Attachment C
DPS Technical, Security, and Accreditation Requirements

1.0 Background

Recent government legislation is placing more emphasis on the need to pursue interoperable, integrated, and cost-effective business practices and capabilities within each organization and across DoD, particularly with respect to information technology. One of the legislative acts that impact DoD information technology, architecture analysis and integration activities is the Information Technology Management Reform Act (ITMRA), also known as the Clinger-Cohen Act of 1996. The ITMRA serves to codify the efficiency, interoperability, and leveraging goals being pursued by the Commands, Services, and Agencies of DoD.

Furthermore, in recognizing the need for joint operations in combat and the reality of a shrinking budget, the Assistant Secretary of Defense (ASD) Command, Control, Communications, and Intelligence (C3I) issued a memorandum on 14 November 1995 to Command, Service, and Agency principals involved in the development of Command, Control, Communications, Computers, and Intelligence (C4I) systems. This directive established a single, unifying DoD technical architecture that will become binding on all future DoD C4I acquisitions" so that "new systems can be born joint and interoperable and existing systems will have baseline to move toward interoperability."

Interoperability is defined as:

(1) The ability of systems, units, or forces to provide services to and accept services from other systems, units, or forces and to make use the services, units, or forces and to use the services so exchanged to enable them to operate effectively together, and

(2) The condition achieved among communications-electronics systems or items of communications-electronics equipment when information or services can be exchanged directly and satisfactorily between them and/or their users.

Interoperability is the key enabler for Information Superiority, a critical objective of Joint Vision 2010. To attain the goal of Information Superiority, DoD developed a working framework, the Global Information Grid (GIG), an integrated DoD enterprise information technology architecture. The GIG presents a globally interconnected end-to-end set of information capabilities, associated processes, and personnel that collect, process, store, disseminate, and manage information that is made available, on demand, to warfighters, policy makers, and support personnel. GIG capability requirements are listed within seven fundamental functions: Process, Store, Transport, Human-GIG interaction, Network management, Information Dissemination Management, and Information Assurance. These functions are organized into four general categories: Computing, Communications, Presentation, and Network Operations. Because the GIG operates as a globally interconnected, end-to-end, interoperable system of systems, all systems that comprise the GIG shall be GIG-enabled to allow plug-and-play interoperability among systems. A system shall be considered GIG-enabled if it has the capabilities described for the seven GIG functions.

In support of these initiatives, DoD has published guidance identifying the various mandates and procedures that are necessary to develop, design, and implement a GIG enabled system. The overarching GIG architecture document, Command, Control, Communications Computers, Intelligence, Surveillance, and Reconnaissance (C4ISR) Architecture Framework standardizes the C4ISR architecture development, directed all systems to be compliant, and certified with the Joint Technical Architecture (JTA).

The DoD developed the Joint Technical Architecture (JTA) and the DA developed a Joint Technical Architecture for the Army (JTA-A) which is directed at supporting a broad range of applications and system implementations. Thus the JTA is a subset of the JTA-A that describes

the component interfaces, protocols, and supporting data formats standards necessary to provide the services required by applications. A list of mandated and emerging standards have been identified by DoD and the Army to be used in this procurement by the contractor (see section 9). The Department of the Army (DA) has directed that all systems that produce, use or exchange information electronically, to include, all IT systems and services that are acquired, procured, or operated, be compliant with the Joint Technical Architecture-Army. The JTA-A in turn mandates use of the Defense Information Infrastructure (DII) Common Operating Environment (COE) and mandated as Common Operating Environment (COE) in DoD Directive 4630.5, dated January 2002. The DII COE or COE emphasizes both software reuse and data reuse, and interoperability for both data and software. The DII COE is not a system, but a foundation for building interoperable systems.

2.0 Technical Requirements

2.1 General Requirements

Attachment C describes the requirements for a technical architecture and the design, development, and implementation of DPS. DPS shall consist of components defined by the Clinger Cohen Act, DoD Directive 4630.5 – Interoperability and Supportability of Information Technology and National Security Systems, DoD Instruction 4630.8 Interoperability and Supportability of Information Technology and National Security Systems, Joint Technical Architecture, Joint Technical Architecture-Army, C4ISR Architecture Framework, Defense Information Infrastructure(DII) Common Operating Environment (COE), Army Networthiness Certification Guidance Document and related documents.

Using the DoD Technical Reference Model (TRM), all service and interface definitions shall be used to identify, associate, or describe a standard in this procurement, solicitation, specification, or deliverable. Further elaboration of a particular service or interface definition (i.e., sub service definition) shall be traced to or identified as their related DoD TRM service or interface category or group. Where new technologies are introduced and identified as impacting interoperability, the respective service or interface category associated with this technology shall be identified or defined where an existing category is deemed not applicable.

The contractor shall use the definitions within this solicitation for terminology. Where the terminology does not exist in this solicitation, the contractor shall use a government-approved resource for terminology definitions. The contractor shall use the references within this solicitation and/or any reference(s) that the government may give to the contractor during the contract period.

Lastly, upon publication of new versions of the documents referenced in this PWS the contractor shall evaluate the impact of these new document(s) for compliance issues and identify new and obsolete mandates issues, risks, solutions, technical document changes, and costs to implement the new mandates and/or specifications or those standards that are no longer in compliance. The contractor shall provide upgrades and compliance testing for implementation based on the current standards within 12 months of the publication and release of the standards.

2.2 IT Requirements

The Contractor shall ensure that all information technology (IT) products and services comply with the requirements listed in Table C-1 below, and any additional requirements in Table C-3 and C-4 (section 9).

IT Requirements
DoD Joint Technical Architecture (JTA)
Joint Technical Architecture-Army (JTA-A)
Defense Transportation System Enterprise Architecture (DTS EA)
Defense Information Infrastructure (DII) Common Operating Environment (COE)

IT Requirements
C4ISR Technical Architecture Framework
Army Networthiness Certification Guidance Document
Clinger Cohen Act: Information Technology Management Reform Act (ITMRA)
DoD Directive 4630.5 – Interoperability and Supportability of Information Technology and National Security Systems
DoD Instruction 4630.8 Interoperability and Supportability of Information Technology and National Security Systems
Department of Defense Directive Number 8500.1 Information Assurance (IA)
Department of Defense Instruction Number 8500.2 Information Assurance (IA) Implementation
DoD Directive 5200.40, DoD Information Technology Security Certification and Accreditation Program (DITSCAP), resulting in accreditation per DoD 8510.1-M (DITSCAP Manual)
Section 508 (New requirements for access by the disabled specified in the Rehabilitation Act, as detailed in 36CFR 1194, Subpart B)

Table C-1: IT Requirements

3.0 Hardware, Software and Licenses

3.1 Hardware Requirements

The contractor shall identify all hardware requirements as part of Task 1 and provide final cost data and obtain approval from the government before purchasing any of the identified hardware. Upon approval, the contractor will acquire the specified hardware, which may include (but are not limited to) hardware for development (to include DII COE segmentation platform), for testing (both for development testing and IV&V testing), for actual production and COOP purposes.

The contractor is responsible for the delivery, actual set-up as well as the implementation of all hardware acquired by the contractor. The contractor shall coordinate these responsibilities with the DECC as applicable. Also, the contractor shall ensure that ownership of all acquired hardware will be transferred to the government. The equipment located at contractor facilities will be sub hand receipted as Government Furnished Equipment (GFE).

3.2 Software and Licenses Requirements

The contractor shall identify all software requirements (including development tools) and provide final cost data and approval from the government before purchasing any of the identified software. Upon approval, the contractor will acquire the specified software, which may include (but are not limited to) software for development, for testing (both for development testing and IV&V testing), for actual production, and COOP purposes. In addition, the contractor shall acquire software for external third party monitoring purposes. This includes systems and web-monitoring tools which meet U.S. Transportation Command (USTRANSCOM) customer assurance standards for proactive event monitoring. With respect to licenses, the government may require the contractor to use Army, DOD and USTRANSCOM Enterprise Licenses.

The contractor is responsible for the delivery, actual set-up as well as the implementation of all software acquired. The contractor shall coordinate these responsibilities with the DECC as applicable. Also, the contractor shall ensure that ownership of the acquired software will be transferred to the government. Software located at contractor facilities will be sub hand receipted as Government Furnished Equipment (GFE).

4.0 DECC

4.1 General Requirements

Defense Enterprise Computing Center (DECC) is operated by the Defense Information Systems Agency (DISA). SDDC will enter into a Service Level Agreement (SLA) specifying responsibilities of DISA in supporting the operation of DPS. SDDC will provide a copy of SLA within 30 days of contract award. The DPS contractor will retain overall responsibility for DPS operations and will ensure timely and effective coordination with DECC personnel for continued optimal operations.

Hardware purchased by the contractor and to be delivered to a DECC facility will be coordinated with DECC personnel in advance. Contractor will assist in the set-up and initialization of the systems. Once operational the Government will be responsible for hardware maintenance located at the DECC. For hardware purchased by the contractor and located on the contractor's premises, the maintenance is the responsibility of the Contractor.

After initial set-up, the contractor shall perform remote maintenance on the DPS servers located at the Defense Enterprise Computing Center for all software maintenance requirements to include but not limited to patches, upgrades, system log reviews, configuration changes, application tuning parameters where root level access is not required. This maintenance shall be performed for the Development, Testing, Independent Verification and Validation (IV&V), Production, Fail-over, and Continuity of Operations (COOP) platforms.

In the event that root access is required for the necessary operation, the contractor shall identify the needed change and coordinate the scheduling and execution of the activity with the DECC. The contractor shall ensure that full testing is completed before upgrades or patches are done in the production environment. The contractor shall ensure that scheduled downtime for the server results in minimal impact to the SDDC customers (refer to section 2.2.14 in the PWS). The contractor shall also ensure and coordinate with the DECC that the DPS servers, located at their sites are fully compliant with Information Assurance Vulnerability Alert (IAVA) advisories, DOD security guidance, and that all patches and service packs are at the current level.

The contractor shall meet the requirements of DoD Directive 5200.40, DoD Information Technology Security Certification and Accreditation Program (DITSCAP), resulting in accreditation per DoD 8510.1-M (DITSCAP Manual). User roles and access requirements shall be determined in conjunction with the user representative, functional manager, certification authority and the Designated Approval Authority (DAA). With respect to DECC operations, the SDDC CIO is the DAA. DITSCAP is a collaborative process with the Government. The contractor will prepare all necessary documentation for DITSCAP certification with support from DECC personnel. The contractor shall be ultimately responsible for meeting, implementing and documenting all security requirements as listed in DODI 8500.2.

4.2 DECC Locations

The Government has identified Columbus, OH and St. Louis, MO as proposed DECC sites. The Government will provide DECC locations after award.

5.0 Additional Requirements

5.1 EDI

The contractor shall provide, develop, integrate and implement EDI interfaces as required to support current and future interfaces with DPS. The contractor shall use an EDI translation software as approved by the Government. Current interfaces information will be provided in the Technical Library.

5.2 XML and Web Browsers

The contractor shall ensure XML functionality in DPS. In addition, DPS shall provide Web-enabled capability supporting multiple browsers, e.g. Microsoft Internet Explorer (at a minimum version 5.5) and Netscape.

5.3 User Registration and Authentication

The contractor shall coordinate access control and authentication for DPS through the SDDC ETA (Electronic Transportation Application) Single Sign-on System. The contractor shall enforce role-based access throughout the application. ETA will provide the role information through use of the ETA Defense Encryption Standard-3 (DES-3) encrypted token. The government shall be responsible for user registration approval and user management.

5.4 Communications

The contractor shall ensure through the DISA DECC that DPS allows for sufficient connectivity and reach to provide access for services at U.S. military installations and activities as well as transportation providers worldwide. DPS shall support two communications entry points: The Defense Information Switched network (DISN), and the DISA De Militarized Zone (DMZ).

Also, DPS shall provide the capability to allow Internet and Unclassified but Sensitive Internet Protocol Router Network (NIPRNet) access to SDDC, military and Government domains.

5.5 Data Volume Requirements

The proposed solution should initially be capable of supporting 500,000 shipments annually (approximately 70% of which will be processed between May and October).

5.6 User Transaction Requirements

The proposed solution should initially provide the capability of supporting approximately 800 concurrent PPSO users (average number of site PPSO users logged on all day), 200 concurrent general DoD users, and 3,600 concurrent Transportation Provider users (average number of site TP users logged on all day) for a total of approximately 4,600 concurrent primary users.

In addition, DPS shall also support Customers (Service and Civilian Members) with limited user access. There will be approximately 3,000 - 4,500 concurrent users for non-peak months and approximately 5,000 - 7,500 concurrent customer users for the summer peak season.

Lastly, DPS shall provide a journalizing capability to capture and track user transactions on-line (for audit trail purposes).

5.7 System Operations Requirements

The contractor shall ensure that DPS provides system operations and customer access to services to support worldwide shippers and TPs 24 hours a day, 7 days a week, 365 days a year. Additional requirements include – but are not limited to the following;

Scheduled maintenance shall be coordinated with the Government (SDDC and DECC) to minimize outage impact on users. The preferred window for maintenance will be between 6pm Saturday and 6am Sunday EST/EDT.

Maximum acceptable outage of scheduled production DPS downtime cannot exceed 4 hours per month, not including downtime as a result of DECC actions or events.

The system will be architected and configured in a manner to provide 100% availability at all times. Individual application components (servers) may be taken offline for up to 4 hours per month to perform scheduled maintenance while providing uninterrupted overall application

functionality, operation and availability. The contractor solution must provide high-availability at all system tiers to avoid a single point of failure at the web, application and database level.

6.0 Data Standardization Requirements

6.1 General Requirements

All systems must implement data standards in their interfaces to other DTS and USTRANSCOM systems; implementing data standards in a physical database is mandatory for all new DTS and USTRANSCOM systems and any legacy systems reengineering its database. Database reengineering is defined as modifying the current database objects vice adding new functionality or new structures.

As standards and other specifications required in this contract evolve or are transitioned from emerging to mandated, the contractor shall provide upgrades for implementation based on the current standards within 12 months (or as determined by the Government) of the publication and release of the standards.

The contractor shall provide transition plans for accomplishing the move from the current standards environment to the DoD Joint Technical Architecture, Joint Technical Architecture-Army, Defense Information Infrastructure (DII) Common Operating Environment (COE), C4ISR Technical Framework, and Networthiness Program compliant environment in an orderly and controlled manner. In particular where noncompliant standards are referenced (i.e., draft standards and other public specifications), the contractor shall provide a method and plan for transitioning from the proposed implementation to a future DoD Joint Technical Architecture, Joint Technical Architecture-Army, Defense Information Infrastructure(DII) Common Operating Environment (COE), C4ISR Technical Framework, and Networthiness Certification Program compliant implementation and shall certify that the transition shall be implemented and completed within 12 months from the date of acceptance of such, unless otherwise specified in the contract. The transition plan shall include problem areas, enhancements to legacy and migration components, redundancy, new components introduced relative to the standards being used, and those that are being proposed for use in support of interoperability.

If a standard is not yet supported by implemented products, intermediate targets shall be identified that provide this incremental functionality and help to transition to the objective and compliant environment. These intermediate targets shall be defined by the contractor and fully described including changes from the baseline. Detailed plans for managing and implementing the intermediate targets shall be included. Each intermediate target shall include a description of the intermediate target environment, major changes from the baseline, and identification of schedules, deliverables, milestones, and organizational resource requirements, as a minimum.

6.2 Logical Data Modeling Requirements

The contractor shall ensure that all data modeling products and deliverables are submitted to the program manager, SDDC CDO and USTRANSCOM CDO (ref. USTRANSCOM Data Management Handbook (Chapter 2, page 2 and 3) for review. Recommended changes from SDDC CDO and US TRANSCOM CDO will be incorporated into future software deliverables. The contractor shall submit updated data models as required by the Government. The contractor shall submit data models in the latest Government version of ERwin format in compliance with Federal Information Processing Standards (FIPS) PUB 184, and the USTRANSCOM Data Management Handbook guidelines for entity, attribute and data element labeling, definition and structure conventions. When appropriate and mutually agreed upon between the government and contractor, the contractor shall make those corrections, additions, deletions, or modifications identified in the technical and functional review process.

The contractor shall use the most recent version of the USTRANSCOM Master Model in the development, normalization, definition, documentation and integration of DPS data requirements

in accordance with the policies defined in the USTRANSCOM Data Management Handbook. The contractor shall keep abreast of the contents of the Master Model and use those standard data elements (attributes) and prime words (entities) that satisfy DPS data requirements. When a data standard is insufficient to meet system data requirements, the contractor shall propose a change to the data standards, following the procedures in Chapter 2, USTRANSCOM Master Model Synchronization and Maintenance, and the USTRANSCOM CDO guidelines for preparation of data standardization proposal packages (see Chapter 6, USTRANSCOM Proposal Package Guide).

6.3 Database Standardization

The contractor shall architect a Logical Data Model (LDM) that is fully compliant with the Master Model. The contractor shall also prepare a Transformation Data Model (TDM) to accompany the LDM. The TDM shall be exactly the same in structure as the LDM, but will replace the entity and attribute names with USTRANSCOM standard access names (table and column names), select a data type for the target RDBMS that accurately implements the data type and length specified in the LDM, and incorporate any domain range restrictions for qualitative data.

The contractor shall maintain a Physical Data Model (PDM) throughout the life cycle of the DPS database that is an accurate reflection of the structure of the DPS Physical Schema. Any change to the system's Physical Schema shall be included in the PDM. All deviations between the system's PDM and the system's government-approved TDM will be specifically documented in the appropriate written deliverables and implemented only after approval by the program manager, SDDC CDO and the USTRANSCOM CDO.

6.4 Interface Standardization Requirements

The contractor shall describe each DPS data element in new or existing interfaces with other DTS or USTRANSCOM systems in terms of the Master Model. This description will specify the Master Model entity and attribute that accurately models the system's requirements and will include any additional standard data elements and their values that qualify the selection of those desired attributes from the Master Model.

For any interface data requirement not contained in the Master Model, the contractor shall prepare an extension to the system logical data model, complete the metadata requirements for new data elements, and submit a standardization change package according to instructions in Chapter 2, 3 and 6 of the USTRANSCOM Data Management Handbook.

7.0 Security

7.1 Contractor Personnel Requirements

Ref. section 1.5.1 in the PWS, of the contractor's, subcontractor's, and/or partner's personnel performing services under this contract, shall be citizens of the United States of America. At least one person of the contractor team shall have a valid and current secret clearance for the purpose of accessing the DISA controlled web-site that will be provided by the Government.

The contractor, subcontractor(s), and/or partner(s) shall possess the capability to articulate well, speak and write fluently in the English Language, and comprehend the English Language.

Overall, all contractor personnel will possess the appropriate personnel security investigation for the position occupied. Contractor personnel will be required to have a background investigation that corresponds with the sensitivity level of the tasks to be performed.

The following guidance will be followed when determining IT Position Category.

IT-I (Privileged) ADP-I positions**

Those positions in which the contractor is directly responsible for the planning, direction, and implementation of a computer security program; major responsibility for the direction, planning and design of a computer system, including the hardware and software; or can access a system during the operation or maintenance in such a way, and with a relatively high risk for causing grave damage, or realize a significant personal gain.

Investigative Requirements:

This is considered a Critical Sensitive position and contractor must possess a current SSBI security investigation.

IT-II (Limited Privileged) ADP-II positions**

Those positions in which the incumbent is responsible for the direction, planning, design, operation, or maintenance of a computer systems, and whose work is technically reviewed by a higher authority of the ADP-I category to ensure the integrity of the system.

Investigative Requirements:

This is considered a Non-Critical Sensitive position and contractor must possess a current NAC/NACI/ANACI

IT III (Non-Privileged) ADP III positions**

All other positions involved in computer activities. This is considered a Non-Sensitive Position and the HQ Security Office must approve contractor prior to access to the network.

** The term IT Position is synonymous with the older term Automated Data Processing (ADP) Position. (See DODI 8500.2, Enclosure 2, page 21-22.

NOTE: The above requirements are for access to unclassified systems only. Contractors who require access to classified systems to fulfill contract requirements will possess a security clearance based on personnel security investigative requirements.

The contractor needs to understand and be aware that SDDC does not complete any personnel security investigations for IT/ADP position categories. With the exception of the NCIC conducted for building access it is incumbent upon the contractor to have the appropriate investigations completed upon start of the contract.

7.2 Information Assurance Requirements

The contractor shall be responsible for ensuring all Information Assurance requirements for systems residing on a DOD network are met.

Since DPS is a DOD system **and is being hosted at the** DECC**,** the contractor must ensure that the Information Assurance Vulnerability Alert (IAVA) process and policies are followed. All vulnerabilities listed in DOD IAVAs must be reviewed and implemented, if required. New IAVAs will be implemented within the time frames specified in the new IAVA.

Furthermore, DPS is a Mission Assurance Category III (MAC III) system. As such, DPS is a system which handles information that is necessary for the conduct of day to day business, but does not materially affect support to deployed or contingency forces in the short-term. The DPS also processes Privacy Act information that requires a confidentiality level of Medium. A Mission Assurance Category III system with Medium confidentiality requires the Information Controls

listed in DODI 8500.2, Enclosure 4 Attachments Two and Five. Implementation of these IA controls within DPS shall constitute the baseline requirements for IA certification and accreditation.

7.3 DITSCAP

The contractor shall meet the requirements of DoD Directive 5200.40, DoD Information Technology Security Certification and Accreditation Program (DITSCAP), resulting in **accreditation** per DoD 8510.1-M (DITSCAP Manual). User ro**les and access requirements shall** be determined in conjunction with the user representative, functional manager, certification authority and the D**esignated Approval Authority (D**AA**)**. While **DITSCAP is a collaborative process with the Government, the contractor** shall **be ultimately responsible for meeting, implementing and documenting all security requirements as listed in DODI 8500.2.**

7.4 Additional Security Requirements

Documents

All documents (hardcopy or electronic) produced for this project, as well as the referenced risk assessments, security plans, contingency plans, and disaster recovery plans, shall be considered FOR OFFICIAL USE ONLY (FOUO) and must be appropriately protected.

LAN Access

Access and use of the Surface Deployment and Distribution Command LAN and related systems also shall be considered FOUO and appropriately protected. HQ SDDC Security Office must approve all contractor access to the LAN.

Building Access

The contractor shall submit pertinent documents to a government representative to process appropriate access to a government facility. The following conditions shall be met before any contractor is permitted access to the Hoffman Complex. There may be additional building access requirements at other Government facilities e.g. DECC, USTRANSCOM.

a. Contractor shall have a current National Agency Check (NAC)/National Agency Check with Inquiries (NACI) (within 10 years) on file and be able to show such proof.

OR

b. Contractor shall undergo a National Crime Information Center (NCIC) background check with favorable results. If the contractor can show such a check has been conducted, the HQ Security Office will review for acceptance/non-acceptance. If check is not accepting according to DOD guidelines, contractor will be required to have NCIC conducted through DOD channels by the HQ Security Office.

HQ Security Office requires ten working days to complete building access processing.

8.0 Architecture

8.1 General Requirements

Architecture is defined as the structure of components, their relationships, and the principles, and guidelines that govern their design and evolution over time. The term “architecture” is generally used to refer to an architecture description and an architecture implementation. An architecture description is a representation of a current or postulated “real-world” configuration of resources, rules, and relationships. Once the representation enters the design, development, and acquisition portion of the system development life-cycle process, the architecture description is then transformed into a real implementation of capabilities and assets in the field. Architectures is one

of the key enablers for interoperability. The contractor shall follow the governance for planning, designing, developing and implementation as identified in Table C-2. In addition, the contractor shall perform and develop system architecture assessments.

In the event an interpretation of a standard is required that will invoke any waiver procedure, such a request for interpretation shall be made within 30 calendar days after Task 1 for government approval, or the event triggering the request for a waiver. Any corrections to the architecture, required as a result of decision(s) made by the Government, during the waiver request process, shall be completed within 12 months of the date of the formal notification to the contractor.

8.2 C4ISP

The contractor shall be responsible for developing, mapping and documenting the technical architecture for DPS in accordance with the C4ISP and C4ISR Architecture Framework. Governance and procedures for this requirement are located in DoD Directive 4630.5 and DoD Instruction 4630.8. See Table C-2 for deliverable timelines.

8.3 DII COE

The contractor shall plan, design and develop DPS to be DII COE Level 7 compliant by initial implementation. Level 7 certification, by DISA, shall be completed within one year after initial implementation. (Note: Contractors are also referred to the current DISA Joint Interoperability and Engineering Organization DII COE Developer Documentation.)

8.4 JTA

The contractor shall plan, design, develop, and implement DPS according to the JTA (which includes JTA-Army). The contractor shall develop a Technical Architecture and mappings to other architecture products as outlined in the C4ISR Architecture Framework document.

8.5 Interoperability

The contractor shall operate in and execute upon platforms that provide the necessary degree of interoperability specified in the accompanying specifications and as modified by this solicitation. The contractor shall provide evidence to show that these products and services conform to and are in compliance with the most recent publications for and related documents that are referenced within these documents or those that maybe mandated during the contract period. Contractors shall use service and interface definitions derived from the DoD Technical Reference Model document.

The contractor shall develop an interoperability certification evaluation plan (ICEP) and participate in DISA's Joint Interoperability Testing and Certification process.

The contractor shall identify corrective actions for deficiencies found during the Joint Interoperability Testing and Certification process to include mandates, risks, solutions, costs, development and implementation specifications.

All standards-based validation testing and compliance issues shall be approved by the Government. The contractor shall have the architecture of the system to include the proposed and/or any system modifications approved by the Government before performing any development, testing, or implementation, to include any capability demonstrations.

8.6 Technical Deliverables' Schedule

The schedule for technical deliverables is outlined in Table C-2.

SOW Task#	Deliverable Title	Format	Number	Calendar Days After TO Start
Section 6 – Data Standardizatio n	Logical Data Model	Erwin	2 Hard Copies 1 Soft Copy to COR	45 Days After Start of Task 2
	Transformation Data Model	ERwin	2 Hard Copies 1 Soft Copy to COR	As Required
	Physical Data Model	Erwin	2 Hard Copies 1 Soft Copy to COR	As Required
	Physical Schema	Government Determined Format	2 Hard Copies 1 Soft Copy to COR	As Required
	Logical Data Model Extensions	Erwin	2 Hard Copies 1 Soft Copy to COR	As Required
Section 7 Security	Systems Security Authorization Agreement	Government Determined Format	2 Hard Copies 1 Soft Copy to COR	256 Days After Start of Task 2
	System Security Plan (SSP)	Government Determined Format	2 Hard Copies 1 Soft Copy to COR	As Required
	Contingency Plan (CP)	Government Determined Format	2 Hard Copies 1 Soft Copy to COR	As Required
	Disaster Recovery Plan (DRP)	Government Determined Format	2 Hard Copies 1 Soft Copy to COR	As Required
	Security Testing & Evaluation Plan	Government Determined Format	2 Hard Copies 1 Soft Copy to COR	As Required
Section 8 Architecture	Technical Architecture Draft	Government Determined Format	2 Hard Copies 1 Soft Copy to COR	80 Days After Start of Task 1
	Technical Architecture Updates	Government Determined Format	2 Hard Copies 1 Soft Copy to COR	As Required
	Technical Architecture Final	Government Determined Format	2 Hard Copies 1 Soft Copy to COR	14 Days After Receipt of Government Comments
	Technical Architecture Mappings and Assessments	Government Determined Format	2 Hard Copies 1 Soft Copy to COR	As Required
	JTA Strategy, Compliance and Transition Plan Outline	Government Determined Format	2 Hard Copies 1 Soft Copy to COR	80 Days After Start of Task 1
	JTA Strategy, Compliance and Transition Plan Draft	Government Determined Format	2 Hard Copies 1 Soft Copy to COR	80Days After Government Comments from JTA Strategy, Compliance and Transition Plan Outline
	JTA Strategy, Compliance and Transition Plan Updates	Government Determined Format	2 Hard Copies 1 Soft Copy to COR	As Required

SOW Task#	Deliverable Title	Format	Number	Calendar Days After TO Start
	JTA Strategy, Compliance and Transition Plan Final	Government Determined Format	2 Hard Copies 1 Soft Copy to COR	14 Days After Receipt of Government Comments
	DII COE Strategy, Compliance and Transition Plan Draft	Government Determined Format	2 Hard Copies 1 Soft Copy to COR	80Days After Start of Task 1
	DII COE Strategy, Compliance and Transition Plan Updates	Government Determined Format	2 Hard Copies 1 Soft Copy to COR	As required
	DII COE Strategy, Compliance and Transition Plan Final	Government Determined Format	2 Hard Copies 1 Soft Copy to COR	As required
	DII COE Assessment Report	Government Determined Format	2 Hard Copies 1 Soft Copy to COR	As Required
	DII COE (I&RTS Documentation and Software) Draft	Government Determined Format	2 Hard Copies 1 Soft Copy to COR	As Required
	DII COE (I&RTS Documentation and Software) Updates	Government Determined Format	2 Hard Copies 1 Soft Copy to COR	As Required
	DII COE (I&RTS Documentation and Software) Final	Government Determined Format	2 Hard Copies 1 Soft Copy to COR	As Required
	C4ISP Document (Technical only) Outline	Government Determined Format	2 Hard Copies 1 Soft Copy to COR	As Required
	C4ISP Document (Technical only) Draft	Government Determined Format	2 Hard Copies 1 Soft Copy to COR	As Required
	C4ISP Document (Technical only) Final	Government Determined Format	2 Hard Copies 1 Soft Copy to COR	As Required
	Developmental Testing – Interoperability Evaluation Plan - Draft	Government Determined Format	2 Hard Copies 1 Soft Copy to COR	As Required
	Developmental Testing – Interoperability Evaluation Plan - Final	Government Determined Format	2 Hard Copies 1 Soft Copy to COR	As Required
	Operational Testing – Interoperability Evaluation Plan - Draft	Government Determined Format	2 Hard Copies 1 Soft Copy to COR	As Required
	Operational Testing –	Government	2 Hard Copies	As Required

SOW Task#	Deliverable Title	Format	Number	Calendar Days After TO Start
	Interoperability Evaluation Plan - Final	Determined Format	1 Soft Copy to COR	
	JITC Testing and Certification Deficiencies Report - - Outline	Government Determined Format	2 Hard Copies 1 Soft Copy to COR	As Required
	JITC Testing and Certification Deficiencies Report - - Draft	Government Determined Format	2 Hard Copies 1 Soft Copy to COR	As Required
	JITC Testing and Certification Deficiencies Report - - Final	Government Determined Format	2 Hard Copies 1 Soft Copy to COR	As Required
	Interface Requirements Specification	Government Determined Format	2 Hard Copies 1Soft Copy to COR	Upon Completion of Interface Design

Table C-2 Technical Deliverables

9.0 Additional Technical Requirements

Table C-3: DPS Technical Requirements

In addition to the Technical Requirements mentioned in Table C-1, DPS must satisfy the following:

1. USTRANSCOM Data Management Handbook August 2003
2. Permit use of multiple browsers
3. PKI-DoD PKI certified – Authenticate through SDDC single sign on (ETA)
4. Password Usage-FIPS Pub 112 (end user single portal entry through SDDC)
5. Internet Protocol - IPv4 (upgradeable to IP v6)
6. EDI and XML capable
7. Support multiple standard and ad hoc reports (currently approximately 200)
8. Support multiple standard Reference Data Tables (currently 125 approx)
9. Provide data interface with multiple existing DoD systems
10. Assign access authority
11. Interface with existing DoD portals
12. Allow immediate access to all entered data as required (DoD and commercial TPs)
13. Data interface with U.S. Bank’s PowerTrack system

14. Support multiple global commercial TPs including acceptance of information sent via EDI in addition to manual input via web interface

15. Interface with other Agency and Department systems

16. Provide Interactive Voice Response capability

17. Support Service Member and spousal access via the web.

18. Secure Socket Layer (SSL)

19. DISA – Joint Interoperability Testing Center and Certification

Table C-4 List of Security and Accreditation Requirements

In addition to the Security and Accreditation Requirements mentioned in Table C-1, DPS must satisfy the provisions of the most recent edition of applicable security and accreditation requirements found in the following to include any references to other documents that maybe identified within:

1. Privacy Act

2. Computer Security Act of 1987

3. Office of Management and Budget (OMB) Circular No. A-130, Appendix III

4. Chairman, Joint Chiefs of Staff Manual 6510.01C, Information Assurance (IA) and Computer Network Defense

5. DoD Directive 5200.28, Security Requirements for Automated Information Systems

6. Common Criteria Standard—Controlled Access Protection Profile

7. Army Regulation (AR) 380-19, Information Systems Security

8. Policy Guidance for the Use of Mobile Code Technologies in DoD Information Systems, November 7, 2000

9. Policy Memorandum: Public Key Enabling (PKE) of Applications, Web Servers, and Networks for the Department of Defense, May 17, 2001

10. Policy Directive 33-28, USTRANSCOM, IA/IP Security Architecture Implementation

11. Government Information Security Act

12. Army Regulation (AR) 380-67, Personnel Security (Note: Depending on the role of the service provider ADP I, II, or III may apply.)

13. DoD Badge Policy/Regulation/Directive

14. Army Regulation (AR) 380-5, Information Security Program

15. Army Regulation (AR) 25-55, For Official Use Only (FOUO) Act

16. Compliance with DoD and individual Service information technology security certification and accreditation process

17. DISA Joint Interoperability Testing Center and Certification