintenance windows/schedules. Note: The DHS hosting provider will complete the operating system patching in coordination with the Contractor. The draft technical, responsible, accountable, consulted, and informed (TRACI) matrix will be provided by the Government and updated by the Contractor and the hosting provider prior to final transition of the FSM Solution from DOI/IBC.

5.4 Software Testing

The Contractor shall perform formal testing of business application and software components and regression testing using an industry standard and best practice, repeatable test methodology, and automated testing tools. The Contractor shall develop test case specification(s), acceptance test procedures, test plans, test scripts, and test reports.

The Contractor shall submit an overall contractor Test and Evaluation (T&E) plan for DHS approval which details their test methodology and approach and how they intend to support the requirements identified in DHS Instruction Guide 026-06-001-01. Note: The Government is not requesting the Contractor to develop the Test and Evaluation Master Plan (TEMP). The TEMP will be provided by the Government as GFI. The Contractor shall conduct T&E tasks as follows:

- Plan, prepare for, and conduct test readiness reviews;
- Develop, update, and perform configuration management of test plans; ensure that test plans include the strategy used to prioritize and select what is versus what is not tested (i.e., due to time constraints) including for regression tests;
- Develop, update, and perform configuration management of test scripts; ensure the scripts contain the steps and data necessary to verify cited requirements and design use cases;
- Execute tests in accordance with test plans and provide in-person and remote access to DHS, Components, and Operational Test Agent (OTA) representatives;
- Develop test reports and perform other post-test activities in accordance with the test plan;
- Ensure defects that are also applicable to the production instance can be readily tracked following the test event; and
- Review past DOI/IBC, Component, and OTA test reports to gauge the potential for past issues to impact the instance received and avoid similar problems.

Note: The Contractor shall conduct Section 508 testing of the FSM Solution. See Attachment G for Section 508 testing requirements.

5.5 Software Documentation

The Contractor shall provide system documentation services required to create, update, and maintain any application, user, and system documentation, along with architectural diagrams for the system and any and all operating environments (development, test (including depicting interfaces with external systems), staging/integration, training, production, etc.). All software code and documentation will be the property of the Government and shall be stored in Government approved and hosted repositories.

5.6 System Administration

The Contractor shall provide system administration services for all business applications developed, hosted, and maintained on behalf of DHS and shall coordinate with the hosting provider for system administration services as required.

The Contractor shall perform preventative maintenance for the FSM Solution acquired, developed, hosted, and maintained on behalf of DHS, to include installation of upgrades and patches to applications and database software and COTS products. The Contractor shall be responsible for configuration of the tools that will be provided as GFE. The Contractor shall coordinate with the hosting provider to manage changes to the infrastructure such as hardware upgrades or operating system (OS) updates that directly affect the FSM Solution. It is important that the Contractor's configuration management plan is closely coupled and compliments the hosting provider's configuration management plan and that all change proposed by either the Contractor on this task order or the Contractor supporting the hosting collaborate and coordinate how change(s) will be introduced into the FSM Solution to ensure availability requirements and customer SLAs are met.

The Contractor shall provide planning, development, test and O&M support to investigate, resolve, track and report business application performance (issues and errors) and how they will coordinate with the infrastructure hosting provider, DHS CIO and the Component CIOs to investigate and resolve network issues that degrade or affect the FSM Solution user's ability to access and use the system. The Contractor shall track and manage open and resolved issues, ensure audit capabilities are enacted to collect and log security audit and application performance data, and shall review audit and performance logs. These items shall be reported in the Monthly Progress Report (MPR).

5.6.1 Database Management and Administration

The Contractor shall perform database management, administration, and documentation for the FSM Solution, to include creation, installation, and maintenance of databases for project and mission support, configuration of accounts per mission-specific requirements, and verification of application and database backup processes for system recovery purposes. The Contractor shall coordinate with the infrastructure hosting provider to complete the tasks in this section and how they shall document the standard operating procedures.

5.7 System Configuration Management Plan (S-CM Plan)

The Contractor shall provide Configuration Management and an S-CM Plan that identifies the processes which will be used for identifying, organizing, documenting, and managing changes to the FSM Solution program as it evolves throughout the DHS SELC/USCG SDLC. The S-CM Plan shall include the managerial and technical activities established to ensure that standard procedures are defined to protect the integrity of the FSM Solution baseline and provide a means for evaluating and improving the program. The S-CM Plan shall include processes for monitoring, metrics/statistics, auditing, and archiving of FSM Solution configuration items. The S-CM Plan must include controls to ensure that changes are checked into a version control system and tasks are created to rectify any non-conformance.

5.7.1 DHS Approved Repositories

All source code and documentation shall be version controlled in DHS approved repositories. The Contractor shall create and maintain all source code and documentation supplied under this

task order, including COTS software items in the DHS approved repositories. The Contractor shall not maintain copies of source code and/or documentation within their site on local workstations or servers. All deliverables, including source code, created to support the FSM Solution shall be checked in daily into the DHS approved repositories in accordance with the System Configuration Management Plan.

5.8 Requirements Management Plan

The Contractor shall provide a Requirements Management Plan that identifies how the Contractor will gather, analyze, document, and control system requirements and how they will provide tractability to user requirements, test scripts, test results, etc. DHS will provide the Contractor with access to Jira as the requirements management tool. The Plan shall detail the tool configuration, procedures and processes for requirements management.

5.9 Data Management Plan and Data Migration Plan

Migration of TSA and the USCG data requires a multi-step process of data analysis, selection, validation, conversion, test and load that will be performed iteratively by TSA and USCG's migration Contractors to allow for proper testing prior to migration of production data. Analysts on the Component Data Migration Teams first analyze the data and identify the business rules that will allow for the correct selection of data to be migrated. The data to be migrated shall include active master record data, such as suppliers and customers, along with open/active transaction records, such as contracts, unliquidated obligations and fixed assets. Next, the selected data is transformed to fit the business rules of the target environment. Transformation includes cross walking legacy data values to new valid lookup values and loading the data into Excel formatted templates for eventual loading into the FSM Solution. The Contractor shall load the data through mock conversion processes that identify data errors that must be corrected before the final production cutover.

The Contractor shall review the existing FSM Solution Data Management Plan, TSA Final Mock Migration Guide, Migration Templates, etc. and recommend updates or changes to the Government. The DMP shall identify DHS information needs, data requirements, data conversion, data security strategies, and the metrics required to demonstrate success. The existing Data Management Plan is provided as Attachment F.

The Contractor shall support TSA and USCG data migrations. The Contractor shall migrate TSA and USCG financial, procurement, asset, general ledger, etc. provided data to the FSM Solution and shall provide:

- Updates to data template rules as defined in the excel templates provided to the Component at least 60 days prior to the beginning of a full Mock Conversion;
- At least one (1) Mock Migration in a non-Multi-Org environment (at a minimum TSA 1 and USCG 1);
- Mini-Mock Migration(s) with Collaboration Session(s) used to validate template, data scenarios, and SME understanding of configuration choices;

- Multiple Mock Migrations into Multi-Org environment (at a minimum TSA 2 and USCG 3);
- Collaboration Review Sessions for each mini (1 day session) and major (1 week session) mock to include the TSA and USCG Data Migration Teams and SMEs;
- Final Cutover Migration;
- Final Cutover Review Session(s) with Data Teams and SMEs to obtain SME signatures that data is loaded as expected prior to final standup, cutover, and reconciliation; and
- One full test event using 100% converted data to ensure converted data is usable, reliable, and correct. This test event is in addition to the test events required for regression, performance, acceptance, and operational testing of the FSM Solution.

The objective of the mini mocks and review sessions is to allow the data migration teams and the SMEs, via small incremental mocks of specific data, to understand how data transformation rules, configuration settings, template rules, etc. will affect the full/final data migration(s). These will help "tweak" migration assumptions, data extraction/transformation rules, template population, data loads, etc. to ensure success when full mock migrations and final cutover are completed.

TSA completed three (3) Mock Migrations into a non-Multi-Org environment and a fourth migration into a Multi-Org environment. The USCG completed one (1) Mock Migration into a non-Multi-Org environment.

Note: The USCG data scenarios for CLM required Oracle to provide SRs to correct the load process. All USCG data scenarios for CLM have not been fully tested/exercised. The Contractor shall be required to work with Oracle to correct the CLM load API, where applicable.

The list of Mock Migrations outlined above are provided as reference for what the Government would expect the Contractor to consider when completing the Discovery Report. The Discovery Report shall detail the Mock Migrations TSA and USCG will need to complete implementation.

The Data Management Plan shall detail how the Contractor shall ensure the quality of the migrated data, the ability of the operational community to use the migrated data, that all the data sent from TSA and USCG is fully loaded, and the General Ledger balances match TSA and USCG balances. The Data Management Plan shall include metrics to define and track the success of the Data Migration.

Note: The data migration environments will be established by the hosting provider with input from the Contractor.

5.10 Data Security Management Plan

The Contractor shall develop and maintain the Data Security Management Plan for the FSM Solution and Program. The plan shall adhere to DHS and USCG Operation System Center (OSC) data security management policies and shall ensure sensitive, privacy, and other data are protected.

Note: The OSC data security management policies will be provided in the Reading Room and as GFI after award. The plan shall detail how data will be securely transmitted between internal sources and external sources. The plan shall provide the instructions for identifying, maintaining, managing, and securing system data.

5.11 Training Plan

The Contractor shall provide a Training Plan. The plan shall include a comprehensive strategy including methods such as: classroom training and materials, online help systems, and Computer-Based Training (CBT). Training may be required outside of the DC area. TSA and USCG are located throughout the Continental US. The Contractor shall propose ways to complete training in other locations outside of the DC metro area.

The Contractor shall provide End User Training to include business processes with hands on exercises and appropriately staged data.

5.12 System Administrator - User Productivity Kit (UPK)

The Contractor shall provide a User Productivity Kit (UPK) administrator and developer(s) to maintain the UPK application and content. The UPK administrator is a critical component to installation, deployment, and maintenance of the UPK application. The following is a list of key responsibilities associated with the UPK administrator role during the initial deployment phase of the software lifecycle and pre content development:

- UPK administrator works directly with the Technical Team (Database Administrator) to install and configure the tool;
- The UPK administrator is responsible for testing connectivity issues and resolving systemic issues; and
- The UPK administrator configures access to the Knowledge Center which is a repository for Oracle-based transactional templates used in Oracle Federal Financials.

The UPK Admin configures the profiles of each UPK developer, establishes security access to the UPK library, and customizes embedded UPK templates to reflect component specific insignia.

The Contractor shall coordinate and collaborate with the TRIO Training SMEs on the setup and use of UPK. The Contractor shall complete a needs assessment for UPK, in conjunction with the TRIO training SMEs and include the assessment into the Discovery Report. The Contractor shall update UPK content at least 3 months prior to go live for TSA and USCG. The Contractor shall coordinate with the DHS hosting provider to host Oracle's UPK, which must be installed on a dedicated UPK server and configured for use by UPK developers (of training content). The UPK developer licenses will be provided by the Government as GFE.

After the UPK application has been successfully installed, the UPK Admin is responsible for the on-going maintenance of the software. The following is list of key responsibilities associated with UPK Admin role post deployment:

- Applying Oracle recommended patches and testing;
- Scheduling backups of development content to minimize file corruption;
- Publishing developer content to the production environment;
- Troubleshooting and resolving technical issues;
- Communicate with Oracle vendors to resolve systemic issues beyond user error; and
- Ensuring components (end-users) have access to customized training material and generic material contained in the Knowledge Center.

5.13 System Integration

The Contractor shall perform system integration to unify the business application components with other subsystems function, develop and maintain interfaces to other business applications for the purposes of data sharing and dissemination, work with the infrastructure hosting provider to incorporate hardware and infrastructure components with business application and software designs to test newly developed software with existing components, develop software prototypes required for system design or capability analysis and ensure improvements do not adversely affect ongoing operations. System integration testing, including interface testing, should be specified in the DHS approved User Acceptance Test Plan.

5.14 Transition of the FSM Solution from DOI/IBC to DHS and O&M Responsibility

The Contractor shall provide transition O&M support functions, support environments, etc. from DOI/IBC to DHS support entities. The following sections provide more details on the specific tasks that the Government has identified to date that will affect the Contractor's methodology. The Contractor shall propose any additional tasks that will be required to assume full O&M and implementation responsibility in their Discovery Report.

5.15 Transition Tasks to Complete Relocation of the FSM Solution

The Contractor shall coordinate with the USCG FINCEN to ensure customer support level agreements are maintained. The Contractor shall provide periodic, on-site support at FINCEN, on an as-needed basis, to ensure the Functional O&M support is communicated, coordinated, maintained, and executed the timeframes required to support the customer SLAs as outlined in the Place of Performance section in the statement of work for this task order.

The Contractor shall participate in meetings to finalize the joint FSM Solution Transition Plan (STP) that includes a detailed project plan for the portions of the STP that the contractor is responsible for executing. The Contractor may be required to travel to DOI/IBC facilities in Denver, Colorado and Reston, Virginia to perform this requirement.

The STP shall include the Technical O&M, specific identified Functional O&M tasking as appropriate, and implementation support for the FSM Solution including T&E activities. The Contractor shall coordinate with all responsible support parties to review and update the TRACI and RACI matrix that clearly define the functions and roles needed for support and who is responsible, accountable, consulted, and informed on those functions. (See Attachment C)

The Contractor shall collaborate, and coordinate with DOI/IBC and the DHS hosting provider to complete the full transition. The items listed below are some of the identified tasks that shall be included in the FSM STP. Additional items most like will be identified during the bi-weekly transition meetings. They include but are not limited to:

- GRC re-implementation
- Re-establish Interconnection Security Agreements (ISAs) for interfaces
- Re-establish interfaces with external and internal customers/vendors
- Re-establish crons/scheduled jobs
- Re-establish Service to load new FAR Clause(s) updates

The Contractor shall include in the Transition Project Plan the timeframes required to complete their identified tasking in their portion of the FSM STP. The Contractor working with the other key members of the transition team shall execute the tasks identified in the FSM STP to transition the FSM Solution to the DHS hosting provider.

5.16 Interim and Full Authority to Operate (ATO)

During all SELC phases, the Contractor shall develop documentation and provide any required information in support of the certification (authorization) / accreditation process requested by the DHS IA Office, who is providing the ISSO to support the FSM Solution ATO and will be coordinating with the hosting provider and this task order Contractor. The system is categorized as Moderate – Moderate – Moderate. In addition, the Contractor security certification (authorization) / accreditation support shall be performed using the DHS certification/ accreditation process, methodology and tools.

DHS Sensitive Systems Policy Directive 4300 A, Section 4.1.4 requires the "Separation of duties to prevent a single individual from being able to disrupt or corrupt a critical security process." The Policy requires the following: "Components shall divide and separate duties and responsibilities of critical IT system functions among different individuals to minimize the possibility that any one individual would have the necessary authority or system access to be able to engage in fraudulent or criminal activity. "Security testing is but one critical systems function that needs to be performed by a provider (either government or contractor) other than the system designer / developer / operator (SDA/SSA). The Contractor shall coordinate with the DHS COR and JPMO, DHS IA and Components offices to complete all required certification (authorization) and accreditation documentation, actions and approvals necessary to obtain an interim Authority to Operate (ATO) prior to deployment of the system for use by DHS, DNDO, TSA and USCG. The Contractor shall support obtaining a full ATO as required within the timeframe established by the DHS IA office. All A&A (formerly C&A) activities shall be conducted in accordance with DHS 4300A for Information Assurance, and all other applicable DHS information assurance policies, procedures, regulations and standards.

The Contractor shall submit a Security Test and Evaluation (ST&E) plan for DHS approval prior to conducting ST&E activities. The ST&E report shall be delivered for information 30 days after test completion. Some of the data from the ST&E may be used by DHS to determine the operational cyber resilience of the solution. The contractor shall support the DHS Operational

Test Agent (OTA) with preparation, conduction, and analysis of the OTA's cyber security threat based penetration testing in the production or production like environment.

5.17 Operations & Maintenance (O&M)

Upon successful completion of OFDs and written approval by the Government, the Contractor shall assume full responsibility for the Contract services specified in this task order in direct support of the FSM Solution. The Contractor shall now be responsible for O&M support over the FSM Solution and shall have established all the documentation, plans, processes, and procedures required to assume full responsibility (i.e., SOPs defined and implemented).

The Contractor shall complete all documentation needed to take responsibility for the FSM Solution, create a system maintenance plan and maintenance requirements list(s) (MRLs) for O&M to include recurring maintenance activities to be conducted during the course of the task order performance period.

The lists of required environments will most likely change as the Contractor performs the discovery of what is in the current support model. The Contractor shall provide in the Discovery Report the correct number of environments that are needed to support the ITIL Services and tools, DHS SELC/USCG SDLC functions based upon TRIO requirements. The Contractor shall collaborate and coordinate with the hosting provider to create and maintain all FSM Solution environments required to support this task order.

5.18 Discovery Analysis and Report

The Contractor shall provide discovery analysis services to "open, inspect, shakeout, and provide a gap analysis" of the FSM Solution, hardware, software, all supporting artifacts and provide a Discovery Report that defines the current configuration and to determine the "state" of the FSM Solution and needs for TRIO implementation. The following list includes the minimum content requirement of the Discovery Report:

- Identify the configuration items were, and were not received from DOI/IBC;
- Identify configuration items that will need to be re-created/implemented after transition;
- Identify the environments provided by DOI/IBC;
- Determine if environments match what is in production;
- Identify any re-sync requirement for the environments;
- Identify all Standard Operating Procedures received;
- Identify training objectives and validate the strategy for training TRIO users;
- Validate sufficiency of the DOI/IBC maintenance plan;
- Identify any requirement to re-sync DNDO data and baseline;
- Validate interfaces and functional configurations against TRIO requirements, SSP documentation, and DNDO known issues to determine follow-on task order requirements;

- Detailed baseline, rework, TSA/USCG implementation tasks, and recommendations; and
- Identify documentation gaps for the Contractor to assume full lifecycle O&M support.

The Contractor shall evaluate Global Configurations for the TRIO, DNDO requirements, TSA requirements (TSA financial, procurement, payroll (TSAPay), TSA Financial Data Warehouse (TFDW), travel, and property/asset management (Sunflower)), and USCG requirements to ensure traceability to functionality and serviceability. All requirements shall be traceable to identified requirements provided in the Requirements Traceability Matrix (RTM). The Contractor shall review the requirements and ensure completeness.

The Contractor shall validate interfaces (ex. Payroll, Travel, IPAC, PCARD, IPP, etc.) and functional configurations against TRIO requirements, DOI/IBC documentation, and other known issues documents. The report shall include information as detailed above as well as any identified deficiencies or issues found by the Contractor during their open/discovery/ shakeout/gap analysis. The Discovery Report shall include the information detailed above, and identify all interface tasks required to stabilize the solution for DNDO, and to allow work to resume for TSA and USCG implementations. The Government provides the following items as a start, the Contractor shall include additional areas as needed:

- The Contractor shall determine the extent to which the FSM Solution has been customized/enhanced that would impact future upgrades and that would need to be considered for rework;
- Provide estimates required to complete rework, known issues, etc.;
- Provide estimates and timeframes to complete the TSA and USCG implementations;
- Determine if interfaces are implemented using Oracle SOA solution or would require rework to implement using the Oracle SOA;
- Review existing documentation and determine how much needs to be updated;
- Determine if the environments need to be updated and re-synched to production;
- Determine the state of the DNDO, TSA, and USCG development environments; and
- Provide a list of known issues with severity ranking included.

5.19 Section 508 Compliance Requirements

The Contractor shall meet all necessary requirements as identified in Attachment G – Section 508 Compliance Requirements to ensure the FSM solution fully meets Section 508 standards. The existing FSM solution does not fully meet the current Section 508 standards. The current Section 508 Standards have been updated and the Revised Section 508 Standards will become applicable on January 18, 2018. To support the January 18th revision of the Section 508 Standards, the Section 508 requirements in this statement of work are divided into those which must be met prior to January 18, 2018, and those which must be met on or after January 18, 2018.

6 DNDO, TSA, AND USCG STABILIZATION/ REWORK

The DNDO FSM Solution development and implementation has achieved initial operational capability, but is not yet at full operational capability. There will be some additional developmental rework to address current manual work-arounds and other issues, before entering the operations and maintenance phase.

DNDO Stabilization/rework, TSA rework and implementation and USCG implementation will need to be completed after DHS assumes full lifecycle support for the FSM Solution.

6.1 DNDO Rework/Stabilization

The Contractor shall correct/rework/stabilize the DNDO FSM Solution. Rework activities necessary for DNDO stabilization will follow the initial Discovery activities of the project, and will include: fixes in code or configurations and development efforts to redesign, develop, and deploy the RICE-W objects required to stabilize DNDO. Identification of the scope of required rework shall be included in the Discovery Report.

6.2 DNDO Operations &Maintenance (O&M) Support

Upon successful transition of the FSM Solution from DOI/IBC, the Contractor shall be responsible for the DNDO production environment. The Contractor shall provide O&M support for the FSM Solution in support of DNDO. This shall include establishing an SLA for the DNDO support levels as well as updating the maintenance requirements list (MRL).

The FSM Solution modules to be supported, along with the estimated number of users per module, are included in the table below.

Functional Area	**Number of End Users**
Federal Administrator	60
Sourcing	150
iProcurement	150
Contract Lifecycle Mgt (CLM)	150 (this count is for sourcing, iProcurement and CLM)
Inventory	5
Purchasing	10
Accounts Payable	65
Fixed Assets	10
Accounts Receivable	35
General Ledger	75
Project Costing	60
Project Billing	20
Advanced Collections	10

Additionally, DNDO support will include OBIA and Kofax Markview.

The DHS OBIA solution includes 'Financial Analytics' and 'Procurement & Spend Analytics'. The design scope limits customization, leveraging Oracle standard/canned solution to support the customers reporting needs. Users access the application using EBS responsibilities integrated with OBIEE. The solution houses a significant number of BI Publisher reports that are displayed on the OBIEE homepage as hyperlinks. The OBIA configuration includes 37 canned reports, 0 custom subject area, 14 out of the box subject areas, and custom objects include 106 BI Publisher reports available to run from hyperlinks displayed on the OBIA homepage.

Further details regarding the Markview configuration can be found in Attachment J.

6.3 TSA Rework/Implementation

The Contractor shall complete the implementation of TSA into the FSM Solution. Testing, primary training, rehearsal data preparation and rehearsal migration shall be completed prior to the end of the third quarter of the federal fiscal year before implementation and transition. Final cutover for TSA and USCG will occur in the first quarter of the fiscal year. TSA notional schedule shows cutover in FY20Q1.

TSA financial, procurement, payroll (TSAPay), Transportation Security Administration Financial Data Warehouse (TFDW), travel, and property/asset management (Sunflower) functionality, serviceability, and traceability are identified requirements in the provided Requirements Traceability Matrix (RTM). Many interfaces and configurations will require verification and potentially modification or development. Discovery will result in a plan to deliver all required remaining work, rework and modifications to deliver full functionality and capability. Remaining functionality and requirements not delivered in the DOI/IBC FSM Solution, but required for TSA to effectively maintain financial management, contract lifecycle management and auditability include, but are not limited to: User Access Management (UAM); Single Sign On (SSO); Sunflower, including integration; the Transportation Security Administration Financial Data Warehouse (TFDW); TSAPay; Contract Lifecycle Management (CLM) Clause Logic Revisions; Configuration of Oracle Complex Purchase Order functionality; Configuration/Development for any Federally mandated requirements between now and go live (ex. PIID updates, OMB Data Act requirements); implementation of required travel interface requirements; Implementation of Oracle SR’s related to the current environment that are delivered in the DOI/IBC FSM Solution; Resolution of outstanding issues that were not resolved prior to acceptance of the application by DHS; modification to the PCARD interface as required for the newly selected DHS PCARD vendor (if required); modification to the existing Oracle configurations to record general ledger transactions at the detail level versus summary level; and other work/re-work necessary.

The Contractor shall develop an executable plan to identify required work and rework necessary to deliver full functionality and capability not received in the FSM Solution delivered by DOI/IBC. (See Attachment D)

6.4 TSA O&M Support

The TSA implementation shall be moved to O&M for support after "go live". The Contractor shall provide O&M support to TSA and shall follow the same protocols/procedures established for DNDO O&M support. The Contractor shall include TSA into the O&M support after implementation. This shall include establishing an SLA for the TSA support levels as well as updating the maintenance requirements list (MRL). This includes the TSA O&M support tasks.

6.5 USCG Implementation

The Contractor shall complete the development and implementation of the USCG on the FSM Solution. The USCG implementation shall commence with deploying CG-LIMS financial, procurement (including MILSTRIP capability) and property functionality, based on the identified requirements in the Requirements Traceability Matrix (RTM), and followed by the remainder of USCG requirements to deploy full USCG functionality, as outlined in Attachment E, including end-user training as part of deployment. CG-LIMS deployment requires the FSM Solution to establish integration no later than FY20Q1. Rework and implementation activities necessary for USCG implementation will follow the initial Discovery phase of the project. USCG notional schedule shows full cutover in FY21Q1. This phased approach shall require the Contractor to support multiple data migrations from multiple source systems. The Contractor shall provide three (3) months of support after USCG implementation.

As part of the Discovery Report, the Contractor shall develop an executable plan to identify required work and rework necessary to deliver full functionality and capability not received in the FSM Solution delivered by DOI/IBC. (See Attachment E)

6.6 USCG O&M Support

USCG implementation shall be moved to O&M for support after "go live". The Contractor shall be required to provide O&M support to USCG and shall follow the same protocols/procedures established for DNDO/TSA O&M support. The Contractor shall include USCG into the O&M support after implementation. This shall include the USCG support levels as well as updating the maintenance requirements list (MRL) to include establishing an SLA for the USCG support level as well as updating the maintenance requirements list (MRL).

6.7 Business/System Availability Requirements

The Contractor shall report downtime for the business application, databases and system interfaces. The Contractor shall coordinate this reporting with the hosting provider. Network and hardware downtime will be reported by the hosting provider. The Contractor shall coordinate with the hosting provider hardware support personnel in executing any downtime event and shall report consolidated downtime for business application, databases and system interfaces supported by the Contractor as well as hardware and network components support by the hosting provider through a single downtime reporting system. The Contractor's business application downtime reporting procedures shall be defined in their business model and detailed in the Program Management Plan.

The Contractor shall communicate/coordinate with the hosting provider to schedule system downtime which shall be communicated in the system downtime report provided to stakeholders and posted to the approved DHS repositories. The Contractor shall work in conjunction with the hosting provider as part of an Integrated Project Team (IPT) to provide support to customers and the FSM Solution. The respective support teams will have their own CM plans that state the processes and procedures for CM of the Configuration Items (CI)/baselines in support of the FSM Solution. There will be times when the Contractor shall be required to follow CM processes of the hosting provider. The Contractor and hosting provider shall work together per the directives set forth in the established Service Level agreements (SLAs). The Contractor shall work with the hosting provider to define, create and maintain the SLA between the two support teams.

6.8 Business Application Availability

The Contractor shall meet the availability requirements for the business applications specified in this task order. The Contractor shall calculate actual business application availability monthly and compare the results of actual performance with the stated requirements in their MPR. The definition of and formula for calculating monthly availability is:

A = [(T - B) / (T - M)] x 100
Where A = availability in percent
T = total minutes in the time period (typically monthly)
M = total minutes of actual downtime for scheduled, approved maintenance in the time period (typically monthly)
B = total minutes of accumulated downtime (actual downtime for scheduled, approved maintenance [M from above] *plus* the total of all actual unscheduled downtime) in the time period (typically monthly).

Note: M reflects only the time the system is actually down for scheduled downtime and does not include any unscheduled downtime. Therefore, the value of M will typically be zero during normal working hours unless scheduled downtime is previously agreed upon with the Government. (See Attachment H).

6.8.1 Scheduled Business Application Downtime

The Contractor shall schedule business application downtime outside the normal working hours for each business application specified in this task order. For each application, the Contractor shall establish and provide in electronic format a schedule of downtime planned to perform preventive maintenance, backups, archiving, application or database upgrades or other activities approved by the Government. The schedule shall be modified as frequently as needed to meet desired performance levels. The Contractor shall also:

- Request Government approval of schedule changes via e-mail at least 24 hours in advance of the implementation of schedule changes
- Schedule system downtime outside the defined normal working hours, local time. Exceptions require prior approval from the Government

- Initiate broadcast announcements to user communities through business application website, electronic bulletin boards, login and sign-on screens, or any other capability or facility that may be provided for such user notifications
- Provide announcements and notifications at least 3 working days prior to scheduled downtime. Announcements shall be for the purpose of communicating advisories to user communities regarding changes in availability of the business application.
- Provide updates to field users if the downtime is expected to exceed the announced time frame.

6.8.2 Unscheduled Business Application Downtime

The Contractor shall respond to unscheduled events or notifications of events that reduce or may reduce the availability of each business application to a level below that required, and shall take corrective actions needed to restore required availability and update documentation affected by the problem correction.

The Contractor shall report unscheduled business application downtime in the MPR. An initial assessment of the downtime even shall be reported to the Government within 24 hours of the downtime event. When a final assessment of the downtime event has been determined, the Contractor shall report their findings to the Government in the MPR. The Contractor shall evaluate trends in unscheduled downtime, recommend improvements to minimize impacts on business application availability requirements, and implement changes as be approved by the Government System CCB in accordance with software maintenance and development specifications.

6.9 System Performance

The system shall adhere to the Key Performance Parameters (KPPs) outlined in Attachment H. With regards to each system parameter, the Contractor shall strive for the objective but at a minimum achieve the threshold. The Contractor shall conduct performance testing to ensure these metrics are continuously being met. The Contractor shall coordinate and collaborate with the hosting provider to conduct this testing and remediate any identified issues. The Contractor shall conduct customer surveys to ensure the users are receiving the expected response times and remediation for issues that arise on a consistent basis. The Contractor shall coordinate and collaborate with other responsible parties (Government and Contractor) to analyze performance issues reported by users by utilizing tools/ appliances to determine where issues exist either in the hardware, network, application, etc, and shall work with the appropriate responsible party to remediate the issue. This Contractor shall work with the hosting provider to meet the KPPs. The Contractor will not be held accountable for performance issues outside of their control, such as hardware and network components.

Note: All KPPs apply universally through DNDO, TSA, and USCG's implementations with the exception of DESIGN: Users. The chart below defines the performance parameters for users through each phase of the implementation.

Component(s)	Total Users	Threshold Concurrent	Objective Concurrent
DNDO	150	50	100
DNDO & TSA	2,000	550	900
DNDO, TSA, & USCG	16,000	1,100	1,700

6.10 Development Methodology

DHS Agile First Policy requires development of new applications and enhancement of existing IT capabilities follows the Agile Software Development methodologies. If the Contractor's development methodology is not Agile, then the Contractor should explain the reasoning for the decision and how their development methodology is better suited for this effort.

The Contractor shall break the work in their integrated master schedule (IMS) into 90 day capability increments. If the Contractor has tasks that do not logically break down to 90 day capability increments, then the Contractor shall provide the reasoning with an explanation for how they intend to show progress on the task to meet the due dates in the IMS.

6.11 Technical Reference Model

The DHS Technical Reference Model (TRM) governs the range of compliant platforms to be utilized to support requirements for this task order. Conformance to these reference models is required in the performance of work described herein and shall be utilized when acquiring tools for this effort. The Contractor shall create all documentation required to insert a new requirement into the DHS TRM. The TRM is available via the Enterprise Architecture Information Repository (EAIR). Once the Contractor is onboard and has a PIV, they will be able to access the EAIR and TRM.

6.12 Service Oriented Architecture (SOA)/Enterprise Service Bus (ESB)

The Contractor shall describe how they would implement SOA for the FSM Solution interfaces. Implementation of SOA and aligning to the USCG's Enterprise Service Bus (ESB) is essential to achieving DHS IT strategic goals and guiding the modernization of DHS system development. Therefore, an understanding of SOA governance in the context of EA and how SOA can be used to elaborate the various EA reference models will be required in completing the requirements of task orders issued under this task order. The Contractor shall support the sharing of data between various Government and Commercial entities using standard protocols that are widely used to send and receive data from other Government and Commercial sources. During the open and inspect tasking, the Contractor shall address the interfaces to include proposing to phase out the traditional point to point integrations that were developed for DNDO.

6.13 Data Exchange Model

The development of a common enterprise data model is critical to an effective SOA implementation strategy. DHS has adopted the National Information Exchange Model (NIEM) as its data exchange model. In the future, this model will govern how the DHS exchanges data both internally (between DHS systems) and externally (with other DHS agencies and systems),

and will therefore conform to DHS data models. The use of established data exchange models will be required in completing the requirements of the task order.

6.14 Industry Best Practices

It is the Government's desire to benefit from industry best practices that will extend the architecture to make DHS IT capabilities more adaptable, agile, interoperable, upgradeable and mission-responsive. The Contractor shall continuously implement and maintain industry best practices for IT software engineering disciplines throughout the performance of this task order.

6.15 Task Order Phase Out

The Contractor shall provide a plan for transitioning work from one Contractor to another. This transition may be to a Government entity, another Contractor or to the incumbent Contractor under a new contract/order. The task order Phase-Out Plan shall be delivered to the Contracting Officer and COR for review no later than 30 days prior to the commencement of the Phase-Out period. The task order Phase-Out Plan shall address, at a minimum, the following items:

- Coordination with Government representatives,
- Review, evaluation and transition of current support services, (i.e., hosting services, etc.)
- Transfer of hardware warranties and software licenses (if applicable),
- Transfer of all necessary business, functional and/or technical documentation,
- Transfer of compiled and uncompiled source code, to include all versions, maintenance updates and patches (if applicable),
- Disposition of Contractor purchased Government owned assets, including equipment, software, licenses, maintenance agreements, etc.,
- Coordination with the Government to account for government keys, ID/access cards, and security codes, and
- All other information as requested by the Government.
- Phase-Out Execution

7 CONTRACTOR PERSONNEL

The contractor shall provide qualified personnel to perform all requirements specified in this Statement of Work. The Contractor shall provide appropriately trained personnel and shall be responsible to ensure that necessary certifications are kept up-to-date in relevant areas.

The Contractor shall notify the Contracting Officer not less than 15 days in advance of replacing any individual designated as key personnel under this task order. The Contractor shall submit written justification for replacement and provide the name and qualifications of any proposed substitute(s). All proposed substitutes shall possess qualifications equal to or superior to those of the key person being replaced and must be approved in writing by the Contracting Officer.

7.1 Key Personnel

The Government has designated the following position as Key Personnel for this task order. Additional Key personnel positions may be included at award.

- Program Manager Level III

The Contractor shall proposal additional Key Personnel with skill sets appropriate to the Contractors technical approach (e.g. Financial and Procurement (CLM) SME, Senior Process Analyst, Senior Database Specialist, Senior Solutions Architect, Senior Test and Evaluation Specialist, Information Assurance Specialist, OCM Consultant, etc.).

7.2 Program Manager Level III (Key Personnel)

The Contractor shall provide a Program Manager who shall have full decision making authority over Contractor staff and be responsible for all Contractor work performed in accordance with the FSM Solution task order. The Program Manager shall be the single point of contact for the CO and the task order COR for technical matters. The name of the Program Manager and the name(s) of any alternate(s) who shall act for the Contractor in the absence of the Program Manager shall be provided to the Government. During any absence of the Program Manager, only one alternate shall have full authority to act for the Contractor on all matters relating to work performed under this task o

8 REPORTING REQUIREMENTS

The Contractor shall provide all written reports in electronic format with read/write capability using applications that are compatible with the current DHS, DNDO, TSA, and USCG Standard Workstation Windows and Microsoft products.

Due to DHS/DNDO/TSA/USCG Internet restrictions, the Contractor shall load all deliverables to the Government furnished portal site and shall notify the COR via email of submission of the deliverables.

8.1 DHS Program and SELC Documentation

The Contractor shall provide the program and system documentation that supports the FSM Solution efforts. The Government intends to collect the documentation as a tool for becoming familiar with the solution, as well as, planning and measuring the level of effort required to prepare for respective Department’s acquisition program and/or engineering oversight reviews.

The Contractor shall cross reference their documentation to the appropriate Government deliverable for each stage and review cycle found in Attachment F: Applicable Documents, Definitions, and Federal Regulations. The required documents will be based upon the Government SELC Tailoring Plan provided and the DHS SELC/USCG SDLC phase.

In addition, the Contractor shall support the Government's efforts to produce Technology Insertion packages/documentation regarding elements of the FSM Solution target architecture's alignment and compliance with the DHS Technical Reference Model (TRM) of approved software.

The Contractor shall provide an overview of the IT service management high level hierarchy and processes that demonstrates how the JPMO and Contractor will provide support services to the FSM Solution customers.

8.2 Weekly Status Reports

The Contractor shall provide a weekly status report and briefing; at a minimum the report shall include the items listed below:

- All activities by technical/functional area
- Updates to the IMS
- Cost, Schedule and Scope Performance Metrics and Forecast
- Deliverables submitted to the DHS COR
- Outstanding deliverables
- Deliverables due for the next reporting period
- Risks and mitigation plans
- Issues and action items
- Recommendations for improved service
- Staff changes

The Contractor shall document minutes at the completion of each weekly briefing.

8.3 Monthly Progress Report

The Contractor shall ensure that a Monthly Progress Report (MPR) is developed and is submitted to the COR no later than the 5th business day of the month. The Government will provide a MPR Template to the Contractor, which follows a quad chart format. Changes proposed to the format by the Contractor shall be approved by the COR. The Contractor shall schedule, present, and facilitate a Monthly Review Meeting where the MPR shall be presented to the Government and Stakeholder SMEs. The MPR provides the Government with visibility into the overall support for the FSM Solution and provides an opportunity to discuss issues, schedules, scheduled tasks, etc. At a minimum, the MPR will include:

- System availability and downtime metrics
- Active and future projects with status
- Cost, Schedule and Scope Performance Metrics
- Project risks
- Monthly accomplishments
- Upcoming activities
- System architecture diagrams

- Security and C&A compliance
- KPP achievement (Attachment H)

8.4 Quality Control Plan

The Contractor shall develop and maintain a Quality Control Plan (QCP) describing the set of procedures used to ensure that services provided will meet the quality goals at the best value to the Government.

The QCP identifies the planned approach, activities, and approvals required to assess and validate project products and deliverables against requirements. The QCP shall describe how the Contractor will meet and comply with the quality standards established in the Contractor's QCP. At a minimum, the QCP must include a self-inspection plan, proposed performance metrics, staffing plan, and an outline of the procedures that the Contractor will use to maintain quality, timeliness, responsiveness, customer satisfaction, and any other requirements set forth in this

8.5 Quality Assurance Report

The Government will audit the Contractor by the quality standards established in the Contractor's QCMP and QCP. The Contractor shall create a Report within five (5) days after the audit. The report shall summarize the quality review activities that occurred, the trends and issues that were identified and provide recommendations for corrective actions. The Contractor shall provide the report to the Government for review and approval within five (5) days after the audit. Corrective actions shall be incorporated into the QCMP and QCP within fifteen (15) days after approval by the Government.

8.6 Program Management Plan

The Contractor shall develop a Program Management Plan (PMP) for the task order which addresses each of the Program Management knowledge areas listed previously. Following Government approval, the PMP shall be applied by the Contractor to manage, track, coordinate, and evaluate the Contractor's performance for all task orders issued. For all tasks exercised to support the FSM Solution and Program, the PMP shall be updated to incorporate those requirements. The planning and control policies and procedures should address identification of milestones, dependencies and critical path items where Government information or activity is required as well as identification of timeline dependencies for subsequent Contractor activities. The PMP must also identify the Contractors program management structure and program management strategy. The plan shall consist of control policies and procedures in accordance with standard industry practices found in Program Management Body of Knowledge (PMBOK) for project administration, execution and tracking, and shall include the following:

- Be CMMI Level 3 certified
- Capability to Implement ITIL IT Service Management.

The Contractor shall update the PMP quarterly.

8.6.1 Work Breakdown Structure (WBS)

The Project Management Plan shall include the Contractors WBS. The Contractor shall develop the WBS based upon their proposed development methodology. The WBS shall provide a common thread for the IMS, allowing consistency in understanding program cost and schedule performance. The Contractor shall be responsible for making all updates to the WBS (and IMS) to ensure consistency between each WBS created for individual tasks. The government shall have visibility into the first three WBS levels.

8.7 Change Management Plan

The Contractor shall provide a Change Management Plan that addresses the change process methodology and model; process flows, diagrams and timelines; the activities in driving the change, communicating and capturing the change; and the approach to measuring and monitoring change. The Change Management Plan shall include the following detailed planning documents to support the execution of the technical activities of the FSM Solution program such as:

- Stakeholder Analysis
- Engagement Plans
- Organizational Impact Assessments
- Role Definition and mapping
- Communications Management
- Training Plans

8.8 Risk Management Plan

The Contractor shall collaborate with the Government and incorporate their details and processes to provide a consolidated Risk Management Plan. The plan shall follow PMBOK standards to detail the processes used to identify, document, analyze, track, prioritize, mitigate, monitor, and report project risk throughout the system engineering life cycle (SELC). The plan must align with the FSM Solution JPMO's Risk Management Plan. The Contractor shall provide the Government with electronic access to any proposed risk management tools and requisite training on these tools.

9 PROGRAM MANAGEMENT

The Contractor shall ensure the full and complete integration of Contractor Program Management processes with DHS Program Management processes for this task order. To support the work required on this task order, the following program management knowledge areas are required:

- Transition/Integration Management
- Quality Management
- Project (Schedule and Scope) Management

- Human Resources Management
- Communications Management
- Change Management
- Risk Management
- Earned Value Management (EVM)
- Cost & Procurement Management

The Contractor shall be responsible for implementing, managing, measuring, and participating in all internal and external processes necessary for the adequate execution of all activities described in this task order. The Contractor shall provide, implement and maintain the requisite organization, disciplines and certifications necessary to manage the personnel and resources required to complete the tasks required to support the FSM Solution and Program.

9.1 Transition/Integration Management

The Contractor shall coordinate with DOI/IBC, the hosting provider, and the Accounting Operations Provider (USCG FINCEN) to ensure that there is no disruption of DHS DNDO, TSA and USCG missions during FSM Solution and task order transition. The Contractor shall add the required tasks and details to complete the transitions to the FSM System Transition Plan (FSM STP) as required supporting the systems, environments, O&M support, etc. transfer to the appropriate DHS support entities. The FSM STP is an evolving document that requires the Contractor to coordinate with the incumbent contractor (DOI/IBC), the hosting provider, and the FINCEN in order to transition the FSM Solution from DOI/IBC to DHS support structures. As such, the Contractor shall update their portion of the plan as required to ensure the final product is executable. Once the plan is finalized, the Contractor shall work with the other support entities to execute the plan.

The Contractor shall notify the JPMO Program Manager and COR in writing when the transition is complete and will confirm that they have assumed full responsibility for the software engineering tasking detailed in the task order. The Contractor shall ensure the completion of the following tasks as part of the task order Phase-In:

- Develop and Execute/Complete Operational Familiarization Demonstrations (OFDs) documents to support all systems/applications and new functions to existing system being supported by this Contractor prior to the conclusion of the task order phase-in period. OFDs provide the Government with assurance that the Contractor has all the documentation in place to maintain support, can execute the processes/procedures that are required for O&M support, and the Contractor has demonstrated their knowledge of the system such that they are able to “take over” the O&M support for the entire system including all environments used for sustainment, rework, and implementation, etc. In the event of an error or conflict in the OFD scripts, the COR, or his or her designate, will determine the validity of the error, and if deemed necessary and appropriate, waive or modify the specific OFD performance requirement in question. The OFD shall be included as a task in the System Transition Project Management Plan and shall be updated as required.(See Attachment I)

- Upon successful completion of OFDs and written approval from the COR in coordination with the JPMO Program Manager, the Contractor shall assume full responsibility for the services specified in this task order.

The Contractor shall ensure the full and complete integration of Contractor Program Management processes with DHS PMO operations. The Contractor shall likewise ensure proper coordination with DOI/IBC, the hosting provider, and USCG Finance Center (FINCEN) to ensure that there is no disruption of DHS missions during FSM Solution lifecycle support transition.

9.2 Quality Control Management Program

The Contractor shall develop and adhere to a Quality Control Management Plan (QCMP) for measuring and attaining quality of performance to ensure products or services are designed and produced to meet or exceed customer requirements under all task orders supported by this Contractor. The Contractor's QCMP shall explain the manner in which the Contractor shall ensure all requirements are being accomplished in accordance with the specifications of this SOW against industry standards.

A sustaining focus throughout the QCMP shall be the attainment of continuous quality improvement. The QCMP shall emphasize deficiency prevention over deficiency detection. The Contractor's QCMP and any services performed will be accepted by the COR only when in full compliance. The Contractor shall demonstrate a concerted effort in improving its QCMP to prevent unsatisfactory performance from recurring in any area and to ensure unsatisfactory performance is addressed and rectified in a timely manner.

9.3 Project (Schedule and Scope) Management

The Contractor's project management model shall address overall tasking and DHS SELC compliance for both development/enhancement and sustainment support activities covering the FSM Solution and Program requirements to ensure that all program support structures are in place and software engineering projects are completed on schedule, within scope and meet established performance, availability and functionality requirements.

9.4 Engineering Tasking

All project initiation or kickoffs and all final product deliverables to be implemented in production will require a Government review and approval. Further, the Project or Release deliverables to production are required to follow the rigor of Configuration Management and must receive Government approval before the engineering change will be introduced to the production environment in a planned and supervised manner. The Contractor shall provide engineering tasking and release notes for all change introduced to production.

9.5 Integrated Schedules

The Contractor shall develop and maintain a comprehensive integrated master schedule (IMS) covering the full scope of this task order. The Contractor shall report any changes to the IMS during the Weekly Status meeting. The IMS should include, but not limited to, resource loading, baselining capability, critical path identification, 90 day increments, and traceability to the Contactor WBS. The Contractor shall ensure that all parties involved in any engineering or sustainment support tasks are engaged via coordinated communication using an integrated schedule to accomplish the tasking. This includes parties not only working directly for the Contractor but also the other Contractors and their staffs that may be supporting other aspects of the DHS' mission and IT capabilities. The Contractor shall ensure that appropriate integrated schedules are used to ensure that communication and coordination is accomplished within the Contractor's assignment of tasking. The Contractor shall further ensure that the appropriate integrated schedule is used to ensure communication and coordination for dependent work they may be producing that affects other DHS Contractors or for other dependent work the Contractor is expecting from the other DHS Contractors/service providers to ensure successful accomplishment of assigned tasking.

9.6 Communications Management

The Contractor shall provide a communications strategy that supports the FSM Solution and Program. The communications strategy shall be used to inform the appropriate stakeholders affected by the FSM Solution and Program availability, implementation, defect resolution, change requests, change in service requirements, status of projects, etc.

9.7 Executive Management and FSM Solution ESC Reports/Briefings

The Contractor shall assist the DHS JPMO with creating and providing reports and metrics of program and project level schedules and updates to Executive Management and other stakeholders as appropriate. The Government will provide clarification on executive management reporting requirements prior to any action taken by the Contractor.

The Contractor shall provide the materials and facilitate an in-person overview of the FSM Solution to the FSM Solution Executive Steering Committee (ESC) as required to inform on the progress and status of the FSM Solution effort.

The Contractor shall assist the Government with executive management reports, briefings, acquisition and DHS SELC stage reviews, FSM Solution overviews, Integrated Baseline Reviews, and completed documentation as required to support reviews.

Some meetings are held ad hoc while others are weekly, bi-weekly, monthly, quarterly, semi-annually, or annually.

9.8 Acquisition, Program & Engineering Oversight Reviews and Governance Support

The Contractor shall actively participate in the Department's acquisition, program and/or engineering oversight reviews. The Contractor shall assist DHS with:

- Creating, editing and updating planning documents and lifecycle deliverables as required for stage review entrance and exit criteria, which will be used as inputs to the oversight reviews
- Coordinating DHS activities associated with the respective oversight reviews
- Creation of documents and assisting with activities in support of DHS governance boards
- The DHS efforts in complying with the Department policies.

9.9 Integrated Baseline Review (IBR)

The Contractor shall support the Government's program manager in IBRs to analyze the risks inherent in the task order planned performance measurement baseline. The Government will provide the Contractor with a proposed agenda for each IBR to assist the Contractor in planning for the IBR. Each IBR should verify that the Contractor is using a reliable performance measurement baseline which includes the entire task order scope of work, is consistent with task order schedule requirements, and has adequate resources assigned. The Contractor shall provide meeting minutes at the completion of each IBR. The initial IBR shall be held two weeks after task order award. Recurring IBR's are expected to be held every three (3) months or as requested by the Government. In support of ongoing IBR's, the Contractor will provide monthly EVM-like metrics for consolidation and analysis by the JPMO.

9.10 Change Management

The Contractor shall provide a change management strategy and structured approach that ensures changes are smoothly and seamlessly implemented to achieve lasting benefits for DHS and its Components. Change directly affects all of DHS from the entry level employee to the senior management. The approach proposed by the Contractor shall take into consideration what each level of the organization needs to transition to the FSM Solution and to ensure customer support agreements are being achieved.

The Contractor shall support the DHS JPMO in the strategy, creation, implementation and dissemination of Government approved communications. As the Department executes change management activities (e.g. implementing service delivery, service management, and governance processes) the Contractor shall be responsible for assisting the DHS JPMO with Departmental, Component, leadership, and stakeholder communications. The Contractor shall schedule and provide monthly progress review meetings with the stakeholders to discuss support structures being implemented/maintained, progress for implementations, and issues defect resolution. The Contractor shall provide the DHS JPMO with:

- The planning, design, development, and implementation of all FSM Solution program and project communications initiatives and materials

- Coordinating FSM Solution communications activities with all relevant stakeholders internal and external to the program
- The development and delivery of oral and written presentations and reports to multiple levels of management, including executive leadership
- The Contractor's communication efforts shall work in conjunction with the Government's Change Management Team(s).

9.11 Risk Management

The Contractor shall perform Risk Management in order to identify, categorize, color code, assess, and prioritize the project and program risks. Several risk management standards have been developed, including standards created by the Project Management Institute, the National Institute for Science and Technology, actuarial societies, and the International Organization for Standardization. The Government will be the final approval entity of all entries, ratings, changes, and deletions of risks.

9.12 Risk Register

The Contractor shall provide, maintain and manage a risk register identifying risks and provide organizational risk assessments which shall be included in the weekly status and monthly project review meetings. The Contractor shall use the risk register in conjunction with the overall risk management strategy to identify, analyze and manage risks. The risk register will contain information on project risks that the project team identifies and will be updated as changes in project tasking effects overall risk assessments. The project team shall consider the extent to which the effects of risks affect the baseline duration estimate for each schedule activity, particularly the risks with high impact.

9.13 Performance Reporting

The Contractor shall provide monthly performance metrics regarding scope, cost, and schedule. The Contractor shall rely on industry standards and best practices for monthly EVM-like submission.

9.14 Cost Management

The Contractor shall track costs associated with development, modernization, and/or enhancement (DME) projects separate from operations and maintenance costs. The Contractor shall provide DME costs to the Government at the conclusion of implementation of the DME build to production. Costs include labor costs, sub-Contractor costs, etc. and shall be tracked and reported in accordance with Federal Accounting Standards Advisory Board Statement of Federal Financial Accounting Standards Number 10 (Preliminary design costs, Development costs and post implementation costs) and cite payment terms. The Government uses this cost information to track and support asset capitalization requirements for IT systems. The Contractor shall support additional reporting based on future Government requirements, which will be based on OMB A-11.

9.15 IT Service, Business, and Operations Management and Governance

The JPMO is responsible for providing support services to customers and governance for the FSM Solution. The JPMO will establish the services and governance structures that will be used to manage the FSM Solution and provide continuous support to its customers. The JPMO has chosen to implement ITIL service framework to support their customers and establish the IT governance.

The Contractor shall implement the IT Infrastructure Library (ITIL) IT Service Management, IT Business Management, and IT Operations Management services/business support functions and define the services required to provide support and governance for the FSM Solution. The Contractor shall coordinate with the Government to design, develop, and implement the IT Service, Business, and Operations Management services/processes. The Contractor shall ensure all ITIL processes work together in a seamless way, provide adequate industry-standard and ITIL Best-Practices compatible with DHS provided tools. The Contractor shall defined and agreed to ITIL processes, make sure the ITIL processes are sufficiently documented using Business Process Modeling Notation (BPMN), and provide continuous improvement process cycles.

The Contractor shall show where the DHS SELC aligns to the ITIL services/processes. All defined ITIL services shall be approved by the Government prior to implementation. All changes proposed shall be reviewed and approved by the Government. The Contractor shall maintain the IT Service, Business, and Operations Management baseline, as well as identify and track artifacts and configuration items.

9.16 IT Engineering Activities

The Contractor shall provide the full range of software engineering services required to develop/deploy, operate, maintain, update and enhance business applications and GOTS/COTS software integration in accordance with the DHS SELC. The Contractor shall perform engineering integration across all software components developed, hosted and/or maintained by DHS to ensure the integrity and compatibility of the applications with DHS enterprise architecture requirements.

The SELC/SDLC Phases provide deliverables that are due or updated during the various DHS SELC/USCG SDLC phases. However, while the DHS SELC/USCG SDLC uses the Waterfall method of development, the Government expects the Contractor to take into consideration their proposed development/deployment methodology to propose the right frequency and timeframe for the DHS SELC/USCG SDLC required deliverables. The Government expects the Contractor to consider a more customer, proactive approach to completing the work in this task order, by proposing a methodology that involves the customer up front and allows for quick corrections to assumptions and design and mitigates the risk of trying to deliver the entire solution for any agency all at once where the user is only involved at the end during user acceptance testing. The Government expects the Contractor to address how they will ensure design/configuration choices meet customer expectations before the final user acceptance testing. The Contractor shall

address how they will include the customer from requirements to design to testing to implementation to ensure design/configuration choices are correct resulting in high customer acceptance of the system.

9.17 Systems Engineering

The Contractor shall ensure the FSM Solution systems, services and capabilities developed, hosted and maintained by DHS fully support mission requirements, objectives and customer service agreements. The Contractor shall provide systems engineering activities conducted in accordance with their proposed business model and development methodology. The Contractor shall include in their methodology the following systems engineering services:

9.18 Technology Exploration

The Contractor shall provide resources to identify and research emerging technologies in the IT arena. Based on this research, the Contractor shall architect prototype solutions and present findings and recommendations to the Government for their consideration.

9.19 System Design, Development & Deployment

The Contractor shall provide an integrated system architecture and designs to meet all system requirements, to include incorporation of appropriate DHS infrastructure components. The Contractor shall include how they will assess all system engineering change requests, maintain a current assessment of all new, pending and active projects for each system, and provide systems coordination with external systems and development agencies utilizing components and services provided via DHS supported systems and infrastructure.

9.20 System Operations & Maintenance (O&M)

The Contractor shall perform operations and maintenance on all business applications developed, deployed and/or maintained supporting the FSM Solution, and how they shall maintain operational services in accordance with project specific requirements. The Contractor shall provide IT support on 24-hour per day by seven days per week basis for sustainment activities.

9.21 System Documentation

The Contractor shall review the FSM Solution existing documentation and shall develop, update, and maintain all documentation supporting the FSM Solution. The Contractor shall conduct review sessions with Government personnel to review draft documents and capture change requests and final review comments which shall be included in the final technical documentation deliverables.

9.22 System Configuration Management

The Contractor shall ensure source code and binary compiles/builds are maintained in the Government designated code repositories and technology transfer and export documentation,

rules, and regulations have been completed for each version of software, in accordance with the DHS SELC policy. The Contractor shall ensure compliance with appropriate processes and the overarching DHS JPMO Program. CM activities to be performed include:

- Preparing software builds for integrated development testing and delivery
- Providing accessibility, control, and traceability of build and version history
- Ensuring definitive control of executable operational configurations.

The FSM Solution Contractor shall propose their methodology to ensure source code and binary compiles/builds are maintained in the Government designated code repositories and technology transfer and export documentation, rules, and regulations have been completed for each version of software, in accordance with the DHS SELC policy.

DHS contractor support under an existing Independent, Verification &Validation (IV&V) task order will be performing IV&V, Configuration Management Audit (CM Audit) and Quality Assurance (QA) Services to monitor and report on activities supporting this task order.

9.23 System Analysis

The Contractor shall perform system analyses, trade studies and assessments to determine options and recommendations for system capabilities, design and development, and provide level of effort, recurring sustainment cost estimates, risk analysis and impact assessments for all system changes and upgrades requiring Program Change Control Board (P-CCB) and System Configuration Control Board (S-CCB) approvals. The Contractor shall determine system functional element interrelationships and interactions, predict system performance and compare competing design alternatives.

The Contractor shall ensure proposed extensions / enhancements are reviewed/approved by the Government prior to work start. The goal for the Government is to ensure updates/upgrades can be accomplished while sustainment recurring costs are minimized.

9.24 System Risk Analysis

The Contractor shall provide a detailed risk analysis/assessment and define risk mitigation processes to provide overall system risk management to support continual identification and assessment of technical, schedule, cost, security and organizational risks involved with the operation of systems.

9.25 System Testing

The Contractor shall perform system testing of software or hardware on a complete, integrated system to evaluate the system's compliance with its specified requirements. System testing shall include all of the "integrated" software components that have successfully passed integration testing and also the software system itself integrated with any applicable hardware system(s).

The Contractor shall identify, test, and remediate defects both within the "inter-assemblages" and also within the system as a whole.

The Contractor shall also provide Components access to “sandbox” environments that mirror the instance to be tested with respect to functionality, configuration, and data. The sandbox environment shall be at least 30 days prior to User Acceptance Testing based upon the agreed upon schedule.

The Contractor shall assist the Government with creating User Acceptance Testing scripts to include providing training to the Government on the application as necessary for new functionality and/or changes to the application/system. The Contractor shall develop and conduct system engineering acceptance tests as required, technology assessments, system upgrade analysis and testing, concept prototyping, product evaluations, and human/computer interface evaluations.

The Contractor shall also submit a User Acceptance Test Plan for DHS approval and incorporate inputs from the OTA who may require (operational test and evaluation (OT&E) data to support integrated DT/OT testing in accordance with the approved TEMP.

9.26 Technology Integration

The Contractor shall assess the potential usefulness of industry technological advances in improving efficiency and/or reducing cost, and maintain knowledge on new and existing technologies relevant to DHS and DHS systems and operations. The Contractor implement technology integration to improve system reliability, scalability, interoperability, and performance.

9.27 System Fielding/Deployment

The Contractor shall provide all support for the fielding of new systems and new, enhanced or updated system capabilities, as required. On a limited basis, the Contractor may be required to travel to a deployment site in support of fielding a new system or new system capability.

The Contractor shall prepare and distribute release notes detailing the contents of the release package, to include descriptions of systems enhancements, bug fixes, data corrections, and hardware and software updates. The Contractor shall maintain version tracking of all software and hardware releases consistent with the DHS/USCG Configuration Management Policy.

9.28 System Training

The Contractor shall create and maintain a Training Plan. The Contractor shall provide all application training to the Customers. All travel in support of system training must be approved in advance by the COR and CO. The specific training requirements and locations will be determined by the Government in the task orders.

10 TECHNICAL FIELD SUPPORT

The Contractor shall provide Tier 3 and Tier 4 (COTS Vendor coordination) Help Desk services to customers. The USCG Finance Center (FINCEN) is the business operations support center for all three TRIO agencies and will provide Tier 1 and 2 help desk support.

The Contractor shall provide technical field support and help desk to the customer. The Contractor shall include strong emphasis on customer and stakeholder satisfaction, cooperation between Government and all Contractors supporting the FSM Solution, delivering all work products in accordance with the Contractor's proposed timelines and agreed to project plans, identifying issues with potential solutions, and problem resolution at the lowest level possible for successful support and implementation of the FSM Solution.

The Contractor shall include how they will provide technical field support for all business applications detailed under this task order. The Contractor shall coordinate with the USCG Finance Center (FINCEN) Tier 1 and 2 Help Desk, as appropriate, for problem resolution for field users to diagnose and correct systems issues experienced in the field. The Contractor shall:

- Populate a Knowledge Management database to attain metrics for Tier 1 support and provide an automated solution for user access and password resets. All Contractors' resolution specifics shall be captured in the Knowledge Management tool/database.
- Coordinate with the Functional and Technical SMEs for ticket resolution at Tier 1 support to attain the metric that tickets are resolved at Tier 1 support 85% of the time within 24 hours of ticket receipt. If the Tier 1 support cannot resolve the issue, the trouble ticket will be escalated to Tier 2, which is the USCG FINCEN Business Operations Group or Tier 3 for Contractor's resolution depending upon the type of issue.
- Track tickets to conclusion.
- Provide metrics to show Help Desk performance.
- Attain a customer service satisfaction rating of at least 80%.
- Coordinate with the Commercial-off the Shelf (COTS) vendor for Tier 4 support. This type of support would require the COTS vendor to provide a patch to the COTS product.
- Ramp up Help Desk support for DNDO, TSA and USCG based upon the projected usage. Average monthly ticket submission for the Trio follows:
  - DNDO – 30 FSM Solution – Start immediately after the Contractor assumes full responsibility for the FSM Solution

Ticket Aging Total of 44 since 10/1

a. >30 days = 7 16%
b. 16-29 days = 6 14%
c. 7-15 days = 15 34%
d. 0-7 days = 16 36%

  - TSA – 307 – based on current CAS Suite – Begins after implementation
  - USCG – 3,800 – based on current CAS Suite – Begins after implementation

The Contractor shall provide a "Rapid Response" Team capability to address priority 1 and 2 issues (user is unable to continue) and/or business operational knowledge issues that prevent business operations from meeting critical business events. Priority/Severity 1 and 2 issues are issues that have no work around or a work around that can only be completed by the technical team and is a temporary solution that requires an emergency release to correct the issue. The Contractor methodology shall be captured in their System Configuration Management Plan (S-CM Plan) that shall align with the Program Change Management Plan (P-CM Plan).

11 INFORMATION ASSURANCE (IA)

The DHS IA program and associated consultation services will be managed under the DHS CISO Information Assurance contract vehicle, in conjunction with TRIO CISOs, in order to ensure that IT investments managed by the DHS meet the requirements of the Federal Information Security Management Act (FISMA), and Federal Managers' Financial Integrity Act (FMFIA). The IA consultants will guide the IT systems developed, hosted and maintained by DHS through the Security Authorization Process, provide oversight and assistance to the Contractor on this task order with on-going computer security functions, and provide consultation in the development and maintenance of disaster recovery capabilities.

It is the responsibility of the Contractor on this task order to ensure that all software enhancement and maintenance activities provided for under this task order are compliant with DHS Information Security Policy, DHS 140.01 as implemented by DHS MD 4300A Sensitive Systems Handbook and DISA STIG. The Contractor shall conform to these IA requirements to include ensuring that all appropriate Contractor personnel achieve and maintain required IA professional certifications as detailed under DoD 8570.1 for the Information Assurance Technical (IAT) and Information Assurance Workforce System Architecture and Engineer (IASAE) specialties.

The task order Contractor shall create and maintain any and all documentation required by DHS CISO and DHS MD 4300A to obtain an Interim and Full Authority to Operate (ATO). The Contractor shall provide a certified Information Systems Security Officer (ISSO) to collaborate and coordinate with DHS CISO to complete the documentation required on this task order for an ATO. The ISSO shall perform all Information Assurance tasks to ensure the FSM Solution maintains its ATO. The Contractor shall coordinate with the hosting provider to run application vulnerability scans on the system as required by DISA and DHS. The Contractor shall provide Plan of Action and Milestones (POAMs) to remediate issues found and track/report the completion of the POAMs that result from the scan. The Contractor shall include the security findings metrics in their Monthly Progress Report. The Contractor shall create a Risk Acceptance Memo (RAM) for Authorizing Official (AO) signature and acceptance for POAMs where the JPMO Program Manager recommends accepting the risk and has gained agreement from the FSM Solution Authorizing Official (AO) and the DHS CISO. The Contractor shall provide ATO data to the OTA in order to assist them in evaluating the operational cyber security of the solution. The contractor shall support the DHS OTA with preparation, conduction, and analysis of the OTA's cyber security threat based penetration testing in the production or production like environment.

12 DISASTER RECOVERY AND BUSINESS CONTINUITY (DRBC)

The Contractor shall be responsible for the DRBC program and shall coordinate with the DHS Component business operations subject matter experts (SMEs) and future infrastructure hosting provider to ensure the DRBC program is defined, documented, and exercised in accordance with DHS policy. The Contractor shall support exercising annual Contingency Plans for each system developed, deployed and maintained by DHS.

The Contractor shall develop specific contingency and disaster recovery plans relevant to each business application, and shall incorporate those plans into the DHS's overall DRBC planning structure. The Contractor shall coordinate testing of each plan with the future infrastructure hosting provider and business operations subject matter experts (SMEs) at least annually, or more frequently if so required by the plan, and shall perform a full evaluation of each test at its completion, making recommendations for improvements or modifications to existing plans, infrastructure (hosting agreements) or procedures as appropriate. The Contractor shall maintain business application processes, policies and procedures related to preparing for recovery or continuation of critical business application functionality. The amount of time to cutover to DR shall be 48 hours.

12.1 System Recovery Support Services

The Contractor shall provide personnel resources to ensure a system recovery capability that will support Government goals and objectives in accordance with established system availability requirements. At a minimum, the Contractor shall provide the capability for primary and backup systems to support recovery of all critical software programs and sensitive Government information.

The Contractor shall describe how they will coordinate an enterprise systems recovery support services plan with the infrastructure hosting provider. This plan shall be provided to the Government for approval and updated semi-annually.

12.2 System Downtime

The Contractor shall describe how they will coordinate with the infrastructure hosting provider to report downtime for the business application, databases and system interfaces, execute any downtime event, and report consolidated downtime for business application, databases and system interfaces supported by the Contractor on this task order as well as hardware and network components supported by the infrastructure hosting provider through a single downtime reporting system. Network and hardware downtime reporting shall be included in the Monthly Progress Report (MPR) for overall system availability requirements to Customers. The Contractor’s defined methodology for business application downtime reporting procedures shall be defined in their business model and detailed in the Program Management Plan

12.3 Software Engineering

Software engineering includes analysis, requirements, design, development, testing, installation, implementation (deployment), and operations and maintenance activities which support the configuration, creation and maintenance of software required to meet new or modified functional requirements resulting from federal law, congressional mandate, or DHS policy and direction. The Contractor shall gather requirements, configure, develop, deploy, implement, maintain, update and change business application and COTS software.

SECTION III – DELIVERY OR PERFORMANCE

1 PERIOD OF PERFORMANCE

The period of performance for this task order encompasses a Base Period of twelve (12) Months, two (2) 12-month Option Periods, and one 11-month Option Period.

2 PLACE OF PERFORMANCE

The place of performance may vary among the Contractor's facilities, DHS headquarters in Washington, DC, DHS Component sites, and DHS service provider sites. Any individual placed in a role that the Government designates as Key under this task order shall be available to be onsite at DHS headquarters in Washington, DC as work requires. The Contractor will be provided temporary office and general engineering space, as required, within the DHS Headquarters facilities or other Government facilities as necessary. Three primary locations will exist for performance of the requirements on this task order with on-site visits to other locations as identified below.

Contractor's Facility. Many of the requirements for this task orders can be performed at the Contractor's facility with on-site visits to the DHS and DHS Component facilities (DHS Headquarters in Washington DC and to locations identified in Section 4.8.1) as necessary to complete the tasks set forth in this task order and all logical follow on task orders.

Government's Facility – DHS HQ. The Program Management support requirements may be performed at the Government's facility to meet the requirements in this task orders. The Contractor Program Manager and a limited number of Key Contractor personnel supporting this task order will be provided temporary "hoteling" type work space at the DHS Headquarters Command located at 300 7th Street SW, Washington, DC 20024 on an as needed basis.

Government's Facility – Non-DHS HQ. A limited number of Contractor personnel supporting this task order may need to be located at other Government facilities to support the requirements on this task order. Contractor performance supporting technical/functional operations and maintenance type tasks may take place at other facilities outside of DHS Headquarters, the Contractor and/or co-location site. The Government and Contractor shall determine which O&M support tasks require Contractor support be located at DHS Component sites. Written approval from the JPMO Program Manager and the Contracting Officer is required prior to executing this need.

3 HOURS OF OPERATION

The Customer Service Level Agreements are required for each Component in the TRIO. The customer SLAs will define the support agreements required by the Components and will drive the operational hours the Contractors is required to support the Customer. For example, support for DNDO is required between the hours of 0630 to 1800. TSA and USCG require support

between the hours of 0630 to 2100 because their users are located throughout the CONUS. Service Level Objectives will be provided to the Contractor from the TRIO for the development and implementation of Service Level Agreements (SLAs) for performance of individual tasks. The SLAs provide both incentives to the Contractor for superior service. The Contractor shall establish metrics that measure the satisfaction of their customers.

There may be occasions when Contractor employees shall be required to work other than normal business hours, including weekends and holidays, to fulfill requirements under this task order.

4 DELIVERABLES AND DELIVERY SCHEDULE

The contractor shall ensure delivery of all draft and final deliverables s in accordance with Deliverables table below. The Government will review all draft and final deliverables to ensure accuracy, functionality, completeness, professional quality, and overall compliance with government policies, regulations, laws, and directives. Written documents shall be concise and clearly written.

The Contractor shall provide all written reports in electronic format with read/write capability using applications that are compatible with the current DHS, DNDO, TSA, and USCG Standard Workstation Windows and Microsoft products.

Due to DHS/DNDO/TSA/USCG Internet restrictions, the Contractor shall load all deliverables to the Government furnished portal site and shall notify the COR via email of submission of the deliverables.

The Contractor shall submit request for change (CR) to the approved/accepted support plans and processes to the CO and COR for approval within ten (10) business days prior to implementation of any changes.

1. Final documentation deliverables shall be provided in hard and soft copy using MS Office products as specified below. Daily, weekly, interim, informal deliverables and working-copy products may be provided by e-mail or disk, as arranged.

2. The government will have ten (10) business days to accept or reject task order deliverables. If a deliverable is rejected and returned to the Contractor for revision, the Contractor shall provide the corrected deliverable within five business days of notification of the request for revision.

3. All Deliverables shall be submitted to the COR identified in this task order. A copy of the Monthly Status Report shall be submitted to the COR and CO.

Table 1 – Deliverables

Deliverable	Requirement	Due Date
Base Period and Option Periods		
Kickoff Meeting	Contractor shall meet with the Contracting Officer, COR, and JPMO to discuss task order Objectives in accordance of the task order SOW	Five (5) business days after task order issuance
Public Trust Forms and Finger Print Cards	The Contractor shall provide a visit request/clearance verification listing for all new employees to demonstrate that a valid SF-85P (Questionnaire for Public Trust Positions) and FD-258 (Finger Print Cards) has been completed for each employee and is kept on-file by the Contractor. This information shall be provided within 14 calendar days of award.	Reoccurring
Non-Disclosure Agreements (DHS Form 11000-6)	Deliver completed, signed Non-Disclosure Agreements for all Contractor employees.	Reoccurring
Government Facility Access List	The Contractor shall provide a revised list of contractor personnel who require access to the DHS, DNDO, TSA, and USCG Components during the course of the task order within 5 days of requiring access in accordance with Section H of the task order.	Reoccurring
Phase-In Project Plan	The Contractor shall provide a Phase-In Project Plan in accordance with the SOW.	Draft 15 business days post-award Final ten (10) business days after Government Review
Staffing Matrix	The Contractor shall provide a Staffing Matrix in accordance with the SOW.	Initially fifteen (15) business days post-award with updates as required
Communications Strategy	The Contractor shall provide a communications strategy in accordance with Section 9.6 of the task order SOW	Initially fifteen (15) business days post-award with updates as required
Travel Request Form	The Contractor shall submit a Travel Request Form for each month when there will be travel in accordance with the SOW.	As Required

Deliverable	Requirement	Due Date
FSM System Transition Plan	The Contractor shall update their portion of the FSM STP in accordance with the SOW 9.1.	As Required
Operational Familiarization Demonstrations (Attachment I)	OFDs are required for all subsequent systems, and new functions to existing systems. OFDs are required for all individuals who assume new positions in accordance with the SOW 9.1.	As Required
Notification in writing of assumption of responsibility for FSM Solution	The Contractor shall notify the Government in writing of the assumption of responsibility for the FSM Solution in accordance with the SOW	Once
DHS Audit Report	DHS Audits shall be coordinated with the Contractor at least five (5) days prior to inspection of the Contractor's quality standards/facility/processes/procedures, etc. The Contractor shall allow the Government Auditors and IV&V Support Personnel access to all information as required to determine the Contractor is following their established quality standards and DHS/TRIO policies, audit requirements, etc. in accordance with the SOW.	As Required - Due five (5) business days after an Audit
Program Management Plan	Complete and deliver an electronic Program Management Plan. This plan will be updated quarterly in accordance with the SOW 8.6.	Draft 15 business days post-award Final due ten (10) business days after Government Review, updates Quarterly
Executive Reports/Briefings	The Contractor shall provide reports/metrics/program-project level schedules and updates to Executive Management and other stakeholders in accordance with the SOW 9.7.	As Required
Acquisition, Program & Eng. Oversight Reviews	The Contractor shall prepare documents required for acquisition reviews in accordance with the SOW.	As Required
Integrated Baseline Review (IBR) Meetings Minutes	The Contractor shall provide meeting minutes at the completion of each IBR in accordance with the SOW 9.9.	Quarterly or more frequent As Required by the Government

Deliverable	Requirement	Due Date
Weekly Status Report	Provide a weekly status report in accordance with the SOW 8.2	Weekly
Monthly Progress Reports and Briefings	Create and deliver Monthly Progress Reports and Briefings for business systems or support areas supported under this task order in accordance with the SOW.	Monthly
EVM-like Metrics/ Data	The Contractor shall provide monthly metrics/ data on scope, schedule, and cost in accordance with industry standards and best practices, SOW 9.9, 9.13.	Monthly
Technology Insertion Packages	The Contactor shall provide Technology Insertion packages/documentation to support proposed IT tools that are not found within the DHS TRM in accordance with the SOW.	As Required
Quality Control Management Plan	The Contractor shall develop and deliver a QCMP to include performance metrics in accordance with the SOW 9.2	Draft 15 business days post-award Final due ten (10) business days after Government Review with annual updates.
Quality Control Plan	The Contactor shall develop and deliver a draft QCP describing how the Contractor will meet and comply with the quality standards established in the Contractor's QCMP in accordance with the SOW 8.4.	Draft 15 business days post-award Final due ten (10) business days after Government Review with annual updates.
Change Management Strategy and Support	Various deliverables in accordance with the SOW.	As Required
Change Management Plan	Provide a consolidated Change Management Plan in accordance with the SOW 8.7.	Initially 15 business days post-award, with annual updates
Risk Management Plan	Create and deliver a Risk Management Plan in accordance with the SOW 8.8.	Initially 15 business days post-award, with annual updates
Disaster Recovery and Business Continuity Plan	The Contractor shall develop specific contingency and disaster recovery plans relevant to each business application	Before delivery of OFD with annual updates

Deliverable	Requirement	Due Date
Disaster Recovery Test Report	The Contractor shall coordinate testing of each plan with the future infrastructure hosting provider and business operations subject matter experts.	As Required
Risk Register	The Contractor shall manage a risk register for identified risks in accordance the SOW 9.12.	As Required
Design ITIL Services – BPMN	Deliver Services and document processes using BPMN in accordance with the SOW 9.15	Contractor to propose timeframes to complete this work
System Availability	The Contractor shall calculate the System Availability and performance, and compare the results of actual performance with stated requirements in accordance with the SOW.	Monthly
Customer Service Level Agreements (SLAs)	The contractor shall provide SLAs in accordance with the SOW 3.0.	DNDO SLA 30 calendar days before assuming O&M support responsibility. TSA 30 calendar before go live. USCG 30 calendar days before go live.
Customer Service Metrics	The Contractor shall provide metrics to measure Customer satisfaction and compare to required level of satisfaction in accordance with the SOW.	Monthly
Phase-Out		
Phase-Out Plan	Create and deliver an electronic Phase-Out Plan in accordance with the task order SOW 6.15.	Once
Government Issued Badges, Identification Cards, Passes, and Vehicle Registrations	The Contractor shall submit a certification to the contracting officer that the Government Issued Badges, Identification Cards, Passes, and Vehicle Registrations have been accounted for all former employees and subcontractor employees. The approved certification shall be attached to the Contractor's final invoice.	Once
IT Security		
IT Security Plan	The Contractor shall provide, implement, and maintain an IT Security Plan in Accordance with HSAR Clause 3052.204-70 Security Requirements for Unclassified Information Technology Resources and NIST Standard 800-171.	Draft within 60 calendar days post-award, Final due 6 months post-award
Security Requirements Not Implemented	The Contractor shall provide in writing to the Contracting Officer any security requirements not implemented at the time of task order award.	Due 30 calendar days post-award

Deliverable	Requirement	Due Date
Program Support Documentation		
System Configuration Management Plan	The Contractor shall provide a System CM Plan in accordance with the SOW 5.7.	Initial 90 calendar days post-award and update as required
Requirements Management Plan	The Contractor shall provide a RMP in accordance with the SOW 5.8.	Initial 90 calendar days post-award and update as required
Data Management Plan	The Contractor shall provide a DMP in accordance with the SOW 5.9.	Initial 90 calendar days post-award and update as required
Data Security Management Plan	The Contractor shall provide a DSMP in accordance with the SOW 5.10.	Initial 90 calendar days post-award and update as required
Information Assurance Deliverables	There are many documents that will need to be created for information assurance. See applicable SOW sections.	As Required to obtain IATO within 90 calendar days and full ATO within 6 months of DHS assuming responsibility of FSM Solution
DHS FSM Solution Policies, Plans, Process, Procedures, Guides, Templates, etc.	The Contractor shall create the JPMO FSM Solution documentation.	Contractor to propose timeframes to complete this work
IT Software Tools, Services, etc. Standard Operating Procedures	The Contractor shall create and deliver SOPs for all IT Software Tools in accordance with the SOW	As Required
IT Software Tools, IT Services, ITIL Framework Services, etc. Training	The Contractor shall configure, create and deliver training for the IT Software tools, IT Services, ITIL Framework Services in accordance with the SOW.	As Required
Discovery Report (Draft)	The Contractor shall provide the Discovery Report in accordance with the SOW 5.18.	Due within thirty (30) calendar days after the FSM Solution is accessible by the Contractor

Deliverable	Requirement	Due Date
Discovery Report (Final)	The Contractor shall provide the Discovery Report in accordance with the SOW 5.18.	Due within sixty (60) Calendar days after the FSM Solution is accessible by the Contractor
TRACI Matrix (Technical O&M)	The Contractor shall create and deliver a TRACI Matrix in accordance with the SOW.	Before O&M OFD sign off
RACI Matrix (Functional O&M)	The Contractor shall create and deliver a RACI Matrix in accordance with the SOW.	Before O&M OFD sign off

The Contractor shall provide the following deliverables to support systems engineering operations during the Development and Testing/Obtain, Implementation/Obtain, and Operations & Maintenance/Produce, Deploy, Support phases of the DHS SELC/USCG SDLC (as applicable) to implement and support the TRIO component. See Sections 5.68 of the task order SOW. These deliverables are updated as the system moves from one phase to the next. New requirements and functionality will also cause updates to existing documentation. See the DHS SELC and USCG SDLC for frequency requirements. Outlined below are some of the more common deliverables. The Contractor shall review the DHS SELC, USCG SDLC .

Deliverable	Requirement	Frequency
Development & Testing/Obtain Phase		
User Support Documentation (Help Files, Tutorials, User Manuals, Oracle UPK)	Create and deliver system specific user support documentation (such help files, tutorials, and user manuals) per Government direction and specifications.	As Required
Operational Familiarization Demonstration (OFD) (Attachment I)	Create, update and perform Operational Familiarization Demonstrations. OFDs are required for all new systems, new functions to existing systems, and all individuals who assume new positions in accordance with the task order SOW.	As Required
Release Candidate Baseline	Create and deliver release notes detailing the baseline functionality to be delivered with the deployment of the new system or new system functionality.	As Required
System Implementation Plan	Create and deliver a System Implementation Plan detailing all activities required to successfully develop and deploy the system or new system functionality.	As Required
System Maintenance Plan	Create and deliver a System Maintenance Plan detailing the system maintenance activities to be	As Required

Deliverable	Requirement	Frequency
	conducted during the course of the task order Performance Period	
System Maintenance Requirements List (MRL)	Create and deliver a System Maintenance Requirements List (MRL) in accordance with the SOW.	As Required
System Documentation Suite	Create and deliver a full set of system documentation	As Required
Test and Evaluation Plan	As required by the Government Program Office, create and deliver a test plan detailing required testing activities, key roles and responsibilities, and schedules/timelines.	As Required
System Test Scripts	Create and deliver test scripts to support testing of the delivered system or new system functionality prior to deployment.	As Required
User Acceptance Test Script	Assist the Government with creating user acceptance test scripts in accordance with the SOW	As Required
Test Report	Create and deliver a report detailing the results of the test execution.	As Required
Section 508 Test Report	Create and deliver a Section 508 Test Report and coordinate updates to the Application with the COTS vendor in accordance with the SOW	As Required
Training Plan	As required by the Government Program Office, create and deliver a Training Plan to support the deployment of the new system or new system functionality.	As Required
Implementation/Obtain		
User Support Documentation (Help Files, Tutorials, User Manuals)	Update baseline system specific user support documentation (such help files, tutorials, and user manuals) as needed.	Incremental updates as needed
Operational Familiarization Demonstration (OFD) (Attachment I)	Update and perform Operational Familiarization Demonstrations. OFDs are required for all new systems, new functions to existing systems, and all individuals who assume new positions in accordance with the task order SOW	Incremental updates as needed
System Maintenance Plan	Update System Maintenance Plan detailing the system maintenance activities to be conducted during the course of the task order Performance Period	Incremental updates as needed
System Maintenance Requirements List (MRL)	Create and deliver a System Maintenance Requirements List (MRL) in accordance with the SOW.	Incremental updates as needed
System Documentation Suite	Update full set of system documentation	Incremental updates as needed
Training Plan	As required by the Government Program Office, update Training Plan to support the deployment of the new	Incremental updates as needed

Deliverable	Requirement	Frequency
	system or new system functionality.	
Operations & Maintenance/Produce, Deploy, Support		
User Support Documentation (Help Files, Tutorials, User Manuals)	Create and deliver system specific user support documentation (such help files, tutorials, and user manuals) per Government direction and specifications.	On-going maintenance/ updates
Operational Familiarization Demonstration (OFD) (Attachment I)	Create, update and perform Operational Familiarization Demonstrations. OFDs are required for all new systems, new functions to existing systems, and all individuals who assume new positions in accordance with the task order SOW.	On-going maintenance/ updates
System Maintenance Plan	Create and deliver a System Maintenance Plan detailing the system maintenance activities to be conducted during the course of the task order Performance Period	On-going maintenance/ updates
System Maintenance Requirements List (MRL)	Create and deliver a System Maintenance Requirements List (MRL) in accordance with the SOW.	On-going maintenance/ updates
System Documentation Suite	Create and deliver a full set of system documentation	On-going maintenance/ updates
System Test Scripts	Create and deliver test scripts to support testing of the delivered system or new system functionality prior to deployment.	On-going maintenance/ updates
System Performance Reports	Conduct periodic system performance reviews to ensure that the system complies with system performance and availability requirements.	Initial plus on-going maintenance/ updates.

SECTION IV - CONTRACT ADMINISTRATION DATA

1 GOVERNMENT FURNISHED EQUIPMENT (GFE)

Government Furnished Equipment (GFE) provided will include access to DHS virtual desktop interface (VDI) or DHS laptops and PIV cards. DHS VDI or laptops(s) will be configured to allow installation of support and/or development tools the Contractor may need to complete the tasks required under this task order. DHS VDI or laptops(s) are required to access the hosting environments. Typical GFE includes: office space, desks, chairs, workstations, telephones, infrastructure, and facilities support.

2 POST AWARD CONFERENCE

The Contractor shall attend a Post Award Conference with the Contracting Officer, JPMO Program Manager, and COR no later than 5 business days after the date of award (or within 10 business days if agreed upon.) The purpose of the Post Award Conference is to discuss technical and contracting objectives of this task order. The post-award conference will be held at the Government's facility or via teleconference. The date, time, and office location will be provided after award.

3 KICK-OFF MEETING

The Contractor's Key Personnel shall meet with the Contracting Officer, COR, JPMO and key stakeholders to discuss the goals for the task order at the Kick-Off Meeting, which will be held five (5) business days after task order issuance at the Government's facility. This meeting will be held to discuss the Phase-In plan, FSM Solution Program, and the goals for the transition, O&M, rework and implementation effort required on this task order. The Contractor shall provide the following task order specific deliverables as draft in their proposal and finalized ten (10) business days after Government review. The Government shall review the documents and provide comments within ten (10) business days of after the kick off meeting.

- Phase-In Project Plan
- Program Management Plan

4 CONTRACT ADMINISTRATION

4.1 Contracting Officer

The Contracting Officer for this task order is:

Ms. Cynthia Aki
DHS Office of Procurement Operations (OPO)
Departmental Operations Acquisition Division (DOAD)
U.S. Department of Homeland Security

Phone Number: (202) 447-5542
E-mail: cynthia.aki@hq.dhs.gov

Copies of all correspondence concerning this task order shall be provided to the Contracting Officer listed above.

4.2 Contracting Officer's Authority

A warranted Contracting Officer is the only person authorized to issue modifications to the task order, approve changes in any of the requirements, or obligate funds. Notwithstanding any clause/provision contained elsewhere in this task order, the authority to modify the task order remains solely with the Contracting Officer. If the Contractor makes any task order changes at the direction of any person other than the Contracting Officer, the change will be considered to have been made without authority and no adjustment will be made in the task order to cover any increases in charges that may result. The Contracting Officer has the authority to perform any and all post-award functions in administering and enforcing the proposed task order in accordance with its terms and conditions.

4.3 Contract Specialist

This task order will be administered by:

Ms. Amanda Aung, Contract Specialist
DHS Office of Procurement Operations (OPO)
Departmental Operations Acquisition Division (DOAD)
U.S. Department of Homeland Security
Phone Number: (202) 447-5214
E-mail: Amanda.Aung@hq.dhs.gov

4.4 CONTRACTING OFFICER'S REPRESENTATIVE (COR)

The COR for this task order is:

[TBD]
DHS Office of the Chief Financial Officer (OCFO)
Office of Financial Management
Joint Program Management Office (JPMO)
U.S. Department of Homeland Security
Phone Number: [TBD]
E-mail: [TBD]

The COR name and contact information will be provided upon task order award.

SECTION V - INVOICE AND PAYMENT PROVISIONS

1 INVOICING

Invoices shall be prepared per in accordance with FAR Clauses 52.232-25 Prompt Payment, 52.232-7 Payments under Time-and-Materials and Labor-Hour Contracts, and 52.232-16 Progress Payments. In addition to invoice preparation as required by the FAR, the Contractor's invoice shall include the following information:

1) Cover sheet identifying DHS;
2) Task order and associated EAGLE II Contract Number;
3) Modification number, if any;
4) DUNS Number;
5) Month services provided
6) CLIN and Accounting Classifications

The invoice shall clearly document by Contract Line Item Number (CLIN) each billed item (Labor Hour [LH], Firm-Fixed Price [FFP], and Travel [T&M],). The Contractor shall invoice monthly, based on the below:

Labor Hour (LH)) - When invoicing for the Labor Hour CLINs, the Contractor shall indicate the associated CLIN and dollar amount invoiced. Supporting documentation shall include labor categories, rates, and hours burned for the billing period; contractor employee name; total cumulative hours to date and dollar amount for contractor employees.

Firm Fixed Price (FFP) – Firm Fixed Price CLINS will be associated with increment based payments aligned to delivery based on agreed upon acceptance criteria and/or definition of done or to milestone payments. The invoicing for FFP CLINS shall align with the Contractor's technical approach to the work as proposed, and the structure of the FFP CLIN invoicing will be mutually agreed upon after award, in accordance with the Contractor's proposed technical approach to the work.

Travel (Reimbursable Cost) – Support for SOW task reference number and task title; identify local or business (TDY) travel; description/purpose of travel, include dates; staff name(s); breakout of all expenses, total travel amount for staff member per trip; total monthly amount for all staff travel grouped by task and total monthly amount for all travel for all tasks.

As appropriate, after award, Labor Hour CLINs may be converted to Firm-Fixed Price CLINs through mutual agreement of both parties, based on the labor categories and rates negotiated at the time of award.

1.1 Invoice Submission

The contractor shall submit one invoice by the 10th business day of each month.

The Contractor shall submit the invoice electronically to the address below:

ATTN: MGTInvoice.Consolidation

E-mail:MGTInvoice.Consolidation@ice.dhs.gov

The Contractor shall simultaneously provide an electronic copy of the invoice to the following individuals at the addresses below:

1) ATTN: Office of Procurement Operations/Amanda Aung (Contract Specialist)

E-mail: Amanda.Aung@hq.dhs.gov

2) ATTN: Office of Procurement Operations/Cynthia Aki (Contracting Officer)

E-mail: Cynthia.Aki@hq.dhs.gov

3) ATTN: Office of the Chief Financial Officer/TBD (COR)

E-mail: TBD

The contractor shall submit invoices to the email address above. Additionally, the contractor shall prepare and submit a sufficient and procurement regulatory compliant invoice and receiving report for technical certification of inspection/acceptance of services and approval for payment. The contractor shall attach back up information to the invoices and receiving reports substantiating all costs for services performed. The receiving agency's written or electronic acceptance by the COR and date of acceptance shall be included as part of the backup documentation.

If the invoice is submitted without all required back up documentation, if required, the invoice shall be rejected. The Government reserves the right to have all invoices and backup documentation reviewed by the Contracting Officer prior to payment approval.

SECTION VI – SPECIAL CONTRACT REQUIREMENTS

1 PERSONNEL QUALIFICATIONS

The contractor shall be responsible for employing technically qualified personnel to perform the work specified in this Statement of Work. The contractor shall maintain the personnel, organization, and administrative control necessary to ensure that the work delivered meets the government's specifications and requirements. The work history of each contractor employee must contain experience directly related to the work he/she is required to perform under this task order.

In addition, the contractor must have the demonstrated ability to reach out to a wide variety of subject matter experts in relevant fields, retain their services, and productively engage them in support of government requirements.

The Contractor shall provide qualified personnel to perform all requirements specified in this SOW Contractors shall ensure all proposed personnel meet or exceed the labor category qualifications as described in their EAGLE, FC1 contract, and that all proposed labor categories are consistent with the Contractors EAGLE II FC 1 contract.

2 DISCLOSURE OF INFORMATION - OFFICIAL USE ONLY

Each officer or employee of the Contractor or Subcontractor at any tier to whom "Official Use Only" information may be made available or disclosed shall be notified in writing by the Contractor that "Official Use Only" information disclosed to such officer or employee can be used only for a purpose and to the extent authorized herein, and that further disclosure of any such "Official Use Only" information, by any means, for a purpose or to an extent unauthorized herein, may subject the offender to criminal sanctions imposed by 18 United States Code (U.S.C.) Sections 641 and 3571. Section 641 of 18 U.S.C. provides, in pertinent part, that whoever knowingly converts to his use or the use of another, or without authority sells, conveys, or disposes of any record of the United States or whoever receives the same with the intent to convert it to his use or gain, knowing it to have been converted, shall be guilty of a crime punishable by a fine or imprisoned up to ten (10) years or both.

3 STANDARD CONDUCT AT GOVERNMENT INSTALLATIONS

The Contractor shall be responsible for maintaining satisfactory standards of employee competency conduct, appearance and integrity and shall be responsible for taking such disciplinary action with respect to his employees as may be necessary. The Contractor is also responsible for ensuring that his employees do not disturb papers on desks, open desk drawers or cabinets, or use Government telephones except as authorized.

In performing on-site work under this task order on a Government installation or in a Government building, the Contractor shall:

Conform to the specific safety requirements established by a task order.

Comply with the safety rules of the Government installation that concern related activities not directly addressed in this task order.

Take all reasonable steps and precautions to prevent accidents and preserve the life and health of Contractor and Government personnel connected in any way with performance under this task order.

Take such additional immediate precautions as the CO or COTR may reasonably require for safety and accident prevention purposes.

4 SECURITY REQUIREMENTS

The work performed under this task order requires employees to complete a favorable fingerprint check and a NACI at a minimum and in some cases a SECRET level clearance. The procedures outlined below shall be followed in order for the DHS Security Office to process background investigations and suitability determinations, as required, in a timely and efficient manner. US citizenship is required for all contractor employees working under this task order.

Carefully read the security clauses in the task order. Compliance with these clauses is not optional.

Contractor employees (to include applicants, temporaries, part-time and replacement employees) under the task order, requiring access to sensitive information, shall undergo a position sensitivity analysis based on the duties each individual will perform on the task order. The results of the position sensitivity analysis shall identify the appropriate background investigation to be conducted. All background investigations will be processed through the DHS Security Office. Prospective Contractor employees shall submit the following completed forms to the DHS Security Office. The Standard Form 85P will be completed electronically, through the Office of Personnel Management's e-QIP SYSTEM. The completed forms must be given to the DHS Security Office no less than thirty (30) days before the start date of the task order or thirty (30) days prior to entry on duty of any employees, whether a replacement, addition, subcontractor employee, or vendor:

- Standard Form 85P, "Questionnaire for Public Trust Positions"
- FD Form 258, "Fingerprint Card" (2 copies)
- DHS Form 11000-6 "Conditional Access to Sensitive but Unclassified Information Non-Disclosure Agreement"
- DHS Form 11000-9, "Disclosure and Authorization Pertaining to Consumer Reports Pursuant to the Fair Credit Reporting Act"
- Only complete packages will be accepted by the DHS Security Office. Specific instructions on submission of packages will be provided upon award of the task order.

DHS may, as appropriate, authorize and grant a favorable entry on duty (EOD) decision based on preliminary suitability 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 a determination that a full employment suitability authorization will follow. A favorable EOD decision or a full employment suitability determination shall in no way prevent, preclude, or bar DHS from withdrawing or terminating access government facilities or information, at any time during the term of the task order. No employee of the Contractor shall be allowed unescorted access to a Government facility without a favorable EOD decision or suitability determination by the Security Office.

Contractor employees waiting for an EOD decision may begin work on the task order provided they do not access sensitive Government information. Limited access to Government buildings is allowable prior to the EOD decision if the Contractor is escorted by a Government employee. This limited access is to allow Contractors to attend briefings, non-recurring meetings and begin transition work.

The Contractor shall notify the DHS Security Office of all terminations/resignations within five (5) days of occurrence. The Contractor shall return to the Contracting Officer Technical Representative (COTR) all DHS issued identification cards and building passes that have either expired or have been collected from terminated employees. If an identification card or building pass is not available to be returned, a report shall be submitted to the COTR, referencing the pass or card number, name of individual to who it was issued and the last known location and disposition of the pass or card.

When sensitive government information is processed on Department telecommunications and automated information systems, the Contractor shall provide for the administrative control of sensitive data being processed. Contractor personnel must have favorably adjudicated background investigations commensurate with the defined sensitivity level.

Contractors who fail to comply with Department security policy are subject to having their access to Department IT systems and facilities terminated, whether or not the failure results in criminal prosecution. Any person who improperly discloses sensitive information is subject to criminal and civil penalties and sanctions under a variety of laws (e.g., Privacy Act).

Failure to follow these instructions may delay the completion of suitability determinations and background checks. Note that any delays in this process that are not caused by the government do not relieve the Contractor from performing under the terms of the task order.

Your POC at the Security Office is:

DHS, Office of Security
Personnel Security Staff
Washington DC 20528
Telephone: (202) 447-5010

5 NON-DISCLOURE AGREEMENT

The Contractor shall submit an executed Attachment B – Non-Disclosure Agreement for each individual performing under this task order. The Contractor shall submit copies of the Non-Disclosure Agreement to the Contracting Officer and COR prior to an individual beginning performance under this task order.

6 ADDITIONAL SECURITY REQUIREMENTS

Contractor access to unclassified, but Security Sensitive information may be required under this SOW. Contractor employees shall safeguard this information against unauthorized disclosure or dissemination. Contractor access to classified information is not currently required under this SOW. However, the Government at a later date may require some contractor personnel to have Secret clearances. Accordingly, all Contractor employees performing on this task order must be eligible for a Secret clearance.

SECTION VII–TASK ORDERCLAUSES

1 INCORPORATED BY REFERENCE

The Contractor's EAGLE II contract clauses are hereby incorporated into this task order. This task order also incorporates one or more clauses by reference with the same force and effect as if they were given in full text. Upon request, the Contracting Officer will make their full text available. Also, the full text of a clause may be accessed electronically at these addresses: https://www.acquisition.gov/far or for DHS specific clauses at http://farsite.hill.af.mil/VFHSARA.HTM

Clause	Title	Date
Additional FAR Clauses Incorporated by Reference		
52.203-13	Contractor Code of Business Ethics and Conduct	Oct 2015
52.203-17	Contractor Employee Whistleblower Rights and Requirement To Inform Employees of Whistleblower Rights	Apr 2014
52.204-2	Security Requirements	Aug 1996
52.204-9	Personal Identity Verification of Contractor Personnel	Jan 2011
52.222-50	Combating Trafficking in Persons	Mar 2015
52.209-10	Prohibition on Contracting with Inverted Domestic Corporations	Nov 2015
52.224-1	Privacy Act Notification	Apr 1984
52.224-2	Privacy Act	Apr 1984
52.227-14	Rights in Data – General ALT IV	
52.228-7	Insurance – Liability to Third Persons	Mar 1996
52.243-3	Changes – Time and Materials or Labor Hours	Sept 2000
52.246-6	Inspection – Time and Material and Labor Hour	May 2001
DHS Clauses Incorporated by Reference		
3052.203-70	Instructions for Contractor Disclosure of Violations	Sept 2012
3052.205-70	Advertisements, Publicizing Awards and Releases	Sept 2012
3052.228-70	Insurance	Dec 2003
3052.242-72	Contracting Officer's Technical Representative	Dec 2003

2 INCORPORATED BY FULL TEXT

FAR 52.217-8: Option to Extend Services (Nov 1999)

The Government may require continued performance of any services within the limits and at the rates specified in the contract. These rates may be adjusted only as a result of revisions to prevailing labor rates provided by the Secretary of Labor. The option provision may be exercised more than once, but the total extension of performance hereunder shall not exceed 6 months. The Contracting Officer may exercise the option by written notice to the Contractor within 30 calendar days.

FAR 52.217-9: Option to Extend the Term of the Contract (Mar 2000)

(a) The Government may extend the term of this contract by written notice to the Contractor within 1 calendar day; provided that the Government gives the Contractor a preliminary written notice of its intent to extend at least 30 days before the contract expires. The preliminary notice does not commit the Government to an extension.

(b) If the Government exercises this option, the extended contract shall be considered to include this option clause.

(c) The total duration of this contract, including the exercise of any options under this clause, shall not exceed shall not exceed 52 (months).

HSAR CLAUSES

3052.204-71 CONTRACTOR EMPLOYEE ACCESS (SEP 2012)

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

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

(2) Sensitive Security Information (SSI), as defined in Title 49, Code of Federal Regulations, Part 1520, as amended, "Policies and Procedures of Safeguarding and Control of SSI," as amended, and any supplementary guidance officially communicated by an authorized official of the Department of Homeland Security (including the Assistant Secretary for the Transportation Security Administration or his/her designee);

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

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

(b) “Information Technology Resources” include, but are not limited to, computer equipment, networking equipment, telecommunications equipment, cabling, network drives, computer drives, network software, computer software, software programs, intranet sites, and internet sites.

(c) Contractor employees working on this contract must complete such forms as may be necessary for security or other reasons, including the conduct of background investigations to determine suitability. Completed forms shall be submitted as directed by the Contracting Officer. Upon the Contracting Officer's request, the Contractor's employees shall be fingerprinted, or subject to other investigations as required. All Contractor employees requiring recurring access to Government facilities or access to sensitive information or IT resources are required to have a favorably adjudicated background investigation prior to commencing work on this contract unless this requirement is waived under Departmental procedures.

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

(e) Work under this contract may involve access to sensitive information. Therefore, the Contractor shall not disclose, orally or in writing, any sensitive information to any person unless authorized in writing by the Contracting Officer. For those Contractor employees authorized access to sensitive information, the Contractor shall ensure that these persons receive training concerning the protection and disclosure of sensitive information both during and after contract performance.

(f) The Contractor shall include the substance of this clause in all subcontracts at any tier where the subcontractor may have access to Government facilities, sensitive information, or resources.(End of clause)

3052.204-71 CONTRACTOR EMPLOYEE ACCESS - ALTERNATE I (Sep 2012)

When the contract will require Contractor employees to have access to Information Technology (IT) resources, add the following paragraphs:

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

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

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

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

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

(1) There must be a compelling reason for using this individual as opposed to a U. S. citizen; and
(2) The waiver must be in the best interest of the Government.

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

HSAR 3052.209-72 ORGANIZATIONAL CONFLICT OF INTEREST (JUN 2006)

(a) Determination. The Government has determined that this effort may result in an actual or potential conflict of interest, or may provide one or more offerors with the potential to attain an unfair competitive advantage. The nature of the conflict of interest and the limitation on future contracting includes access to DHS business confidential, financial and procurement sensitive information; To the extent that the work under this contract requires access to proprietary, business confidential, or financial data of other companies, and as long as these data remain proprietary or confidential, the Contractor shall protect these data from unauthorized use and disclosure.

(b) If any such conflict of interest is found to exist, the Contracting Officer may (1) disqualify the offeror, or (2) determine that it is otherwise in the best interest of the United States to contract with the offeror and include the appropriate provisions to avoid, neutralize, mitigate, or waive such conflict in the contract awarded. After discussion with the offeror, the Contracting Officer may determine that the actual conflict cannot be avoided, neutralized, mitigated or otherwise resolved to the satisfaction of the Government, and the offeror may be found ineligible for award.

(c) Disclosure: The offeror hereby represents, to the best of its knowledge that:

___ (1) It is not aware of any facts which create any actual or potential organizational conflicts of interest relating to the award of this contract, or ___ (2) It has included information in its proposal,

providing all current information bearing on the existence of any actual or potential organizational conflicts of interest, and has included a mitigation plan in accordance with paragraph (d) of this provision.

(d) Mitigation. If an offeror with a potential or actual conflict of interest or unfair competitive advantage believes the conflict can be avoided, neutralized, or mitigated, the offeror shall submit a mitigation plan to the Government for review. Award of a contract where an actual or potential conflict of interest exists shall not occur before Government approval of the mitigation plan. If a mitigation plan is approved, the restrictions of this provision do not apply to the extent defined in the mitigation plan.

(e) Other Relevant Information: In addition to the mitigation plan, the Contracting Officer may require further relevant information from the offeror. The Contracting Officer will use all information submitted by the offeror, and any other relevant information known to DHS, to determine whether an award to the offeror may take place, and whether the mitigation plan adequately neutralizes or mitigates the conflict.

(f) Corporation Change. The successful offeror shall inform the Contracting Officer within thirty (30) calendar days of the effective date of any corporate mergers, acquisitions, and/or divestures that may affect this provision.

(g) Flow-down. The contractor shall insert the substance of this clause in each first tier subcontract that exceeds the simplified acquisition threshold.

(End of provision)

HSAR 3052.209-73 LIMITATION OF FUTURE CONTRACTING (JUN 2006)

(a) The Contracting Officer has determined that this acquisition may give rise to a potential organizational conflict of interest. Accordingly, the attention of prospective offerors is invited to FAR Subpart 9.5 --Organizational Conflicts of Interest.

(b) The nature of this conflict is access to DHS business confidential, financial and procurement sensitive information.

(c) The restrictions upon future contracting are as follows:

(1) If the Contractor, under the terms of this contract, or through the performance of tasks pursuant to this contract, is required to develop specifications or statements of work that are to be incorporated into a solicitation, the Contractor shall be ineligible to perform the work described in that solicitation as a prime or first-tier subcontractor under an ensuing DHS contract. This restriction shall remain in effect for a reasonable time, as agreed to by the Contracting Officer and the Contractor, sufficient to avoid unfair competitive advantage or potential bias (this time shall in no case be less than the duration of the initial production contract). DHS shall not unilaterally require the Contractor to prepare such specifications or statements of work under this contract.

(2) To the extent that the work under this contract requires access to proprietary, business confidential, or financial data of other companies, and as long as these data remain proprietary or

confidential, the Contractor shall protect these data from unauthorized use and disclosure and agrees not to use them to compete with those other companies. (End of clause)

HSAR 3052.215-70 - Key Personnel or Facilities (Dec 2003)

(a) The personnel or facilities specified below are considered essential to the work being performed under this contract and may, with the consent of the contracting parties, be changed from time to time during the course of the contract by adding or deleting personnel or facilities, as appropriate.

(b) Before removing or replacing any of the specified individuals or facilities, the Contractor shall notify the Contracting Officer, in writing, no less than 15 business days in advance before the change becomes effective. The Contractor shall submit sufficient information to support the proposed action and to enable the Contracting Officer to evaluate the potential impact of the change on this contract. The Contractor shall not remove or replace personnel or facilities until the Contracting Officer approves the change.

The Key Personnel under this task order:

- Program Manager Level III

(End of Clause)

HSAR Class Deviation 15-01 SAFEGUARDING OF SENSITIVE INFORMATION [MAR 2015]

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

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

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

PII is a subset of sensitive information. Examples of PII include, but are not limited to: name, date of birth, mailing address, telephone number, Social Security number (SSN), email address, zip code, account numbers, certificate/license numbers, vehicle identifiers including license

plates, uniform resource locators (URLs), static Internet protocol addresses, biometric identifiers such as fingerprint, voiceprint, iris scan, photographic facial images, or any other unique identifying number or characteristic, and any information where it is reasonably foreseeable that the information will be linked with other information to identify the individual.

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

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

(2) Sensitive Security Information (SSI), as defined in Title 49, Code of Federal Regulations, Part 1520, as amended, "Policies and Procedures of Safeguarding and Control of SSI," as amended, and any supplementary guidance officially communicated by an authorized official of the Department of Homeland Security (including the Assistant Secretary for the Transportation Security Administration or his/her designee);

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

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

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

"Sensitive Personally Identifiable Information (SPII)" is a subset of PII, which if lost, compromised or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. Some forms of PII are sensitive as stand-alone elements. Examples of such PII include: Social Security numbers (SSN), driver's license or state identification number, Alien Registration Numbers (A-number), financial account

number, and biometric identifiers such as fingerprint, voiceprint, or iris scan. Additional examples include any groupings of information that contain an individual's name or other unique identifier plus one or more of the following elements:

(1) Truncated SSN (such as last 4 digits)

(2) Date of birth (month, day, and year)

(3) Citizenship or immigration status

(4) Ethnic or religious affiliation

(5) Sexual orientation

(6) Criminal History

(7) Medical Information

(8) System authentication information such as mother's maiden name, account passwords or personal identification numbers (PIN)

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

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

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

(2) DHS Sensitive Systems Policy Directive 4300A

(3) DHS 4300A Sensitive Systems Handbook and Attachments

(4) DHS Security Authorization Process Guide

(5) DHS Handbook for Safeguarding Sensitive Personally Identifiable Information

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

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

(8) DHS Privacy Incident Handling Guidance

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

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

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

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

(1) Department of Homeland Security (DHS) policies and procedures on Contractor personnel security requirements are set forth in various Management Directives (MDs), Directives, and Instructions. *MD11042.1, Safeguarding Sensitive but Unclassified (For Official Use Only) Information* describes how Contractors must handle sensitive but unclassified information. DHS uses the term "FOR OFFICIAL USE ONLY" to identify sensitive but unclassified information that is not otherwise categorized by statute or regulation. Examples of sensitive information that are categorized by statute or regulation are PCII, SSI, etc. The *DHS Sensitive Systems Policy Directive 4300A* and the *DHS 4300A Sensitive Systems Handbook* provide the policies and procedures on security for Information Technology (IT) resources. The *DHS Handbook for Safeguarding Sensitive Personally Identifiable Information* provides guidelines to help safeguard SPII in both paper and electronic form. *DHS Instruction Handbook121-01-007 Department of Homeland Security Personnel Suitability and Security Program* establishes procedures, program responsibilities, minimum standards, and reporting protocols for the DHS Personnel Suitability and Security Program.

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

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

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

(e) *Authority to Operate*. The Contractor shall not input, store, process, output, and/or transmit sensitive information within a Contractor IT system without an Authority to Operate (ATO)

signed by the Headquarters or Component CIO, or designee, in consultation with the Headquarters or Component Privacy Officer. Unless otherwise specified in the ATO letter, the ATO is valid for three (3) years. The Contractor shall adhere to current Government policies, procedures, and guidance for the Security Authorization (SA) process as defined below.

(1) Complete the Security Authorization process. The SA process shall proceed according to the *DHS Sensitive Systems Policy Directive 4300A* (Version 11.0, April 30, 2014), or any successor publication, *DHS 4300A Sensitive Systems Handbook* (Version 9.1, July 24, 2012), or any successor publication, and the *Security Authorization Process Guide* including templates.

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

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

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

system, and providing timely review of relevant compliance documents for factual accuracy. Information on the DHS privacy compliance process, including PTAs, PIAs, and SORNs, is accessible at http://www.dhs.gov/privacy-compliance.

(2) *Renewal of ATO.* Unless otherwise specified in the ATO letter, the ATO shall be renewed every three (3) years. The Contractor is required to update its SA package as part of the ATO renewal process. The Contractor shall update its SA package by one of the following methods: (1) Updating the SA documentation in the DHS automated information assurance tool for acceptance by the Headquarters or Component CIO, or designee, at least 90 days before the ATO expiration date for review and verification of security controls; or (2) Submitting an updated SA package directly to the COR for approval by the Headquarters or Component CIO, or designee, at least 90 days before the ATO expiration date for review and verification of security controls. The 90 day review process is independent of the system production date and therefore it is important that the Contractor build the review into project schedules. The reviews may include onsite visits that involve physical or logical inspection of the Contractor environment to ensure controls are in place.

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

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

(5) *Revocation of ATO.* In the event of a sensitive information incident, the Government may suspend or revoke an existing ATO (either in part or in whole). If an ATO is suspended or revoked in accordance with this provision, the Contracting Officer may direct the Contractor to take additional security measures to secure sensitive information. These measures may include

restricting access to sensitive information on the Contractor IT system under this contract. Restricting access may include disconnecting the system processing, storing, or transmitting the sensitive information from the Internet or other networks or applying additional security controls.

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

(f) *Sensitive Information Incident Reporting Requirements.*

(1) All known or suspected sensitive information incidents shall be reported to the Headquarters or Component Security Operations Center (SOC) within one hour of discovery in accordance with *4300A Sensitive Systems Handbook Incident Response and Reporting* requirements. When notifying the Headquarters or Component SOC, the Contractor shall also notify the Contracting Officer, COR, Headquarters or Component Privacy Officer, and US-CERT using the contact information identified in the contract. If the incident is reported by phone or the Contracting Officer's email address is not immediately available, the Contractor shall contact the Contracting Officer immediately after reporting the incident to the Headquarters or Component SOC. The Contractor shall not include any sensitive information in the subject or body of any e-mail. To transmit sensitive information, the Contractor shall use *FIPS 140-2Security Requirements for Cryptographic Modules* compliant encryption methods to protect sensitive information in attachments to email. Passwords shall not be communicated in the same email as the attachment. A sensitive information incident shall not, by itself, be interpreted as evidence that the Contractor has failed to provide adequate information security safeguards for sensitive information, or has otherwise failed to meet the requirements of the contract.

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

(i) Data Universal Numbering System (DUNS);
(ii) Contract numbers affected unless all contracts by the company are affected;
(iii) Facility CAGE code if the location of the event is different than the prime contractor location;
(iv) Point of contact (POC) if different than the POC recorded in the System for Award Management (address, position, telephone, email);
(v) Contracting Officer POC (address, telephone, email);
(vi) Contract clearance level;

(vii) Name of subcontractor and CAGE code if this was an incident on a subcontractor network;
(viii) Government programs, platforms or systems involved;
(ix) Location(s) of incident;
(x) Date and time the incident was discovered;
(xi) Server names where sensitive information resided at the time of the incident, both at the Contractor and subcontractor level;
(xii) Description of the Government PII and/or SPII contained within the system;
(xiii) Number of people potentially affected and the estimate or actual number of records exposed and/or contained within the system; and
(xiv) Any additional information relevant to the incident.

(g) *Sensitive Information Incident Response Requirements.*

(1) All determinations related to sensitive information incidents, including response activities, notifications to affected individuals and/or Federal agencies, and related services (e.g., credit monitoring) will be made in writing by the Contracting Officer in consultation with the Headquarters or Component CIO and Headquarters or Component Privacy Officer.
(2) The Contractor shall provide full access and cooperation for all activities determined by the Government to be required to ensure an effective incident response, including providing all requested images, log files, and event information to facilitate rapid resolution of sensitive information incidents.
(3) Incident response activities determined to be required by the Government may include, but are not limited to, the following:
(i) Inspections,
(ii) Investigations,
(iii) Forensic reviews, and
(iv) Data analyses and processing.

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

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

(2) Subject to Government analysis of the incident and the terms of its instructions to the Contractor regarding any resulting notification, the notification method may consist of letters to affected individuals sent by first class mail, electronic means, or general public notice, as

approved by the Government. Notification may require the Contractor's use of address verification and/or address location services. At a minimum, the notification shall include:

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

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

(1) Provide notification to affected individuals as described above; and/or
(2) Provide credit monitoring services to individuals whose data was under the control of the Contractor or resided in the Contractor IT system at the time of the sensitive information incident for a period beginning the date of the incident and extending not less than 18 months from the date the individual is notified. Credit monitoring services shall be provided from a company with which the Contractor has no affiliation. At a minimum, credit monitoring services shall include:
(i) Triple credit bureau monitoring;
(ii) Daily customer service;
(iii) Alerts provided to the individual for changes and fraud; and
(iv) Assistance to the individual with enrollment in the services and the use of fraud alerts; and/or
(3) Establish a dedicated call center. Call center services shall include:
(i) A dedicated telephone number to contact customer service within a fixed period;
(ii) Information necessary for registrants/enrollees to access credit reports and credit scores;
(iii) Weekly reports on call center volume, issue escalation (i.e., those calls that cannot be handled by call center staff and must be resolved by call center management or DHS, as appropriate), and other key metrics;
(iv) Escalation of calls that cannot be handled by call center staff to call center management or DHS, as appropriate;
(v) Customized FAQs, approved in writing by the Contracting Officer in coordination with the Headquarters or Component Chief Privacy Officer; and
(vi) Information for registrants to contact customer service representatives and fraud resolution representatives for credit monitoring assistance.

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

SECTION VIII – INSTRUCTION TO OFFERORS

(This section will be removed upon award.)

1 INTRODUCTION

This acquisition will be conducted under the auspices of the DHS Procurement Innovation Lab (PIL). The PIL is a virtual lab that experiments with innovative techniques for increasing efficiencies in the procurement process and institutionalizing best practices. There is nothing you need to do differently for this requirement. The PIL project team may reach out to successful and unsuccessful offerors to assess effectiveness of the procurement process and the innovative techniques applied. The anonymous feedback will be used to further refine DHS procurement practices. Additional information on the PIL may be found at *www.dhs.gov/pil*.

This RFP is issued under the DHS EAGLE II Strategic Sourcing Contract Vehicles, Functional Category 1 (Unrestricted). Only prime contractors under Functional Category 1 may submit an offer for this requirement. This procurement will be conducted in accordance with FAR 16.505.

2 GENERAL INSTRUCTIONS

Offerors shall submit the written portion of their Proposal as .pdf documents, via email in accordance with the instructions contained herein. Offerors shall submit their Pricing proposal as a completed Schedule B attachment in MS Excel format as provided.

Each electronic file shall be clearly named in accordance with the solicitation provisions. The Offeror's electronic Proposal shall be submitted according to the requirements set forth below:

Proposals will be considered late unless the Offeror completes the entire transmission of the Proposal before the closing date and time for receipt of Proposals under this solicitation. Late Proposals may not be eligible for award. Proposal transmission must be completed by the date and time indicated below. Please Note: As applicable, these submission instructions will also apply to any future correspondence related to this solicitation.

2.1 Errors, Omissions or Ambiguities

If an Offeror believes the solicitation, including the instructions to Offerors, contains an error, omission or ambiguity, or is otherwise unsound, the Offeror shall immediately notify the Contract Specialist and Contracting Officer in writing with supporting rationale.

2.2 False Statements in Offers

Offerors must provide full, accurate and complete information as required by this solicitation and its attachments. The penalty for making false statements in offers is prescribed in 18 U.S.C. 1001.

2.3 Authorized Personnel

The Offeror shall provide the name, title, address, e-mail, and phone number of the company representative(s) who can obligate the Offeror contractually. Also, the Offeror shall identify the individual(s) authorized to negotiate with the Government by providing the name, title, address, e-mail, and phone number of the individual(s).

2.4 No Prior Knowledge

Offerors shall assume the Government has no prior knowledge of their experience and will base its evaluation on the information presented in the Offeror's proposal.

2.5 Confidential or Proprietary Information

In the event an Offeror is concerned that information submitted in response to this solicitation contains confidential financial and proprietary information, including trade secrets, then the information must be clearly marked. In the event an Offeror considers specific information to be confidential, they shall provide a written declaration to the Contracting Officer containing the supporting rationale for their contention that the information constitutes an exception to release under Federal Law. The Proposal shall clearly demonstrate the Offeror's understanding of the overall and specific requirements of the Statement of Work (SOW); convey the Offeror's capabilities for transforming their understanding into accomplishments for performing the requirements.

2.6 Proposal Preparation Costs

The Government will not pay any costs incurred by any Offeror in the preparation and submission of a Proposal in response to this RFP.

2.7 Proposal Validity Period

Proposals shall be valid for a minimum of ninety (90) days.

3 QUESTIONS AND AMENDMENTS

All questions regarding this RFP shall be submitted in writing to the Contract Specialist, Ms. Amanda Aung at Amanda.Aung@hq.dhs.gov and the Contracting Officer, Ms. Cynthia Aki at Cynthia.Aki@hq.dhs.gov. **Questions are due no later than 4:00pm (ET), November 2, 2017.**

Questions asked via telephone or voicemail will not be accepted and will not be addressed in any amendments to the RFP.

The Government recommends that the Offeror ensures that questions are written to enable a clear understanding as to the Offeror's issues or concerns with the referenced area of the solicitation. Statements expressing opinions, sentiments, or conjectures are not considered valid inquiries or comments for this purpose and will not receive a response from the Government.

Answers to questions will be provided to all prospective Offerors, giving due regard to the proper protection of proprietary information. In order to receive responses to questions, Offerors shall cite, at a minimum, the section, paragraph, number, and page number in the format shown below. Further, Offerors are reminded that DHS will not address hypothetical questions aimed toward receiving a potential "evaluation decision" from DHS.

When submitting questions and comments, please refer to the specific text of the RFP in the following format:

Email "subject line" shall read:

RFP No.: **70RDAD18R00000001** – Questions Submitted (Contractor Name)

Questions ***shall be*** submitted in a Microsoft Excel (2003 or later version when available) file in the following format:

	Solicitation or Attachments RFP Section	Paragraph No.	Page No.(s)	Question Category (Contract or Technical)	Question
1					
2					

All questions will be answered in an amendment and provided to all Offerors via email. DHS will not attribute any question(s) asked to the submitting Offeror(s).

If Amendments to the solicitation are issued, all Offerors must acknowledge the Amendments by signing the accompanying Standard Form 30 and returning the signed Standard Form 30 for all Amendments issued with the Offeror's proposal submission. Failure to acknowledge all Amendments issued by the Government may result in the proposal submitted in response to the solicitation being found non-responsive by the Government.

4 PROPOSAL CONTENT AND SUBMISSION INSTRUCTIONS

4.1 Optional Down-Selection / Phased Evaluation

In accordance with FAR Part **16.505** and the EAGLE II Ordering Guide, the Government reserves the right to down-select in order to complete its evaluation and make a best value award decision.

If deemed in the best interest of the Government, the down-select will reduce the number of proposals based on the Government's evaluation of Factor 1 and Factor 2. These are the most important evaluation factors for award.

The down-select will be announced by the Government and Offerors not included in the down-select will have an opportunity to be debriefed in accordance with the EAGLE II contract Section G.4.5(k) and (l).

4.2 Technical Proposal Submission Due Date

Responses for the written proposal submission of this solicitation shall be received no later than **12:00 pm, (ET) on November 14, 2017** to the email addresses identified herein.

4.3 Technical Proposal Submission Content

4.3.1 Demonstrated Prior Experience & Past Performance (10 pages; plus any required Subcontractor letters – Subcontractor letters do not count against page limitation for this submission.)

Prime Contractors shall provide demonstrated prior experience from two or more contracts/task orders performed within the last five (5) years, which shall include at least one instance of demonstrated prior experience from the Prime Contractor's Major Subcontractor, leading and completing financial system modernization efforts (including financial, procurement and asset management) for the Federal Government. The cited demonstrated prior experience should include management and coordination of multiple support teams and subcontractor relationships that resulted in achieving quality performance under contracts that were of a comparable size, scope and complexity to the DHS financial system modernization requirement. Demonstrated prior experience may also include work performed for state or local governments or private entities. The demonstrated prior experience shall explain the Offeror's success in transitioning Government financial systems of a comparable size, scope and complexity to the DHS financial system modernization requirement described in this solicitation, and where different sub-units were transitioned during different phases of the development lifecycle, similar to the DHS TRIO requirement. Demonstrated prior experience shall also evidence the Offeror's demonstrated prior experience supporting the Oracle e-Business Suite Version 12.

Comparability of size, scope and complexity will be in relation to the DHS financial system modernization requirement as documented in Section II related to size, scope and complexity, such as number of transactions, transaction volume, component budgets, user base, and other relevant data related to size and scope. A Major Subcontractor is defined as a subcontractor performing at least 25% (in hours or dollars) of the requirement relevant to the prospective contract/task order.

If demonstrated prior experience of Major Subcontractors is submitted, the Offeror must clearly identify the owner of the demonstrated prior experience and submit a letter of commitment to team with the Prime Offeror signed by an individual of the Subcontractor's firm authorized to make such a commitment and on the subcontractor's letterhead, that confirms a Subcontracting agreement is in place and that explains the role of the Subcontractor for the current DHS requirement. These letters of commitment from the Subcontractor's shall not count against the page limitation. **Major Subcontractors may only team and propose with one Prime Offeror in response to this solicitation.** Additionally, the Government will evaluate most favorably examples of Major Subcontractor demonstrated prior experience where the Prime Offeror and Major Subcontractor performed together/previously teamed.

For each example of prior experience provided, the Offeror shall, at a minimum, document:

- Name of project, duration, and dollar value.
- Government Agency or Company for whom work was performed and a name, title, e-mail and phone number for a representative of that client agency or company that can attest to the work performed.
- Brief description of project (sufficient to establish relevance of experience to the DHS TRIO requirement), and role of Prime or Major Subcontractor which clearly identifies the level and type of services performed under the contract, and the role of the Prime or Major Subcontractor in performing the work.
- Point of Contact from the Government entity (name, title, current phone number, and current e-mail) familiar with the project and can confirm level and quality of the Offerors referenced past performance experience and work. The Government reserves the right to communicate with the Point of Contact provided.

The Offeror is permitted to submit on-going projects as demonstrated prior experience (for itself or Major Subcontractors) if 12 months of performance, at a minimum, under the on-going contract has been completed and if the Offeror clearly describes the stage that the project is at/what has been completed under performance to date.

The Government will contact the identified representative of the Government agency or company as part of the past performance reference checks to confirm the level and quality of this demonstrated prior experience.

4.3.2 Key Personnel (2 pages per resume for each proposed Key Personnel)

The Offeror shall submit resumes for all proposed Key Personnel. The resumes shall demonstrate that the proposed Key Personnel meet the experience and education requirements for the labor category of both the Offeror's EAGLE II IDIQ and any additional requirements set forth in this solicitation for Key Personnel. The resumes shall demonstrate the technical competency of each proposed Key Personnel to support the requirements of the scope and contractual obligations contained within this solicitation and the Offeror's EAGLE II IDIQ contract for each Key Personnel. Key Personnel proposed must be an employee of the Prime Offeror or a Major Subcontractor to the Prime Offeror. **Major Subcontractors may only team and propose with one Prime Offeror in response to this solicitation.** The resumes shall identify the proposed Key Personnel as either "Existing Employee of the Prime Offeror" or "Existing Employee of Major Subcontractor".

A Program Manager Level III is required to be a Key Personnel.

The Offeror shall submit resumes for any number of additional Key Personnel that possess skillsets the Offeror identifies as crucial for successful performance under a resultant task order. The intent of permitting Offerors flexibility in identifying additional Key Personnel is to provide the Offeror an opportunity to staff the task order as most appropriate to the Offeror's proposed technical approach to the work.

The resumes for all additional proposed Key Personnel shall document the role the proposed Key Personnel will serve under a resultant task order, mapped to one of the Offeror's approved

EAGLE II Labor Categories. The resume shall also clearly specify what crucial skillset is being met by the proposed Key Personnel.

The Government reserves the right to incorporate any aspect of the Offeror's written proposal submission into a resultant task order award.

4.3.3 Technical Approach (40 pages)

The Offeror shall provide a written Technical Approach in response to the RFP and the SOW. The Technical Approach shall describe how the Offeror will meet or exceed the requirements of the SOW.

The Technical Approach shall describe the Offeror's proposed plan to conduct discovery activities for the DHS TRIO financial system that is currently residing with DOI/IBC, in order to effectively establish a baseline from which to migrate and transition the DHS DNDO, TSA and USCG financial system from DOI/IBC to the DHS hosting provider, and to support a plan forward for the work needed to support full implementation of the financial system for DNDO, TSA, and USCG. The Offeror shall also consider the SOW and describe its proposed approach to provide sustainment support (O&M) for the DHS TRIO FSM Solution once implementation has been completed.

The Technical Approach shall include, at a minimum, the following details of the Offeror's approach:

1. The Offeror's approach for successfully navigating the complexity of the DHS FSM environment and proactively responding to the organizational evolution and transformation necessary to successfully implement the modernized financial system for the DHS TRIO.
2. The Offeror's assessment of the difficulties and risks which may be encountered, and the Offeror's approach to addressing the noted difficulties and risks while still successfully performing the work. This assessment shall include a description of what the Offeror requires from the Government in order to ensure success, as well as the Offeror's identification of barriers that would reduce or delay success.
3. The Offeror's list of tools that are required to successfully perform work under a resultant task order, and the rationale for the need for the tools. These tools would be assessed and if acceptable, separately procured by the Government. Therefore, if a tool is essential to the proposed technical approach, it is imperative that the Offeror clearly specify this and the risks to performance without such proposed tool.
4. The Offeror's demonstration of how the FSM Solution will meet all requirements for compliance with Section 508 and the applicable IT security requirements detailed in this solicitation.

The Technical Approach shall also include, at a minimum, the following details regarding the Offeror's proposed software development/implementation methodology:

1. The methodology to be provided to perform the work in response to the solicitation, including how the Offeror proposes to scope and envision the project, and prioritize work;
2. A description of the team processes, including the number of team members, the team member roles, and how work will be structured under a resultant task order.
3. The process through which development/implementation under a resultant task order will result in delivery of a quality, functioning FSM Solution. The Offeror shall propose a high-level description of how it proposes the Government shall inspect and accept work/delivery under a resultant task order, and how work and delivery aligns to the CLIN contract type proposed by the Offeror.
4. The process for working with the Government to capture requirements, prioritize and accomplish work under a resultant task order.

The Technical Approach shall also include the Offeror's proposed innovations to support improvements of the DHS FSM Program requirement as described in the SOW. The innovations shall describe ways to do things differently in order to support an increase in value to the customer. The innovations can be related to people, processes and/or technologies.

The Offeror shall affirm that is has CMMI Level III certification in its Technical Approach.

The Government reserves the right to include all or portions of the proposed Technical Approach into a resultant task order.

5 PRICE PROPOSAL (no page limitations)

Offerors shall include the following information in the cover letter of its price proposal:

- Dun & Bradstreet Number (DUNS)
- EAGLE II, FC1 Contract Number
- Contact Name
- Contact Telephone and E-mail Address
  Complete Business Mailing Address

The Price Volume shall be clearly organized and presented in order to allow an evaluation by the Government. An Offeror's proposal is presumed to represent the Offeror's best efforts to respond to the RFP. Furthermore, the services priced in the price volume must be consistent with the services that are described in other volumes of the proposal. Inconsistency, if unexplained, raises a fundamental issue regarding the Offeror's understanding of the RFP, as well as of the Offeror's ability to meet the requirements of the RFP.

It is the Government's intent to permit Offerors the ability to propose the labor categories and hours for each team under the CLIN structure in Excel Workbook (Pricing Template), as well as associate each CLIN with the Offeror's proposed contract type (Labor Hours or Firm-Fixed-Price), such that flexibility in the CLIN structure is permitted to ensure the best fit between the Offeror's proposed technical approach and the Offeror's proposed price. The Government reserves the right to negotiate any changes to CLIN contract type after completion of transition

and discovery, with the objective of ensuring timely, incremental delivery of a quality, functioning modernized financial system. Such negotiation would be through mutual agreement of the Government and the Contractor and would be based on the labor categories and rates proposed in response to this solicitation and awarded on a resultant task order.

The proposal must identify and justify any Government Furnished Equipment (GFE) and/or Government-Furnished Information (GFI) required for task order performance that is not already provided for in the RFP.

The Offeror is encouraged to provide discounts to its EAGLE II labor rates where possible. The reduced labor rates will apply only to the respective task order and will not change the fixed rates in the Attachment B-1, Labor Rate Tables of the Offeror's EAGLE II IDIQ Contract.

Each CLIN should be associated with the requisite labor categories under the Offeror's EAGLE II IDIQ contract needed to perform the work associated with each respective CLIN. If additional labor categories not included in the Offeror's EAGLE II IDIQ contract are required to perform the scope of work under a resultant task order, the Offeror shall comply with the EAGLE II IDIQ contract requirements for proposing additional labor categories.

The Schedule B Attachment – Pricing Template requires the Offeror to input its proposed EAGLE II labor categories, EAGLE II labor rates, discounts and hours proposed for each proposed labor category for each CLIN. The Offeror must propose either a firm-fixed price or labor hour contract type for each CLIN. Additionally, the Surge CLINs across the base and all option periods are pre-set to an established percentage of the Offeror's associated price for the corresponding CLIN. The Pricing Template will calculate the total proposed price for the Offeror for each sub-CLIN and CLIN, both for each period of performance and for the total period of performance.

For Surge CLINs, the Pricing Template will calculate the established set percentage based on the proposed price of the related CLIN. This formula/percentage will be consistent across all Offers.

Additionally, the Time & Materials (T&M) Travel CLINs for each period of performance are set Not-To-Exceed amounts that are consistent across all Offers.

The Offeror shall submit all assumptions, conditions and exceptions to any of the terms and conditions of this solicitation in the pricing section. If not noted in the proposal, it will be assumed that the Offeror proposes no assumptions for award, and agrees to comply with all of the terms and conditions as set forth herein. It is not the responsibility of the Government to seek out and identify assumptions, conditions or exceptions buried within the Offeror's proposal.

Each assumption, exception or dependency shall be specifically related to a paragraph and/or specific section of the RFP or associated clearly with an aspect of the pricing proposed. The Offeror shall provide a rationale in support of any noted assumption, exception or dependency, explaining its effect in comparison to the RFP. This information shall be provided in the format with content as outlined in the table below, and is to be included in the price volume.

RFP Section/Document	Paragraph/Page	Requirement/Portion and Assumption, Condition or Exception	Rationale
RFP, Schedule, Attachment	Applicable paragraph and/or page number(s)	Identify the requirement or portion to which an assumption, exception or dependency is being taken and detail the assumption, condition or exception	Justify why the requirement will not be met, the rationale for the assumption, condition or exception, and/or discuss reasons why not meeting the Government's terms and conditions might be advantageous to the Government.

Assumptions, exceptions or dependencies do not make a proposal automatically unacceptable but will be considered as part of the evaluation of the Offeror's price as it relates to the Offeror's overall proposed solution.

The total proposed price will be used as the basis of price evaluation. The total proposed price will consist of the total proposed price for the base period of performance and all option periods of performance. The Surge and Travel CLINs will be included in the total evaluated price. While price will be factored in a best value determination based primarily on competition, due to the potential variations in technical approaches to the work that each Offeror may propose, a determination of reasonableness as it relates to the Offeror's overall proposed solution will also be part of the Government's evaluation and will be considered for award. The Government reserves the right to utilize other proposal information received from the Offeror to assist in making a determination of reasonableness, including a review of the technical approach proposed in comparison to the total proposed price.

6 ORAL PRESENTATIONS

Following the Government's evaluation of Factors 1 and 2, Offerors may receive an invitation to oral presentations which will include the date, time and location for its scheduled oral presentation. This notification will afford the Offeror at **least 3 calendar days** advance notice of the date, time and location of the Offeror's scheduled oral presentation. The order in which Offerors are scheduled for oral presentations will be randomly selected by the Government. The oral presentation will be held in-person in the Washington, DC metropolitan area. Travel costs for the oral presentation will not be reimbursed.

6.1 Oral Presentation Format

The oral presentation is intended to provide the opportunity for the Offeror to detail its proposed approach to meet or exceed the requirements of the solicitation. The oral presentation shall not provide the Offeror any opportunity to revise or change any of the previously provided written proposal documentation, and is therefore not construed to be discussions with the Offeror.

The Government intends for the oral presentation to proceed as follows:

Oral Presentation Portion	Oral Presentation Component	Maximum Time Allotment: 3 Hours (does not include Portion 1)
1	Introduction and Oral Presentation Process and Expectations.	Not specified
2	The Offeror shall present its PowerPoint slide presentation.	Up to 90 minutes
3	The Government shall caucus among themselves to prepare clarifying questions. Offerors shall receive a break.	Up to 30 minutes
4	The Government will ask clarifying questions, and will also ask a standard set of on-the-spot scenario-based questions of Offerors. The Offeror will respond to the Government's clarifying questions and standard on-the-spot scenario-based questions.	Up to 60 minutes

Offerors can expect the presentation will be conducted in a conference room with a table of sufficient size to accommodate the participants, including the Government attendees.

The Offeror shall furnish their own electronic devices, including additional computers, tablets or smart phones into the oral presentation conference room.

The Offeror Participants shall not reach back, by telephone, e-mail or any other means, to any other personnel or persons for assistance during the oral presentation. There will not be internet or wifi access during the oral presentation.

6.1.1 Oral Presentation Procedures (Prepared PowerPoint Slide Presentation (30 slides maximum)

The Offeror shall submit a .PDF file of up to 30 PowerPoint slides which the offeror intends to present during its scheduled oral presentation. Presentation slides will be due at 12:00 pm one day prior to the commencement of scheduled Oral Presentations. The due date will be included in the 3 day advance notification. The presentation slides will not be evaluated, as the evaluation will be based on the oral presentation. The presentation slides are intended solely to help the evaluators follow the Offeror's oral presentation. Advance submission of the PowerPoint slides is solely to protect the integrity of maintaining equal submission development time for all Offerors regardless of the scheduled date for oral presentations.

The Government reserves the right to record the oral presentation. Additionally, the Government reserves the right to include aspects of the Offeror's oral presentation as special terms and conditions to any resultant task order.

6.2 Offeror Participants

The Offeror's participants in the oral presentations shall be limited to the Program Manager Level III Key Personnel proposed by the Offeror, up to four (4) of the Offeror's additional proposed Key Personnel, and a responsible corporate official. Thus, the Offeror may have no more than 6 participants attend oral presentations. Participants in the oral presentation are limited to personnel of the Prime Offeror and Major Subcontractors. **It is important to recall that Major Subcontractors may only team and propose with one Prime Offeror in response to this solicitation.**

Offerors shall provide the name and e-mail of the Offeror Participants for the oral presentation via email to Contracting Officer and Contract Specialist prior to their scheduled date of their Oral Presentation. The Government will validate that all Offeror participants, with the exception of the responsible corporate official, were submitted as proposed Key Personnel with the Offeror's written proposal submission, and will deny participation by any submitted participant who was not proposed as a Key Personnel, again, with the exception of the responsible corporate official.

6.3 Oral Presentation Content

The Offeror shall prepare and present an oral presentation which shall address the offerors approach to the following task areas identified below. During oral presentations, the Government will also ask Offerors a standard set of on-the-spot technical and management questions.

6.3.1 Implementation Services

The Oral Presentation addressing implementation services shall include the following elements:

6.3.1.1 Strategy - The Offeror shall describe its proposed strategy for working with DHS to configure and fully implement the financial system. The strategy shall address the ability to assume full lifecycle support of the Financial System Modernization solution from DOI/IBC and support the residual configuration and implementation of the financial system necessary to achieve full implementation.

6.3.1.2 Integration Services: The Offeror shall describe its proposed integration services for interfaces with DHS systems, federal systems, and other external systems, to include the proposed system interface development methodology to support a service-oriented architecture and framework.

6.3.1.3 Software Development Methodology: The Offeror shall detail its proposed methodology for software design, development, testing and release. Additionally, the Offeror's proposed approach shall detail how the methodology will support the maintenance of stable

production environments, address technical debt, and align with the DHS Systems Engineering Life Cycle (SELC) and Agile First Policy.

6.3.1.4 Data Migration: The Offeror shall describe its proposed methodology for data conversion and migration support services.

6.3.1.5 Delivery: The Offeror shall describe its processes and procedures to comply with and deliver the requirements of the Statement of Work (SOW), including the specific documentation it will produce and deliver to the Government. However, the Government recognizes that the Offeror may have different processes and procedures to more effectively meet the key success factors identified in the SOW. Thus, the Offeror is encouraged to propose innovations to the documentation and deliverables specified in the SOW. If any innovations are being proposed to the documentation and deliverables specified in the SOW, the Offeror shall clearly detail the innovations and provide a description of the value the innovations will bring to the DHS financial system.

6.3.1.6 Intellectual Property: The Offeror shall describe how the services provided will ensure the DHS financial system development is: 1) transparent in design and practice to the Government oversight personnel; 2) capable of being seamlessly handed over to a successor contractor, including any documentation and licensing of any third party software components or modules; and 3) capable of being contemporaneously archived to assure stability and the ability to survive outages. The Offeror shall describe how it will be compliant with the Data Rights clause contained within the solicitation.

6.3.2 IT Security

The Oral Presentation addressing IT Security shall include the following elements:

6.3.2.1 IT Security Compliance: The Offeror shall detail its proposed methodology, including providing any supporting information or documentation, that demonstrates that all software products and software development supported under performance this task order will be compliant and current with Federal Financial System and IT Security requirements set forth in this solicitation, including compliance with any DHS, legislative, Office of Management and Budget (OMB), Department of Treasury, or other federal mandates affecting financial systems management and reporting or related IT systems and security that are current, enacted, or promulgated after the award of a resultant task order. The Offeror shall describe its proposed approach for privacy protection, security readiness, and DHS accessibility compliance (Section 508), and describe how its proposed approach minimizes the IT security risk of performance under a resultant task order. The Offeror shall include a description of its solution for redundancy and reliability including disaster recovery and continuity of operations.

6.3.2.2 IT Security Release Management: The Offeror shall provide a schedule of estimated major release upgrades over the life of the contract period of performance for all software detailed in the solicitation. The Offeror shall describe its philosophy and approach to technology refresh, patching and upgrades as well as the Offeror's controls for testing and deployment of new technologies/releases, including its proposed system configuration methodology.

6.3.2.3 IT Security Management: The Offeror shall detail how it will ensure security management and access control methodology for all environments.

6.3.3 Sustainment / Operations & Maintenance

The Oral Presentation addressing Sustainment/Operations & Maintenance shall include the Offerors proposed processes and procedures for operations & maintenance support for the DHS financial system. The processes and procedures shall include, but are not limited to: version 3processes to meet SLA requirements (including subscription services, help desk tickets, user access requests), and management of enhancement requests, software bug fixes, and standard application patches (i.e, Oracle, Sunflower).

6.3.4 Staffing and Management

The Oral Presentation addressing staffing and management services shall include the following elements:

6.3.4.1 Staffing Plan and Organization Structure: The Offeror shall detail its proposed organizational structure, including the roles and responsibilities of each company or organization that is a member of the team. The Offeror shall detail its process for ensuring sufficient experienced personnel, who have both technical and domain expertise, are recruited, on-boarded, and retained by the Offeror throughout the duration of the task order period of performance. The staffing plan and organizational structure shall discuss the roles of each labor category under each CLIN; where and why the proposed Key Personnel are situated within the staffing plan and organizational structure, including the CLIN structure for each period of performance; and how the staffing plan and organizational structure ensures timely delivery of the full operational capacity financial management system for the TRIO.

6.3.4.2 Organizational Change Management: The Offeror shall describe its proposed organizational change management support, including its proposed business processes, the communication mediums and forums for the anticipated changes, and how it plans to align group expectations and communications to targeted stakeholder.

6.3.4.3 Training: The Offeror shall describe its proposed training development and delivery methodology for delivering both initial and recurring training to users, including training activities to move users from the old system to the new system. The training development and delivery methodology shall detail the approach to provide financial, procurement and asset management training.

6.3.4.4 Performance: The Offeror shall describe its management approach to ensure quality performance under a resultant task order, to include meeting or exceeding all key performance parameters and performance metrics for the financial systems modernization requirement. The Offeror shall describe its methodology and strategy for collecting and providing monthly EVM-like performance metrics.

SECTION IX – EVALUATION

(This section will be removed upon award.)

1 BASIS FOR AWARD

One award will be made to the responsible Offeror submitting an overall proposal that is determined most advantageous to the Government, price and non-price factors considered. The basis for award will be best value in accordance with FAR 16.505. Evaluation will be conducted and selection will be made in accordance with the guidelines provided in the Federal Acquisition Regulation (FAR), Homeland Security Acquisition Manual (HSAM), and this RFP.

The Government will not make an award at a significantly higher overall price to achieve a marginal increase in superior technical capability. The Government will conduct a tradeoff analysis that involves the assessment of benefits of superior technical quotation features (i.e., benefits clearly attributable to increased productivity, increased probability of successful task order performance, and unique and innovative approaches or capabilities) versus the added price. Overall price to the Government may become the ultimate determining criterion for award of the task order as proposals become more equal based on other criteria.

2 EVALUATION PROCESS

2.1 Fair Opportunity

This RFP is conducted under the fair opportunity guidelines of FAR 16.505 which outlines the ordering procedures for orders issued under Multiple Award Indefinite Delivery Indefinite Quantity contracts. Award will be based on a determination of best value to the Government, price and non-price factors considered. “Best value” means the expected outcome of an acquisition that, in the Government’s estimation, provides the greatest overall benefit in response to the requirement. Best value evaluation is, in and of itself, is a subjective assessment by the Government of the proposed solution that provides the optimal results to the Government.

This method does not use any aspects of FAR subpart 15.3. The use of this fair opportunity process does not obligate the Government to determine a competitive range, conduct discussions with any Offerors, solicit proposals or revisions thereto, or use any other source selection techniques associated with FAR subpart 15.3.

2.2 Comparative Analysis

Following receipt of responses (including oral presentations), and completion of evaluation of each eligible individual Offeror’s response, the Government may perform a comparative analysis (comparing Offeror responses to one another) to select the Offeror that is best suited to fulfill the requirements, based on the Offerors’ responses to the factors outlined in this RFP and their relative importance.

2.3 Award on Initial Responses

The Government anticipates selecting the best-suited Offeror from initial responses, without engaging in exchanges with Offerors. Offerors are strongly encouraged to submit their best technical solutions and price in response to this RFP.

2.4 Exchanges with Best-Suited Offeror

Once the Government determines the Offeror that is the best-suited (i.e., the apparent successful Offeror), the Government reserves the right to communicate with only that Offeror to address any remaining issues, if necessary, and finalize a task order with that Offeror. These issues may include technical and price. If the parties cannot successfully address any remaining issues, as determined pertinent at the sole discretion of the Government, the Government reserves the right to communicate with the next best-suited Offeror based on the original analysis and address any remaining issues. Once the Government has begun communications with the next best-suited Offeror, no further communications with the previous Offeror will be entertained until after the task order has been awarded. This process shall continue until an agreement is successfully reached and a task order is awarded.

3 EVALUATION FACTORS FOR AWARD

3.1 Evaluation Factors and Relative Order of Importance

The Government will evaluate Offeror's proposal submissions based on the following evaluation factors and relative order of importance.

- Factor 1 – Demonstrated Prior Experience & Past Performance
- Factor 2 – Capability of Proposed Key Personnel
- Factor 3 - Technical and Management Approach
    - Sub-Element A – Technical Approach
    - Sub-Element B – Oral Presentation
- Factor 4 – Price

The evaluation factors are listed in descending order of importance. All non-price evaluation factors, when combined, are significantly more important than price. As the non-price merits of competing Offeror's proposals approach equal, Price will become more important in the best value trade-off decision.

Additionally, given the criticality of information security to this requirement, the responsibility determination may also consider information related counter-intelligence matters (such as ongoing open investigations by a law enforcement or counterintelligence agency, or significant issues with foreign ownership, control or influence with the company) as well as security issues (such as current or prior unsatisfactory security ratings as granted by the Defense Security Service or other US Government Department or Agency).

3.2 Factor 1 – Demonstrated Prior Experience & Past Performance Reference Checks

The Government will evaluate the Offeror's demonstrated prior experience by evaluating (1) the Prime Contractors demonstrated prior experience from two or more contracts/task orders performed within the last five (5) years, including at least one instance of demonstrated prior experience from the Prime Contractor's Major Subcontractor, in leading and successfully completing financial system modernization efforts (including financial, procurement and asset management) for the Federal Government; (2) the extent to which the cited demonstrated prior experience includes management and coordination of multiple support teams and subcontractor relationships that resulted in achieving quality performance under contracts that were of a comparable size, scope and complexity to the DHS financial system modernization requirement (3) the extent to which the demonstrated prior experience include work performed for state or local governments or private entities; (4) the extent to which the demonstrated prior experience explains the Offeror's experience in transitioning Government financial systems of a comparable size, scope and complexity to the DHS financial system modernization requirement described in this solicitation, and where different sub-units were transitioned during different phases of the development lifecycle, similar to the DHS TRIO requirement, (5) the extent to which the demonstrated prior experience includes evidence the Offeror's demonstrated prior experience supporting the Oracle e-Business Suite Version 12; and (6) conducting past performance reference checks on the Offerors demonstrated prior experience.

3.3 Factor 2 - Capability of Proposed Key Personnel

The Government will evaluate qualifications (resumes) for all proposed Key Personnel by evaluating (1) the extent to which all proposed Key Personnel resumes demonstrate that the proposed Key Personnel meet the experience and education requirements for the labor category of the Offeror's EAGLE II IDIQ contract and (2) the resumes demonstrate the technical competency of each proposed Key Personnel to support the requirements of the scope and contractual obligations contained within this solicitation and the Offeror's EAGLE II IDIQ contract for each Key Personnel.

3.4 Factor 3 – Technical and Management Approach

The Government will evaluate the Offeror's Technical and Management Approach by evaluating (1) the Offeror's proposed plan to conduct discovery activities for the DHS TRIO financial system; (2) the Offeror's proposed software development/implementation methodology; (3) the Offeror's proposed innovations to support improvements of the DHS FSM; (4) if the Offeror's affirms that it has CMMI Level III certification; and (5) the Offeror's Oral Presentation.

3.5 Evaluation Ratings

In its evaluation, the Government will consider the benefits and risks associated with the Offeror's proposed approaches to arrive at a confidence assessment of the Offeror's likelihood of successfully performing the work and meeting the requirements of the solicitation. The table below shows the ratings the Government will assign in its evaluation of these factors.

RATINGS FOR FACTOR 1, Factor 2, and Factor 3	
Rating	Definition
High Confidence	The Government has high confidence that the Offeror understands the requirement, proposes a sound approach, and will be successful in performing the contract with little or no Government intervention.
Some Confidence	The Government has some confidence that the Offeror understands the requirement, proposes a sound approach, and will be successful in performing the contract with some Government intervention.
Low Confidence	The Government has low confidence that the Offeror understands the requirement, proposes a sound approach, or will be successful in performing the contract even with Government intervention.

Note that for Factor 3 the confidence rating will be assigned based on the evaluation of the Offeror's written technical approach and the Offeror's oral presentation. The Offeror's written submission for the oral presentation (PowerPoint Slides) will only be evaluated to the extent there is an issue with consistency and alignment between the written PowerPoint Slides and the Offeror's oral presentation.

4.2 Factor 4 – Price

The total proposed price will be used as the basis of price evaluation, and will be the total evaluated price evaluated in accordance with FAR 15.404(1)(b). The total proposed price will consist of the total proposed price for the base period of performance and all option periods of performance. The Surge and Travel CLINs will be included in the total evaluated price. While price will be factored in a best value determination based primarily on competition, due to the potential variations in technical approaches to the work that each Offeror may propose, a determination of reasonableness as it relates to the Offeror's overall proposed solution will also be part of the Government's evaluation and will be considered for award. The Government reserves the right to utilize other proposal information received from the Offeror to assist in making a determination of reasonableness, including a review of the technical approach proposed in comparison to the total proposed price.

4.4 Evaluation of Options

The Government will also evaluate the option periods in accordance with FAR 52.217-5 Evaluation of Options (JUL 1990): Except when it is determined in accordance with FAR 17.206(b) not to be in the Government's best interests, the Government will evaluate quotes for award purposes by adding the total price for all options to the total price for the base period. Evaluation of options will not obligate the Government to exercise the option(s).

If needed, the Government intends to exercise the option or options under FAR 52.217-8 without further competition or need for a limited source justification. For purposes of evaluation, the potential need to exercise the option under FAR 52.217-8 to extend the period of contract performance for the maximum period of six (6) months beyond the last option period will be considered the same for all Offerors. In considering the price of the base period and any option periods, the Government will consider that if the extension of service clause (FAR 52.217-8) is exercised, it will be on the exact same rates and terms, other than length of performance, as the base or option period being extended. The Government will determine whether the price, inclusive of all options (including the options available under FAR 52.217-8), is fair and reasonable, and whether the price of the base period and all option periods (including the option(s) represented by FAR 52.217-8), in combination with the other evaluation criteria specified in the solicitation, represents the best value to the Government.