

**Program Management and Reporting System/  
Integrated Workplace Management System  
Indefinite Quantity Indefinite Delivery  
Statement of Work (SOW)**

**Part I: General Information**

**1.1 Project Name and Purpose**

The Program Management and Reporting System (PMRS) project is an initiative of the U.S. Customs and Border Protection (CBP) Office of Administration, Facilities Management and Engineering Directorate (FM&E). Initially CBP termed this initiative PMRS, although through extensive market research CBP has learned that the industry-accepted term for this type of solution is an integrated workplace management system (IWMS). Gartner, Inc., a leading information technology research and advisory firm defines IWMS solutions as *“enterprise level software solutions that integrate four key components of functionality: project management, real estate portfolio and lease management, space management (moves, adds and changes), and maintenance management. The software operates from a single database and offers workflow tools, executive dashboards, and predefined and customized reporting capabilities.”* In addition, Gartner defines an IWMS as an unbundled offering from other vendor system offerings. Only the term IWMS shall be used throughout the remainder of this document.

This SOW defines the IWMS software and services required for an Indefinite Delivery Indefinite Quantity (IDIQ) contract for Department of Homeland Security (DHS) Components.

This initiative is aligned with the following DHS strategic goals and objectives:

- Objective 4.1: Ensure Preparedness
- Objective 5.1: Improve Department Governance and Performance
- Objective 5.3: Integrate DHS Policy, Planning and Operations Coordination

**1.2 Background**

Currently DHS manages a real property portfolio of over 30,000 assets in the U.S. and internationally. This includes owned and leased, General Services Administration (GSA) owned and leased, and free space agreements. Each facility and structure enables DHS employees to efficiently and effectively carry out the mission of DHS. DHS's diverse physical asset portfolio consists of a wide variety of asset classes including real property, land, structures, fleet, mission assets, and weapons.

There is presently a capability gap where a mission of such complexity and magnitude requires a robust integrated facilities lifecycle management solution that provides its personnel with the tools necessary to execute its mission. A lifecycle management solution providing an integrated planning, management, tracking, and reporting capability presently does not exist as a single integrated solution. The 11 DHS Components utilize 9 different systems to manage their respective real property portfolios. These systems provide basic facility-related functions.

To provide asset support to DHS' more than 225,000 employees in jobs that range from aviation and border security to emergency response, from cybersecurity analyst to chemical facility inspector, an IWMS solution is required. DHS has grown substantially since its inception and many legacy Components' missions have expanded. CBP is a prime example of a legacy agency that was forged (from U.S. Customs Service, U.S. Border Patrol, and parts of U.S. Department of Agriculture) and folded under DHS:

- The number of CBP's owned real property assets has grown from 300 to over 1,500.

- The value of CBP's capitalized real property assets has grown from \$287 million to over \$1.9 billion.
- The value of CBP's open capitalized real property projects has increased from \$8 million to over \$3.1 billion.
- The annual cost of CBP's General Services Administration (GSA) rent has risen from \$195 million to over \$379 million.

### **1.3 Scope**

The Contractor shall deliver an IWMS that provides integrated facilities and asset lifecycle management, from planning, project management and acquisition through sustainment and disposal. The system shall be a "commercial off the shelf" (COTS) product. The contractor shall also provide services to support the installation, integration, and implementation of the software. To ensure that the software and services are both provided via this contract, the contractor must either be an IWMS manufacturer or a IWMS manufacturer certified partner (with the ability to provide software and services).

Individual TO's written against the awarded IDIQ may be placed by any DHS Component including:

- DHS Headquarters
- Directorate for National Protection and Programs
- Directorate for Science and Technology (S&T)
- Federal Law Enforcement Training Center (FLETC)
- Federal Emergency Management Agency (FEMA)
- Immigration and Customs Enforcement (ICE)
- Transportation Security Administration (TSA)
- U.S. Citizenship and Immigration Services (CIS)
- U.S. Coast Guard (USCG)
- U.S. Customs and Border Protection (CBP)
- U.S. Secret Service

### **1.4 Period of Performance**

The Period of Performance is 1 - Base Year with 4 – one-year Option Periods.

### **1.5 Place of Performance**

Component-specific requirements for place of performance shall be detailed in each respective TO. Work may be performed at the Contractor's facility, but Components reserve the right to request contractors perform services on-site as well (for example Washington, DC, and/or Indianapolis). The Contractor should price in the cost of having at 1 least one person in two locations, per TO. In addition, the contractor should price in the cost of 3 training sessions per TO, at two separate locations for the customer's Project Team and End-Users.

DHS and its Components are consolidating all development, testing, production, and disaster recovery environments to the two DHS Enterprise Data Centers (Stennis Data Center located in Stennis, Mississippi, and Electronic Data Systems (EDS) located near Washington, DC). Components will only host IWMS software at a DHS Enterprise Data Center.

### **1.6 Deliverables**

The contractor will be paid by successful completion of deliverables that are required within the TO that may include, but are not limited to the following:

- a) IWMS software installation, initial environment set-up, and supporting documentation to include, but not limited to installation and administration documentation, underlying design documentation, and user guides
- b) Project team training
- c) Critical Design Review, to include:
  - i. Detailed Process/Data Design
  - ii. Interface Design
  - iii. Data Conversion Design
- d) Test Readiness Review 1, to include:
  - i. Package Configuration and Unit Test
- e) Test Readiness Review 2, to include:
  - i. Interface Development and Unit Test
  - ii. Data Conversions and Unit Test
  - iii. Role/Security Configuration
- f) Production Readiness Review 1, to include:
  - i. Integration Test (to include all solution components)
- g) Production Readiness Review 2, to include:
  - i. Security Accreditation Package
  - ii. System Acceptance Test
  - iii. User Acceptance Test
  - iv. Initial Production User Set-up
  - v. End User Training and Training Materials
  - vi. Operations Support Documentation and Help Desk Documentation
- h) Operational Readiness Review, to include:
  - i. Certification and Accreditation
  - ii. Resolution of Defects
  - iii. Automation of Batch Operation and System Administration

The cumulative dollar value of the deliverables listed in each TO will equal the total dollar value of the TO Functionality(ies) being acquired.

## **Part II: Performance Requirements and Constraints**

### **2.1 Overall**

The contractor shall provide an IWMS and services to configure, integrate, and implement the software. The IWMS shall provide an integrated asset lifecycle management solution, capable of integrating with Component's enterprise financial systems (i.e. SAP, Sunflower, etc.). Services shall be delivered in conjunction with Government technical staff. Software and services objectives are outlined below.

#### **2.1.1 Software**

The contractor shall provide perpetual licenses to the IWMS software. IWMS upgrades shall be provided to the contracting Component(s) during the period of performance.

Functional Requirements – All IT software shall comply with the latest version of the DHS Systems Engineering Life Cycle (SELC) Guide, which is included in the Acquisition Management Policy (Directive 102-01) (available upon request). The software shall provide the following scalable capabilities as further defined in B.3.1 - 15 of Attachment B:

- a) Enterprise Base/Overarching
- b) Project Management

- c) Strategic Master Planning
- d) Capital Budgeting
- e) Real Property and Lease Administration
- f) Space/Move Management
- g) Environmental and Energy Planning and Compliance
- h) Computer-aided Drafting (CAD) Integration
- i) Geographic Information System (GIS) Integration
- j) Maintenance Management
- k) Facility Condition Assessments
- l) Service Desk/Work Order Management
- m) Mobile Technology
- n) Enhanced Reporting/Dashboards
- o) Asset Management

### **2.1.2 Service**

The contractor shall also provide services encompassing all components of the solution (including all applicable documentation) based on Component's functional requirements, as directed in each TO. Potential services include:

- a) Manage initial software installation and environmental set-up
- b) Conduct concept development and planning
- c) Lead requirements definition and analysis
- d) Perform systems design, development, configuration, and integration
  - i. Core module/process functionality
  - ii. Reporting, scorecards, and dashboards
  - iii. Interfaces
  - iv. Data conversion
  - v. Roles/profiles and security
- e) Conduct testing
  - i. Unit testing
  - ii. Integration testing
  - iii. User acceptance testing
  - iv. Statutory/regulatory and Departmental compliance testing
  - v. Performance/stress testing
  - vi. Security, certification and accreditation testing
  - vii. Cutover testing and data conversion
- f) Perform implementation
  - i. Conduct initial project team training.
  - ii. Prepare end-user training curriculum, prepare individual training module content such as work instructions/scripts, training manuals, exercises, virtual learning materials, training videos, and any additional training materials.
  - iii. Conduct end-user training courses.
- g) Provide technical support (advice), direction, and/or best practices on any and all phases of software implementation, including but not limited to landscape strategy and migration processes/procedures, configuration management practices, security/role strategy and design, scripts and batch scheduling, capacity planning/performance tuning, periodic "housekeeping," data conversion strategy, and system administration tasks.
- h) Prepare production support documentation to include but not limited to installation manuals, user guides, operator manuals, and help desk documentation (scripts, frequently asked questions, etc.).

- i) Manage subsequent software upgrades from preparation and testing through production implementation

### **2.1.3 Software Maintenance**

a) Annual access for maintenance and upgrades may be contracted by subsequent TO(s) with or without initial software purchase (i.e. through annual software licensing). Software maintenance shall include:

- i. Renewal of user licenses.
  - ii. Publishing of bug/defect fixes, patches, and updates/upgrades in both functional and technical capabilities to maintain the operability and usability of the software product:
    - A. Product Updates: General releases containing error corrections and incremental feature enhancements.
    - B. Operating System Upgrades: General releases enabling the software to be used on upgraded versions of the operating system with which the software was designed to be used.
    - C. Documentation Upgrades: When necessary to correct errors in the documentation or to supplement updates to the software.
  - iii. Access to technical support resources to include but not limited to: inquiries, defect identification, escalation, etc. in support of ongoing technical and functional operations.
  - iv. Access to user blogs, discussion forums, on-line help libraries and FAQs (frequently asked questions), hosted chat rooms, and/or web-based general technical support for users self diagnostics.
- b) The contractor shall provide estimates of the efforts and/or costs related to the IWMS life cycle (inception to retirement) for the following topics based on a 10 year timeframe:
- i. Customization and configuration management
  - ii. Implementation/Integration/Installation
  - iii. Development of inbound and outbound interfaces to enterprise management systems (such as SAP)
  - iv. Software upgrades
  - v. Software licensing and maintenance

### **2.2 Contractor Qualifications and Skills**

DHS Components have high volume, high performance and real-time applications operating in an environment that requires specialized, demonstrated management and technical expertise, as well as clearable personnel. The Contractor shall provide the necessary skill mix, experience, and required number of qualified personnel, with the requisite security clearances.

### **2.3 Project Management and Organizational Process**

The Contractor shall provide the requisite internal controls and management oversight for successful performance of each TO effort. The management and organizational objective is to allow the Contractor the maximum flexibility to innovatively manage the program schedule, performance, risks, warranties, subcontracts, and data to provide the services that satisfy the requirements of the TO. Another requirement is to maintain clear government visibility into the program schedule, performance, and risk. The Contractor shall provide a well defined and comprehensive Transition Plan, Implementation Plan for Code and Other Asset Reuse, and a Quality Assurance Management/Surveillance Plan for all TO's.

DHS/Components expect that the following shall be met in the performance of this effort as required within the TO:

- a) Establishing program management practices that provide accurate and timely schedule and performance information throughout the life cycle of the program. This may include providing project management and control reports as defined for the tasks under the SOW.
- b) Demonstrating that the Contractor's Transition Plan, Implementation Plan for Code and Other Asset Reuse, and Quality Assurance Management/Surveillance Plan, result in mitigation of significant risks and actual cost/schedule savings to the Government.
- c) Ensuring that the acquiring Component obtains sufficient rights to the software technical data, such that the Government can maintain and modify the deliverables using Government personnel and third party contractors.
- d) Using electronic technologies to reduce paper copies of program information generated throughout the life cycle of this contract.
- e) Using electronic technologies to communicate and pass data between Government and contractor organizations.

## **2.4 Technical**

DHS expects that the Contractor will achieve the following technical requirements in the performance of this effort:

- a) Through the introduction of new technology, enhanced capabilities, and process improvements, optimize the Component(s) enterprise architecture to continuously improve and evolve hardware, software, and communications in order that it may easily adapt to new technical requirements. Additionally, this shall include:
  - i. The timely delivery of new capabilities and releases.
  - ii. Capabilities that are designed to the DHS and acquiring Component enterprise architecture and transportable between DHS data centers. (Stennis and EDS).
  - iii. DHS/Component Service-Oriented Architecture (SOA) is intended for all projects. New systems and upgrades will use the SOA and all legacy systems will transition to the target SOA enterprise architecture, as fast as feasibly and economically possible. The DHS/Component SOA shall allow for the reuse of existing assets, applications, and investments where new services can be created from an existing IT infrastructure of systems.
- b) All Contractor deliverables shall support an enterprise Service Oriented Architecture (SOA). This includes separation of data from applications, separation of applications from the presentation layer, and creation of reusable services:
  - i. Component solutions shall be mainstream (product and company), maintainable, and should be based on current state-of-the-art technology and processes.
  - ii. Component solutions must be robust, scalable and adaptable to meet changing user requirements and demands. Most components must be capable of supporting 24x7 operations, with no user downtime.
  - iii. All systems releases shall go through rigorous functional and stress testing, using copies of operational data and transaction loads before going operational.
- c) Security will be designed into every system and shall provide for Discretionary Access Controls, single sign-on and auditing. National Information Assurance Program (NIAP) certification of products is desirable.
- d) Secure information sharing is an essential part of the enterprise architecture. Components shall share information by rule and withhold by exception.
  - i. Achieving improved performance, reliability, security, and reduced cost of the delivered service throughout the life of this effort. The Government anticipates a potential cost reduction in operations and maintenance costs for reinvestment in product improvements, as stated in Section 2.1.3.

- ii. Ensuring that system installation will minimally impact other systems located in the designated facility. Additionally, improving customer service by increasing accessibility to clients and values, as well as improving communications.
- iii. Using Component procedures for developing and documenting procedures for managing system engineering, software and hardware development. The Contractor shall utilize IT industry best practices and models such as Capability Maturity Model Integrated (CMMI), Project Management Body of Knowledge (PMBOK), and Information Technology Infrastructure Library (ITIL) to the maximum extent in achievement of this objective.
- iv. Improving testing and configuration management practices and capabilities.
- v. Enhancing quality, timeliness, accuracy, and consistency.

## **2.5 Constraints**

As this will be an enterprise system at the Component level, Components must work with their respective Office of Information Technology (OIT) to ensure all IT requirements and approvals are met.

## **PART III: ATTACHMENTS**

Please see the following attachments to this Statement of Work, which provide additional information, and other technical requirements and special provisions:

Attachment A: Special Provisions and Considerations

Attachment B: Unique Technical and Program Requirements

## **Attachment A: Special Provisions and Considerations**

### **A.1 Information Technology Compliancy and Standards**

#### **A.1.1 Section 508 Compliance**

The contractor must provide a comprehensive specific list of all its electronic and information technology (EIT) products (supplies and services) that fully comply with Section 508 of the Rehabilitation Act of 1973, per the 1998 Amendments, and the Architectural and Transportation Barriers Compliance Board's Electronic and Information Technology Accessibility Standards at 36 CFR Part 1194.

The contractor must ensure that the list is easily accessible by typical users beginning five calendar days after award. The contractor must maintain this detailed listing of compliant products for the full contract term, including all forms of extensions, and must ensure that it is current within three calendar days of changes to its product line.

(a) Section 508 of the Rehabilitation Act, as amended by the Workforce Investment Act of 1998 (P.L. 105-220) requires that when Federal agencies develop, procure, maintain, or use electronic and information technology, they must ensure that it is accessible to people with disabilities. Federal employees and members of the public who have disabilities must have equal access to and use of information and data that is comparable to that enjoyed by non-disabled Federal employees and members of the public. All deliverables within this work statement shall comply with the applicable technical and functional performance criteria of Section 508 unless exempt.

(b) All EIT deliverables within this work statement shall comply with the applicable technical and functional performance criteria of Section 508 unless exempt. Specifically, the following applicable standards have been identified:

-36 CFR 1194.21 – Software Applications and Operating Systems, applies to all EIT software applications and operating systems procured or developed under this work statement including but not limited to GOTS and COTS software. In addition, this standard is to be applied to Web-based applications when needed to fulfill the functional performance criteria. This standard also applies to some Web based applications as described within 36 CFR 1194.22.

-36 CFR 1194.22 – Web-based Intranet and Internet Information and Applications, applies to all Web-based deliverables, including documentation and reports procured or developed under this work statement. When any Web application uses a dynamic (non-static) interface, embeds custom user control(s), embeds video or multimedia, uses proprietary or technical approaches such as, but not limited to, Flash or Asynchronous JavaScript and XML (AJAX) then “1194.21 Software” standards also apply to fulfill functional performance criteria.

-36 CFR 1194.23 – Telecommunications Products, applies to all telecommunications products including end-user interfaces such as telephones and non end-user interfaces such as switches, circuits, etc. that are procured, developed or used by the Federal Government.

-36 CFR 1194.24 – Video and Multimedia Products, applies to all video and multimedia products that are procured or developed under this work statement. Any video or multimedia presentation shall also comply with the software standards (1194.21) when the presentation is through the use of a Web or Software application interface having user controls available.

-36 CFR 1194.25 – Self Contained, Closed Products, applies to all EIT products such as printers, copiers, fax machines, kiosks, etc. that are procured or developed under this work statement.

-36 CFR 1194.26 – Desktop and Portable Computers, applies to all desktop and portable computers, including but not limited to laptops and personal data assistants (PDA) that are procured or developed under this work statement.

-36 CFR 1194.31 – Functional Performance Criteria, applies to all EIT deliverables regardless of delivery method. All EIT deliverable shall use technical standards, regardless of technology, to fulfill the functional performance criteria.

-36 CFR 1194.41 – Information Documentation and Support, applies to all documents, reports, as

well as help and support services. To ensure that documents and reports fulfill the required “1194.31 Functional Performance Criteria”, they shall comply with the technical standard associated with Web-based Intranet and Internet Information and Applications at a minimum. In addition, any help or support provided in this work statement that offer telephone support, such as, but not limited to, a help desk shall have the ability to transmit and receive messages.

Exceptions for this work statement have been determined by DHS and only the exceptions described herein may be applied. Any request for additional exceptions shall be sent to the COTR and determination will be made in accordance with DHS MD 4010.2. DHS has identified the following exceptions that may apply:

-36 CFR 1194.2(b) – (COTS/GOTS products), When procuring a product, each agency shall procure products which comply with the provisions in this part when such products are available in the commercial marketplace or when such products are developed in response to a Government solicitation. Agencies cannot claim a product as a whole is not commercially available because no product in the marketplace meets all the standards. If products are commercially available that meet some but not all of the standards, the agency must procure the product that best meets the standards. When applying this standard, all procurements of EIT shall have documentation of market research that identify a list of products or services that first meet the agency business needs, and from that list of products or services, an analysis that the selected product met more of the accessibility requirements than the non-selected products as required by FAR 39.2. Any selection of a product or service that meets less accessibility standards due to a significant difficulty or expense shall only be permitted under an undue burden claim and requires approval from the DHS Office of Accessible Systems and Technology (OAST) in accordance with DHS MD 4010.2.

-36 CFR 1194.3(b) – Incidental to Contract, all EIT that is exclusively owned and used by the contractor to fulfill this work statement does not require compliance with Section 508. This exception does not apply to any EIT deliverable, service or item that will be used by any Federal employee(s) or member(s) of the public. This exception only applies to those contractors assigned to fulfill the obligations of this work statement and for the purposes of this requirement, are not considered members of the public.

### **A.1.2 Homeland Security Enterprise Architecture Requirements**

(a) The Contractor shall ensure that all computer hardware and software designs conform to the DHS and Component enterprise architecture (EA), the DHS and Component Technical Reference Models (TRM), and all DHS and Component policies and guidelines as promulgated by the DHS and Component Chief Information Officers (CIO), Chief Technology Officers (CTO) and Chief Architects (CA) such as the Component Information Technology Enterprise Principles and the [DHS Service Oriented Architecture - Technical Framework](#).

(b) The Contractor shall conform to the Federal Enterprise Architecture (FEA) model and the DHS and Component versions of the FEA model as described in their respective EAs. Models will be submitted using Business Process Modeling Notation (BPMN 1.1, BPMN 2.0 when available) and the Component Architectural Modeling Standards for all models. Universal Modeling Language (UML2) may be used for infrastructure only. Data semantics shall be in conformance with the National Information Exchange Model (NIEM). Development solutions will also ensure compliance with the current version of the DHS and Component target architectures.

(c) Where possible, the Contractor shall use DHS/Component approved products, standards, services, and profiles as reflected by the hardware software, application, and infrastructure components of the DHS/Component TRM/standards profile. If new hardware, software and infrastructure components are required to develop, test, or implement the program, these products will be coordinated through the DHS and Components' formal technology insertion process which includes a trade study with no less than four alternatives, one of which shall

reflect the status quo and one shall reflect multi-agency collaboration. The DHS/Component TRM/standards profile will be updated as technology insertions are accomplished.

(d) All developed IT hardware or software and recommended solutions shall be compliant with the HLS (Homeland Security) EA (Enterprise Architecture).

(e) Compliance with the HLS EA shall be derived from and aligned through the Component EA.

(f) All data assets, information exchanges and data standards, whether adopted or developed, shall be submitted to the DHS Enterprise Data Management Office (EDMO) for review and insertion into the DHS Data Reference Model.

(g) In compliance with OMB mandates, all network hardware provided under the scope of this Statement of Work and associated TOs shall be IPv6 compatible without modification, upgrade, or replacement.

### **A.1.3 Systems Engineering Life Cycle**

The Contractor shall be governed by and comply with the provisions of the DHS Systems Engineering Life Cycle Guide and Acquisition Management Policy (Directive 102-01). Any Contractor-specific best practices recommendations may be incorporated in a tailoring of the DHS Systems Engineering Life Cycle Guide. However, this action must be prior approved by the COTR.

### **A.1.4 Security Review and Reporting**

(a) The Contractor shall include security as an integral element in the management of this contract. The Contractor shall conduct reviews and report the status of the implementation and enforcement of the security requirements contained in this contract and identified references.

(b) The Government may elect to conduct periodic reviews to ensure that the security requirements contained in this contract are being implemented and enforced. The Contractor shall afford DHS, including the Office of Inspector General, the Component's Chief Information Security Officer, authorized Contracting Officer's Technical Representative (COTR), and other government oversight organizations, access to the Contractor's and subcontractors' facilities, installations, operations, documentation, databases, and personnel used in the performance of this contract. Access shall be provided to the extent necessary for the Government to carry out a program of inspection, investigation, and audit to safeguard against threats and hazards to the integrity, availability, and confidentiality of DHS/Component data or the function of computer systems operated on behalf of DHS/Component, and to preserve evidence of computer crime.

### **A.1.5 Access to Unclassified Facilities, Information Technology Resources, and Sensitive Information**

The assurance of the security of unclassified facilities, Information Technology (IT) resources, and sensitive information during the acquisition process and contract performance are essential to the DHS mission. DHS Management Directive (MD) 11042.1 *Safeguarding Sensitive But Unclassified (For Official Use Only) Information*, describes how contractors must handle sensitive but unclassified information. DHS MD 4300.1 *Information Technology Systems Security* and the *DHS Sensitive Systems Handbook* prescribe policies and procedures on security for IT resources. Contractors shall comply with these policies and procedures, any replacement publications, or any other current or future DHS policies and procedures covering contractors specifically for all TOs that require access to DHS facilities, IT resources or sensitive information. Contractors shall not use or redistribute any DHS information processed, stored, or transmitted by the contractor except as specified in the TO.

### **A.1.6 Security Certification/Accreditation**

The acquiring Component shall provide personnel with the appropriate clearance levels to support the security certification/accreditation processes under this Agreement in accordance with DHS MD 4300A, DHS Sensitive Systems Policy and Handbook. During all SDLC phases

of Component systems, Component personnel shall develop documentation and provide any required information for all levels of classification in support of the certification/accreditation process. In addition, all security certification/accreditation will be performed using the DHS certification/accreditation process, methodology and tools.

#### **A.1.7 General Rules of Behavior for Users of DHS/Component Systems and IR Resources that Access, Store, Receive, and/or Transmit Sensitive Information**

(a) Be advised that general rules of behavior shall apply to all Department of Homeland Security (DHS)/Component support Contractors who use DHS/Component systems and IT resources, such as laptop computers and portable electronic devices (PED) to access, store, receive, or transmit sensitive information. PEDs include personal digital assistants or PDAs (e.g., Palm Pilots), cell phones, text messaging systems (e.g., Blackberry), and plug-in and wireless peripherals that employ removable media (e.g., CDs, DVDs). PEDs also encompass USB flash memory (thumb) drives, external drives, and diskettes. The general rules of behavior are consistent with IT security policy and procedures within DHS Management Directive 4300.1 (Information Technology Systems Security), DHS Sensitive Systems Policy Directive 4300A, and the DHS 4300A Sensitive Systems Handbook. The rules of behavior shall apply to all Contractor employees at Component on-site and at any alternative off-site workplaces, as well as Contractor employees on official travel.

(b) Upon award of contract, the COTR shall provide each Contractor employee with a copy of the DHS/Component "General Rules of Behavior." The employee shall be required to sign and date an attached "Acknowledgement Form." The signed and dated forms shall be returned to the COTR within three (3) days of award or entry on-board.

#### **A.1.8 Interconnection Security Agreement (ISA).**

(a) Interconnections between DHS and non-DHS IT systems shall be established through controlled interfaces and via approved service providers. The controlled interfaces shall be accredited at the highest security level of information on the network. Connections with other Federal agencies shall be documented based on interagency agreements; memoranda of understanding; service level agreements; or interconnect service agreements. DHS Components shall document interconnections with other external networks with an Interconnection Security Agreement (ISA). Interconnections between DHS Components shall require an ISA when there is a difference in the security categorizations for confidentiality, integrity, and availability for the two networks. Additionally, connectivity between internal Component IT systems and all non-Component systems or networks is prohibited without an approved Memorandum of Understanding (MOU) and Interconnection Security Agreement (ISA). ISAs shall be signed by both Decision Approval Authority (DAA) or by the official designated by the DAA to have signatory authority.

(b) The Contractor shall provide personnel capable of developing Interconnection Security Agreements (ISAs), as required. These ISAs shall be fully compliance with both DHS and the acquiring Component IT security policies. Contractor personnel capability is based on the knowledge of NIST 800-47, DHS 4300A, network security concepts and requirements, and solid understanding of the concept behind ISAs.

(c) The Contractor shall perform duties related to MOUs and ISAs, such as:

- i. Identifying ALL connections between the acquiring Component and non-Component organizations related to their specific area or system through close coordination with the network engineering teams and ensuring all are addressed by an appropriate ISA.
- ii. Ensuring that ALL connections between the acquiring Component and non-Component organizations related to their specific area or system are addressed by an appropriate MOU through coordination with the Component's Office of Rules and Regulations (OR&R).

- iii. Developing and supporting an enterprise depository or database capable of supporting extensive query and report capabilities, including non-Component organization name, Component system(s), approval date, expiration date, POCs, addresses, FIPS-199 category.
- iv. Reviewing Interconnection Security Agreements (ISA's) as part of the annual Federal Information Security Management Act (FISMA) self-assessment.
- v. Supporting all data calls for ISA status on enterprise or system basis; including ability to provide softcopy of ISA document artifact upon request.
- vi. Monitoring compliance of the non-Component organization with the security control requirements contained within the ISA through random security test and evaluation (ST&E) coordinated with the network administrators, ST&E team, associated infrastructure Information System Security Officers (ISSOs), and system owner.
- vii. Resolving any security audit findings or plans of action and milestones (POA&M) related to ISAs associated with specific area or system within the allotted time.

### **A.1.7 Homeland Security Geospatial Information System Compliance**

All implementations shall comply with the policies and requirements set forth in the DHS Geospatial Information Infrastructure (GII), including the following:

- a) All developed solutions and requirements shall be compliant with the HLS EA.
- b) All IT hardware or software shall be compliant with the HLS EA Technical Reference Model (TRM) Standards and Products Profile.
- c) The DHS geospatial data model shall be used building to the GII.
- d) All data within the GII, whether adopted or developed, shall be submitted to the DHS Enterprise Data Management Office (EDMO) for review and insertion into the DHS Data Reference Model.

## **A.2 Contract Management Requirements**

### **A.2.1 Government Furnished Property, Information, and Equipment**

- (a) The DHS/Component intends to furnish only that equipment necessary for the Contractor to carry out its work efforts under this Work Statement at the government facility. This only includes desk, chair, desk phone, and desktop computer. While performing work under this Work Statement in DHS/Component facilities, the Contractor may have the use of other normal office EIT devices, such as FAX machines (not classified), copiers, projectors, etc.
- (b) The DHS/Component will not provide to the Contractor cell phone or other portable devices, such as Blackberries or other PDAs. Neither will DHS/Component provide the Contractor with laptop computers.

### **A.2.2 Invoice Requirements**

#### **(a) Period of Invoice**

Invoices shall be submitted per successfully completed deliverable as defined in the TO SOW.

#### **(b) Invoice Submission Method**

Invoice submission processes shall be identified within each TO.

#### **(c) Invoice Detail**

Invoices shall contain the following information:

- Company name and address
- Name and address of person to whom payment is to be sent, including EFT information, if applicable
- Name, title, and phone number of the person to notify in the event of defective invoices

- Deliverable(s) and their respective costs that are being invoiced for including beginning and end dates of the Deliverable(s).
- TO Number.
- TO Modification Number.
- Total value of the TO and as appropriate TO modification(s)
- Certification/signed by a competent company official.

### **A.2.3 Government Consent of Publication/Endorsement**

Under no circumstances shall the Contractor, or anyone acting on behalf of the Contractor, refer to the supplies, services, or equipment furnished pursuant to the provisions of this contract in any news release or commercial advertising without first obtaining explicit written consent to do so from the Contracting Officer.

The Contractor agrees not to refer to awards in commercial advertising in such a manner as to state or imply that the product or service provided is endorsed or preferred by the Federal Government or is considered by the Government to be superior to other products or services.

### **A.2.4 DISCLOSURE OF INFORMATION (MAR 2003)**

(a) Technical Data Rights: The Contractor shall not use, disclose, reproduce, or otherwise divulge or transfuse to any persons any technical information or data licensed for use by the Government that bears any type of restrictive or proprietary legend except as may be necessary in the performance of the contract. Refer to the Rights in Data clause for additional information.

## **A.3 Security Requirements**

### **A.3.1 General Security**

(a) All Government furnished information must be protected to the degree and extent required by local rules, regulations, and procedures. Contractor shall conform to all Component security policies.

(b) All services provided under this Work Statement must be compliant with DHS Information Security Policy, identified in MD 4300.1, "Information Technology Systems Security Program and 4300A Sensitive Systems Handbook"

(<http://www.uscg.mil/acquisITION/nais/RFP/SectionJ/DHS-MD-4300-1.pdf>)

## **A.4 Contractor Employees**

### **A.4.1 Key Personnel**

(a) In accordance with DHS and acquiring Component policies, all supporting key personnel are designated as emergency/essential personnel.

(b) DHS/acquiring Component requires that the Contractor provide the following Key Personnel:

- b.i Project Manager shall serve as a point of contact for the COTR and interface between the government and the contractor employees. The Project Manager will provide centralized administration of all work performed under this contract.
- b.ii Lead Configurator shall provide primary leadership and expertise to the combined team and other contractor team members in all material matters related to core package design, configuration and testing, including solution adaptation.
- b.iii Integration Lead shall provide overall solution leadership/expertise to the combined Team and other contractor team members particularly related to the critical interoperability of and integration with other applications or technologies.

(c) The Contractor shall not make any personnel changes of Key Personnel unless an individual's sudden illness, death, or termination of employment necessitates such substitutions. In case of these occurrences, the Contractor shall notify the Contracting Officer promptly and submit documentation pertaining to the proposed substitution in writing.

(d) The Contractor must provide a detailed explanation of the circumstances causing the proposed substitution. All resumes submitted for each proposed substitution must have qualifications that are equal to or superior to the qualifications of the person being substituted to perform the work under this Work Statement.

(e) The Contracting Officer and COTR shall evaluate the resume of each request to verify the qualifications of every new employee being assigned to this Work Statement.

#### **A.4.1.1 Key Personnel & Skill Level**

(a) **Project Manager:** The Project Manager shall be a single point of contact for the Contracting Officer and the Contracting Officer's Technical Representative. It is anticipated that the Project Manager shall be one of the senior level employees provided by the Contractor for this work effort. **The name of Project Manager, and the name(s) of any alternate(s) who shall act for the Contractor in the absence of the Project Manager, shall be provided to the Government as part of the Contractor's proposal.** During any absence of the Project Manager, only one alternate shall have full authority to act for the Contractor on all matters relating to work performed under this Work Statement. The Project Manager and all designated alternates shall be able to read, write, speak and understand English proficiently. Additionally, the Contractor shall not replace the Project Manager without prior approval from the Contracting Officer. The Project Manager or alternate shall be available to the COTR via telephone between the hours of 0630 and 1700 EST, each business day and shall respond to a request for discussion or contract resolution within one hour of notification. Additionally, the Project Manager must be able to communicate effectively orally and in writing. **EXPERIENCE:** Ten or more years applied to complex computer systems and a bachelor's or master's degree.

#### **(b) Lead Configurator**

The Lead Configurator shall provide primary leadership and expertise to the combined team and other contractor team members in all material matters related to core package design, configuration and testing, including solution adaptation to best meet requirements, such as but not limited to:

- Core (functional) business process/data design, module configuration/set-up and testing (including related workflow)
- Reporting and dashboard design, configuration and testing
- Security/role design, configuration and testing
- Configuration techniques, methods, tools and best practices
- Configuration management practices, particularly in preparation for and conduct of various testing phases, including related migration of the configuration elements from Development to Test to Production environments.

The Lead Configurator shall also serve as the primary liaison/point of contact to the contractor's extended team of technical IWMS resources to spearhead inquiries and COTS-related issue investigation/resolution. Must have strong communication and collaboration skills.

**EXPERIENCE:** Should possess minimum of 4 years facilities management business process expertise and 3 years of hands-on IWMS COTS configuration expertise (full life-cycle for projects of comparable size/complexity) – 2 years of which should be with the Contractor's IWMS product suite. Should also have a bachelor's or masters degree in applicable discipline.

### (c) **Integration Lead**

The Integration Lead shall provide overall solution leadership/expertise to the combined Team and other contractor team members particularly related to the critical interoperability of and integration with other applications or technologies, such as:

- Definition of SAP integration strategy (in conjunction with business representatives and functional and technical ERP Teams)
- Identification, design, development and testing of specific ERP interfaces for (in conjunction with business and ERP Teams) to facilitate bi-directional exchanges and/or synchronization of transactional and master data
- Integration with GIS, CAD and e-mail systems, as well as handheld/mobile technology capabilities
- Integration with or links to other supporting applications/capabilities, such as RSMeans, Primavera or MS Project

The Integration Lead shall serve as primary point of contact for all integration matters across the diverse application and technology components that comprise the overall "solution."

**EXPERIENCE:** Should possess minimum of 3 years of hands-on experience with Contractor's IWMS products, at least 1 year and 1 full life-cycle project of comparable size/complexity integrating with a major COTS ERP vendor (i.e. SAP, Sunflower, Oracle), 2 years integrating contractor's IWMS with GIS and CAD capabilities. Must have strong communication and collaboration skills. Should have bachelor's or masters degree in applicable discipline.

#### **A.4.2 Security Clearances: Personnel Security Background Data**

(a) All personnel employed by the Contractor and/or responsible to the Contractor for the work performed shall either currently possess or be able to favorably pass a full field five (5) year background investigation required by the acquiring Component policies and procedures for employment. This policy also applies to any new personnel hired as replacement(s) during the term of this contract.

(b) **The Contractor shall submit within ten (10) working days after award** of this contract a list containing the full name, social security number, and date of birth of those people who claim to have successfully passed a background investigation by DHS, or submit such information and documentation as may be required by the Government to have a background investigation performed for all personnel. The information must be correct and reviewed by the designated Component Security Official for completeness. Normally, information requested for a background investigation consists of SF-85P, "Questionnaire For Public Trust Positions," or SF-86, "Questionnaire for Sensitive Positions (For National Security)" TDF 67-32.5, "U.S. USCS Authorization for Release of Information," FD-258, "Fingerprint Chart," and a Financial Statement. Failure of any contract personnel to successfully pass a background investigation shall be cause for the candidate's dismissal from the project and replacement by a similar and equally qualified candidate as determined and approved by the Contracting Officer (CO) and the COTR. This policy also applies to any personnel hired as replacements during the term of the contract.

(c) Contractor shall immediately notify the CO and the COTR of any personnel changes. Written approval and confirmation is required for phone notification. This includes, but is not limited to, resignations, terminations, and reassignment.

(d) In accordance with Customs Directive No. 51715-006, "Separation Procedures for Contractor Employees (CF-242)," the Contractor is responsible for ensuring that contract employees separating from the agency complete the relevant portions of the CF-242. This requirement covers all contract employees who depart while the contract is still active (including resignations, terminations, etc.); or upon final completion of the work effort. Failure of a

Contractor to properly comply with these requirements shall be documented and considered when completing Contractor Performance Reports.

(e) The Contractor shall notify the COTR of any changes in access requirements for its personnel no later than one day after any personnel changes occur. This includes name changes, resignations, terminations, and transfers to another contract. The Contractor is responsible for the completion and timely submission to the COTR of the CF-242 for all departing contract personnel. Contractor shall provide the following information on behalf of their personnel to the COTR: Full Name, Social Security Number, Effective Date of Employment, and Reason for Change, as applicable.

(f) The Government may, at its discretion, direct the Contractor to remove any contract employee from DHS facilities for misconduct or security reasons. Removal does not relieve the Contractor of the responsibility to continue providing the services required under this Work Statement. The Contracting Officer will provide the Contractor with a written explanation to support any request to remove an employee. Additionally, the Contractor shall not employ any person who is an employee of the United States Government, if that employment would, or would appear to cause a conflict of interest.

#### **A.4.3 Government Furnished Information and Contractor Non-Disclosures**

Any information made available to the Contractor by the Government shall be used only for the purpose of carrying out the provisions of the contract and shall not be divulged or made known in any manner to any persons except as may be necessary in the performance of the contract.

**Contractor employees shall be required to sign Non-Disclosure Statements that shall be provided by the COTR, per TO.**

#### **A.4.4 Work Hours**

(a) Contractor employees working at government locations can typically work 8 hours a day, 5 days a week. The COTR may approve extended hours based on manning at the Government location(s).

(b) DHS/Components observe the following Federal holidays as days off and any other day(s) designated by Federal statute, by Executive Order or by the Presidential proclamation:

New Year's Day	Labor Day
Martin Luther King's Birthday	Columbus Day
Presidents' Day	Veteran's Day
Memorial Day	Thanksgiving Day
Independence Day	Christmas Day

When any such Holiday falls on a Saturday, the preceding Friday is observed. When any such day falls on a Sunday, the following Monday is observed. Observance of such days by Government personnel shall not be cause for an extension to the delivery schedule or period of performance or adjustment to the price, except as set forth in the contract.

Except for designated around-the-clock or emergency operations, contractor personnel will not be able to perform on site under this contract with DHS/Component on holidays set forth above or when the Government building is closed (i.e. due to inclement weather conditions). In the event Contractor personnel work during a holiday other than those above, no form of holiday or other premium compensation will be reimbursed.

In the event CBP grants administrative leave to its Government employees, at the site, on-site contractor personnel shall also be dismissed if the site is being closed. However, the Contractor shall continue to provide sufficient personnel to perform around-the-clock requirements of critical efforts already in progress or scheduled and shall be guided by the instructions issued by

the Contracting Officer or her/his duly appointed representative (i.e. COTR). In each instance when the site is closed to Contractor personnel as a result of inclement weather, potentially hazardous conditions, explosions, or other special circumstances; the Contractor will direct its staff as necessary to take actions such as reporting to its own site(s) or taking appropriate leave consistent with its policies. The cost of salaries and wages to the Contractor for the period of any such site closure are not reimbursable by the Government.

#### **A.4.5 Meetings/Conferences**

Pre-award meetings or conferences may be necessary to resolve problems and to facilitate understanding of the technical requirements of the contract or task orders. All costs associated with attendance at pre-award meetings/conferences shall be at the contractor's expense.

#### **A.4.6 POST AWARD CONFERENCE**

A post-award conference may be held within ten (10) business days after contract award and or TO award. If held, the Contractor shall participate in this conference. The purpose of the post award conference is to aid both the Contractor and the Government in achieving a clear and mutual understanding of all contract requirements and to identify and resolve potential problems. All Post Award costs shall be borne by the contractor.

#### **A.4.7 CONTRACTOR IDENTIFICATION.**

The Contractor shall ensure that its employees identify themselves as employees of their respective company while working on DHS/Component contracts. For example, Contractor personnel shall introduce themselves and sign attendance logs as employees of their company, not as DHS/Component employees.

Contractor employees shall be required to wear DHS/Component identification badges at all times when working in Government facilities. The Contractor shall ensure that their personnel use the following format signature on all official emails generated by DHS/CBP computers:

- Name
- Position or Professional Title
- Company Name
- Supporting the XXX Division/Office...
- Component Name
- Phone
- FAX
- Other contact information as desired

#### **A.4.8 Mandatory and Other Training**

##### **(a) Security Awareness and Records Management Training**

Security Awareness and Records Management training for all agency personnel, Contractor employees, and other users is mandatory. The training will involve information regarding the risks to agency information and information systems and their obligations in complying with agency information security policies and procedures.

(b) A key objective of an effective IT security training program is to ensure that each employee understands his or her roles and responsibilities and is adequately trained to perform them. The DHS cannot protect the confidentiality, integrity, and availability of its IT systems and the information they contain without the knowledge and active participation of its employees in the implementation of sound security principles.

(c) The Contractor shall be responsible for ensuring that its personnel received the requisite security training depending upon individual work effort and/or roles and responsibilities.

Contractor personnel shall be required to complete one or more levels of DHS security training:

- 1) Initial training in IT security concepts and procedures

- 2) Annual refresher training (if the effort duration is greater than 12 months)
- 3) Role-based training. Role-based training may be required for Contractor personnel who are involved in IT efforts and who are required to perform any IT security responsibilities.
- (d) DHS policy requires Contractors/Subcontractors receive security training commensurate with their responsibilities for performing work under the terms and conditions of their contracted agreements. The contractor shall ensure that each contractor/subcontractor employee has completed the necessary DHS/Component Computer Security Awareness Training prior to performing any work, and, thereafter, completing a DHS/Component – specified fiscal year refresher course during the period of performance under this Statement of Objectives.
- (e) **The Contractor shall maintain a listing by name and title of each contractor/subcontractor employee working under this Work Statement who has completed the required training. Any additional security training completed by the Contractor or subcontractor employees shall be included in the first Monthly Status Report. Any revisions to this listing as a result of staffing changes shall be submitted in the next Monthly Status Report.**

#### **A.4.9 EMPLOYEE CONDUCT.**

The Contractor shall be responsible for maintaining satisfactory standards of employee competency, conduct, appearance, and integrity at all times and shall be responsible for their employee's performance and the quality of the employees' services.

#### **A.4.10 CONTRACTOR INPUT AND TRACKING.**

- (a) The Contractor shall require that each employee under the contract has:
  - (1) Entered information into the acquiring Component's web-based phone system
  - (2) Provided information to be entered into the acquiring Component's Contractor Tracking System.

#### **A.5 CONTRACTING OFFICER'S TECHNICAL REPRESENTATIVE (COTR)**

The COTR will be identified in writing by the Contracting Officer after award of the IDIQ. A Component COTR will be assigned to an individual TO, as necessary.