War Planning and Execution Infrastructure Support

3 August 2018

Table of Contents

NETCENTS-2
War Planning and Execution Infrastructure Support
Task Order Performance Work Statement
(PWS)

Name:	**Deliberate and Crisis Action Planning and Execution Segments (DCAPES) Program Management Office (PMO)**
Organization:	**AFLCMC/HIBZ**
Address:	**201 East Moore Drive** **Maxwell AFB-Gunter Annex AL 36114**

Executive Summary

Deliberate and Crisis Action Planning and Execution Segments (DCAPES) Program Office has a requirement for services to assist the government with technical support of government provisioned development, integration, test, and deployment environments for both the DCAPES and Logistics Feasibility Analysis Capability (LOGFAC) programs. These technical environments will be located at the Capabilities Integration Environment (CIE), and the contractor will be responsible for adhering to policies and procedures established by the CIE or other government provider.

NETCENTS-2 Application Services Task Order PWS

WAR PLANNING AND EXECUTION INFRASTRUCTURE SUPPORT

1. PURPOSE

The Air Force Life Cycle Management Center, Force Capabilities Division (AFLCMC/HIB), Deliberate and Crisis Action Planning and Execution Segments (DCAPES) Program Management Office (PMO) at Maxwell Air Force Base-Gunter Annex, Alabama has a requirement to establish multiple technical environments to be used for applications development, integration, testing, and User First Look. This PWS will be used to acquire the services needed to support the establishment of these environments. Additionally, the Government requires services to oversee the Government infrastructure and to assist contracted developers in employment of available infrastructure capabilities.

The Infrastructure Support responsibilities encompass Information Technology Service Management activities.

Identification

AFLCMC/HIBZ
DCAPES Program Office
201 East Moore Drive, Bldg 856, Room 164
MAFB-Gunter Annex, AL 36114

1.1. BACKGROUND

The DCAPES PMO employs a Government-owned, contractor-operated set of common hardware, common support tools and common documentation. The integrated environment takes advantage of virtualization and in-house support.

The DCAPES PMO considers the following as key objectives for infrastructure support:

a. Efficient use of hardware through resource pooling across multiple war planning and execution capabilities
b. Efficient scalability to accommodate new configuration items, expanded configuration items, or additional users that are geographically dispersed;
c. Faster deployment of software and capabilities through standardization and continuous integration,
d. Support to application sustainers and application developers with infrastructure interoperability, practical knowledge, and development environments
e. Promote early and continuous collaboration among stakeholders (developers, testers, and users) throughout the development cycle
f. Share knowledge, experience and lessons learned related to infrastructure interoperability and development environments among developers to improve and accelerate software development and deployment
g. Support rapid provisioning of development and test capabilities including timely instantiation and teardown of configurations of infrastructure services for sustainment and development purposes

2. SCOPE

The DCAPES Program Management Office (PMO) has the overall responsibility for acquisition and delivery of Warfighter capabilities for the WPE mission areas.

The Capabilities Integration Environment (CIE) is the current Government-designated hosting location for the DCAPES development, sustainment, integration, User First Look, and Helpdesk environments, providing the requisite infrastructure including connectivity to the environment. The contractor will be responsible for supporting the establishment of Government environments and coordinating with the CIE on the management of the resulting capabilities which will reside in the CIE or other designated environment(s).

Capability providers (developers) will employ the resulting DCAPES environments to develop, test, and deploy DCAPES capabilities into the CIE. DCAPES requires the contractor toprovide the services necessary to assist capability providers in successfully deploying capabilities into the CIE environments and insuring compliance of products with Government requirements including security and interoperability.

The scope includes responsiblility for supporing the PMO in its use of other Government-designated environments or tools to develop, test, and deploy WPE capabilities. This effort includes the requirement for the contractor to assist the PMO in the determination of life cycle management tools for Requirements Management, Project Reporting, Document Management, and collaboration with stakeholders.

2.1. Government-Provisioned Infrastructure and Frameworks

The contractor shall support the PMO in employment of Government-Provisioned Infrastructure and Enterprise Services to support development, sustainment, testing, and fielding of WPE capabilities.

The PMO will act as liaison among the contractor staff members and program offices of the Government-Provisioned infrastructure providers and facilitate the cooperative working environment described in section 3.2.5. For example, the PMO will sponsor Common Access Cards, host meetings or teleconferences as appropriate, coordinate access to mission subject matter experts, address core hardware resource needs, and officiate delivery of contractor products. The PMO will retain responsibility for the overall technical direction of software and systems implementation.

At this time, the organizations providing infrastructure and frameworks are the Capabilities Integration Environment (CIE), DISA, and the JPES Framework. The following paragraphs introduce each of these providers. The contractor shall be knowledgeable on the technical characteristics of these environments including:

- Methods of interoperability at the programming and systems level
- Procedures and design constraints in establishing interoperability
- Specific instructions for employment, deployment and/or installation of provisioned services or their components

- Details related to security services restrictions, accessibility of services, and messaging between services
- Other DoD standards, implementation specifics, technical specifications, or application interface initialization constraints

This knowledge is intended to support DCAPES developers in their efforts to access and exploit government provisioned services in the design and delivery of software components; however, ultimate responsibility for functioning software and its delivery rests with the DCAPES developers and sustainers.

2.1.1. Capabilities Integration Environment (CIE)

The CIE provides a set of enterprise services in support of development, integration, and test activities in an accredited environment. The contractor shall comply with the CIE process for provisioning the environments.

The CIE maintains functionally compliant target environments for development and testing activities. The CIE provides facility resources, engineering assistance, hardware provisioning services, software installation, systems administration, database administration support, and VPN access for developers to connect to environments that are compliant with technical and engineering standards.

The contractor shall support establishment and maintenance of environments within CIE facilities for exclusive use in support of WPE capabilities. This will require the contractor to collaborate with the CIE to leverage CIE-provided services (see DCAPES-CIE Service Level Agreement).

2.1.2. Defense Information Systems Agency (DISA)

DISA now hosts DCAPES in multiple environments (production, test, help desk and training). The contractor shall maintain knowledge of DISA policies and procedures as they relate to the PMO's responsibilities for software delivery and deployment.

DISA provides Forge.mil facilities for project management and development activities and hosting services (See DISA Terms and Conditions). Project Forge provides a life-cycle management tool suite for on-demand, multi-tenant project tracking in multi-user scenarios. ProjectForge suite covers Project Reporting, Document Management, and collaboration with stakeholders. Other capabilities available through Forge.mil are source code management, bug and issue tracking, and release management.

2.1.3. Joint Planning and Execution Services (JPES)

JPES is the DoD's system that supports the policies, processes, procedures, and reporting structures needed to plan, execute, mobilize, deploy, employ, sustain, redeploy, and demobilize activities associated with Joint Operations. The JPES Framework (JFW) is composed of enterprise components that provide management, storage, and access to authoritative planning data. JPES is a critical interface partner with DCAPES.

3. REQUIREMENTS/DESCRIPTION OF SERVICES

The DCAPES system is in a SIPRNET production environment; however, development is performed in unclassified environments on the NIPRNET.

DCAPES currently conducts all development, integration and testing on DCAPES assets in the Capabilities Integration Environment (CIE). DCAPES environments are designed to mimic the DISA DECC to support the new production environment.

The environments supporting the DISA DECC incorporate T4-2, T5-2 and T7-2 servers with 40+ DCAPES and JOPES enclaves. These enclaves use Oracle Dataguard configured to mirror the data across the Primary, Secondary and Tertiary enclaves. These servers are hosted within the Capabilities Integration Environment (CIE).

Environmental hardware includes 4-ORACLE T4-2, 2-ORACLE T5-2 and 5-ORACLE T7-2 servers using a Solaris 11 OS PDOMs, with 300+ LDOMs running Solaris 10 OS and 15+ LDOMs running Solaris 11 OS. DCAPES PMO also utilizes HP Blade servers, which includes the following operating systems: Windows Server 2008 r2, RHEL 6, and Oracle Linux release 6 update 5. The HP Blade servers primarily support the Windows based Business Intelligence (BI) capability for DCAPES and developer software tools such as SVN and Jenkins.

The DCAPES environments also rely on three different Storage Area Networks (SAN). The environments on HP Blade servers use the HP SAN with a capacity of 4.7TB owned by the DCAPES PMO.

The environments using the T4-2, T5-2, and T7-2 servers use the CIE SANs (SAN Tier 1 and Tier 2 storage). The DCAPES PMO uses a total of 120TBs of auto tiered storage 70 TBs on the Hitachi SAN and 50 TBs on the new 3PAR SAN.

The contractor will be responsible for adhering to policies and procedures established by the CIE or other government provider.

The contractor shall work collaboratively with the CIE and DCAPES PMO team to support establishment and maintenance of environment instances required for WPE programs. An instance is defined as a logical segment of hardware and software configured to support a specific purpose for a defined period of time (e.g., development instance, test instance, User First Look instance). The contractor shall document its concept and overall technical approach to managing the environments and their instances, components, and COTs products in Environment Architecture and Specifications (A008).

The contractor shall support the CIE in their understanding of DCAPES system software and COTS applications, and administration and maintenance of those network services and operating system requirements. The DCAPES application developer/sustainer will be responsible for providing patches, Security Technical Implementation Guide (STIG) and Information Assurance Vulnerability Alert (IAVA) updates (see for the DCAPES Software Patch Management Process). The contractor shall coordinate these efforts between the CIE, developer/sustainer, and the DCAPES PMO.

The contractor shall configure CIE infrastructure environments to support up to 100 users for each instance. The infrastructure contractor shall support distributed computing solutions on multiple OS platforms. Additionally, the contractor shall be responsible for supporting the promotion of software code and configuration changes from the development environment to CIE testing. The timing of these promotions will align with the DCAPES PMO's Integrated Master Schedule (IMS) and will be in coordination with the development contractor(s) and the government.

The contractor shall support production deployments and fielding efforts with the DCAPES PMO and development partners and shall adhere to the software change management governance and practices in use by the DCAPES program.

3.1. Systems Sustainment

The contractor shall provide services to support, maintain and operate the DCAPES CIE Infrastructure services. The contractor shall maintain existing and new environments IAW disciplined engineering practices and sustain applications, databases and interfaces in compliance with applicable AF/DoD standards.

3.2. Systems Support and Integration

The system support and integration of the DCAPES environment comprises the installation and configuration of network devices and software systems, including databases. The contractor will be responsible for performing day-to-day activities, including but not limited to, access control via VPN and RDP accounts to servers, Windows and Unix-based management, system design and implementation, system deployments, architectural design and layout, system maintenance, installation of developer tools, and facilitating access from developers, from initial request for access to final grant of access via the CIE.

3.2.1. Establish Environments

Establish and manage use of DCAPES and JOPES suites as well as life cycle management tools on Government-provided hardware. (A003)

a. Create appropriate installation, backup and restore, failover, or other system administration processes and recommend policies for DCAPES PMO/CIE adoption.
b. Assist the PMO in determining the appropriate life cycle management tools for Requirements Management, Project Reporting, Document Management, and collaboration with stakeholders.
c. Perform functions as the Site Administrator for the selected life cycle management tools for the duration of the contract.
d. Develop and deliver policies and procedures for Government/developer interaction(s) with Government-selected development and lifecycle management tools (A004).
e. Transfer ownership, control, and responsibility for all material from all life cycle management repositories/tools to the Government (A010) at the end of the contract.

3.2.2. Integration & Interoperability Support

a. Assist the program office with employment of development infrastructure
b. Create and maintain practices and procedures for employment of government-sourced environments: including day-to-day operations supporting environment users (A004)
c. Contribute to identification and specification of technical, architectural, messaging, and data standards in capability documents for software development (A009)
d. Prepare environment capacity projections based on software delivery needs and monitor capacity utilization to keep environments cost effective (A009)

3.2.3. Service Request and Incident Management (A004, A005)

The contractor shall employ the capabilities of the selected life cycle management tool to document, record, prioritize, track, and report on lessons learned and other information relating to Incidents and Service Requests in the DCAPES development environments.

The contractor shall have experience using HP Quality Center or other Government designated tool for tracking defects, ticket creation, testing, and generating problem reports. The discrepancies/incidents are currently recorded, prioritized, and tracked in HP Quality Center.

The contractor and developer will propose solutions to resolve discrepancies and implement the proposed solutions after the approval from DCAPES PMO. The contractor's engineers and administrators are responsible for resolving incidents and maintain lessons learned documentation.

3.2.4. Remote End-User Administration Service

The contractor shall support remote access connectivity to DCAPES PMO resources, setting up Virtual Private Network access, user IDs, and other end-user administration services designated by DCAPES PMO relating to the government network and selected life cycle management tool.

User accounts accessing the DCAPES servers through VPN are a contractually controlled CIE function per the signed Service Level Agreement (SLA) between the DCAPES PMO and the CIE dated 01 Sept 2017. Request for access is facilitated by this contract's System Administrator. The System Administrator processes requests to ensure the request contains the correct data and forwards the request to the CIE System Integrator assigned to the DCAPES personnel for creation. Account requests are initialized by receipt of DD Form 2875 from the DCAPES PMO.

3.2.5. Cooperation and Coordination with Other Contractors and Government Offices

The relationship between the contractor and the multiple entities involved in the DCAPES lifecycle are complex and will require establishment of procedures and policies for their governance. The contractor will be responsible for assisting the Program Office in developing these policies and procedures.

There may be multiple contractors (i.e. from more than one contract vehicle and/or company) supporting AFLCMC/HI and other DoD activities, tasked to work related activities. Also, there may be multiple Government Offices supporting DCAPES for activities such as interface, data services, and interoperability development and testing.

The contractor shall work with these other contractors and other Government Offices as required to accomplish Government requirements, goals, and objectives as efficiently and effectively as possible. This may include, but is not limited to sharing or coordinating information resulting from the work required by this PWS or previous Government efforts, and/or working as a team to perform tasks in concert, including contributions to and compliance with the integrated master schedules. Cooperation shall involve sharing source code, collaboration on web service development and integration IAW applicable guidance and policies.

3.2.6. Test Support

The contractor shall support test activities in both the Capabilities Integration Environment (CIE) at Gunter Annex, AL, and any other environments as applicable. Test events will encompass pre-Government Delivery testing and post-Government Delivery testing.

Test support includes events and activities in the UFL environment(s) similar to beta testing.

3.2.7. Pre-Delivery Testing

The contractor shall support testing in the CIE environments used by developers for Unit, Module,

and Integration testing, as well as Demonstrations, UFL, and Performance Testing. Physical environment standup will be the responsibility of the contractor with CIE support. Configuration of installed components will be the responsibility of the developers.

The contractor shall maintain a library of test tools (scripts, test harnesses, test cases, etc.) and test equipment (simulation hardware in CIE) to support automated builds and automated testing. (A003)

3.2.8. Post-Delivery Testing

The contractor shall be involved with all aspects of Post-Delivery Testing. This testing will consist of two distinct phases, compliance and Government Test, with a differing level of involvement for the contractor during each phase. The contractor will be responsible for installation of deliveries using the delivery Installation Plan (IP), review of all delivered documentation, and working with Functionals to ensure delivered software not only installs but functions as expected. All of the results from these actions will be included in the FCA/PCA report.

The contractor will review the documentation with each release and ensure it meets quality standards (Joint Command and Control Reference Architecture (JC2RA) standards and DoDAF StdV-1 Standards Profile). The contractor will then load the delivery packages in a suite to be used for validation following the developer-provided Installation Plan. Any issues encountered will be documented and solutions identified. The contractor will work with the developer to find solutions to issues found and with the DCAPES Functionals to test that the delivery works as required. A final Physical Configuration Audit and Functional Configuration Audit report will be written and provided to the DCAPES PMO. The report will contain inputs from application of the Installation Procedures, items the contractor and PMO personnel found on supporting documentation, and items found during the DCAPES Functionals testing.

3.2.9. Compliance Testing

The contractor shall perform a physical configuration audit of each delivery.

The contractor shall maintain a library of tools used to verify and validate compliance of the delivered software article with standards. This testing includes scanning tools or the execution of implementation procedures. The scope of this testing will be determined by the Infrastructure contractor and Government together for each relevant form of software deliverable. (A002, A003, A004, A007)

3.2.10. Government Test Events

The contractor shall provide remote and/or on-site support as required for Government-run test events. These test events may include Developmental Testing, Operational Testing, Security Testing, Joint Interoperability Testing or other events as determined by the Government. This testing will be executed by the Government, with the contractor providing support related to the environments in which the testing is being executed, and serving as a member on any associated deficiency review boards.

3.2.11. Database Administration (A003)

a. Support the developers/sustainers in the backup of data, cleansing services for data, verification of data integrity, and implementation of access controls

b. Support developers of data exposure services in interoperating with the DCAPES system.

The DBA monitors the health, configuration, resource utilization and performance of both DCAPES and JOPES databases within the CIE. The DCAPES DBA also performs complex database installations and upgrades using documentation provided by the development contractor and in the case of DCAPES software, provides quality control feedback on database related documentation.

In addition to database administration duties for DCAPES, the contractor will provide DBA services for DCAPES lifecycle management tools used by the PMO. These currently include Project Forge, Quality Center, and Subversion (as part of Project Forge). The PMO is in the process of replacing the DCAPES DISA-hosted Project Forge repository (forge.mil) with a CIE-hosted CollabNet (TeamForge) instance. The contractor will assist in this transition if it remains incomplete at the time of contract award.

3.2.12. Systems Administration (A003)

a. Support the installation and maintenance of computer systems
b. Assist with planning and response to service outages
c. Participate in efforts to diagnose software and hardware failures
d. Ensure security preventive measures are fully functioning
e. Monitor and provide guidance on potential enhancements to system performance

DCAPES System Administrator will install and maintain a DCAPES Help Desk Suite for developmental purposes mirroring DISA DECC implementations, and the DCAPES physical and virtual suites. These suites are used for test, integration, development and user first look functions to support DCAPES development. The system administrator manages interface definition and compliance policies of the PMO amongst the DCAPES and other external directories and systems that use the Identity Data Directory (IDD). The system administrator will be the central point of contact for all incident reports from generation to resolution.

In addition to system administration duties for DCAPES, the contractor will provide SA services for DCAPES lifecycle management tools used by the PMO. These currently include Project Forge, Quality Center, and Subversion (as part of Project Forge). The PMO is in the process of replacing the DCAPES DISA-hosted Project Forge repository (forge.mil) with a CIE-hosted CollabNet (TeamForge) instance. The contractor will assist in this transition if it remains incomplete at the time of contract award.

3.2.13. IAVA and COTS Update Compliance

Information Assurance Vulnerability Alert (IAVA) are cybersecurity vulnerabilities that are released weekly by DISA, AFCYBER, and/or USCYBERCOM.

The contractor shall orchestrate the response to IAVAs across the supported environments.

The contractor shall ensure that all system or application deliverables meet the requirements of DoD and AF cybersecurity policy. Furthermore, the contractor shall ensure that personnel performing cybersecurity activities obtain, and remain current with, required technical and/or management certifications. These persons will hold requisite level of certification for the duties to be performed according to DoDD 8140.01 and DoD 8570.01-M.

The contractor will employ a patch management process to insure the following minimum actions

are accomplished:

a. As part of orchestration, perform evaluation and/or impact analysis to determine which of the supported environments are affected and the responsible organizations for providing the response (A008)
b. Track IAVA or COTS patch update responses to closure in the CIE
c. Make changes/updates to affected software versions required to comply with IAVAs or COTS patch updates
d. Provide the Program Office with inputs into Plan of Action and Milestones (POA&M), Risk Assessment Report (RAR), and/or System Security Plan (SSP) that may be required as the result of IAVA and COTS patch updates
e. Make changes/updates to affected software versions required to comply with IAVA or COTS patch updates

3.3. Information Services

3.3.1. Registering Services

The contractor shall assist the developer by supporting the registration of ADS exposure services, aggregation services and presentation services. Support will be limited to providing DCAPES specific information related to firewalls, whitelisting Universal Resource Locators (URLs), and ordering, staging and installing certicates.

3.3.2. Web Services

The contractor shall assist the developer in the creation and maintenance of DCAPES web services using standards as defined within the Enterprise Architecture to enable sharing of data across different applications in an enterprise.

3.4. Systems Operations

Systems operations requirements must comply with applicable documents and standards specified in Section 8 of this PWS.

The contractor shall provide operational support services including, but not limited to, database administration, systems administration, customer orientation and help desk support for the provisioned Infrastructure environments in accordance with AFI 33-115 Network Operations and DoD 8570.01M Information Assurance Workforce Improvement Program.

3.4.1. Database Administration

- Create and test backups of data, provide data cleansing services, verify data integrity, implement access controls.
- Assist developers of data exposure services with engagement of the database.

3.4.2. Systems Administration

- Install, support and maintain computer systems.
- Plan and respond to service outages.
- Diagnose software and hardware failures to resolution.
- Implement and ensure security preventive measures are fully functioning.
- Monitor and enhance system performance.

3.4.3. Customer Familiarization

The contractor shall maintain an entry level briefing on environment use: Introduction to the

Development and Sustainment Environment (A006). Develop, maintain and/or update materials related to use of the environments. In particular, the contractor shall communicate to users the established processes and policies for User First Look (A003).

Ensure materials stay current with the services offered throughout the life of the Task Order.

3.4.4. Help Desk Support

Provide trouble reporting and on-call technical assistance for provisioned environments during normal business hours.

4. ENGINEERING REQUIREMENTS

Engineering requirements take the form of:

a. Configuration Management
b. Cybersecurity practices

4.1. Configuration Management

The contractor shall maintain configuration control of environments, sprints, releases, baselines delivered by the development team, contractor-produced documentation, automated test cases, and other configuration items. The contractor will coordinate CM activities and responsibilities with the CIE and DISA to ensure security and version control of the environments.

The preferred performance and delivery method for all reports and configuration items will be in the selected life cycle management tool.

In 2018, the PMO began migration of DCAPES artifacts associated with development and configuration management from ProjectForge to CollabNet (TeamForge). The DCAPES TeamForge site will consist of a core TeamForge application and several tightly integrated services that support it.

- The core TeamForge application provides the Web interface that users see, and the API that other applications can interact with. It also includes the file system where some user content is stored, such as wiki pages.
- The site database is where most of the user-created content is stored and accessed. Documents, discussion posts, tracker artifacts, project administration settings: all that sort of thing lives in the database.
- The source control server ties any number of Subversion, CVS or Perforce repositories into the TeamForge site.
- The Extract transform and load (ETL) server pulls data from the site database and populates the datamart to generate charts and graphs about how people are using the site.
- The datamart is an abstraction of the site database, optimized to support the reporting functionality.

The contractor will be responsible for all System Administration tasks for the DCAPES TeamForge instance, including establishing site administrator, project manager, and other role-based permissions. The contractor will also be responsible for integrating the TeamForge instance with other 3rd party tools such as HP Application Life Cycle Management (ALM), Unified Functional Tester (UFT), etc.

Configuration management for developmental configuration items involves source code, executables, and developmental documents and artifacts:

a. Management of software configuration items, source code, and other developer deliveries
   - Including facilities for version control, programmer check-in and check-out, version numbering, and version recall
   - Including versions of build lists, versions of APIs and ADS messages, runtimes and source code
b. Maintaining related documentation in the DCAPES project folders (or related equivalent) in the selected life cycle management tool, including:
   - Frequently Asked Questions document
   - Updates as appropriate to the Design Documents (e.g. design decisions, analysis of alternatives, risks/impacts to other releases, design evaluation criteria, appropriate diagrams/figures/tables, use cases)
   - Updates as appropriate to the Architecture Documents (e.g. diagrams, figures, tables, reference, sequences, ports, protocols, services, internal connectivity calls, process or thread interactions)
c. Produce a handbook for developers defining the CM processes and rules for using the environments (A003)
   - Verify that developed products comply with CM processes and guidelines prior to delivery to the PMO
   - Participate in configuration audits
   - Manage, support and maintain the lifecycle management tool accounts and projects
   - Resolving any/all issues with integrator delivered CIs identified by the PMO, GCCS-AF, or DISA
   - Identify, record, and report on all DCAPES components (hardware, software, process, documentation and services) that are under the control and scope of CM

4.2. Cybersecurity

The contractor shall ensure that all system deliverables meet the requirements of DoD and AF cybersecurity policy.

Cybersecurity is achieved through application of the Risk Management Framework (RMF). As a standard approach to cybersecurity, all information and information systems shall be safeguarded through the application of the Security Technical Implementation Guides (STIGs), Security Requirements Guides (SRGs), or COTS security best practices.

The contractor responsibilities will include, but not be limited to, the following (see). Provide support to PMO's assessment and authorization (A&A) efforts by providing the expertise to evaluate or apply COTS patches/STIGS to the CIE.

- Coordinate with the CIE's management team to ensure Enterprise Security Posture System (ESPS) is configured on all environments.

- Assist government with efforts to ensure cybersecurity management support and testing of activities.

4.2.1. Personnel Cybersecurity

The contractor shall provide cybersecurity support, protecting information and information systems,

and ensuring confidentiality, integrity, authentication, availability and non- repudiation. The contractor shall provide application services support for Certification and Accreditation (C&A) processes, RMF processes, SISSU processes, Enterprise Information Technology Data Repository (EITDR) certification or ICD 503. (See paragraph 6.6)

IAW DFARS 239.7103(b), Information Assurance Contractor Training and Certification (JAN 2008):

(a) The Contractor shall ensure that personnel accessing information systems have the proper and current information assurance certification to perform information assurance functions in accordance with DoD 8570.01-M, Information Assurance Workforce Improvement Program. The Contractor shall meet the applicable information assurance certification requirements, including—

(1) DoD-approved information assurance workforce certifications appropriate for each category and level as listed in the current version of DoD 8570.01-M; and

(2) Appropriate operating systems certification for information assurance technical positions as required by DoD 8570.01-M.

(b) Upon request by the Government, the Contractor shall provide documentation supporting the information assurance certification status of personnel performing information assurance functions.

(c) Contractor personnel who do not have proper and current certifications shall be denied access to DoD information systems for the purpose of performing information assurance functions.

Contractor personnel will require privileged access to Government-hosted environments. At least one of the IAT Level 1 certifications is required as specified in DoD Directive 8570.01-M.

4.2.2. System Cybersecurity

The contractor shall verify and validate compliance of deliverables with DoD and AF cybersecurity policy, specifically DoDI 8500.01, Cybersecurity, and AFI 17-130, Cybersecurity Program Management. The contractor shall also support activities and meet the requirements of DoDI 8520.02, Public Key Infrastructure (PKI) and Public Key (PK) Enabling, in order to achieve standardized, PKI-supported capabilities for biometrics, digital signatures, encryption, identification and authentication.

5. Program Management / Project Management

The contractor shall identify a Program Manager or a Project Manager who shall be the primary representative responsible for all work awarded under this task order, participating in Program/Project Management Reviews and ensuring all standards referenced herein are adhered to.

5.1. Task Order Management

The contractor shall establish and provide a qualified workforce capable of performing the required tasks. The contractor shall participate in the PMO Weekly Production Meeting and provide minutes (A001). The contractor shall provide weekly (A005) and monthly status and progress reports (A004,).

5.2. Performance Management Reviews

Within ten (10) business days following the task award date, contractor shall attend a Kick-Off

Meeting to review task order goals and objectives, and to discuss technical requirements, administrative matters, deliverables, security requirements, transition, Government Furnished Information/Materials/Equipment (GFI/GFM/GFE), the milestone schedule, review cycles, and invoicing. At the meeting the contractor shall present their plan for meeting tasks and schedules. The meeting shall be attended by all contractor key personnel and shall be held at the Government facility.

Additional meetings will be held on at least an annual basis to review contractor performance and progress toward meeting performance specified in the Service Delivery Summary. During these meetings, the contractor should be prepared to present the results of contractor actions taken to improve efficiencies in hardware and software resources, improving environment scalability, reducing build time, and any other performance improvements, and lessons learned or recommendations for improvements.

5.3. Schedule

The contractor shall support and contribute to the master schedules produced by those using the infrastructure. The contractor shall commit to and be measured for performance by their ability to support agreed upon integrated master schedules. The contractor shall report status for their tasks in the master schedule and provide schedules of upcoming tasks during the PMO Weekly Production Meeting and document schedule tasks in the Weekly Status Report.

5.4. Personnel Security

This task order requires personnel to have SECRET security clearances, and requires all employees to be United States citizens. The contractor will request security clearances for personnel requiring access to classified information within 15 business days after contract award. This task order requires access to systems as a condition of award, therefore application/cost for the appropriate Personnel Security Investigations (PSI) shall be the responsibility of the contractor. The contractor shall diligently pursue obtaining the appropriate PSI for its employees prior to assigning them to work this task order.

Authorized user access to information systems is based on the assigned duties and the Automated Data Processing (ADP) position categories identified in DoD 5200.2-R, Appendix 10. All positions on this contract are ADP-II category (also referred to as IT-II) and are Noncritical-Sensitive Positions requiring a SECRET Security Clearance based on a NACLC/ANACI background investigation.

Computer and Network Access Requirements: Contractor personnel working on this contract must complete the required security investigation to obtain the required security clearance. This must be accomplished before operating government-furnished computer workstations or systems that have access to Air Force e-mail systems or computer systems that access classified information.

In accordance with DoD 5200.2-R, Personnel Security Program (Jan 87), contractor personnel using unclassified automated information systems, including e-mail, shall have, at a minimum, a completed favorable National Agency Check plus Written Inquiries (NACI).

The contractor shall comply with the DoD 5200.2-R, Personnel Security Program and AFI 33-119, Air Force Messaging, requirements. The Contract Security Classification Specification (DD Form

254) will encompass all security requirements.

All contractors located on military installations shall also comply with Operations Security (OPSEC) requirements as set forth in DoD Directive 5205.02, Operations Security Program and AFI 10-701, Operations Security.

The contractor must consider Anti-Terrorism (AT) measures when the effort could affect the security of operating forces (particularly in-transit forces), information systems and communications systems IAW DoD Instructions 2000.16, Anti-Terrorism Standards.

5.5. Transmission and Storage of Classified Material

No classified material or reports are anticipated under this task order; however, much of the documentation is marked as For Official Use Only (FOUO) and must be stored and handled properly.

5.6. Protection of System Data

The contractor shall protect system design-related documents and operational data whether in written form or in electronic form via a network in accordance with all applicable policies and procedures for such data, including DoD Regulation 5400.7-R and DoD Manual 5200.01(v1-v4) to include latest changes, and applicable service/agency/ combatant command policies and procedures. The contractor shall protect system design related documents and operational data at least to the level provided by Secure Socket Layer (SSL)/Transport Security Layer (TSL)-protected web site connections with certificate and or user ID/password-based access controls. In either case, the certificates used by the contractor for these protections shall be DoD or IC approved Public Key Infrastructure (PKI) certificates issued by a DoD or IC approved External Certification Authority (ECA) and shall make use of at least 128-bit encryption.

5.7. Sensitive Data

Personnel may be required to have access to sensitive data during performance of this task order. Contractor and subcontractor personnel shall not divulge any information about files, data processing activities or functions, user IDs, passwords, information covered by the Privacy Act of 1974, or any other sensitive knowledge.

5.8. System and Network Authorization Access Requests

Contractor personnel will require access to DoD, DISA, or Air Force computing equipment or networks, and shall have the employee, prime or subcontracted, sign and submit a System Authorization Access Report (SAAR), DD Form 2875.

6. CONTRACTUAL REQUIREMENTS

6.1. Contractors Use of NETCENTS-2 Products Contract

The contractor shall obtain all products and associated peripheral equipment required of this task order from the NETCENTS-2 Products contract as stipulated in Section H Clause H098 of the ID/IQ contract.

6.2. Place of Performance

The primary place of performance will be the on Gunter Annex, Maxwell AFB AL. Travel to other

Government or contractor facilities is not contemplated as part of this task order but may be required. If so, the CO will provide specific travel requests and instructions. No exercise and deployment support is contemplated at any location other than Maxwell AFB-Gunter Annex, AL

6.3. Normal Hours of Operation

The average workweek is 40 hours; the average workday is 8 hours and the window in which those 8 hours are normally scheduled between 7:30 AM and 4:30 PM, Monday through Friday, except for days listed below as Government Holidays. However, the government may require the contractor to provide support during other than normal hours and surge in war fighting activity.

The following legal holidays are observed:

- New Year's Day, January 1st
- Dr. Martin Luther King, Jr. Day, 3rd Monday in January
- Washington's Birthday, 3rd Monday in February
- Memorial Day, Last Monday in May
- Independence Day, July 4th
- Labor Day, 1st Monday in September
- Columbus Day, 2nd Monday in October
- Veterans Day, November 11th
- Thanksgiving Day, 4th Thursday in November
- Christmas Day, December 25th

Note: In accordance with the Office of Personnel Management (OPM), when a holiday falls on a nonworkday -- Saturday or Sunday -- the holiday usually is observed on Monday (if the holiday falls on Sunday) or Friday (if the holiday falls on Saturday). The COR will advise the contractor of any observances that fall outside usual practices.

6.4. Government Furnished Property

The Government will furnish or make available working space, network access, and equipment to include:

a. Windows PC with Microsoft Office Suite (Outlook, Word, Excel, PowerPoint, etc.)
b. Telephone (local and long distance calls authorized as dictated by contract performance requirements)
c. Facsimile
d. Copier
e. Printer

Copies of required Government furnished materials cited in the solicitation, PWS, DD Form 254, and/or in the contract will be provided to the contractor in hard copy or soft copy. All materials will remain the property of the Government and will be returned to the cognizant Government QAP upon request or at the end of the contract period of performance.

6.5. Billable Hours

In order for man-hours to be billed, deliverable services must have been performed in direct support of a requirement in this PWS. In the course of business, situations may arise where Government facilities may not be available for performance of the TO requirements (i.e., base closure due to weather, Force Protection conditions, etc.). When the base is officially closed no contractor services will be provided and no charges will be incurred and/or billed to any TO. There

may also be occasions when support contractors are invited to participate in morale and recreational activities (i.e., holiday parties, golf outings, sports days and other various social events). Contractor employees shall not be directed to attend such events by the Government. Since a contract employee is not a government employee, the contract employee cannot be granted the same duty time activities as Government employees. Participation in such events is not billable to the TO and contractor employee participation should be IAW the employees' company's policies and compensation system.

6.6. Non-Personal Services

The Government will neither supervise contractor employees nor control the method by which the contractor performs the required tasks. Under no circumstances shall the Government assign tasks to, or prepare work schedules for, individual contractor employees. It shall be the responsibility of the contractor to manage its employees and to guard against any actions that are of the nature of personal services or give the perception of personal services. If the contractor feels that any actions constitute, or are perceived to constitute personal services, it shall be the contractor's responsibility to notify the Task Order (TO) Contracting Officers CO immediately. These services shall not be used to perform work of a policy/decision making or management nature, i.e., inherently Governmental functions. All decisions relative to programs supported by the contractor shall be the sole responsibility of the Government. These operating procedures may be superseded by Theater Commander's direction during deployments.

6.7. Contractor Identification

All contractor/subcontractor personnel shall be required to wear AF-approved or provided picture identification badges so as to distinguish themselves from Government employees. When conversing with Government personnel during business meetings, over the telephone or via electronic mail, contractor/subcontractor personnel shall identify themselves as such to avoid situations arising where sensitive topics might be better discussed solely between Government employees. Contractors/subcontractors shall identify themselves on any attendance sheet or any coordination documents they may review. Electronic mail signature blocks shall identify their company affiliation. Where practicable, contractor/subcontractors occupying collocated space with their Government program customer should identify their work space area with their name and company affiliation. ***Refer to Clause H063 of the overarching ID/IQ contract.***

6.8. Performance Reporting

The contractor's task order performance will be monitored by the Government and reported in Contractor Performance Assessment Reports (CPARs) or a Customer Survey, depending on the dollar amount of the task order. Performance standards shall include the contractor's ability to provide or satisfy the following:

- Provide satisfactory solutions to requirements with the necessary customer support.
- Provide solutions and services that meet or exceed specified performance parameters.
- Deliver timely and quality deliverables to include accurate reports and responsive proposals.
- Ensure solutions to requirements are in compliance with applicable policy and regulation.

6.9. Program Management/Project Management

The contractor shall identify a Program Manager or a Project Manager who shall be the primary representative responsible for all work awarded under this task order, participating in Program/Project Management Reviews and ensuring all standards referenced herein are adhered to.

6.9.1. Services Delivery Summary

Reference Section 7, Services Delivery Summary, of this PWS for specific performance objectives.

The contractor's performance at the contract level will be assessed quarterly by a process that measures success towards achieving defined performance objectives. The Services Delivery Summary will be in accordance with AFI 63-101, Acquisition and Sustainment Life Cycle Management, AFI 10-601, Capabilities-Based Requirements Development and FAR Subpart 37.6, Performance-Based Acquisition.

6.9.2. Task Order Management

The contractor shall establish and provide a qualified workforce capable of performing the required tasks. The workforce may include a project/task order manager who will oversee all aspects of the task order. The contractor shall use key performance parameters to monitor work performance, measure results, ensure delivery of contracted product deliverables and solutions, support management and decision-making and facilitate communications. The contractor shall identify risks, resolve problems and verify effectiveness of corrective actions. The contractor shall institute and maintain a process that ensures problems and action items discussed with the Government are tracked through resolution and shall provide timely status reporting. Results of contractor actions taken to improve performance shall be tracked and lessons learned incorporated into applicable processes. The contractor shall establish and maintain a documented set of disciplined, mature and continuously improving processes for administering all contract and Task Order efforts with an emphasis on cost-efficiency, schedule, performance, responsiveness and consistently high-quality delivery. The contractor shall provide transition plans as required.

6.9.3. Documentation and Data Management

The contractor shall establish, maintain, and administer an integrated data management system for collection, control, publishing, and delivery of all program documents. The data management system shall include but not be limited to the following types of documents: CDRLs, White Papers, Status Reports, Audit Reports, Agendas, Presentation Materials, Minutes, Contract Letters, and Task Order Proposals. The contractor shall provide the Government with electronic access to this data, including access to printable reports. Access does not replace the requirement to deliver required documentation to the Government.

6.9.4. Records, Files, and Documents

All physical records, files, documents, and work papers, provided and/or generated by the Government and/or generated for the Government in performance of this PWS, maintained by the contractor which are to be transferred or released to the Government or successor contractor, shall become and remain Government property and shall be maintained and disposed of IAW AFMAN 33-363, Management of Records; AFI 33-364, Records Disposition – Procedures and

Responsibilities; the Federal Acquisition Regulation, and/or the Defense Federal Acquisition Regulation Supplement, as applicable. Nothing in this section alters the rights of the Government or the contractor with respect to patents, data rights, copyrights, or any other intellectual property or proprietary information as set forth in any other part of this PWS or the Application Services contract of which this PWS is a part (including all clauses that are or shall be included or incorporated by reference into that contract).

6.9.5. Personnel Security

Individuals performing work under these task orders shall comply with applicable program security requirements as stated in the task order.

This task orders may require personnel security clearances up to and including Top Secret and may require all employees to be United States citizens. The security clearance requirements will depend on the security level required by the proposed task order. The task orders may also require access to sensitive compartmented information (SCI) for which SCI eligibility will be required. Contractors shall be able to obtain adequate security clearances prior to performing services under the task order. The Contract Security Classification Specification (DD Form 254) will be at the basic contract and task order level and will encompass all security requirements.

All contractors located on military installations shall also comply with Operations Security (OPSEC) requirements as set forth in DoD Directive 5205.02, Operations Security Program and AFI 10-701, Operations Security. In accordance with DoD 5200.2-R, Personnel Security Program (Jan 87), DoD military, civilian, consultants and contractor personnel using unclassified automated information systems, including e-mail, shall have, at a minimum, a completed favorable National Agency Check plus Written Inquiries (NACI).

The types of Personnel Security Investigations (PSI) required for the contractor vary in scope of investigative effort depending upon requirements of the Government and/or conditions of the Task Order. In cases where access to systems such as e-mail is a requirement of the Government, application/cost for the PSI shall be the responsibility of the Government. In cases where access to systems is as a condition of the Task Order, application/cost for the appropriate PSI shall be the responsibility of the contractor. In such instances, the contractor shall diligently pursue obtaining the appropriate PSI for its employees prior to assigning them to work any active task order. Acquisition planning must consider Anti-Terrorism (AT) measures when the effort to be contracted could affect the security of operating forces (particularly in- transit forces), information systems and communications systems IAW DoD Instructions 2000.16 Anti-Terrorism Standards.

6.9.6. Transmission of Classified Material

The contractor shall transmit and deliver classified material/reports IAW the National Industrial Security Program Operating Manual (DoD 5220.22-M). These requirements shall be accomplished as specified in this task order.

6.9.7. Protection of System Data

Unless otherwise stated in the task order, the contractor shall protect system design-related documents and operational data whether in written form or in electronic form via a network in accordance with all applicable policies and procedures for such data, including DoD Regulation 5400.7-R and DoD Manual 5200.01(v1-v4) to include latest changes, and applicable

service/agency/combatant command policies and procedures. The contractor shall protect system design related documents and operational data at least to the level provided by Secure Sockets Layer (SSL)/Transport Security Layer (TSL)-protected web site connections with certificate and or user ID/password-based access controls. In either case, the certificates used by the contractor for these protections shall be DoD or IC approved Public Key Infrastructure (PKI) certificates issued by a DoD or IC approved External Certification Authority (ECA) and shall make use of at least 128-bit encryption.

6.9.8. System and Network Authorization Access Requests

For contractor personnel who require access to DoD, DISA or Air Force computing equipment or networks, the contractor shall have the employee, prime or subcontracted, sign and submit a System Authorization Access Report (SAAR), DD Form 2875.

6.9.9. Travel

The contractor shall coordinate specific travel arrangements with the individual Contracting Officer or Contracting Officer's Representative to obtain advance, written approval for the travel about to be conducted. The contractor's request for travel shall be in writing and contain the dates, locations and estimated costs of the travel in accordance with the basic contract clause H047.

If any travel arrangements cause additional costs to the task order that exceed those previously negotiated, written approval by CO is required, prior to undertaking such travel. Costs associated with contractor travel shall be in accordance with FAR Part 31.205-46, Travel Costs. The contractor shall travel using the lower cost mode transportation commensurate with the mission requirements. When necessary to use air travel, the contractor shall use the tourist class, economy class, or similar accommodations to the extent they are available and commensurate with the mission requirements. Travel will be reimbursed on a cost reimbursable basis; no profit or fee will be paid. No profit or fee will be added; however, DCAA approved burden rates are authorized.

6.9.10. Other Direct Cost (ODC)

The contractor shall identify ODC and miscellaneous items as specified in each task order. No profit or fee will be added; however, DCAA approved burden rates are authorized.

6.10. Training

Contractor personnel are required to possess the skills necessary to support their company's minimum requirements of the labor category under which they are performing. Training necessary to meet minimum requirements will not be paid for by the Government or charged to TOs by contractors.

6.10.1. Mission-Unique Training

In situations where the Government organization being supported requires some unique level of support because of program/mission-unique needs, then the contractor may directly charge the TO on a cost reimbursable basis. Unique training required for successful support must be specifically authorized by the TO CO. Labor expenses and travel related expenses may be allowed to be billed on a cost reimbursement basis. Tuition/Registration/Book fees (costs) may also be recoverable on a cost reimbursable basis if specifically authorized by the TO CO. The agency requiring the unique support must document the TO file with a signed memorandum that such contemplated labor,

travel and costs to be reimbursed by the Government are mission essential and in direct support of unique or special requirements to support the billing of such costs against the TO.

6.10.2. Other Government-Provided Training

The contractor's employees may participate in other Government provided training, on a non-discriminatory basis as among contractors, under the following circumstances:

- The contractor employees' participation is on a space-available basis,
- The contractor employees' participation does not negatively impact performance of this task order,
- The Government incurs no additional cost in providing the training due to the contractor employees' participation, and
- Man-hours spent due to the contractor employees' participation in such training are not invoiced to the task order.

6.11. Data Rights and Non-Commercial Computer Software

In order to implement the provisions at DFARS 252.227-7013(b) and (e) and DFARS 252.227-7014(b) and (e) and DFARS 252.227-7017, the contractor shall disclose to the ordering Contracting Officer and ordering office in any proposal for a task order, or after award of a task order if not previously disclosed in the proposal, any technical data or non-commercial computer software and computer software/source code documentation developed exclusively at government expense in performance of the task order. This disclosure shall be made whether or not an express requirement for the disclosure is included or not included in the PWS or solicitation for the order. The disclosure shall indicate the rights asserted in the technical data and non-commercial computer software by the contractor and rights that would be acquired by the government if the data or non-commercial software was required to be delivered under the task order and its CDRL requirements and any cost/price associated with delivery. This disclosure requirement also applies to segregable routines of non-commercial software that may be developed exclusively at Government expense to integrate Commercial Software components or applications provided under a commercial software license or developed to enable Commercial Software to meet requirements of this Task Order. Performance of this disclosure requirement shall be considered a material performance requirement of any task order under which such technical data or non-commercial computer software is developed exclusively at Government expense.

6.12. Software Support and Data Rights

Unless specified otherwise in the Task Order, the contractor shall fully support all unique software developed to support integrated solutions on this contract. The contractor shall be able to support all software revisions deployed or resident on the system and sub-systems. The data rights ownership/licensing guidance is specified in Section I, Clause 252.227-7013 and 252.227-7015 in the overarching contract section B, Defense Federal Acquisition Regulation Supplement Contract Clauses.

6.13. COTS Manuals and Supplemental Data

The contractor shall provide documentation for all systems services delivered under this Task Order. The contractor shall provide COTS manuals, supplemental data for COTS manuals, and documentation IAW best commercial practices. This documentation shall include users' manuals,

operators' manuals, maintenance manuals, and network and application interfaces if specified in the task order. (A007, A011).

6.14. Enterprise Software Initiative

In situations where the purchase of new COTS software is needed to satisfy the requirements of a particular task order, the contractor shall use available existing enterprise licenses. If enterprise licenses are unavailable, then products will be obtained via the DoD Enterprise Software Initiative (ESI) Blanket Purchase Agreements (BPAs). If products are unavailable from ESI, then products will be acquired through the NETCENTS-2 Products contract. The updated listing of COTS software available from DoD ESI sources can be viewed on the web at http://www.esi.mil.

6.15. Software License Management

For government provisioned development, integration, test, and User First Look instances that require and/or contain COTS, the contractor shall provide maintenance and support of those software licenses to manage their relationship to the overall system life-cycle, which would include applications, license agreements, and software upgrades. The contractor shall provide asset inventory and services that track maintenance agreements, service contracts, and licenses (A003). The contractor shall provide support summary information to include the license ordering information, deployment and support of the products included in the license or maintenance agreement. The contractor shall support common practices for ordering assets, tracking orders and assets, and tagging the assets. The contractor shall support application installation, operations, customer support, training, maintenance, sustainment, and configuration control, to include the procurement of supporting software licenses.

6.16. Transition Plans, Transition-Out Services (End-of-Contract)

When ordered by the Government, the contractor shall transition services to the Government or a follow on contractor in accordance with FAR 52.237-3 "Continuity of Services." Within 30 Days of issuing the order for transition services, the Government will identify the services contractor who shall perform throughout the Termination Period ("Critical Services"). The contractor shall provide and perform all services in accordance with the conditions and support parameters stated in this PWS.

Upon receipt of order, the contractor shall collaborate with stakeholders, including related IT service providers, to develop an Exit Plan. The Exit Plan shall articulate the activities and roles and responsibilities, as well as the timetable, documentation and data, required for completing an orderly transition to the Government Organization(s) and/or contractor(s), following termination or expiration of the contract regardless of the cause. Upon approval of the plan, the contract shall transition the services to the successor in accordance with the approved Exit Plan. (A010)

7. SERVICES DELIVERY SUMMARY

The contractor's performance at the contract level will be assessed quarterly by a process that measures success towards achieving defined performance objectives. The Services Delivery Summary will be in accordance with AFI 63-101, Acquisition and Sustainment Life Cycle Management, AFI 10-601, Capabilities-Based Requirements Development and FAR Subpart 37.6, Performance-Based Acquisition. Attachment 1 contains the Quality Assurance Surveillance Plan (QASP).

Table 1 – Performance Objectives

Desired Outcome		Performance	Performance Threshold	
Overall Outcome	**Specific Outcome**	Objective	**Target**	**Tolerance**
Efficient use of hardware through resource pooling across multiple war planning and execution capabilities	Contractor identifies efficiencies and opportunities for resource pooling	Semi-annual Environment Capacity Plan addresses opportunities for reducing capacity needs or pooling of resources	More than one opportunity identified per year	One opportunity identified per year
Efficient scalability to accommodate new configuration items, expanded configuration items, or additional users that are geographically dispersed	Contractor identifies opportunities for improving scalability	Semi-annual Environment Capacity Plan addresses scalability considerations (applies to lifecycle tools as well as environments; may include recommendations for different COTS products)	More than one consideration identified per year	One consideration identified per year
Faster deployment of software and capabilities through standardization and continuous integration	Environment build times reduced and/or improvement made to continuous integration	Contractor implements methods or processes that increase speed of builds or improve Government's ability to perform continuous integration	More than one improvement identified per year	One improvement identified per year
Support to application sustainers and application developers with infrastructure interoperability, practical knowledge, and development environments	Availability of environments does not impede development contractor	Development environments delivered on time (no later than the COR approved need date)	Development environments provided on-time 100% of the time	Development environments provided on-time 90% of the time
Promote early and continuous collaboration among	Contractor maintains accurate system	IT systems inventory updates and accuracy	IT system inventories include all systems and	IT system inventories include all systems and

stakeholders (developers, testers, and users) throughout the development cycle	inventory, including hardware, software products		software and a 100% accuracy rate is maintained at all times	software and a 98% accuracy rate is maintained at all times
Share knowledge, experience and lessons learned related to infrastructure interoperability and development environments among developers to improve and accelerate software development and deployment	Contractor produces Lessons Learned documentation	Contractor produces Lessons Learned documentation to identify process improvements, standardization, or other knowledge which increases developer understanding some aspect of the infrastructure environment or lifecycle tools	More than one Lesson Learned or similar report produced per year	One Lesson Learned or similar report produced per year
Support rapid provisioning of development and test capabilities including timely instantiation and teardown of configurations of infrastructure services for sustainment and development purposes	Improvements identified	Contractor recommends changes to processes for provisioning, build, teardown, etc. which results in improvements	More than one recommendation per year	One recommendation per year
Compliance with Application Services Support requirements (delivery, quality)	Ensure compliance with Application Services deliverables requirements	Deliver the Application Services with predetermined outcomes on time	Documentation submitted IAW CDRLs verifies task order was completed on time	95% of the time.
	Ensure delivery of all	Completed on time or ahead of schedule	CDRLs are delivered as	95% of the time

	CDRLs by the contractor within the timeframe identified		identified	
	Ensure adherence to quality requirements of all CDRLs by the contractor	Quality CDRLs (conforming to design, specifications, or requirements are delivered according to performance parameters	CDRLs are delivered as identified	95% of the time
Compliance with Application Services Requirements	Ensure Application Services provided by the contractor are fulfilled within the timeframe identified by the task order	Task orders are completed on time or ahead of schedule	Documentation submitted IAW CDRLs verifies task order was completed on time	95% of the time
Meeting schedule commitments	Contractor successfully meets schedule milestones relating to infrastructure tasks in agreed upon master schedules	Meets milestones	100%	- 10%

7.1. Security Facility Clearance Requirements

No security clearances required.

7.2. Personnel Security Clearance Requirements

No security clearances required.

7.2.1. Additional Investigation Requirements

Anyone working on the contract that does not require a security clearance must have at a minimum a favorably adjudicated National Agency Check with Written Inquiries (NACI) investigation to access a government furnished information system or environment. This investigation must be submitted by the contract company. Note: AFI 31-501, and AFI 31-601 for unescorted entry to restricted areas, access to sensitive unclassified information, access to government automated information systems (AIS) and/or sensitive equipment.

7.3. Security Manager Appointment

The contractor shall appoint a security manager for the on base long-term visitor group. The security manager may be a full-time position or an additional duty position. The security manager shall provide contractor employees with training required by DoDM 5200.01, Volume 3, Enclosure 5, DoD Information Security Program, AFPD 31-4, Information Security and AFI 31-401, Information Security Program Management. The contractor security manager shall provide initial and follow-on training to contractor personnel who work in Air Force controlled or restricted areas. Air Force restricted and controlled areas are explained in AFI 31-101, Air Force Integrated Defense Plan.

7.4. Visit Requests

Contractors participating in the National Industrial Security Program are authorized to use Joint Personnel Adjudication System (JPAS) in lieu of sending Visitor Authorization Letters (VALs) for classified visit to Department of Defense facilities and military installations. VALs are only required if the contractor isn't using JPAS or if contractor personnel whom access level and affiliation are not accurately reflected in JPAS. However, some agencies may still require VALs to be submitted for access to their facilities. Visit requests must be sent to servicing government's security management office (SMO) code. The SMO code for AFLCMC Des is MG1MFD3Q6. Each contractor performing work on the contract will require a separate SMO Code visit request from the contactor. The visit request must include all prime and subcontract workers on the contract.

7.5. Obtaining and Retrieving Identification Media

As prescribed by the AFFAR 5352.242-9000 Contractor Access to Air Force Installations, AFFAR 5352.242-9001, Common Access Cards (CAC) for Contractor Personnel and FAR 52.204-9, Personal Identity Verification of Contractor Personnel, the contractor must comply with the requirements set forth in these guidance. Contractors requesting a CAC for personnel on the contract will submit on company letterhead the names and all other personnel information as prescribed by the contracting officer to begin the identification processing effort. Contracting officers will follow installation specific guidance regarding the issuance and recovery of all identification media issued to the contractors by the government. Failure to return all government issued identification upon termination of contract or service, termination of employees or expiration of the identification may result in withholding of final payment.

7.6. Pass and Identification Items

NOTE: Contact your local Security Office to determine the appropriate identification for this task order.]

The contractor shall ensure the following identification items as required for contract performance are obtained for employees:

- DoD Common Access Card (AFI 36-3026).
- Base-specific identification as required by local base and/or building security policies.

Failure to return all government issued identification upon termination of contract or service, termination of employees or expiration of the identification may result in withholding of final payment.

7.7. Visitor Group Security Agreement (VGSA)

The contractor shall enter into a long-term visitor group security agreement for contract performance on base. This agreement shall outline how the contractor integrates security

requirements for contract operations with the Air Force to ensure effective and economical operation on the installation. The agreement shall include:

- Security support provided by the Air Force to the contractor shall include storage containers for classified information/material, use of base destruction facilities, classified reproduction facilities, use of base classified mail services, security badging, base visitor control, investigation of security incidents, base traffic regulations and the use of security forms and conducting inspections required by DoD 5220.22-R, *Industrial Security Regulation,* Air Force Policy Directive 31-6, *Industrial Security,* Air Force Instruction 31- 601, *Industrial Security Program Management,* DoDM 5200.01, Volumes 1-4, *DoD Information Security Program,* and AFI 31-401, *Information Security Program Management.*

- Security support requiring joint Air Force and contractor coordination includes packaging classified information, mailing and receiving classified materials, implementing emergency procedures for protection of classified information, security checks and internal security controls for protection of classified material and high-value pilferable property.

- On base, the long-term visitor group security agreement may take the place of a *Standard Practice Procedure* (SPP).

7.8. Information Security

The contractors performing duties associated with this task order must adhere to all the standards for protecting classified information as specified in DoDM 5200.01, Volumes 1-4, *DoD Information Security Program*, Air Force Instruction 31-401, *Information Security Program Management* and all applicable supplements and operating instructions.

7.9. Unescorted Entry to Secure Rooms

Contractor personnel requiring unescorted entry to secure rooms designated by the installation commander shall comply with base access requirements and these additional security instructions; DoD 5200.2-R, *DoD Personnel Security Program,* AFI 31-101, *Air Force Integrated Defense Plan* and AFI 31-501, *Personnel Security Program Management* as applicable.

Contractor personnel shall be the subject of a favorably adjudicated National Agency Check with Local Agency Check (NACLC) investigation to qualify for unescorted entry to a secure room. Contractor personnel must contact their Contracting Officer Representative (COR) and the appropriate secure room monitor for permission.

7.10. Computer and Network Access Requirements

Contractor personnel working on this contract must be designated in one of the below AIS positions and complete the required security investigation to obtain the required security clearance. This must be accomplished before operating ***government furnished*** computer workstations or systems that have access to ***Air Force*** e-mail systems or computer systems that access classified information. The contractor shall comply with the DoD 5200.2-R, *Personnel Security Program* and AFMAN 33-152, *User Responsibilities and Guidance for Information Systems*, requirements. **(Please check one):**

( ) AIS-II Position - Noncritical-Sensitive Positions. Security Clearance: SECRET

based on a NACLC/ANACI background investigation. Responsibility for systems design, operation, testing, maintenance and/or monitoring that is carried out under technical review of higher authority in the AIS-I category, includes, but is not limited to; access to and/or processing of proprietary data, information requiring protection under the Privacy Act of 18 1974 and Government-developed privileged information involving the award of.

(X) AIS-III Position - Nonsensitive Positions. No security clearance required but is a **Trusted Position** based on a favorable NACI background investigation. All other positions involved in U.S. Government computer activities.

7.11. Reporting Requirements

The contractor shall comply with requirements from AFI 71-101, Volume-1 and *Criminal Investigations,* and Volume-2 *Protective Service Matters*. Contractor personnel shall report to an appropriate authority any information or circumstances of which they are aware may pose a threat to the security of DoD personnel, contractor personnel, resources and classified or unclassified defense information. Contractor employees shall be briefed by their immediate supervisor upon initial on-base assignment and as required thereafter.

7.12. Physical Security

Contractor employees shall comply with base Operations Plans/instructions for FPCON procedures, Random Antiterrorism Measures (RAMS) and Operation Security (OPSEC), Emergency Management (EM) and local search/identification requirements. The contractor shall safeguard all government property including controlled forms provided for contractor use. At the close of each work period, government training equipment, facilities, support equipment and other valuable materials shall be secured.

7.13. Wireless Electronic Devices

The following devices are not allowed in areas where classified information is discussed, briefed or processed: cell phones, camera cell phones, cordless telephones, wireless microphones, wireless keyboards, wireless mice, wireless or Infrared Local Area Networks (LANs). The term ***"Area"*** above refers to a room and/or to a space the size of a 3-meter radius sphere, centering on the classified source. In areas where classified information is discussed, briefed or processed, wireless pointer/mice devices are allowed for presentations only. This is an acceptable EMSEC risk. All other Personal Electronic Devices, PEDs. All other wireless PEDs not specifically addressed above, that are used for storing, and processing and/or transmitting information shall not be operated in areas where classified information is electronically stored, processed or transmitted.

7.14. Operating Instructions

The contractor will adhere to the all Air Force activity Operating Instructions (OI) and local Security Program Management for internal circulation control, protection of resources and to regulate entry into Air Force controlled areas during normal, simulated and actual emergency operations to include local written OIs.

7.15. Government Authorization

The contractor shall ensure its employees do not allow government issued keys to be used by personnel other than current authorized contractor employees. Contractor employees shall not use keys to open work areas for personnel other than contractor employees engaged in performance of duties, unless authorized by the government functional director.

7.16. Access Lock Combinations

Access lock combinations are "*For Official Use Only"* and will be protected from disclosure to unauthorized personnel. The contractor will adhere to the Air Force activity operating instructions ensuring lock combinations are not revealed to un-cleared /unauthorized persons and ensure the safeguard procedures are implemented. The contractor is not authorized to record lock combinations without written approval by the government functional director.

7.17. Security Combinations

Combinations to security containers, secure rooms or vaults are classified information and must be properly safeguarded. Only contractor employees, who have the proper security clearance and the need-to-know, will be given combinations to security containers, secure rooms or vaults. Contractor employees are responsible for properly safeguarding combinations. Contractor employees will not record security containers, secure rooms or vaults combinations without written approval by the government functional director. Contractors will not change combinations to security containers, secure rooms or vaults without written approval by the security officer and the government functional director.

7.18. Security Alarm Access Codes

Security alarm access codes are "*For Official Use Only*" and will be protected from unauthorized personnel. Security alarm access codes will be given to contractors employees who require entry into areas with security alarms. Contractor employees will adhere to the Air Force activity operating instructions and will properly safeguard alarm access codes to prevent unauthorized disclosure. Contractors will not record alarm access codes without written approval by the government functional director.

7.19. Freedom of Information Act Program (FOIA)

The contractor shall comply with DoD Regulation 5400.7-R/Air Force Supplement, *DoD Freedom of Information Act Program,* requirements. The regulation sets policy and procedures for the disclosure of records to the public and for marking, handling, transmitting and safeguarding for *Official Use Only (FOUO)* material. The contractor shall comply with AFI 33-332, *Air Force Privacy Act Program*, when collecting and maintaining information protected by the Privacy Act of 1974 authorized by Title 10, United States Code, Section 8013. The contractor shall maintain records in accordance with Air Force manual (AFMAN) 33-363, Management of Records; and disposed of in accordance with Air Force Records Information Management System (AFRIMS) Records Disposition Schedule (RDS) located at https://www.my.af.mil/gcss-af61a/afrims/afrims/.

7.20. Traffic Laws:

The contractor and their employees shall comply with all installation traffic regulations.

7.21. Cellular Phone Operation Policy

The contractor shall comply with local base policies regarding cellular phone operation.

7.22. Security Education and Training

The contractors are required to participate in the government's in-house and web-based security training program under the terms of the contract. The government will provide the contractor with access to the on-line system. Annually, all contractors will complete all required security training. Required annual training includes Force Protection (FP), Information Protection (IP), Cybersecurity and OPSEC. If contract team members will be using the SIPRNet, users will also have to comply with the organizational Derivative Classification Training as a condition of access.

8. DATA DELIVERABLES

The Government reserves the right to review all data deliverables for a period of 10 working days prior to acceptance. No data deliverable will be assumed to be accepted by the Government until the 10-day period has passed, unless the Government explicitly states otherwise in this task order.

The Government requires all deliverables that include Scientific and Technical Information (STINFO), as determined by the Government, be properly marked IAW DoD Directive 5230.24 and AFI 61-204 prior to initial coordination or final delivery. Failure to mark deliverables as instructed by the Government will result in non-compliance and non-acceptance of the deliverable. The contractor shall include the proper markings on any deliverable deemed STINFO regardless of media type, stage of completeness, or method of distribution. Therefore, even draft documents containing STINFO and STINFO sent via e-mail require correct markings. Additionally, as required by individual Task/Delivery Orders, the contractor shall formally deliver as a CDRL all intellectual property, software, licensing, physical records, files, documents, working papers, and other data for which the Government shall treat as deliverable.

CDRL #	Title & Data Item Description Reference	Sub-Title, Special Instructions, and PWS References
A001	Report, Record of Meeting Minutes DI-ADMN 81505	Meeting Minutes PWS ref 6.1
A002	Configuration Audit Summary Report DI-CMAN 81022C	In conjunction with configuration audits (PWS 4.1.9)
A003	Software Center Operator Manual DI-IPSC 81444A	Processes and Procedures for WPE Developmental Environment Use Adapt as need for ITIL and contractor format Draft 30 days after award Final 60 days after award Updates at 3 month intervals for additional topics and updates as needed, Topics to cover and references: --Use of Lifecycle Management Tools and Repository Structure (PWS ref 4.1.1) --Practices and Procedures for Day-to-day Operations (PWS refs 4.1.1, 4.1.2, 4.1.3, 4.1.7, 4.1.9, 4.1.11, 4.1.2, 4.1.13, 5.2)

CDRL #	Title & Data Item Description Reference	Sub-Title, Special Instructions, and PWS References
		--User First Look, Test Support Products and Process (PWS refs 4.1.13, 7.8)
A004	Status Report DI MGMT 80368A	Monthly (PWS ref 6.1)
A005	Status Report, Weekly DI-MISC 81183A	Weekly Status Report and Schedules Include schedule status for related PMO Integrated Master Schedule tasks Provide schedules of contractor's upcoming tasks (PWS ref 6.1, 6.2)
A006	Briefing Material DI-MGMT-81605	Introduction to the WPE Development and Sustainment Environment: (PWS ref 4.1.13) Performance Management Reviews (PWS ref 6.2)
A007	Technical Report DI-MSIC-80508B	Provide Technical Reports on the following topics (sub-titles) in coordination with the PMO's Integrated Master Schedule: -- Environment Capacity Plan and Report: Formally delivered capacity plan, to include forecasts of capacity needs and results of monitoring (planned vs. actual) (PWS ref 4.1.2) --Compliance of Software Deliverables: reports of examination and analyses of developer and sustainer delivered software for compliance with standards and architecture. Include lists of applicable standards and architectures; include any automated tests, checks, comparisons, or other evidence of compliance (PWS ref 4.1.9) --Standards Projections and Evaluations: Forecast and recommendations associated with standards and architectural evolution (PWS refs 4.1.2) --Contractor Information Assurance Plan: implementation activities to accomplish IA objectives (PWS ref 5.4) -- Ad Hoc Reports: The PMO may request Technical Reports for various topics, such as Impact Assessments for IA (PWS ref 4.1.14) or other issues, Lessons Learned,

CDRL #	Title & Data Item Description Reference	Sub-Title, Special Instructions, and PWS References
		etc. (PWS ref 4.1.3)
A008	Conceptual Design Drawings and Models DI-SESS 81001D	Environment Architecture and Specifications: Description and illustration of the overall environment. Other drawings and models to complement and illuminate briefings and deliverables, kept under configuration management, electronically accessible (PWS ref 4)
A009	Commercial Off-The-Shelf (COTS) Manual Supplemental Data DI-TMSS-81816	Provide supplemental data, procedures and implementation notes for initialization parameters, tailored software use instructions pertaining to COTS products employed in the environment, delivery timed to Initial Operating Capability of the product (PWS ref 7.6)
A010	Exit Plan	Final 60 days after award (PWS ref 7.9)
A011	Performance and Cost Report DI-FNCL-80912	Monthly Progress Report

9. APPLICABLE STANDARDS AND REFERENCES

The Contractor shall ensure that services, solutions and products meet the standards identified in the AF Standard Center of Excellence Repository (SCOER) located at http://www.netcents.af.mil/contracts/netcents-2/appsrvs/documents as well as the DISA GIG Technical Guidance Federation Information website located at https://gtg.csd.disa.mil/

In addition to the core Application Services Standards and References identified in the NETCENTS-2 contract, DCAPES requires the contractor meet the standards identified in the DCAPES Information Support Plans, to include the DoDAF architecture products, as applicable, and comply with the Joint Command and Control (JC2) Reference Architecture. The list below is not all-inclusive and the most current version of the document will take precedence.

- The JC2 Architecture products are available for download from:

  https://intelshare.intelink.gov/sites/jc2oa/default.aspx

- Deliberate and Crisis Action Planning and Execution Segments Information Support Plan (ISP), version 6.0.x, dated 12 January 2017, or most current version

- The basic references for architecture and ISPs are listed below:

  DoDI 8330.01, Interoperability of Information Technology (IT) and National Security Systems (NSS)

CJCSI 6212.01, Net Ready Key Performance Parameter

DoDAF v2.02, The DoDAF Architecture Framework Version,
https://dodcio.defense.gov/Library/DoD-Architecture-Framework/

APPENDIX A-1

DCAPES Software Patch Management Process

DCAPES_SW Patch Management Proces