Attachment 1
HTC711-19-Q-D024
Amendment 3

PERFORMANCE WORK STATEMENT FOR
UNITED STATES TRANSPORTATION COMMAND
MILITARY SURFACE DEPLOYMENT AND DISTRIBUTION COMMAND (SDDC)
DEPUTY CHIEF OF STAFF (DCS) FOR INFORMATION MANAGEMENT (G6)
SDDC IT SUPPORT SERVICES (SCITSS) CONTRACT

1 September 2019

This page left intentionally blank

PERFORMANCE WORK STATEMENT (PWS)
SDDC/USTRANSCOM/TCC
SDDC IT Support Services

Table of Contents

PERFORMANCE WORK STATEMENT
SDDC Cloud IT Support Services
October 2019

1.0 DESCRIPTION OF SERVICES

1.1 Background.

As the Army component of the United States Transportation Command (USTRANSCOM) and a major Department of Army (DA) Command, SDDC performs a vital role for the Department of Defense (DOD) in deploying, redeploying, and sustaining United States forces worldwide. To facilitate this mission, SDDC has developed a number of integrated transportation and business system capabilities that support the various DOD functional, financial and operational elements. SDDC's technology programs leveraged against new technologies within the command have increased the efficiency, effectiveness and security of DOD's business processes.

The Information Management Automated Systems Division, AMSSD-IMA, is responsible for effectively integrating plans, programs, projects, automated systems, and operations, encompassing a wide range of information management disciplines and transportation functional components. To meet this objective, AMSSD-IMA has minimized redundancy and improved interoperability and efficiencies among SDDC systems, organizational components, business processes, and customers by performing enterprise-wide IT activities in a centralized environment. This environment includes IT infrastructure hosted in a virtualized environment on shared hardware and software; coordinated and integrated system and application requirements; centrally managed interfaces; and integration of new and existing technology to enhance Enterprise's IT activities and infrastructure to support the DOD's net-centric environment. Currently, AMSSD-IMA is migrating its hosted business systems into the USTC GovCloud. This move further reduces redundant hosting services, improves application response time, throughput, and reduces the cost associated with application hosting and IT infrastructure support.

1.2 Scope.

The purpose of this contract is to provide SDDC Cloud IT Support Services and SDDC GovCloud IT Support Services. This contract will manage the use, performance, delivery of IT services both on-premises (on-prem), and in the GovCloud, in addition to, cloud services support between the cloud provider (USTC's / cloud service provider (CSP) and cloud consumers (SDDC, USTC and AMC systems that SDDC manages). It will provide database engineering, systems administration and infrastructure support services, operating system and virtual private cloud (VPC) engineering, DevOps pipeline support of SDDC, USTC and AMC business and transportation applications that SDDC manages. These services will apply to SDDC business/transportation systems hosted in the USTC GovCloud and the existing systems residing in the locally maintained centralized enclave (CE) a.k.a. On-Prem. Specifically, the contractor shall provide the following types of services in support of the SDDC, USTC and AMC, business and transportation systems both locally (CE) and in the GovCloud that SDDC manages or will manage.

A. GovCloud and On-Prem IT Support Services
B. Cloud Services and Cloud Tool Support Services (e.g. Azure, AWS, and Google Cloud etc.) to support the operational hosting environment (e.g. provisioning, storage, configuration, management, deploy, monitoring, disaster recovery etc.)
C. Application Migration (Lift and Shift) to the GovCloud
D. Application Refactoring/Redeveloping or Reinstall applications to Cloud Native
E. Sustainment and Maintenance of current On-Prem/GovCloud applications, services and systems
F. Decommissioning of CE/On-Prem infrastructure and hardware to include offsite locations No Later Than 30 September 2020
G. Engineering and Sustaining Virtual Private Clouds, Active Directory, Gateways, Firewalls, DNS, Load Balancing etc.
H. Operating System/ System Administration (OS/SA) support for Windows, x86 and RHEL operating systems.

I. Database Engineering Support (DBA) Oracle, MS SQL
J. Secure File Transfer Protocol(SFTP), Electronic Data Interface (EDI), Managed File Transfer System (MFTS), Secure Mail Transport Protocol (SMTP)
K. Information Assurance Vulnerability Assessment (IAVA) remediation and mitigation
L. Host Based Security Systems (HBSS)
M. Engineering, Administration and Management Support Services for Windows Server Update Services (WSUS), Microsoft System Center Configuration Manager (SCCM) Red Hat Satellite server
N. Centrify infrastructure server administration and support where applicable
O. Tier II/III Application, DBA and SA Support break fix support
P. Information Assurance Infrastructure Only Support/ Patch Management, Access Management and STIG
Q. Cybersecurity/Information Assurance artifacts to support the DOD Risk Management Framework (RMF) and where approved, DIACAP process to achieve Interim Authority to Test (IATT) and/or Authority to Operate (ATO) for Initial operational capability (IOC) thru fully operational capable (FOC) of the application.

The Contractor shall coordinate with the Government to ensure all activities are well synchronized and integrated with other SDDC/USTRANSCOM/AMC efforts.

Unless otherwise specified in this PWS, all days designated are calendar days. The Contractor shall authorize periodic Government inspections and reviews to ensure compliance with DOD requirements.

The PWS includes the following task areas, which shall be severable CLINS/Task Areas:

Task Area 1: Contract Level and Project Management
Task Area 2: Sustainment and Maintenance (On-Prem)*
Task Area 3: Sustainment and Maintenance (GovCloud)
Task Area 4: Enhancements/Application Migration (GovCloud)
Task Area 5: Configuration Management (On Prem)*
Task Area 6: Configuration Management (GovCloud)
Task Area 7: Information Assurance (On Prem)*
Task Area 8: Information Assurance (GovCloud)

* It is the Government's intent to decommission the On-Prem environment by 30 September 2020 and it is anticipated that On-Prem Support Services will no longer be needed after this date. Tasks 2, 5, and 7 are marked optional for potential use after Option Period 1.

1.3 Specific Tasks

1.3.1 Task Area 1: Contract Level and Project Management.

This task consists of the functional activities relating to the administration and management of this effort. The contractor shall provide project management of all projects and tasks within the scope of this contract. The Contractor's Lead principal project manager shall have oversight of all tasks and projects within the scope of this contract.

1.3.1.1 Subtask 1: Monthly Status Reporting (MSR).

The contractor shall prepare and sustain a project Work Breakdown Structure (WBS) and integrated master schedule that defines all tasks, sub tasks, durations, resources, and dependencies for all projects on this contract. The milestone schedule shall be created in Microsoft Project and provided no later than the 5th business day of each month as part of the MSR. The project WBS and integrated master schedule shall be maintained and kept up-to-date to identify all in-progress and planned projects, hardware and software upgrades or changes (routine and complex), and related SDDC/G6 GovCloud IT Support Services/On Prem tasks as they progress to completion. The contractor shall deliver the project WBS and integrated master schedule with each of the lowest level tasks not exceeding four

(4) weeks duration and each lowest level task having a predecessor task that describes the dependence on the start or finish of another task in the project integrated master schedule.
The MSR format shall be approved by the COR and contain:

- A brief synopsis of the efforts completed, deliverables provided, conferences/trips conducted or attended during the reporting period
- Project WBS and integrated master schedule
- Risk assessment and mitigation recommendations
- Proposed activities NOT included in the Project WBS and integrated master schedule, including planned Authorized System Interruption (ASI)'s for the following month
- Monthly report of hours/employee for labor hour tasks

Deliverable: MSR no later than the 5th business day of the month

1.3.1.2 Subtask 2: Quarterly Program Management Reviews (PMRs)

The contractor shall participate in *quarterly* PMRs as scheduled by the COR to begin the first month of each contract period; meeting typically lasts no more than an hour. The contractor shall present status, progress, recommendations, and concerns in the development of any tasks or documentation described within this PWS. The presentation shall reflect resolution to prior PMR actions items, new action items, record discussion activity, decisions made, date, locations, attendees, and a copy of the presentation slides used. The contractor shall provide the draft PMR slides to the COR and to the SDDC/G6 GovCloud Program Manager no later than two (2) days prior to the meeting, and minutes of the PMR no later than five (5) business days after the meeting

Deliverable: Draft PMR slides no later than two (2) days prior to the meeting; PMR slides, to include updates to the Project WBS and integrated master schedule, provided at the meeting.

1.3.1.3 Subtask 3: Employment Status Report.

The contractor shall provide an employee status report (listing/spreadsheet) containing names and labor categories of personnel supporting the tasks identified in paragraph 1.2. The report shall be provided within thirty (30) calendar days after contract award and updates to the COR no later than 4:00 PM central time the first work day of the following week after contractor staffing levels or personnel are changed.

Deliverable: Employment Status Report, within thirty (30) calendar days of contract award; updates no later than 4:00 PM central time the first work day of the following week after contractor staffing levels or personnel change.

1.3.1.4 Subtask 4: Contractor Management Report (CMR).

The Office of the Assistant Secretary of the Army (Manpower & Reserve Affairs) operates and maintains a secure Army data collection site where the contractor shall report ALL contractor man-power (including subcontractor manpower) required for performance of this contract. The contractor shall completely fill in all the information in the format using the following web address https://www.ecmra.mil/Default.aspx. The required information includes:

(1) Contracting Office, Contracting Officer, Contracting Officer's Representative
(2) Task order number
(3) Beginning and ending dates covered by reporting period
(4) Contractor name, address, phone number, e-mail address, identity of contractor employee entering date
(5) Estimated direct labor hours (including sub-contractors)
(6) Estimated direct labor dollars paid this reporting period (including sub-contractor)
(7) Total payments (including subcontractor)
(8) Predominant FSC for each sub-contractor if different
(9) Estimated data collection cost

(10) Organizational title associated with the UIC for the Army Requiring Activity (the Army Requiring Activity is responsible for providing the contractor with its UIC for the purposes of reporting this information)
(11) Locations where contractor and sub-contractors perform the work (specified by zip code in the United States and nearest city, country, when in an overseas location, using standardized nomenclature provided on website)
(12) Presence of deployment or contingency contract language
(13) Number of contractor and sub-contractor employees deployed in theater this reporting period (by country).

In addition, the contractor shall submit estimated total cost (if any) incurred to comply with the reporting requirement. Reporting period will be the period of performance not to exceed 12 months ending 30 September of each Government fiscal year and shall be reported NLT 31 October of each Government fiscal year. Assistance or questions about the CMR may be directed to the CMR Helpdesk by phone at 703-377-6199 or E-mail contractormanpower@hqda.army.mil or website: https://www.ecmra.mil/help/help.html

Deliverable: CMR update, 10 days prior to 31 October of each calendar year of the contract.

1.3.1.5 Subtask 5: Meeting Agenda/Meeting Minutes.

The contractor shall provide a meeting agenda and meeting minutes for all meetings as specified in each Task Area. The contractor shall provide the meeting agenda two business days prior to each meeting, and meeting minutes two business days following completion of each meeting.

Deliverable: Meeting agenda /meeting minutes. Agenda two (2) business days before the meeting; Minutes two (2) business days after the meeting.

1.3.2 Task Area 2: Sustainment and Maintenance On-Prem. (Optional after Option Period 1)

The contractor shall support the SDDC CE PoR Dev, Staging, Altsite, Test and Production. The Contractor shall provide non- duty hour support to the CE/ PoR sustainment and maintenance support to enable all on-prem systems, services and capabilities are fully functioning. The Contractor shall provide break fix on-prem support on normal duty days between the hours of 0700-1700 CT and during Authorized Maintenance periods (2000-0200 CT) usually the 2nd and 4th Wednesday of the month. At all other times, the Contractor shall provide emergency support either on-site or via SDDC approved remote access solution provided by the Government in order to respond within 30 minutes or less to On-Prem emergency support requests.

The contractor shall provide the operational support in the form of operating system and database engineering/administration, virtual machines and infrastructure support; network engineering to maintain applications capabilities hosted On-Prem/ CE environments. The contractor shall maintain SDDC applications database instances (SQL and, Oracle) in the CE environments. Backup and Recovery, Electronic Data Interface (EDI), MFTS, File Transfer, virtual machine images for Windows, x86 and RHEL server architectures for applications hosted in the Centralized Enclave.

1.3.2.1 Subtask 1: Maintenance and Sustainment of SDDC IT Infrastructure

The contractor shall provide technical engineering and sustainment support for the CE production, Training, Altsite, Staging, Testing, and Development environments for all systems shown in Appendix C.

The contractor shall provide technical engineering sustainment support including, but is not limited to network engineering and maintenance, enterprise CE support services, storage management, and backup and recovery management. Database administration and System administration. Operating system upgrades and patching and. technical requirements gathering for migrating applications/systems to the GovCloud.

The contractor shall migrate both SDDC On-Prem systems/applications and enterprise support services to the GovCloud to include EDI/MFTS. These services will facilitate On-Prem to Cloud support and vice versa, for applications that rely on these on-prem enterprise services to be operationally ready, where these GovCloud services not yet offered, or until identical type services are available in GovCloud.

The contractor shall resolve all Information Assurance Vulnerability Assessment (IAVA) reports within the periods specified within the IAVA. IAVA resolution may include implementing new technical solutions, patches and upgrades in the production, pre-production and DevOps environments/pipelines.

The contractor shall support the SDDC On-Prem IT infrastructure until decommissioned, which presently includes but is not limited to the following: Fifty-Five (55) Solaris servers with 30 global zones and 110 non-global zones. Sixty (60) Windows servers and 800 Virtual Machines; 80 Cisco/F5 Switches, 15 Avocent Keyboard/Video/Mouse (KVM), 15 DIGI Keyboard/Video/Mouse (KVM), 12 NetApp Storage appliances, 5 DXI backup appliances 55 Oracle databases, SQL databases and one EM7 Monitoring server. These servers and appliances are not static and may change in number and type.

The contractor shall provide technical sustainment support to include (but not limited to):

A. Provide hardware, network, firewall, operating system, database and assist application teams in application sustainment of On-Prem
B. Maintain load balancing, fail over procedures, and automated testing support utilizing provided tools and business rules in On-Prem
C. Provide support, configuration installation and maintenance of an enterprise backup and recovery solutions for applications On-Prem
D. Provide proactive monitoring on the core operating systems and databases on all SDDC hosted systems for On-Prem where applicable.
E. Coordinate and cooperate with the SDDC, USTC and IA/Cyber Program Manager Offices (PMO) to maintain compliance with the current governance for the certification and accreditation process to help them maintain their Authority to Operate (ATO) and Interim Authority to Operate (IATO).
F. Assist application teams providing application support to facilitate third party Security Accreditation testing.
G. Facilitate meetings with application PMs and their POCs in the development and maintenance of Service Level Agreements (SLA's). Service Level Agreements shall include, but are not limited to application technical and software requirements and architecture; release and change control processes; points of contact including roles and responsibilities; escalation procedures; Mission Assurance Category (MAC) level; and application recovery procedures
H. Provide an agenda prior to the meeting and minutes after the meeting.
I. The contractor shall produce and update SLA, as required, for all CE hosted systems identified in Appendix C. The contractor shall update agreements with changes because of the annual review between the supported application team and COR.
J. Develop and maintain documentation, including rack elevation diagrams where applicable, server and hardware characteristics/inventory (cradle to grave), operating system and related software, systems supported, and architecture documentation for all CE hosted system until On-Prem environment is defunct and decommissioned.
K. The contactor shall develop and maintain a systems administration logbooks; this document will contain (or reference) hardware/software descriptions, configuration files, custom scripts, startup/shutdown and backup/recovery procedures, systems changes and problem resolutions. The contractor shall provide updated documentation at the end of each quarter.
L. Assist with creation, sustainment and maintenance virtual machine image templates for the CE applications and operating systems
M. Perform infrastructure Analysis, and future planning where applicable
N. Perform a lead role in an Enterprise Configuration Change Control board, recommending and implementing technically and fiscally responsible solutions supporting automated systems for both On-Prem/CE

O. Provide subject matter expertise in support of maintaining and migration of On-prem enterprise technologies such as Electronic Data Interchange (EDI), File Transfer Manager (FTM/MFTS), to the GovCloud
P. Perform Backup/Restore/Recovery of environments, including, but not limited to: daily backups; catalog tapes; maintain tape inventory; send/receive tapes to/from off-site storage; perform restores as required;
Q. Author and execute Disaster Recovery (DR) plan, as required
R. Design, implement and sustain data replication from production environment to recovery environments.
S. Using provided change management tools and software the contractor shall schedule Authorized Service Interruption (ASI) at least 10 calendar days prior or IAW establish change management policies
T. The contractor will ensure all hardware and software planned maintenance actions planned as part of a scheduled maintenance ASI are completed within the ASI allotted time, where applicable
U. Contractor shall immediately notify the COR/ACOR upon identification of any unplanned system downtime and submit the required Outage Report documenting the failure based on existing knowledge. Reports shall state the nature of the failure, status, and estimated time to resolve or if not yet resolved, and provide root-cause analysis, diagnosis, and recommendations to prevent future occurrences. The documentation shall be delivered to the COR within one (1) business day of failure.
V. Implement system changes as necessitated by the Information Assurance Vulnerability Management Program The Information Assurance Vulnerability Management Program frequently issues Information Assurance Vulnerability Alerts (IAVAs) that give notification of recently discovered vulnerabilities, specify deadlines for acknowledging receipt of the notice, and specify deadlines for implementing any corrective actions, such as a system patch or disabling of system services.
W. Provide after core hours operational CE monitoring and break/fix sustainment to ensure the CE SDDC missions systems are operational at all times outside of scheduled outages.

Contractor shall review and update CE IT infrastructure (on-prem) documentation (provided as GFI) to include, but not limited to:

A. Physical connectivity diagrams
B. Logical architecture diagrams
C. Equipment rack elevation diagrams
D. Configuration Diagrams

The contractor shall provide operating system, network and database administration to On-Prem applications for Dev thru production environments to include, but not limited:

A. VERITAS and Microsoft clusters and configurations
B. Solaris 10/11 and Windows 2008R2 Advanced Server with virtualization
C. Windows 2012 operating systems
D. Machine images RHEL, Windows
E. Subnets, Firewalls, DNS
F. F5 load balancing
G. NetApp Storage appliances with redundancy
H. Sun Java web/app servers
I. Oracle 11g/12x Database and Oracle app servers installation, configuration and maintenance
    1. install, configure and maintain Oracle RDBMS with partitioning, Data Mining and OLAP Data Warehousing;
    2. Oracle SQL Net data communications to assist application teams in supporting the interface between the Power Center and Cognos applications
    3. Establish and maintain optimal tuning in all database environments in accordance with Oracle data warehousing design and maintenance best practices.
J. Microsoft SQL Database servers installation, configuration and maintenance
    1. install, configure and maintain SQL RDBMS with partitioning, Data Mining and Data Warehousing;
    2. SQL data communications to support interfaces
    3. establish and maintain optimal tuning in all database environments in accordance with SQL data warehousing design and maintenance best practices

Deliverables:
Service Level Agreements (SLA's) for CE hosted systems updated 90 days prior to annual RMF review.
Server/virtual machines Installation and Configuration Guides, (updated semi-annually, 30-Jun and 31-Dec.).

1. Systems administration logbook, Physical connectivity diagrams, Logical architecture diagrams, SOP's, Configuration Guides updated the last working day of each Quarter (30-Sep, 31-Dec, 31-Mar, 30-Jun) or within 15 days of change.

2. ASI and Outage Reports, within two hours after each outage (historically less than 10 per month).

3. Server and hardware characteristics/inventory within five business days after change.

4. Server Maintenance Report by the fifth (5^{th}) business day of each month.

5. Disaster Recovery Summary Report NLT 30 days after Recovery Site Exercise.

6. Disaster Recovery Test Plan 10 business days prior to upcoming recovery site exercise.

7. Hardware and software planned maintenance actions as part of a scheduled maintenance ASI completed within the ASI allotted time 95% of the time.

1.3.2.2 Subtask 2: Installation of Secured Application Software

The contractor shall be responsible to assist application teams in the successful installation of government-owned software onto the government-owned GovCloud environment infrastructure for Native and Non-Native, application systems, virtual servers. The Government IA team will perform security scanning and monitoring on the software installation kits and pass the approved installation guides and software kits to the SDDC PMO software development team. Then the PMO team will install the government-owned software onto the government-owned production, staging, development environments and if applicable, the recovery site.

1.3.2.3 Subtask 3: Disaster Recovery/Contingency Operations. The contractor shall complete all required tasks to ensure CE recovery site IT infrastructure properly configured at the CE recovery site location to ensure Network, Server hardware and software, storage, and backup appliances installed and configured to allow all CE hosted systems to operate at the recovery site. The contractor shall provide support to the Government during emergency operations in accordance with approved disaster recovery and contingency operations plans. The contractor shall ensure resources/key personnel are available throughout an emergency in accordance with the established plan.

The contractor shall provide technical engineering on-site support as needed for the recovery site to include (but not limited to):

A. Assisting application teams in Application installation and configuration support to Program Managers at CE recovery site. The contractor shall facilitate discussion with Application PM Support staff to produce application install and configuration documentation used for reference in sustaining and supporting PM applications at recovery site as well as the primary site.

B. Plan and conduct semi-annual recovery site exercises as specified by the COR/ACOR. The contractor shall facilitate monthly recovery site exercise status meetings with CE-hosted Program Managers and recovery site hosting agency as specified by the COR/ACOR. The frequency of these meetings shall increase to bi-weekly two months prior to the semi-annual recovery site exercise and weekly one month prior. The contractor shall produce an agenda and meeting minutes as described in 1.3.1.5 Subtask 5 of this PWS.

C. The recovery site will exercise in January and July of each calendar year or 2 times a calendar year. The contractor shall develop a recovery site plan and provide this to the COR 10 business days prior to the recovery site exercise.

D. For each recovery exercise, the contractor shall submit a recovery site Summary Report within 30 days after the event is completed. The report will include lessons learned; recommendations; and, areas to be re-tested. The contractor shall deliver the report to the Contracting Officer Representative (COR) and alternate COR (ACOR).

E. In the event of disaster, the Contractor shall sustain SDDC/G6 hosted systems at the recovery site.

Deliverables: Fully Operational recovery site e.g. failover, availability and replication. Recovery site exercise status meetings agendas and meeting minutes as described in this PWS. Recovery Site Exercise Plan for CE 10 business days prior to the DRE. Disaster Recovery Summary Report, within 30 days after the event is completed.

1.3.2.4 Subtask 4: Database Administration

The Contractor shall administer CE hosted databases (SQL, and Oracle) on various platforms (i.e., UNIX/Solaris, Windows, and RHEL etc.). Database administration subtasks include, but are not limited to the following list.

A. Develop policies and procedures as they relate to database maintenance, security and archiving
B. Installation and maintenance of Data Base Software and patches
C. Database instance creation
D. Configuration and testing of initial installations
E. Upgrade of hosted databases
F. Manage Database user administration, including role and privilege management
G. Conduct Performance Monitoring and Tuning
H. Configuration and Installation of tables, triggers, procedures, and packages
I. Management of logs, rollback segments, and archived logs
J. Configure and monitor Database backups including both hot and cold backups
K. Oracle Database exports and imports as required
L. Database Report Creation
M. Create, configure, and maintain SQL* Loader utility scripts
N. Database recovery including disaster recovery techniques
O. Parallel Query configuration and tuning
P. Storage management
Q. Auditing database activities
R. Configuration and management of Database unique networking components
S. Configuration and management of listener process
T. Monitor and manage alert logs and trace files
U. Normal and emergency database startup and shutdown processes
V. Management of initialization and configuration files
W. Oracle client software and interfacing with the database
X. Database sizing and cleaning
Y. Database replication
Z. Comply with appropriate Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIGs), and any other upgrades/modifications.
AA. Provide support to data analysis and engineering effort for new data requirements
BB. Provide after hour support for database break/fix sustainment to ensure CE is operational at all times outside of scheduled outages.
CC. Support SDDC outages/upgrades during non-duty hours. Typical CE maintenance outages occur on alternating Wednesdays, usually twice each month.

1.3.2.5 Subtask 5: Network Administration

The Contractor shall perform Network administration, analysis and engineering for the CE Network Infrastructure. In this role, the contractor shall perform numerous tasks, including, but not limited to:

A. Develop of policies and procedures as they relate to network maintenance and security

B. Deploy, configure, maintain and monitor infrastructure environments and related network equipment
C. Insure overall integrity of the network, server deployment, security, and ensure network connectivity throughout the CE IT infrastructure
D. Provide Tier III support as required to work on break/fix issues that could not be resolved at Tier I (helpdesk) or Tier II (network technician) levels
E. Design and deploy network enclaves as required
F. Provide network address and routing protocol, assignment/management, and configuration
G. Provide routing, authentication, authorization, configuration, and manage directory services
H. Provide maintenance of CE network routers, firewalls, appliances, VPN gateways, and intrusion detection systems
I. Scheduling and implementing network routine maintenance tasks
J. Making sure that network backups are performed and conduct test restores
K. Roll out Network software installations, upgrades and patches as required.
L. Monitor for Network security breaches
M. Ensure connectivity works for all users accessing CE IT infrastructure and configure security connection to the NIPRNET
N. Network performance monitoring and tuning
O. Provide Network recovery as required
P. Monitor and manage logs and trace files
Q. Management of initialization and configuration files
R. Comply with appropriate Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIGs), and any other upgrades/modifications
S. Provide non-duty hours network break/fix sustainment to ensure the CE is operational at all times outside of scheduled outages
T. Support CE outages/upgrades during non-duty hours. Typical CE maintenance outages occur on alternating Sundays, usually only twice each month

1.3.2.6 Subtask 6: System Administration

The Contractor shall perform System administration, analysis and engineering for CE machine image/virtual servers. In this role, the contractor shall perform numerous tasks, including, but not limited to:

A. Development of policy and procedures as they relate to application hosting, machine image and server maintenance, and security
B. Deploy, configure, maintain and monitor
C. Install, support, maintain and upgrade all CE virtual server, servers operating systems and machine image's
D. Plans and responds to service outages and all server related issues
E. Create and maintain scripts, perform light programming when required to automate tasks
F. Performs project management on server-related projects
G. Add, configure, spin-up virtual servers
H. Manage Active Directory across various platforms
I. Install software (e.g. third party)
J. Allocate system storage and plan for future storage requirements for all CE hosted systems
K. Provide Tier II and Tier III support as required and applicable to resolve machine image/virtual server issues for on-prem applications that could not be resolved at the Tier I (helpdesk), or at the application level
L. Ensure CE Application/Systems server backups are successfully performed
M. Provides server recovery support as required for applications, operating systems patching and full database recovery in CE
N. Monitor and manage virtual server logs and trace files in CE
O. Manage server initialization and configuration files for virtual systems/instances in CE
P. Perform server Performance Monitoring and Tuning for Non-Native/virtual systems/instances in CE
Q. Schedule and implement server routine maintenance tasks for Non-Native/virtual systems/instances in both CE

R. Roll out server software installs, upgrades and patches as required for Non-Native/virtual systems/instances in both CE
S. Monitor for server security breaches on prem only.
T. Comply with appropriate Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIGs), and any other upgrades/modifications
U. Provide non-duty hours system administration break/fix sustainment to ensure the CE is operational at all times outside of scheduled outages

1.3.2.7 Subtask 7: Tier II/III Help Desk Support

The Contractor shall provide normal working hours CE Tier II/III Help Desk Support for on-prem application issues. The CE Tier II/III Help Desk Support shall include the detailed analysis and troubleshooting of CE program operating systems and databases issues on-prem virtual systems to address infrastructure problems to successful resolution. These tasks include but are not limited to:

A. Assisting application program staff with troubleshooting CE IT Infrastructure related problems.
B. Providing initial interaction with vendors to handle day-to-day emergency hardware and troubleshooting.
C. Assisting with installs and troubleshoots software issues with CE application staff for third party software in support SDDC PMO Application and Systems (e.g. Axway, Data Guard, Golder Gate, Sentinel etc.) Installation and configuration within the GovCloud in pre-prod, Devops, failover zones and production environments, where applicable.
D. Creating, deleting or modifying elevated user accounts on all CE servers and appliances and GovCloud
E. Monitoring the service request queues, assigning and closing tickets and answers incoming phone calls and e-mail to the helpdesk on Prem
F. Aids in the creation and maintenance of CE helpdesk policies and procedures.
G. Tracks and manages CE IT asset inventory.
H. Creates and maintain technical documentation.
I. Performs system monitoring and analysis, assists in troubleshooting system hardware and software.
J. Assists in operating system upgrades (e.g. STIG, security and patch management)

1.3.2.8 Subtask 8: Host Based Security System (HBSS) Support

The Contractor shall perform System administration, analysis and HBSS support for all CE and GovCloud **HBSS server and client components operating within the USTC AWS GovCloud infrastructure. HBSS Server components include but not limited to (ePO) Management Suite, HBSS SIM Connector, and Asset Publishing Service (APS) Operational Attribute Module (OAM). CE and GovCloud HBSS client include but not limited to (Asset Configuration Compliance Module (ACCM), Antivirus/Antispyware (AV/AS), Asset Baseline Monitor (ABM), Device Control Module (DCM), Host Intrusion Prevention System (HIPS), Rogue System Detection, Policy Auditor (PA**). In this role, the contractor shall perform numerous tasks, including, but not limited to:

A. Development of policy and procedures as they relate to HBSS, server and client maintenance and reporting
B. Deploy, configure, maintain and monitor CE HBSS server and client infrastructure.
C. Install, support, maintain and upgrade all **CE** HBSS server and client server hardware and Operating System and HBSS software
D. Plans and responds to HBSS service outages and all HBSS server and client related issues
E. Create and maintain HBSS scripts, perform light programming when required to automate HBSS tasks
F. Performs project management on HBSS related projects
G. Add and configure new HBSS servers
H. Sets up HBSS user accounts
I. Installs HBSS software
J. Plan for future HBSS requirements for all **CE** hosted systems and VDI clients
K. Provide HBSS Tier I, II and Tier II support as required to resolve **CE** HBSS server and client issues
L. Ensure HBSS server backups are successfully performed, and conducts test

M. Provides HBSS server recovery as required
N. Monitor and manages HBSS server logs and trace files
O. Manage HBSS server initialization and configuration files
P. Perform HBS server and client Performance Monitoring and Tuning
Q. Schedules and implement HBSS server and client routine maintenance tasks
R. Rolls out HBSS server and client software installs, upgrades and patches as required.
S. Monitors HBSS server and Clients for security breaches
T. Comply with appropriate Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIGs), and any other upgrades/modifications for HBSS server
U. Provide 24x7x365 HBSS system administration break/fix sustainment to ensure the **CE** HBSS is operational at all times outside of scheduled outages
V. Support **CE** HBSS outages/upgrades during non-duty hours. Typical **CE** HBSS maintenance outages occur on alternating Wednesdays, usually only twice each month
W. Execute the following re-occurring HBSS tasks:
    i. Daily Task
        1. Check Server Task Log and correct errors
        2. Evaluate HIPS events
        3. Evaluate Module versions on clients (for updating)
        4. Evaluate RSD (Rogue Systems)
    ii. Operational Tasks
        1. Create/modify HIPS policy/Exceptions
        2. Maintain Database Rollups
        3. Patch EPO / HBSS Servers in accordance with DOD IAVM notices
        4. Perform Daily Backups
        5. Perform Account Management
        6. Perform Troubleshooting and resolve HBSS client module issues
        7. Update Extension\software Packages
        8. Validate configuration against the DISA STIGS
        9. Implement DOD mandated Tasking Orders
    iii. Provide monthly basis metrics on information HBSS to Government
        1. List of HBSS security infrastructure mechanism rule/policy modifications implemented
        2. Number of compatible devices with all applicable HBSS modules installed
        3. Number of compatible devices with applicable HBSS modules missing or non-functional
        4. List and status of rogue systems identified (i.e. removed from network, device not compatible, still being investigated, HBSS now functional

1.3.2.9 Subtask 9: Virtual Desktop Infrastructure Support (VMWARE)

The Contractor shall perform System administration, analysis and sustainment and maintenance support for the CE VDI infrastructure and all its components. These tasks include but are not limited to the following:

1. Administration
2. Software upgrades
3. Agent updates
4. Security patching
5. Configuring View Connection Server
6. Configuring Role-Based Delegated Administration
7. Preparing Unmanaged desktop sources
8. Creating and Preparing Virtual machines
9. Creating Desktop pools
10. Setting up authentication
11. Entitling Users and groups
12. Managing users and administrators
13. Setting up Authentication
14. Configuring Policies

15. Configuring user profiles
16. Managing linked clone desktops
17. Managing Desktop Pools and sessions
18. Managing physical computers and terminal servers
19. Managing Thin-applications
20. Managing local desktops/workstations
21. Managing machines
22. Maintaining/Troubleshooting view components
23. Using VD admin Commands
24. Setting up /Provisioning VDI Clients
25. Add/Delete access groups
26. Managing application pools, farms and RDS hosts
27. Manage Global, predefined roles and internal privileges

1.3.2.10 Subtask 10: On-Prem Decommissioning Activities for all environments and equipment

The contractor shall decommission all On-prem environments by 30 Sep 2020 the decommissioning "Execution" activities should start NLT 1 May 2020 all other activities such as planning, coordination, scheduling will be completed NLT 15 Feb 2020. The contractor will provide monthly status updates on the decommissioning progress. These briefs will identify schedule risks along with risk mitigation recommendations and COAs for decommissioning "execution" activities with a recommended COA NLT 15 Jan 2020. The contactor will conduct a full inventory of all equipment and reconcile the list against the SDDC Property Book Office (PBO) inventory items that are on the hand receipt of the On-Prem Centralized Enclave. All discrepancies will be identified and researched and reconciled. The reconciliation activities will be conducted in coordination with the PBO POC in order to resolve all discrepancies. A final high-level report and briefing will be delivered to the government detailing the final disposition of all hardware (racks, servers, switches, routers, cabling, tools, storage devices, other enclosed devices etc) along with PBO supporting documentation of disposition.

DELIVERABLES:
1. Status update brief before the 15th of November, December, January and February
2. Final PBO/Hand Receipt reconciliation document. Due before 30 Sep 2020
3. Disposition report and Project Close out brief. Due before 30 Sep 2020)

1.3.3 Task Area 3: Sustainment and Maintenance GovCloud.

The contractor shall support the following GovCloud application maturity levels (AML's), Semi-Automated Applications and Non-Automated or Manual, transportation business systems and business systems, in persistent non-production, production and Devops environments and pipelines.

The Contractor shall provide non-duty hours GovCloud sustainment and maintenance support to enable hosted systems, services and capabilities are fully functioning. Specifically those services not addressed by the USTC managed services team for non-native systems/applications. The Contractor shall provide break fix cloud support on normal duty days between the hours of 0700-1700 CT and during Authorized Service Interruptions (ASI) maintenance periods (0800-1200 /2000-0200) CT) usually the 2nd and 4th Wednesday of the month. At all other times, the Contractor shall provide emergency support either on-site or via USTC approved remote access solution provided by the Government in order to respond within 30 minutes or less to GovCloud emergency support requests.

The contractor shall provide the operational support in the form of operating system and database engineering/administration, VPC engineering and infrastructure support, network engineering to maintain applications capabilities hosted in the GovCloud environments. Specifically through the GovCloud DevOps, pipeline thru production pipelines. The contractor shall maintain SDDC application database instances (SQL and, Oracle). Backup and Recovery, Data Replication/Failover, Electronic Data Interface (EDI), MFTS, SCCM, Satellite, Non-native machine image's for Windows, x86 and RHEL servers architectures. The applications currently hosted in the USTC GovCloud listed in Appendix C.

1.3.3.1 Subtask 1: Maintenance and Sustainment of SDDC IT Infrastructure

The contractor shall provide technical engineering, migration and sustainment support for and to the GovCloud Production, Replication Zones (A/B), Regions, Staging (pre-prod), Partner Testing/Interface Testing, and Development environments/ pipelines for all SDDC systems.

The contractor shall provide technical engineering sustainment support including, but is not limited to network/VPC engineering and maintenance, enterprise GovCloud support services, storage management, backup and recovery management. Database administration and System administration. Operating system upgrades and security patching for the GovCloud SDDC systems/applications.

The contractor shall support services in and to the GovCloud to include VPC, MFTS, SCCM, RHEL, Satellite/Active Directory OU'S, and Group Policies/F5 Load Balance/Firewall and DNS services. These services will facilitate GovCloud support for applications that rely on GovCloud infrastructure.

The contractor shall resolve all Information Assurance Vulnerability Assessment (IAVA) reports within the periods specified within the IAVA. IAVA resolution may include implementing new technical solutions, patches and upgrades in the production, pre-production, partner testing and DevOps environments/pipelines or where applicable. The contractor shall provide technical sustainment support to include (but not limited to):

A. Provide vpc, network, firewall, operating system, database and assist application teams in application sustainment in GovCloud environments where applicable
B. Maintain load balancing, fail over procedures, data replication and automated testing support utilizing tools provided and business rules in the GovCloud.
C. Provide support, configuration installation and maintenance of an enterprise backup and recovery/Failover solutions for non-native applications in the GovCloud
D. Provide proactive monitoring on the core operating systems and databases on all SDDC hosted systems for GovCloud hosted systems/applications
E. Coordinate and cooperate with the SDDC, USTC and IA/Cyber Program Manager Offices (PMO) to maintain compliance with the current governance for the certification and accreditation process to help applications/systems maintain their Authority to Operate (ATO) and Interim Authority to Operate (IATO).
F. Assist application teams providing application support to facilitate third party Security Accreditation testing.
G. Facilitate meetings with application PMs and their POCs in the development and maintenance of Service Level Agreements (SLA's). Service Level Agreements shall include, but are not limited to application technical and software requirements and architecture; release and change control processes; points of contact including roles and responsibilities; escalation procedures; Mission Assurance Category (MAC) level; and application recovery procedures IAW with GovCloud and CCP policies and standards.
H. Provide meeting agenda prior to the meeting and minutes after the meeting.
I. The contractor shall update SLA, as required, for all SDDC GovCloud hosted systems
J. Develop and maintain documentation and diagrams of the SDDC VPC's. These are associated with network/infrastructure support for systems/applications residing in the GovCloud (e.g. DevOps pipeline, non-prod, production, partner testing, firewall, DNS, failover zones and active directory structures.
K. The contactor shall develop and maintain a systems administration logbooks; this document will contain (or reference) virtual machine and software descriptions, configuration files, custom scripts, startup/shutdown and backup/recovery procedures, systems changes and problem resolutions. The contractor shall provide updated documentation at the end of each quarter.
L. Assist with creation, sustainment and maintenance of program specific blueprints, cookbooks and machine image templates for SDDC GovCloud applications and operating systems
M. Perform infrastructure Analysis, and future planning where applicable
N. Perform a lead role in an Enterprise Configuration Change Control board for SDDC systems recommending and implementing technically and fiscally responsible solutions supporting SDDC systems IAW USTC GovCloud change control policies and procedures.

O. Provide subject matter expertise in support of maintaining and migration of On-prem enterprise technologies and services where applicable in support of the following services but not limited to: (MFTS, SCCM, RHEL Satellite servers and EDI.
P. Develop and Sustain Backup/Recovery/Failover and Data Replication of applications and their databases IAW program requirements, GovCloud and Cloud Service Provider (CSP) policies and procedures.
Q. Using provided change management tools and software the contractor shall schedule Authorized Service Interruption (ASI) IAW established configuration control and change management policies IAW USTC GovCloud and CSP
R. The contractor shall support the installation and management of software updates as required in both the NIPRNET/SIPRNET hosted in the Cloud environments.
S. Sustainment and Maintenance support may include both NIPR and SIPR (non-prod/prod) depending upon program requirements but will not require an increase in pre-requisites such as a Secret clearance requirement.
T. The contractor will ensure all planned maintenance actions completed within the ASI allotted time.
U. Contractor shall immediately notify the COR/PM upon identification of any unplanned system downtime and submit the required Outage Report, within 2 hours of the outage, documenting the failure based on existing knowledge. The reports shall include the nature of the failure, status, and estimated time to resolve, if not yet resolved. The after action report shall provide root-cause analysis, diagnosis, and recommendations to prevent future occurrences. The documentation shall be delivered to the COR/PM within one (1) business after resolution.
V. Implement system changes as necessitated by the Information Assurance Vulnerability Management Program The Information Assurance Vulnerability Management Program frequently issues Information Assurance Vulnerability Alerts (IAVAs) that give notification of recently discovered vulnerabilities, specify deadlines for acknowledging receipt of the notice, and specify deadlines for implementing any corrective actions, such as a system patch or disabling of system services.
W. Provide non-duty hour operational support IAW USTC CSP and SDDC standard operating procedures (SOP) for monitoring and break/fix sustainment to ensure SDDC missions systems are operational at all times outside of scheduled outages.

Contractor shall review and update Cloud infrastructure/architecture diagrams for SDDC VPC's, DevOps pipeline and Active Directory (AD) that support SDDC systems within the GovCloud:

A. AD architecture diagrams
B. SDDC VPC Diagrams
C. DevOps pipeline Diagrams
D. SDDC IP space ranges

The contractor shall provide operating system, network and database administration to GovCloud applications for Dev thru production environments/pipelines e.g. pre-prod, non-prod, persistent non-prod, partner testing and development environments where applicable to include, but not limited:

A. Machine Images and their operating systems (e.g. Windows 2012/2016, 2008r2 and RHEL)
B. Virtual Private Clouds, Subnets, Firewalls, DNS, Active Directory Structure for SDDC programs
C. Infrastructure blueprints to create base environment to host system and application
D. Cookbooks for performing tasks such as installing packages or creating directories, managing users and services, creating files and directories, running commands and scripts etc.
E. Load balancing (e.g. F5), Firewalls (e.g. Palo Alto)
F. NetApp or similar Storage appliances with redundancy or similar cloud technologies
G. Web/app servers (e.g. Java, Cold Fusion etc.)
H. Oracle Database and Oracle app servers installation, configuration and maintenance
    1. install, configure and maintain Oracle RDBMS with partitioning, Data Mining and OLAP Data Warehousing;
    2. Oracle SQLNet data communications to assist application teams in supporting the interface between the Power Center and Cognos applications

3. Establish and maintain optimal tuning in all database environments in accordance with Oracle data warehousing design and maintenance best practices.

I. Microsoft SQL Database servers installation, configuration and maintenance
   1. install, configure and maintain SQL RDBMS with partitioning, Data Mining and Data Warehousing;
   2. SQL data communications to support interfaces
   3. Establish and maintain optimal tuning in all database environments in accordance with SQL data warehousing design and maintenance best practices

J. Utilizing Cloud tools and services or their equivalents to include but not limited to: JIRA, Confluence, Chef, Jenkins, Nessus, Fortify, F5,VMware,Cisco VPN, Elastic Compute Cloud (EC2), Elastic Block Store (EBS), Simple Storage Service (S3), Identity and Access Management (IAM), Lambda, Simple Workflow Service (SWF), Elastic Load Balancer (ELB), Cloud Watch, Cloud Trail, Dynamo DB, ElastiCache, RedShift, Cloud Formation, Config, Trusted Advisor, Simple Notification Services (SNS),Simple Queuing Services(SQS), HBSS, WSUS, SCCM, SFTP,
YUM, WebLogic and IIS.

Deliverables:

1. Service Level Agreements (SLA's) NLT than 30 days after a program has become system of record (SoR), updated 30 days prior to annual RMF review.

2. Guides on Creating, Managing and Deploying Apps and Cookbooks and Standard Blueprints due initially NLT 30 days after program becomes system of record (SoR) and updated no later than 15 days after a change

3. Guides for Provisioning Machine Images (e.g. via subscription service or from the moshpit).

4. SDDC AD architecture diagrams, SDDC VPC Diagrams, DevOps pipeline Diagrams initially due NLT 30 days after creation and updated no later than 15 days after a change.

5. ASI and Outage Reports

1.3.3.2 Subtask 2: Installation of Secured Application Software. The contractor shall assist application teams in the successful installation of government-owned software into the GovCloud environments for SDDC applications, machine images /servers where applicable. The Government IA team will perform security scanning and monitoring on the software installation kits and pass the approved installation guides and software kits to the SDDC PMO software development team. The PMO team will install the government-owned software into the government-owned GovCloud environments as applicable.

1.3.3.3 Subtask 3: Disaster Recovery/Contingency Operations GovCloud. The contractor shall develop sustain and follow automated and manual failover and recovery procedures in accordance with (IAW) USTC GovCloud established failover architecture and backup solutions (e.g. EC2,availability zones and regions and backup policies). The contractor shall provide support to the Government during emergency operations in accordance with approved USTC GovCloud disaster recovery and contingency operations plans. The contractor shall ensure resources/key personnel are available throughout an emergency in accordance with the established plan.

1.3.3.4 Subtask 4: Database Administration

A. The Contractor shall administer GovCloud hosted databases (SQL and Oracle) on various platforms (i.e., Windows, and RHEL etc.). Database administration subtasks include, but are not limited to the following list.
B. Test, validate and implement performance and resource optimization improvements in consultation with GovCloud development Teams
C. Maintain development and production environments
D. Monitor and maintain database security and database software

E. Database & Application(SQL & PL/SQL) performance tuning
F. Backup and recovery (RMAN and traditional)
G. Root cause analysis of production-related database issues
H. On-call for production databases - daily maintenance, monitoring, problem resolution and internal customer and dev support
I. Experience managing servers in large-scale, geographically diverse environments.
J. Review, design and develop data models in conjunction with the application development teams
K. Design, develop, and implement Oracle database instances for the development and production environments
L. Changing the Global Name of a Database
M. Creating and Sizing Tablespaces
N. Setting the Default Tablespace
O. Setting the Default Temporary Tablespace
P. Check pointing the Database
Q. Setting Distributed Recovery
R. Authoring/configuring Replication across zones and or regions
S. Setting the Database Time Zone
T. Working with Oracle External Tables
U. Working with Automatic Workload Repository (AWR)
V. Adjusting Database Links for Use with DB Instances in a VPC
W. Validating DB Instance Files
X. Validating a Tablespace
Y. Use cloud tools to facilitate data replication and data loads
Z. Utilize Cloud tools such as database migration service (DMS) or other cloud tools for database management

1.3.3.5 Subtask 5: Network Administration

The Contractor shall perform Network administration, analysis and engineering for the SDDC EIP VPC(s) within the GovCloud Network Infrastructure. These SDDC managed services shall include but not be limited to SCCM, RH Satellite and MFTS services support (In this role, the contractor shall perform numerous tasks, including, but not limited to:

A. Engineer, deploy, configure, maintain and monitor infrastructure environments and related network devices and protocols
B. Ensure overall integrity of the network, VPN connections, tunnels, VPC gateway, VPN redundancy security, and firewalls
C. Provide Tier III support as required to work on issues that could not be resolved at Tier I (helpdesk) or Tier II (SDDC application) levels
D. Design/engineer network architecture as required to support SDDC systems
E. Provide engineering and administration support to these managed services (e.g. MFTS, SCCM and RHEL Satellite)
F. Provide routing, authentication, authorization, configuration, and manage directory services where applicable
G. Provide maintenance of GovCloud network firewalls, protocols, VPN, VPC and gateways for SDDC systems not covered under USTC managed services
H. Ensure connectivity works for all users accessing GovCloud infrastructure and specifically management services supporting SDDC applications
I. Network performance monitoring and tuning where applicable and not performed by USTC managed services
J. Build Active Directory (AD) OU’s and manage accounts, permissions, group policies, passwords and groups, dns and directory services for SDDC systems where USTC managed services does not.
K. Monitor and manage logs and trace files
L. Management of initialization and configuration files

M. Comply with appropriate Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIGs), and any other upgrades/modifications as required.

1.3.3.6 Subtask 6: System Administration

The Contractor shall perform System administration, analysis and engineering for GovCloud machine image/virtual servers. In this role, the contractor shall perform numerous tasks, including, but not limited to:

A. Development of policy and procedures as they relate to application hosting, machine image and server maintenance, and security
B. Deploy, configure, maintain and monitor server, VPC/VPN infrastructures and GovCloud machine images
C. Install, support, maintain and upgrade all GovCloud machine images, servers and operating systems
D. Plans and responds to service outages and all server related issues
E. Create and maintain scripts, perform light programming when required to automate tasks
F. Performs project management
G. Apply EC2 instance scripts (e.g. Centrify, hbss, Nessus)
H. Apply group policy updates
I. Add, configure, spin-up new machine image's and virtual servers
J. Assist in the creation and maintenance of maintain Cookbooks and Blueprints with SDDC PM offices/POR.
K. Manage SDDC Active Directory components (OU, group policies and permissions), SCCM,MFTS,RHEL Satellite servers and Firewall requests
L. Install software (e.g. Dataguard and Golden Gate)
M. Allocate system storage and plan for future storage requirements for all SDDC GovCloud hosted systems
N. Provide Tier III support as required and applicable to resolve machine image/virtual server issues for SDDC systems and services that could not be resolved at USTC CCOE Managed services level
O. Ensure SDDC GovCloud Application/Systems server backups are successfully performed
P. Provides server recovery support as required for SDDC applications, operating systems and full database recovery (failover zones/regions) in GovCloud.
Q. Monitor and manage virtual server logs and trace files in GovCloud for SDDC systems
R. Manage server initialization and configuration files for SDDC virtual systems/instances in GovCloud
S. Perform server Performance Monitoring and Tuning for SDDC virtual systems/instances in GovCloud
T. Schedule and implement server routine maintenance tasks for SDDC virtual systems/instances in GovCloud
U. Roll out server software installs, upgrades and patches as required for SDDC virtual systems/instances in GovCloud
V. Comply with appropriate Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIGs), and any other upgrades/modifications
W. Support SDDC GovCloud outages/upgrades during non-duty hours as applicable.

1.3.3.7 Subtask 7: Tier II/III Help Desk Support.

A. The Contractor shall provide normal duty hours GovCloud Tier II to SDDC G6 Application Support for application issues. The SDDC GovCloud Tier III Support shall include the detailed analysis and troubleshooting the root cause of SDDC GovCloud infrastructure related issues. Tier III SDDC G6 support shall troubleshoot root-cause issues for SDDC/EIP VPC's and their associated managed services. This also includes Program operating systems and databases issues for SDDC systems to address infrastructure problems to a successful resolution. These tasks include but are not limited to:
B. Assisting with installs and troubleshoots software issues with GovCloud application staff for third party software in support SDDC PMO Application and Systems (e.g. Data Guard, Golden Gate, Sentinel etc.)
C. Installation and configuration within the GovCloud in Devops through prod, db failover zones/regions and production environments, where applicable.
D. Managing Active Directory OU's, group policies and permissions
E. Managing SDDC VPC's

F. Create, delete or modify elevated user accounts/privileges related to SDDC GovCloud EIP VPC and AD.
G. Monitoring the service request queues, assigning and closing associated with SDDC tier II and III support or IAW USTC GovCloud managed services policies and procedures.
H. Create and maintain technical documentation.
I. Perform system monitoring and analysis, assists in troubleshooting DevOps through production pipeline issues for SDDC applications, systems and services
J. Assists in operating system upgrades (e.g. STIG security and patch management, machine images (e.g. gold, silver and bronze)

1.3.3.8 Subtask 8: Host Based Security System (HBSS) Support

A. The Contractor shall perform System administration, analysis and HBSS support for SDDC GovCloud assets in accordance with (IAW) USTC Managed Services policies and procedures for HBSS server and agent management for all SDDC GovCloud non-native assets. These tasks shall include **HBSS server and client components operating within the USTC AWS GovCloud infrastructure. HBSS Server components include but not limited to** (**ePO) Management Suite, HBSS SIM Connector, and Asset Publishing Service (APS) Operational Attribute Module (OAM). GovCloud HBSS client include but not limited to (Asset Configuration Compliance Module (ACCM), Antivirus/Antispyware (AV/AS), Asset Baseline Monitor (ABM), Device Control Module (DCM), Host Intrusion Prevention System (HIPS), Rogue System Detection, Policy Auditor (PA**). In this role, the contractor shall perform numerous tasks, including, but not limited to:
B. Development of policy and procedures as they relate to HBSS, server and client maintenance and reporting
C. Deploy, configure, maintain and monitor GovCloud HBSS server and client infrastructure.
D. Install, support, maintain and upgrade all **GovCloud** HBSS server and client server hardware and Operating System and HBSS software
E. Plans and responds to HBSS service outages and all HBSS server and client related issues
F. Create and maintain HBSS scripts, perform light programming when required to automate HBSS tasks
G. Performs project management on HBSS related projects
H. Add and configure new HBSS servers
I. Sets up HBSS user accounts
J. Installs HBSS software
K. Plan for future HBSS requirements for all **GovCloud** hosted systems and VDI clients
L. Provide HBSS Tier II support as required to resolve **GovCloud** HBSS server and client issues
M. Ensure HBSS server backups are successfully performed, and conducts test
N. Provides HBSS server recovery as required
O. Monitor and manages HBSS server logs and trace files
P. Manage HBSS server initialization and configuration files
Q. Perform HBS server and client Performance Monitoring and Tuning
R. Schedules and implement HBSS server and client routine maintenance tasks
S. Rolls out HBSS server and client software installs, upgrades and patches as required.
T. Monitors HBSS server and Clients for security breaches
U. Comply with appropriate Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIGs), and any other upgrades/modifications for HBSS server
V. Provide after normal duty hours support HBSS system administration break/fix sustainment to ensure the **GovCloud** HBSS is operational at all times outside of scheduled outages
W. Support **GovCloud** HBSS outages/upgrades during non-duty hours. Typical **GovCloud** HBSS maintenance outages occur on alternating Wednesdays, usually only twice each month
X. Execute the following re-occurring HBSS tasks:
    i. Daily Task
        1. Check Server Task Log and correct errors
        2. Evaluate HIPS events
        3. Evaluate Module versions on clients (for updating)
        4. Evaluate RSD (Rogue Systems)
    ii. Operational Tasks

1. Create/modify HIPS policy/Exceptions
2. Maintain Database Rollups
3. Patch EPO / HBSS Servers in accordance with DOD IAVM notices
4. Perform Daily Backups
5. Perform Account Management
6. Perform Troubleshooting and resolve HBSS client module issues
7. Update Extension\software Packages
8. Validate configuration against the DISA STIGS
9. Implement DOD mandated Tasking Orders

iii. Provide monthly basis metrics on information HBSS to Government

1. List of HBSS security infrastructure mechanism rule/policy modifications implemented
2. Number of compatible devices with all applicable HBSS modules installed
3. Number of compatible devices with applicable HBSS modules missing or non-functional
4. List and status of rogue systems identified (i.e. removed from network, device not compatible, still being investigated, HBSS now functional

1.3.4 Task Area 4: Enhancements GovCloud (Optional)
Task Area 4 is marked optional for potential use and may be negotiated and added during the life of this contract.

1.3.4.1 Subtask 1: Requirements Analysis

1.3.4.1.1 Requirements Analysis, Systems Analysis, and Design. The Contractor shall provide technical and functional collaboration with Government personnel (e.g., working group) to perform requirements analysis, systems analysis, and design.

1.3.4.1.2 Entry Criterion. The Government will provide to the Contractor the Technical Requirements Specification (TRS).

1.3.4.1.3 Requirements Analysis. The Contractor shall review and analyze requirements and collaborate with Government personnel to gain mutual understanding of the requirement as documented in the supporting TRS. Upon completion of requirements analysis, the Contractor shall deliver a requirements analysis report that provides an impact analysis and technical approach. Upon the COR's approval of the requirements analysis report, the Contractor shall proceed with the systems analysis and design.

1.3.4.1.4 Systems Analysis and Design. The Contractor shall employ standard engineering methodologies and best practices to perform systems analysis and design. The Contractor shall collaborate with the Government throughout the technical design process and provide technical design documents for Government approval.

1.3.4.1.5 Exit Criteria. The exit criterion for this task is COR's approval of the Systems Analysis and Design artifacts.

1.3.4.1.6 Requirement Execution: Upon COR approval of the Systems Analysis and Design, the Contractor will forward the Contracting Officer a labor hour breakdown for the effort. If the Contracting Officer determines the breakdown reasonable, the Contracting Officer will authorize the Contractor to begin work. If the Contracting Officer does not find the breakdown reasonable, the Contractor and the Government will re-enter into technical discussions.

Deliverables: Systems Analysis and Designs, Labor Hour Breakdowns

1.3.4.2 Subtask 2: Application-level Administration

The contractor shall assist SDDC PMO in developing plans that will support SDDC/G6 application teams to migrate applications to the GovCloud and assist in plans to refactor/redevelop or reinstall applications towards becoming cloud native applications.

1.3.4.3 Subtask 3: Application Migration to GovCloud

The contractor shall perform the following sub-tasks to migrate new systems into the GovCloud.

The contractor shall develop an executable plan to migrate applicable systems to the USTC GovCloud hosting environment or equivalent government owned cloud environment. The contractor shall:

A. Develop and maintain System Migration Plans in conjunction with PMO's migrating applications throughout the migration period. The contractor shall provide a draft plan that describes the objectives with details on how they should be migrated into the GovCloud. The documentation included in the plan shall consist of a milestone schedule, test plan for each migrating system, issues and risks, stakeholder roles and responsibilities, and the migrating systems/application documentation of the current system.
B. Ninety days prior to actual execution of the migration, develop and deliver a detailed executable plan that includes identification of milestone tasks, estimated timelines and risks to accomplish migrating the systems to the GovCloud environments. Determine VPC is as needed (e.g. partner testing etc.), database and failover requirements and additional requirements relating to cookbook and blueprint development and configuration. This shall include assumptions, roles, and responsibilities for both IT Services contractors and the PM office.
C. The contractor in conjunction with PMO application teams shall assess the application for suitability, which shall include application design, architecture, performance, availability, network impact, security and privacy requirements.

D. The contractor shall recommend a migration method to become Cloud Native:
    1. Refactor (including optimize and automated pipeline actions)
    2. Redevelop (including appdev and big data actions)
    3. Reinstall (only considered as last resort

The contractor shall support the migration of systems to the GovCloud environments. The contractor shall:

A. Migrate systems from their existing architecture to the GovCloud environments (Lift and Shift).
B. Build out management services to support SDDC systems
    1. Database Engineering and Administration (prod/no-prod): Oracle, MS-SQL, RDS
    2. Enterprise Services: MFTS, SFTP, AD, SCCM, Satellite (RHEL), WSUS
    3. Active Directory: Group policies, Organization Units (OU), Account Management
    4. System Engineering and Administration (prod/non-prod): Windows, RHEL7
    5. OS/DB Patching and Management (prod/non-prod): Windows, RHEL7.
C. Provide enterprise systems integration and engineering, documentation, migration, implementation, and testing support for systems migrating into the GovCloud environments.
D. Upon migration, the contractor shall support migrating systems with installation and configuration of application/program specific third party software with vendor, Patch Non-Native operating systems and install, build, configure, populate databases (e.g. Microsoft SQL and Oracle), cookbooks, blueprints within the pre-prod, production and DevOps environments/pipelines vpc's that hosts the migrated systems.

Deliverable: System Migration Plan Ninety (90) days prior to actual execution of the migration. Program/ Application assessment that includes recommended migration method.

The following subtasks will assist in the management of SDDC assets in the GovCloud and they are subject to changes and additions.

1.3.4.4 Subtask 4: Storage Management (GovCloud)

- Simple Storage Service (S3) Buckets

- Creating Replication Rules
- Creating Lifecycle Policies
- Data Transfer Services
- Amazon Elastic File System
- Amazon Elastic Book Store

1.3.4.5 Subtask 5: Security Services Management (GovCloud)

- Firewalls
- Active Directory
- Certificate Management
- Key management
- Account management
- Logging and auditing

1.3.4.6 Subtask 6: Network Services Management (GovCloud)

- Routing
- DNS
- NTP
- SMTP
- SFTP
- IdAM

1.3.4.7 Subtask 7: Root-Level Administration (GovCloud)

- Routing
- DNS
- NTP
- SMTP
- SFTP
- IdAM
- Firewalls
- Active Directory
- Certificate Management
- Key management
- Account management
- Logging and auditing

1.3.5 Task Area 5: Configuration Management On- Prem. (Optional after Option Period 1)

The contractor's SDDC/G6 configuration management processes must compliment the Government configuration management processes. The CE Program Management Office (PMO) has assigned a Government Configuration Manager (GCM) that works closely with the Contractor's Configuration Manager. The GCM oversees the contractor team's configuration management activities.

1.3.5.1 Subtask 1: Configuration Management (CM).

The Contractor's Configuration Manager (CCM) shall provide input to Technical Configuration Management Plan (CMP) and processes that are consistent with and complement the GCM processes. The CMP includes the following:

- SDDC/G6 configuration management processes/procedures
- Methods, procedures, and controls
- Change control
- CM audits of total configuration to include hardware, software, and firmware

- CM Process

Deliverable: Annual Update to the program CMP, required no later than 15 calendar days after the start of each contract period.

1.3.5.2 Subtask 2: Change Control.

The contractor shall provide change control for all CE and GovCloud infrastructure baselines and configuration items to include software. The Government will provide the contractor with web access to the SDDC Enterprise Change Control Tool (CCT), currently supported by Serena Business Management (SBM) software and the GovCloud Service Now CCT or an equivalent tool. The Government's CCT is a tool shared by the CE IT Services PMO staff and the contractor staff and configured to support the CE configuration management process; hosted within the CE On-Prem environments. The contractor shall comply with all G Configuration Management standards and processes as published.

The contractor shall evaluate all planned changes. The contractor shall provide their evaluation upon request. Evaluations include, not be limited to, requirement clarification, requirements analysis, determination if the requirement is feasible, cost (labor hours) estimation, adherence to standards, and the consequences of the proposed change. This information provided to the Government for evaluation via the CCT and/or as a separate document depending upon the amount of information required or provided. This evaluation shall help the PMO staff coordinate change implementation with the CE hosted systems.

Deliverables: Change requests and their analysis, evaluation, and tracking captured within the CCT.

1.3.5.3 Subtask 3: Asset Management.

The contractor shall provide updates to the Government on hardware and software inventory monthly or (as appropriate), warranties, maintenance support agreements, software licensing, and accountability for equipment purchases/upgrades. The Government will maintain and update the enterprise asset database that identifies all existing infrastructure assets, hardware, and COTS software.

1.3.5.4 Subtask 4: Configuration Control Board (CCB).

The contractor's Configuration Manager (CM) shall participate in the Government's CCB. The contractor's CM shall act as the liaison between the Government and contractor to provide any additional information that the CCB requires. The contractor shall participate in a weekly Enterprise CCB lasting no more than one hour per meeting. Participation will help ensure contractor activities focus in the areas the Government deems important, and changes within the government's CE environments, ensuring proper vetting across all affected programs and environments

The contractor shall participate in as required CE CCB meetings. The contractor shall analyze new technical changes prior to the meeting and provide information to the Government team in order to prioritize CE application, database and operating system and infrastructure level changes where applicable. This analysis shall be captured in the CCT. The CE EIP team PM and the CCB will determine the priority for all changes. The contractor shall be responsible for documenting the CE CCB Minutes, and shall deliver the minutes to the SDDC responsible party within five (5) workdays of the meeting.

Deliverable: CCB Minutes, within 5 work days of the meeting.

1.3.6 Task Area 6: Configuration Management GovCloud

The contractor shall follow the USTC Configuration Management standard operating procedures (SOP). These include CCOE enterprise infrastructure, configuration control board, infrastructure change requests, infrastructure authorized service interruptions (ASI's) and configuration management standards to support all SDDC GovCloud application and infrastructure changes. This should work in conjunction with SDDC configuration management policies and tools until the application becomes cloud native, at which point they will adhere solely USTC

GovCloud CM policies and procedures. The contractor shall participate in the weekly configuration control meetings as established by the USTC CCOE to represent the SDDC GovCloud configuration CCB's and ASI's.

1.3.6.1 Subtask 1: Configuration Management (CM).

The Contractor's shall continue to follow the SDDC and USTC GovCloud business processes and policies for configuration control and management.

1.3.6.2 Subtask 2: Change Control.

The contractor shall provide change control for all SDDC GovCloud infrastructure baselines and configuration items to include software. The Government will provide the contractor with web access to the SDDC/GovCloud Change Control Tool (CCT), currently supported by Serena Business Management (SBM) software and Service Now. The contractor shall comply with all SDDC and USTC GovCloud configuration controls and management standards and processes.

The contractor shall evaluate all planned changes. The contractor shall provide their evaluation upon request. Evaluations include, but not limited to, requirement clarification, requirements analysis, determination if the requirement is feasible, cost (labor hours) estimation, adherence to standards, and the consequences of the proposed change. This information provided to the Government for evaluation via the CCT and/or as a separate document, depending upon the amount of information required or provided. This evaluation shall help the PMO staff coordinate change implementation with the contractor for SDDC GovCloud hosted systems.

Deliverables: Change requests and their analysis, evaluation, and tracking captured within the CCT.

1.3.6.3 Subtask 3: Configuration Control Board (CCB).

The contractor's Configuration Manager (CM) shall participate in the Government's CCB. The contractor's CM shall act as the liaison between the Government and contractor to provide any additional information that the CCB requires. The contractor shall participate in a weekly enterprise CCB lasting no more than one hour per meeting. Participation will help ensure contractor activities focus in the areas the Government deems important, and changes within the SDDC GovCloud environments, ensuring proper vetting across all affected programs and environments.

. The contractor shall analyze new technical changes prior to the meeting and provide information to the Government team in order to prioritize SDDC GovCloud application, database and operating system and infrastructure level changes where applicable. This analysis shall be captured in the CCT. The SDDC PM and contractor will determine the priority for all changes. The contractor shall be responsible for documenting the SDDC GovCloud CCB Minutes, and shall deliver the minutes to the SDDC CM PMO staff within five (1) workday of the meeting.

Deliverable: CCB Minutes, within 1 work day of the meeting.

1.3.7 Task Area 7: Information Assurance (IA) On Prem (Optional after Option Period 1)

The contractor shall work with the Government and Contractor Information Assurance Team as designated within SDDC/USTRANSCOM/TCC to provide and share system security data and program information.

1.3.7.1 Subtask 1: Information Assurance Training.

Contract employees shall attend/complete the following security training as prescribed by DOD and SDDC instructions and update the Army Training and Certification Tracking System (ATCTS) to reflect the current-status. All contractor personnel shall create an account in the ATCTS and complete a profile survey; based on that survey, the contractor shall complete all appropriate information assurance training.

Annual Training:

- DOD IA Awareness Training

One-Time Training:

- Army Wide Network Security Focus Training (WNSF)
- SAFE Home Computing
- Personally Identifiable Information (PII)
- Portable Electronic Devices and Removable Storage Media
- Phishing Awareness

Specialized Training, required for privileged access:

-Information Assurance Fundamentals (IASO)
-DOD 8570 Baseline Certification and Computing Environment Certification

1.3.7.2 Subtask 2: Accreditation Sustainment.

The contractor shall provide CE specific input for the development of CE security documentation and the updating of existing CE security documentation to facilitate the security accreditation of the CE Infrastructure, IAW the current certification and accreditation guidance (current guidance is DODI 8510.01.RMF. Migrating to NIST Risk Management Framework model). The contractor shall sustain the CE/GovCloud Infrastructure and its environments in compliance with the DISA STIGs. The results of the DISA STIG documentation must always reflect the status of the CE /GovCloud Infrastructure, which may require monthly updates. The contractor may be required to provide a number of updates to existing certification and accreditation documentation, such as network diagrams, ports and protocol listings, CE Infrastructure certification package when required, and other existing documentation. The contractor will be required to provide a monthly update to the program manager for the CE/GovCloud Infrastructure's RMF Plan of Action and Milestones (POA&M). POA&Ms maintained within the Enterprise Mission Assurance Support Service (eMASS).

Deliverable: Updated certification and accreditation documentation, to include:

- Updated network diagrams, ports and protocol matrix, certification package, as changes are made to the CE infrastructures
- Monthly update to application's RMF POA&Ms, no later than the 5th business day of each month

1.3.7.3 Subtask 3: Operational readiness and secure state of CE IT Infrastructure

Contractor is responsible for the operational readiness and secure state of CE IT Infrastructure including:

A. Reporting all suspected security violations immediately to key personnel.
B. Advising the SDDC IASO of security anomalies and vulnerabilities associated with the
C. Information systems hosted in the CE IT Infrastructure.
D. Providing potential means of fixing identified vulnerabilities.
E. Participating in the information system security incident-reporting program.
F. Coordinating with the SDDC and USTRANSCOM IAM and IASOs to investigate and resolve security problems.

1.3.7.3.1 The contractor shall submit an incident report to the COR within 4 hours of discovery of any suspected cyber intrusion event that affect DOD unclassified information systems hosted in the CE IT infrastructure. Initial report shall be provided even if some details are not yet available, with follow-on detailed reporting within 24 hours.

1.3.7.3.2 In the event of a known or potential intrusion, the contractor agrees to perform follow-on actions directed by the Government, including counterintelligence or law enforcement investigative agency, to further characterize and evaluate the suspect activity.

1.3.7.3.3 The contractor acknowledges that damage assessments may be necessary to ascertain intruder methodology and identify systems compromised because of the intrusion.

1.3.7.3.4 Once an intrusion is identified, the contractor agrees to take all reasonable and appropriate steps to preserve any and all evidence, information, data, logs, electronic files and similar type information reference NIST Special Publication 800-61: Computer Security Incident Handling Guide, current version) related to the intrusion. This shall be for subsequent forensic analysis that the government can accomplish an accurate and complete damage assessment. The contractor must ensure data preservation until the government (e.g. removing an affected system, while still powered on, from the network meets the intent of this requirement can perform forensic analysis.

1.3.7.3.5 Any follow-on actions will be coordinated with the contractor via the Contracting Officer's Representative (COR).

1.3.8 Task Area 8: Information Assurance (IA) GovCloud

The contractor shall work with the Government and Contractor Information Assurance Team as designated within SDDC and USTRANSCOM to provide and share system security data and program information (e.g. sop's, business processes and federal guidelines).

1.3.8.1 Subtask 1: Information Assurance Training.

Contract employees shall attend/complete the following security training as prescribed by DOD and SDDC instructions and update the Army Training and Certification Tracking System (ATCTS) to reflect the current-status. All contractor personnel shall create an account in the ATCTS and complete a profile survey; based on that survey, the contractor shall complete all appropriate information assurance training.

Annual Training:
- DOD IA Awareness Training

One-Time Training:
- Army Wide Network Security Focus Training (WNSF)
- SAFE Home Computing
- Personally Identifiable Information (PII)
- Portable Electronic Devices and Removable Storage Media
- Phishing Awareness

Specialized Training, required for privileged access:
- Information Assurance Fundamentals (IASO)
- DOD 8570 Baseline Certification and Computing Environment Certification

1.3.8.2 Subtask 2: Accreditation Sustainment.

The contractor shall provide input for the development of security documentation and the updating of existing security documentation to facilitate the security accreditation of the Infrastructure, IAW the current certification and accreditation guidance (current guidance is DODI 8510.01.RMF. Migrating to NIST Risk Management Framework model). The contractor shall sustain the SDDC GovCloud Infrastructure and its environments in compliance with the DISA STIGs. The results of the DISA STIG documentation must always reflect the status of the GovCloud Infrastructure, which may require monthly updates. The contractor may be required to provide a number of updates to existing certification and accreditation documentation, such as network diagrams, ports and protocol listings, Infrastructure certification package when required, and other existing documentation. The contractor will be required to provide a monthly update to the program manager for the SDDC GovCloud Infrastructure's RMF Plan of Action and Milestones (POA&M). POA&Ms maintained within the Enterprise Mission Assurance Support Service (eMASS).

Deliverable: Updated certification and accreditation documentation, to include:

1. Updated network diagrams, ports and protocol matrix, certification package, SLA as changes are made to the SDDC GovCloud infrastructures
2. Monthly update to application's RMF POA&Ms, no later than the 5th business day of each month

1.3.8.3 Subtask 3: Operational readiness and secure state of SDDC GovCloud Infrastructure

Contractor is responsible for the operational readiness and secure state of SDDC GovCloud Infrastructure including:

1. Reporting all suspected security violations immediately to key personnel IAW USTC GovCloud standards and policies
2. Advising the SDDC IASO of security anomalies and vulnerabilities associated with SDDC systems hosted in the GovCloud
   .
3. Providing potential means of fixing identified vulnerabilities.
4. Participating in the information system security incident-reporting program.
5. Coordinating with the SDDC and USTRANSCOM IAM and IASOs to investigate and resolve security problems.

1.3.8.3.1 Th**e** contractor shall submit an incident report to the COR within 4 hours of discovery of any suspected cyber intrusion event that affect DOD unclassified information systems hosted in the SDDC GovCloud infrastructure. Initial reports provided even if some details are not yet available, with follow-on detailed reporting within 24 hours.

1.3.8.3.2 In the event of a known or potential intrusion, the contractor agrees to perform follow-on actions directed by the Government, including counterintelligence or law enforcement investigative agency, to further characterize and evaluate the suspect activity.

1.3.8.3.3 The contractor acknowledges that damage assessments may be necessary to ascertain intruder methodology and identify systems compromised because of the intrusion.

1.3.8.3.4 Once an intrusion is identified, the contractor agrees to take all reasonable and appropriate steps to preserve any and all evidence, information, data, logs, electronic files and similar type information reference NIST Special Publication 800-61: Computer Security Incident Handling Guide, current version) related to the intrusion. This shall be for subsequent forensic analysis that the government can accomplish an accurate and complete damage assessment. The contractor must ensure data preservation until the government (e.g. removing an affected system, while still powered on, from the network meets the intent of this requirement can perform forensic analysis.

1.3.8.3.5 Any follow-on actions will be coordinated with the contractor via the Contracting Officer's Representative (COR).

2. DELIVERABLES

The Contractor shall be responsible for taking corrective action based upon the impact and severity of identified weaknesses. All deliverables shall electronically delivered via email, SFTP or updates to the appropriate website or tool (e.g., the CMR website or the help-desk ticket system). If submitted via email and the size or the firewall prevents its delivery, the Contractor shall deliver the requirements via SFTP or via compact disk/digital videodisk (CD/DVD). The files delivered by SFTP or CD/DVD shall be properly labeled to identify the content to include version number and date. All deliverables shall meet professional standards and meet the requirements set forth in contractual documentation. The contractor shall provide all deliverables electronically in Army-approved versions of Microsoft Office (Word, Excel, PowerPoint, Project, etc.) formats pursuant to the following schedule.

3. SERVICE DELIVERY SUMMARY

The Services Delivery Summary (SDS) represents the most important contract objectives that, when met, will ensure contract performance is satisfactory. Although not all PWS requirements listed in the SDS, the Contractor shall comply with all requirements in the PWS.

PWS Para	Performance Objective	Performance Threshold

1.3.1.1	Monthly Status Reports to include WBS with Milestone Schedule/Project Plan (On-prem/GovCloud)	99% of the time report is provided on time and is accurate
1.3.1.5	Meeting Agenda and Minutes (On-prem/GovCloud)	98% of the time reports are timely, complete, professionally sound and accurate
1.3.2.1 1.3.3.1	Server Installation and Configuration Guides (On-prem/GovCloud)	98% of the time reports are timely, complete, professionally sound and accurate
1.3.2.1 1.3.3.1	System Documentation (On-prem/GovCloud)	99% of the time, provided on time and is accurate
1.3.2.1 1.3.3.1	System Administration Logbook (On-prem/GovCloud)	99% of the time, provided on time and is accurate
1.3.2.1	Physical connectivity diagrams (On-Prem)	98% of the time reports are timely, complete, professionally sound and accurate
1.3.2.1 1.3.3.1	Logical architecture diagrams (On-prem/GovCloud)	98% of the time reports are timely, complete, professionally sound and accurate
1.3.2.1	Equipment rack elevation diagrams (On Prem)	98% of the time reports are timely, complete, professionally sound and accurate
1.3.2.1	CE Operational Capability (On-prem)	99.5% of the time, Sustain operations to enable all hosted capabilities are fully functioning
1.3.2.1 1.3.3.1	Unplanned Outage Report (On-prem/GovCloud)	99% of the time reports are timely, accurate, complete, and professionally sound. Other than planned outages, Servers and hosted capabilities are available and functioning properly 99.9% of the time each quarter.
1.3.2.1 1.3.3.1	Completion of planned maintenance actions ASI (On-prem/GovCloud)	95% of the time scheduled maintenance ASI actions are completed within allotted time
1.3.2.10	On-Prem Decomm Status Update Brief	Brief due before: 15th of November, December, January and February 2020.
1.3.2.10	On-Prem Decomm: Final PBO Hand Receipt Reconciliation Document	Due before 30 September 2020
1.3.2.10	Disposition Report and Project Closeout Brief	Due before 30 September 2020
1.3.4.3	Migration Plan	99% of the time, provided on time and is accurate

4. GOVERNMENT-FURNISHED AND CONTRACTOR-FURNISHED EQUIPMENT AND INFORMATION

4.1 Government Furnished Equipment (GFE):

All GFE will be maintained IAW FAR 52.245-1, Government Property, and Army Regulation 25-2, Para 4-5. The contractor shall notify the Government of any/all software malfunctions and shall safeguard and provide property accountability for all GFE.

The Government will provide laptops to access specific applications via Client Virtual Public Network (VPN), Virtual Desktop infrastructure (VDI) and Remote Desktop (RD) solutions. SDDC and USTC accounts will be required to obtain access to these solutions.

Information services available on the Government furnished computers are used for official business only. Examples of information services include SDDC/USTC GovCloud network, Internet, Intranet, World Wide Web and electronic mail.

Access to Government information services is granted as a privilege and use of such services constitutes consent to monitoring. Information services use will be monitored to ensure the protection of SDDC/USTC networks and information and to verify and enforce compliance with this contractual requirement.

In the event contractor personnel use Government furnished computers and/or information services for other than official business, the contractor shall be required to provide the Government with monetary consideration. Misuse by a contractor employee may also result in that employee losing access to Government systems and determined disqualified for Government system access. The contractor shall ensure that workload performed by disqualified employees are transferred to a qualified individual within 10 working days. Employee disqualifications for Government system access shall not relieve the contractor from meeting the performance standards and thresholds required by this PWS.

The following are examples of misuse of information services:

- Illegal, fraudulent, or malicious activities.
- Partisan political activity, political or religious lobbying or advocacy, or activities on behalf of organizations having no affiliation with SDDC, USTC or DOD.
- Activities whose purposes are for personal or commercial financial gain. These activities may include chain letters, solicitation of business or services, sales of personal property.
- Unauthorized fundraising or similar activities, whether for commercial, personal, or charitable purposes.
- Accessing, storing, processing, displaying, or distributing offensive or obscene material such as pornography and hate literature.
- Annoying or harassing another person, e.g., by sending or displaying uninvited e-mail of a personal nature or by using lewd or offensive language in an e-mail message.
- Using another person's account or identity without his or her explicit permission, e.g., by forging e-mail.
- Viewing, damaging, or deleting files or communications belonging to others without appropriate authorization or permission.
- Permitting any unauthorized person to access a SDDC, USTC or DOD owned system.
- Modifying or altering the operating systems or system configuration (including the installation of software) without obtaining written authorization from the KO.

The Contractor is responsible for maintaining the development and test environment (as applicable) to mirror Pre Production and production environments.

5. GENERAL INFORMATION

5.1 Place of Performance

Performance will be at the Government-site and the contractor site. The Government will provide workstations/office spaces for contractor personnel at the SDDC Government site. Contractors who work outside of SAFB, IL. may be required to participate in meetings via phone and will be provided a call-in number to meet this requirement. Administrators must be able to access servers located on SAFB. Personnel entering locations where servers are hosted must have a valid Secret clearance before entry.

Permanent Off-Site Employees or Permanent Work from Home (WFH) shall not be team leads, supervisors or project/program managers that work outside of the commuting area. These positions require face-to-face meetings and daily interaction with SDDC leadership, COR, ACOR and program managers and component peers for joint projects and coordination. Government furnished equipment (GFE) hand receipt(s) shall be signed initially by the contractors on-site PM and subsequently by the off-site contract employee and returned within seven business days upon receipt of equipment to SDDC for proper inventory. The GFE is shipped to the employee via FEDEX or another carrier at SDDC expense. The incumbent contractor recipient shall ship the GFE back in the same or similar container as to deter equipment damage after receiving a shipping label(s) from SDDC upon leaving the contract or contract expiration.

5.2 Work Hours

Contractor personnel are expected to conform to agency operating hours (0700 – 1700 CST) unless otherwise approved by the COR. Work will generally consist of 40-hour work week, Monday through Friday, excluding federal holidays. Personnel shall support short notice adjustments to their daily work hours. The contractor shall

provide non-duty hour monitoring and break-fix capability to sustain SDDC applications and management service operations and ensure it is fully functioning to support the hosted capabilities.

5.3 Period of Performance

Base Period:	01 September 2019 through 30 September 2019
Option Year One:	01 October 2019 through 30 September 2020
Option Year Two:	01 October 2020 through 30 September 2021.
Option Year Three:	01 October 2021through 30 September 2022.
Option Year Four:	01 October 2022 through 30 September 2023.
Option Year Five:	01 October 2023 through 30 September 2024.

Contractor shall have 30 days advance notification prior to exercising Optional CLINs.

5.4 Cooperation with Other Contractors and Government Personnel.

The contractor shall cooperate with other contractors and Government personnel performing work for SDDC and USTC. The contractor shall be willing to adjust scheduling and performance to accommodate additional support if required by modification. The contractor shall avoid interfering with the performance of work by other contractors or Government employees while not compromising health, safety or security. Any disagreement or cause of delay shall be brought immediately to the attention of the Contracting Officer and COR/ACOR/PM.

5.5 Contractor Employees.

The Contractor shall provide personnel with expertise in the subject matter areas to comply with the terms of this requirement. The Contractor personnel shall be capable of working independently. At no additional expense to the Government, the contractor shall ensure that personnel assigned to this project retain appropriate certifications and remain current in the technical skills required to support and execute this task. New employees are required to attend mandatory SDDC security briefings, to complete mandatory information assurance training, and to complete a number of forms to work on the SDDC/USTC network. Contractor must work with the COR to complete these activities as soon as possible in order to be an effective member of the SDDC team.

5.6 Non-Disclosure Agreement (NDA) for Contractor Employees

In performance of this contract, the Contractor may have access to sensitive, non-public information. The Contractor agrees, (a) to use and protect such information from unauthorized disclosure in accordance with DTM 08-027 - Security of Unclassified DOD Information on Non-DOD Information Systems, 31 July 2009; (b) to use and disclose such information only for the purpose of performing this contract and to not use or disclose such information for any personal or commercial purpose; (c) to obtain permission of the Government before disclosing/discussing such information with a third party; (d) to return and/or electronically purge, upon Government request, any non-public, sensitive information no longer require for Contractor performance; and (e) to advise the Government of any unauthorized release of such information. Upon request, the Contractor shall have its employees assigned to this contract execute a non-disclosure agreement for delivery to the Government. The Government will require Contractor personnel to sign a non-disclosure statement (Appendix F) to protect non-public information of other Contractors and/or the Government.

5.7 Quality Assurance.

The contractor shall support Government agency reviews and audits of all services and support provided under this PWS. The contractor shall be prepared to support Quality Assurance reviews conducted by the Government. The Government reserves the right to authorize an independent verification and validation of the contractor's procedures, methods, data, equipment, and other services provided at any time during the performance of this PWS.

5.8 Requirements Affecting Contractor Personnel Performing Mission Essential Services.

The COR has designated there will be no Mission Essential Contractor personnel.

5.9 Travel

Performance under this contract may require contractor travel within CONUS. The Government will reimburse the contractor for travel expenses subject to the Federal Acquisition Regulation (FAR) and the Joint Travel Regulation (JTR).

Prior to incurring any long distance travel expenses, the contractor shall obtain written approval from the COR approving the travel dates, expected duration, origin and destination, purpose, estimated costs, and the number and names of personnel traveling. In addition, the contractor shall receive COR confirmation on availability of funds prior to traveling.

All travel arrangements shall be the responsibility of the contractor, to include airfare reservations, lodging reservations, and rental car reservations. The contractor should make all effort to schedule travel far enough in advance to take advantage of reduced airfares.

The contractor shall submit a trip report to include the following details: purpose, location, length of trip, travelers, and actual travel costs, individuals contacted during trip, synopsis of all discussions, future actions identified, decisions made, and issues of concern arising during the trip within five (5) business days of the trip conclusion. The Government will not reimburse local travel and related expenses to the contractor for daily travel to or from Scott AFB and/or the contractor's facility.

5.10 Other Direct Costs (ODCs)

The Contractor may recommend software and hardware solutions to improve ISDDC, PAT, EDI, and SOA capabilities. The Government will reimburse allowable ODCs incurred in the performance of this PWS. The contractor shall submit ODC requests in writing to the COR for authorization at least five business days in advance of incurring any expenses. The request shall contain estimated costs supported by a minimum of three competitive quotes. Contractor invoices (along with associated receipts) shall support all ODC reimbursement requests. In no event shall the contractor be authorized to purchase ODCs that exceed the ODC amount funded in the contract. General and Administrative overhead charges will not be accepted or paid for approved ODC purchases.

5.10.1 Software

Software licenses shall be transferable to the Government at no additional cost and shall not conflict with Federal law. Prior to purchase, the licenses shall be submitted to the Contracting Officer for review. If the Contracting Officer determines provisions are inconsistent with Federal law and regulation, the contractor shall negotiate changes with the software vendor at no additional cost to the Government. After the Contracting Officer's review and approval the license provisions, price quotes for software and licenses shall be submitted to the COR for review and approval prior to purchase. The contractor shall obtain the COR’s approval prior to proceeding with any software and licenses procurement

5.10.2 Hardware

The contractor shall obtain the CORs approval prior to proceeding with any IT hardware (in accordance with USTRANSCOM standards) in support of the CE. Any hardware purchased by the contactor for use by the Federal Government shall become the property of the Federal Government. Any hardware authorized by the COR for purchase must have all required approvals that would have been required had the Government purchased the hardware

6.0 SECURITY (PHYSICAL, PERSONNEL, INFORMATION, INDUSTRIAL, OPERATIONS, ANTITERRORISM, and FORCE PROTECTION) REQUIREMENTS. (MANDATORY)

6.1 General Security Information. The overall classification of work associated with this PWS is SECRET. Tasks associated with the deliverables in this PWS require a SECRET Facility clearance (FCL) with eligibility and access for all contract employees, who requires classified access, will possess a SECRET personnel clearance (PCL). All classified material handled by the contractor will be safeguarded and derivatively classified IAW Executive Order (EO) 13526 and per SDDC Regulation 380-5 (Information Security Regulation) and all applicable Office of the Secretary of Defense (OSD) Classification Guides. A completed/signed DD 254 is attached to this PWS with classification requirements and guidance.

6.2 Personnel Clearance (PCL) / Investigation Requirements. Personnel working on this contract will require a favorably completed Tier 3 background investigation, resulting in SECRET eligibility (or higher) when adjudicated by the Department of Defense Consolidated Adjudication Facility (DOD CAF). National Background Investigations Bureau (NBIBSecret clearance eligibility is accepted and granted by the Vetting Risk Operations Center (VROC) when the VROC has opened the investigation. The Facility Security Officer (FSO) is responsible for ensuring Tier 3 investigations are submitted to the NBIB and a minimum of SECRET is granted prior to contract start day.

6.2.1 Contracts that require Handling or Access to Classified Information. Contractor shall comply with FAR 52.204-2, Security Requirements. This clause involves access to information classified "Confidential," "Secret," or "Top Secret" and requires contractors to comply with: (1) The Security Agreement (DD Form 441), including the National Industrial Security Program Operating Manual (DOD 5220.22-M) and, (2) any revisions to DOD 5220.22-M, notice of which has been furnished to the contractor.

6.2.2 Access and General Protection/Security Policy and Procedures. The contractor and all associated subcontractors employees shall provide all information required for background checks, to meet installation access requirements. Information will be provided to the installation Provost Marshal Office, Director of Emergency Services or Security Office. Contractor workforce must comply with all personal identity verification requirements (FAR clause 52.204-9, Personal Identity and Verification of Contractor Personnel) as directed by DOD, HQDA and/or local policy. In addition, the variations otherwise authorized by the changes clause of this contract, should the Force Protection Condition (FPCON) at any individual facility or installation change, the Government may require changes in contractor security requirements.

6.3 Company Facility Clearance (FCL). The awarded contract company (and subcontract companies) shall have and maintain a valid FCL at the SECRET level or higher at time of quote submission. FCL procedures and security guidelines for adjudicative requirements are outlined in DOD 5220.22-M, DOD 5200.22-R and AR 380-67. FCLs must be awarded by the Defense Security Service Facility Clearance Branch.

6.4 Clearance / Investigation Validation Checks. Upon award of this contract, the names and social security numbers of all contract employees supporting this contract must be submitted to the SDDC G3-4 for vetting in the Joint Personnel Adjudication System (JPAS) to ensure investigative requirements are met before contract start date. This requirement will be completed prior to the COR/Trusted Agent (TA) submitting contract employees for their Common Access Card (CAC) through in the DOD Trusted Associate Sponsorship System (TASS). If contract member does not meet the appropriate investigative requirement, the contract employee will be denied the ability to work in support of this contract.

6.5. Common Access Card (CAC) Issuance. Upon notification by the SDDC G3/4 that contractor personnel meet the required investigative levels, personnel will be approved in the TASS application, with an expiration date on their CAC, for the current period either of performance or up to no more than 3 years.

6.5.1 Contractors Requiring a Common Access Card. Before CAC issuance, the contractor employee requires, at a minimum, a favorably adjudicated Tier 1 or higher investigation in accordance with Army Directive 2014-05. The contractor employee will be issued a CAC only if duties involve one of the following: (1) both physical access to a DOD facility and access, via logon, to DOD networks on-site or remotely, (2) remote access, via logon, do a DOD network using DOD-approved remote access procedures; or, (3) physical access to DOD facilities or non-DOD federally controlled facilities on behalf of the DOD, on a recurring basis for a period of 6 months or more.

6.6 Scott AFB/USTRANSCOM/HQ SDDC Physical Access. Only personnel assigned physically on Scott AFB at least 4 days a week will be issued an AF FM 1199 (line badge) unless an exception to policy is approved by the 375 SFS through SDDC G34.

6.7 Visit Authorization. Visit(s) by contract personnel not permanently assigned on Scott AFB will require an electronic visit request in JPAS to Security Management Office (SMO) Code: USTC-SDDC.

6.7.1 Permanently assigned contractors: Those contractors permanently assigned to Scott AFB will require electronic JPAS visit requests submitted to SMO Code: SSC-CONT. The POC block is the contract number and phone number block will include COR phone number and last name.

6.7.2 Hard copy visit requests: These are accepted for companies that do not have JPAS access. Hard copy visit requests and must be submitted on company letterhead to the SDDC/USTRANSCOM Protection Service Center (PSC). Visit requests to SAFB will not exceed a 180-day duration and will not be valid if the visit extends past the base or option years of this contract period.

6.8 In/Out-Processing. Upon termination or completion of this contract, the contractor employee will surrender all Government supplies, materials, classified material and equipment to the COR. In addition, the contractors' CACs and any security badges issued will be turned in to the SDDC/USTRANSCOM PSC at SAFB, IL or to the COR. Off-site contractors will return the CAC to the COR. This will be accomplished on the last day of the contract or upon any termination/reassignment of a contract employee. CORs who retrieve the CAC and security badges, due to short notice terminations or release of contract employees, will revoke access in TASS and turn in the CAC and security badge in to the PSC for final processing/out-processing. All on-site contract personnel will complete an in/out-processing checklist supplied by the COR/CO or SDDC G1/4.

6.9 Security briefing/debriefing statement. (Standard Form 312) will be completed upon start/completion of the contract, if assigned to SDDC at SAFB, IL. This will be completed/executed by the SDDC/USTRANSCOM PSC during in and out-processing.

6.10 Security Training. Contractor employees assigned to HQ SDDC at SAFB will attend/complete the following training within 30 days of contract start as prescribed by DOD, Army and SDDC Regulations: Employee Initial Security Briefing, Operations Security (OPSEC), Threat Awareness and Reporting Program (TARP), DOD Antiterrorism (AT) Level 1 Training, Active Shooter and Workplace Violence Training. This also includes IA training required for specific computing platforms and applications. All Security training, to include Annual Security Awareness Training, is required annually.

6.10.1 AT Level 1 Training. Contractor employees, to include subcontractor employees, requiring access to Army installations, facilities and controlled areas shall complete AT Level I awareness training within 30 calendar days after contract start date or effective date of incorporation of this requirement into the contract, whichever is applicable. The contractor shall submit certificates of completion for each affected contractor employee and subcontractor employee to the COR or to the contracting officer, if a COR is not assigned, within 30 calendar days after completion of training by all employees and subcontractor personnel. AT level I awareness training is available at the following website: http://jko.jten.mil.

6.10.2 Threat Awareness Reporting Program. For all contractors with security clearances. Per AR 381-12, Threat Awareness and Reporting Program (TARP), contractor employees must receive annual TARP training by a CI agent or other trainer as specified in 2-4b.

6.10.3 Initial Security and AT Level I Training. Will be provided by SDDC G34 for contractor employees assigned to HQ SDDC at SAFB; attendance is required within the first 10 days of contract start day at SAFB. Contractor personnel assigned elsewhere shall attend security training established by their respective Government security offices and/or installations.

6.10.4 Contractor employees will report training completion to the COR.

6.10.5 IWatch Training. The contractor and all associated subcontractors shall brief all employees on the local iWatch program (training standards provided by the requiring activity ATO). This local developed training will be used to inform employees of the types of behavior to watch for and instruct employees to report suspicious activity to the CO. This training shall be completed within 30 calendar days of contract award and within 30 calendar days of new employees commencing performance with the results reported to the COR NLT 30 calendar days after contract award.

6.11 Security Permissions on DOD Systems. The contractor shall ensure the roles/privileges assigned to contract employees on the Government computing platforms are limited to the roles/privileges essential to that individual's performance of his/her assignments. These roles/privileges can be limited or revoked by the Government for any reason.

6.12 Security Compliance / Deviations. If the Government notifies the contractor that the employment or the continued employment of any contractor employee is prejudicial to the interests or endangers the security of the United States of America, that person shall be removed and barred from the worksite.

6.12.1 Circumstances surrounding the removal of contract employees include security deviations/incidents and credible derogatory information received or uncovered on contract members during the course of the contractual period. The contract company shall make any changes necessary in the appointment(s), at no cost to the government.

6.12.2 Contracting officers or contracting officer representatives will ensure Army contractors with security clearances comply with threat awareness and reporting requirements specified in AR 381-12. Additionally, persons employed by Army contractors will report threat-related incidents, behavioral indicators, and other matters of Counter-Intelligence (CI) interest specified in AR 381-12, chapter 3, to the Facility Security Officer, the nearest military CI Office, the Federal Bureau of Investigation, or the Defense Security Service.

6.12.3 Contractor employees will comply with base access and control procedures.

6.12.4 Operations Security (OPSEC)/ Contracts that require OPSEC training: Per AR 530-1, the contractor employees must complete Level I OPSEC Awareness training. New employees must be trained with 30 calendar days of their reporting for duty and annually thereafter. All information furnished to the Contractor is to be used FOR OFFICIAL USE ONLY (FOUO). The Contractor is required to be aware of OPSEC requirements from SDDC. Information determined as FOUO or included as part of the OPSEC Critical Information List (CIL) is not to be released to the public.

6.13 FPCON Impact on Work Levels (US Installation Only). Contractors working on base are not considered mission essential in this PWS; therefore, access to the installation during increased force protection condition (FPCON) CHARLIE and DELTA is not authorized.

6.14 Security Regulation Compliance. The contractor will be required to comply with all security regulations and directives as identified herein and other security requirements in this contract. The contractor shall not divulge any financial, planning, programming, or budgeting information without the express consent of the Government as outlined in Operational Security (OPSEC) and Information Security regulations.

6.15 Defense Electronic libraries:
Assist – Quick Search: http://quicksearch.dla.mil
CJCS: http://www.dtic.mil/doctrine/doctrine/cjcs.htm
Department of Defense: http://www.esd.whs.mil/dd/dod-issuances/
USTRANSCOM: https://ww2.ustranscom.mil/publications/pubs_index.cfm

Governing guidance and directives:
DD Form 254, Contract Security Classification Specification, November 1, 2017.
DoD 5200.08-R, "Physical Security Program," May 27, 2009.
DoD 5220-22-M, National Industrial Security Program Operating Manual (NISPOM)," May 18, 2016.

DoD Directive 5230.25, "Withholding of Unclassified Technical Data from Public Disclosure," August 18, 1995.
DoD Instruction 2000.12, "DoD Antiterrorism (AT) Program," May 8, 2017.
DoD Instruction O-2000.16, "DoD Antiterrorism (AT) Standards Program Implementation, Volume 1: DoD AT Standards," May 5, 2017.
DoD Instruction O-2000.16, "DoD Antiterrorism (AT) Standards Program Implementation, Volume 2: DoD force Protection condition (FPCON) System, May 8, 2017.
DoD Instruction 5200.01, "DoD Information Security Program and Protection of Sensitive Compartmented Information (SCI), April 21, 2016.
DoD Instruction 5200.02, "Personnel Security Program," September 9, 2014.
DoD Instruction 8330.01, "Interoperability of Information Technology (IT), Including National Security Systems (NSS)," December 18, 2017.
DoD Instruction 8500.01, "Cybersecurity," March 14, 2014.
DoD Instruction 8510.01, "Risk Management Framework (RMF) for DoD Information Technology (IT)," July 28, 2017.
DoD Instruction 8582.01, "Security of Unclassified DoD Information on Non-DoD Information Systems," October 27, 2017.
DoD Manual 1000.13, Volume 1, "DoD Identification (ID) Cards: ID Card Life-Cycle," January 23, 2014.
DoD Manual 5200.01, Volume 1, "DoD Information Security Program: Overview, Classification, and Declassification", February 24, 2012.
DoD Manual 5200.01 Volume 2, "DoD Information Security Program: Marking of Classified Information," March 19, 2013.
DoD Manual 5200.01 Volume 3, "DoD Information Security Program: Protection of Classified Information," March 19, 2013
DoD Manual 5200.01 Volume 4, "DoD Information Security Program: Controlled Unclassified Information (CUI)," February 24, 2012
DoD Manual 5200.02, "Procedures for the DoD Personnel Security Program (PSP)," April 3, 2017
DoD Manual 5220.22, Volume 3, "National Industrial Security Program: Procedures for Government Activities Relating to Foreign Ownership, Control, or Influence (FOCI)," April 17, 2014 FD Form 258, fingerprint Card
USTRANSCOM Instruction 31-02, "Security Classification Guide," 6 April 2018
USTRANSCOM Instruction 31-12, "Operations Security," February 19, 2015

Scott Air Force Base: AF Instruction 31-101_AMC, January 4, 2014 Scott AFB Supplement is a restricted publication: Send only to .mil domains when forwarding - Not for public distribution

Federal Information Processing Standards (FIPS) and National Institute of Standards and Technology (NIST): https://csrc.nist.gov/publications

FIPS 199, "Standards for Security Categorization of Federal Information and Information Systems," February 2004
FIPS 200, "Minimum Security Requirements for Federal Information and Information Systems," March 2006

•NIST SP 800-18 Revision 1, "Guide for Developing Security Plans for Federal Information Systems" February 2006
•NIST SP 800-30 Revision 1, "Guide for Conducting Risk Assessments," September 2012
•NIST SP 800-37 Revision 1, "Guide for Applying the Risk Management Framework to Federal Information Systems: a Security life Cycle Approach," June 5, 2014
•NIST SP 800-53, Revision 4, "Security and Privacy Controls for Federal Information Systems and Organizations," January 22, 2015
•NIST SP 800-53A Revision 4, "Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans," December 18, 2014
•NIST SP 800-60 Volume 1, Revision 1, "Guide for Mapping Types of Information and Information Systems to Security Categories," August 2008
•NIST SP 800-61 Revision 2, "Computer Security Incident Handling Guide," August 2012
•NIST Special Publication 800-171 Revision 1 "Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations, "December 2016

Committee on National Security Systems (CNSS): https://www.cnss.gov/CNSS/issuances/Instructions.cfm
CNSS Instruction 1253, "Security Categorization and Control Selection for National Security Systems," March 27, 2014

Army:
AR 25-2 (Information Assurance)
AR 190-13 (Physical Security Program)
AR 380-5 (Department of the Army Information Security Program)
AR 380-20 (Restricted Areas)
AR 380-49 (Industrial Security Program)
AR 380-67 (Personnel Security Program)
AR 381-12 (Threat Awareness and Reporting Program)
AR 525-13 (Antiterrorism)
AR 530-1 (Operations Security)

Army regulations found at http://armypubs.army.mil/

SDDC:
SDDC Regulation 190-13 (SDDC Physical Security Program)
SDDC Regulation 380-2 (SDDC Operations Security Program)
SDDC Regulation 380-5 (SDDC Information Security Program)

Forms:
DD 254, DOD, Contract Security Classification Specification

DOD forms found at: http://www.dtic.mil/whs/directives/corres/pub1.html l

HQ SDDC Industrial Security Point of Contact:
(b) (6) or (b) (6)
1 Soldier Way
SDDC G3-4
SAFB, IL. 62225
Commercial: 618-220-6559
Email at (b) (6) or (b) (6)

HQ SDDC G3-4 Approval: (b) (6) 14 DEC 18
HQ SDDC G3-4 Tracking #:

USTRANSCOM Protection Programs Division (Industrial Security) Points of Contact:
USTRANSCOM
Attn: TCJ34 (b) (6)
508 Scott Drive
Scott AFB IL 62225
Commercial: 618-220-7892/220-6531 (respectively)
Email at (b) (6) or (b) (6)
USTC TCJ34 Approval: (b) (6) USTRANSCOM PSC, 618-220-6531
USTC TCJ34 Tracking #: USTRANSCOM-FP-0015-19

7.0 CYBER SECURITY

7.1 BASIC SAFEGUARDING OF COVERED CONTRACTOR INFORMATION SYSTEMS

(a) *Definitions*. As used in this clause--

"Covered contractor information system," means an information system that is owned or operated by a contractor that processes, stores, or transmits Federal contract information.

"Federal contract information" means information, not intended for public release, that is provided by or generated for the Government under a contract to develop or deliver a product or service to the Government, but not including information provided by the Government to the public (such as on public Web sites) or simple transactional information, such as necessary to process payments.

"Information" means any communication or representation of knowledge such as facts, data, or opinions, in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual (Committee on National Security Systems Instruction (CNSSI) 4009).

"Information system" means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information (44 U.S.C. 3502).

"Safeguarding," means measures or controls that are prescribed to protect information systems.

(b) Safeguarding requirements and procedures.

(1) The Contractor shall apply the following basic safeguarding requirements and procedures to protect covered contractor information systems. Requirements and procedures for basic safeguarding of covered contractor information systems shall include, at a minimum, the following security controls:

(i) Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).

(ii) Limit information system access to the types of transactions and functions that authorized users are permitted to execute.

(iii) Verify and control/limit connections to and use of external information systems.

(iv) Control information posted or processed on publicly accessible information systems.

(v) Identify information system users, processes acting on behalf of users, or devices.

(vi) Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.

(vii) Sanitize or destroy information system media containing Federal Contract Information before disposal or release for reuse.

(viii) Limit physical access to organizational information systems, equipment, and the respective operating environments to authorized individuals.

(ix) Escort visitors and monitor visitor activity; maintain audit logs of physical access; and control and manage physical access devices.

(x) Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.

(xi) Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.

(xii) Identify, report, and correct information and information system flaws in a timely manner.

(xiii) Provide protection from malicious code at appropriate locations within organizational information systems.

(xiv) Update malicious code protection mechanisms when new releases are available.

(xv) Perform periodic scans of the information system and real-time scans of files from external sources as files are downloaded, opened, or executed.

(2) *Other requirements*. This clause does not relieve the Contractor of any other specific safeguarding requirements specified by Federal agencies and departments relating to covered contractor information systems generally or other Federal safeguarding requirements for controlled unclassified information (CUI) as established by Executive Order 13556.

(c) *Subcontracts*. The Contractor shall include the substance of this clause, including this paragraph (c), in subcontracts under this contract (including subcontracts for the acquisition of commercial items, other than commercially available off-the-shelf items), in which the subcontractor may have Federal contract information residing in or transiting through its information system.

7.2 SAFEGUARDING COVERED DEFENSE INFORMATION AND CYBER INCIDENT REPORTING

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

“Adequate security” means protective measures that are commensurate with the consequences and probability of loss, misuse, or unauthorized access to, or modification of information.

“Compromise” means disclosure of information to unauthorized persons, or a violation of the security policy of a system, in which unauthorized intentional or unintentional disclosure, modification, destruction, or loss of an object, or the copying of information to unauthorized media may have occurred.

“Contractor attributional/proprietary information” means information that identifies the contractor(s), whether directly or indirectly, by the grouping of information that can be traced back to the contractor(s) (e.g., program description, facility locations), personally identifiable information, as well as trade secrets, commercial or financial information, or other commercially sensitive information that is not customarily shared outside of the company.

“Controlled technical information” means technical information with military or space application that is subject to controls on the access, use, reproduction, modification, performance, display, release, disclosure, or dissemination. Controlled technical information would meet the criteria, if disseminated, for distribution statements B through F using the criteria set forth in DOD Instruction 5230.24, Distribution Statements on Technical Documents. The term does not include information that is lawfully publicly available without restrictions.

Covered contractor information system.

“Covered contractor information system,” means an unclassified information system that is owned, or operated by or for, a contractor and that processes, stores, or transmits
Covered defense information.

"Covered defense information" means unclassified controlled technical information or other information, as described in the Controlled Unclassified Information (CUI) Registry at http://www.archives.gov/cui/registry/category-list.html, that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Government wide policies, and is—

(1) Marked or otherwise identified in the contract, task order, or delivery order and provided to the contractor by or on behalf of DOD in support of the performance of the contract; or

(2) Collected, developed, received, transmitted, used, or stored by or on behalf of the contractor in support of the performance of the contract.

"Cyber incident" means actions taken through the use of computer networks that result in a compromise or an actual or potentially adverse effect on an information system and/or the information residing therein.

"Forensic analysis" means the practice of gathering, retaining, and analyzing computer-related data for investigative purposes in a manner that maintains the integrity of the data.

"Information system" means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

"Malicious software" means computer software or firmware intended to perform an unauthorized process that will have adverse impact on the confidentiality, integrity, or availability of an information system. This definition includes a virus, worm, Trojan horse, or other code-based entity that infects a host, as well as spyware and some forms of adware.

"Media" means physical devices or writing surfaces including, but is not limited to, magnetic tapes, optical disks, magnetic disks, large-scale integration memory chips, and

Print-outs onto which covered defense information is recorded, stored, or printed within a covered contractor information system.

''Operationally critical support'' means supplies or services designated by the Government as critical for airlift, sealift, intermodal transportation services, or logistical support that is essential to the mobilization, deployment, or sustainment of the Armed Forces in a contingency operation.

"Rapidly report" means within 72 hours of discovery of any cyber incident.

"Technical information" means technical data or computer software, as those terms are

defined in the clause at DFARS 252.227-7013, Rights in Technical Data—

Noncommercial Items, regardless of whether or not the clause is incorporated in this

solicitation or contract. Examples of technical information include research and engineering data, engineering drawings, and associated lists, specifications, standards, process sheets, manuals, technical reports, technical orders, catalog-item identifications, data sets, studies and analyses and related information, and computer software executable code and source code.

(b) *Adequate security*. The Contractor shall provide adequate security on all covered contractor information systems. To provide adequate security, the Contractor shall implement, at a minimum, the following information security protections:

(1) For covered contractor information systems that are part of an Information Technology (IT) service or system operated on behalf of the Government, the following security requirements apply:

(i) Cloud computing services shall be subject to the security requirements specified in the clause 252.239-7010, Cloud Computing Services, of this contract.

(ii) Any other such IT service or system (i.e., other than cloud computing) shall be subject to the security requirements specified elsewhere in this contract.

(2) For covered contractor information systems that are not part of an IT service or system operated on behalf of the Government and therefore are not subject to the security requirement specified at paragraph (b)(1) of this clause, the following security requirements apply:

(i) Except as provided in paragraph (b)(2)(ii) of this clause, the covered contractor information system shall be subject to the security requirements in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171, "Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations" (available via the internet at http://dx.doi.org/10.6028/NIST.SP.800-171) in effect at the time the solicitation is issued or as authorized by the Contracting Officer.

(ii)(A) The Contractor shall implement NIST SP 800-171, as soon as practical, but not later than December 31, 2017. For all contracts awarded prior to October 1, 2017, the Contractor shall notify the DOD Chief Information Officer (CIO), via email at osd.dibcsia@mail.mil, within 30 days of contract award, of any security requirements specified by NIST SP 800-171 not implemented at the time of contract award.

(B) The Contractor shall submit requests to vary from NIST SP 800-171 in writing to the Contracting Officer, for consideration by the DOD CIO. The Contractor need not implement any security requirement adjudicated by an authorized representative of the DOD CIO to be non-applicable or to have an alternative, but equally effective, security measure that may be implemented in its place.

(C) If the DOD CIO has previously adjudicated the contractor's requests indicating that a requirement is not applicable or that an alternative security measure is equally effective, a copy of that approval shall be provided to the Contracting Officer when requesting its recognition under this contract.

(D) If the Contractor intends to use an external cloud service provider to store, process, or transmit any covered defense information in performance of this contract, the Contractor shall require and ensure that the cloud service provider meets security requirements equivalent to those established by the Government for the Federal Risk and Authorization Management Program (Fed RAMP) Moderate baseline (https://www.fedramp.gov/resources/documents/) and that the cloud service provider complies with requirements in paragraphs (c) through (g) of this clause for cyber incident reporting, malicious software, media preservation and protection, access to additional information and equipment necessary for forensic analysis, and cyber incident damage assessment.

(3) Apply other information systems security measures when the Contractor reasonably determines that information systems security measures, in addition to those identified in paragraphs (b)(1) and (2) of this clause, may be required to provide adequate security in a

dynamic environment or to accommodate special circumstances (e.g., medical devices) and any individual, isolated, or temporary deficiencies based on an assessed risk or vulnerability. These measures may be addressed in a system security plan.

(c) *Cyber incident reporting requirement.*

(1) When the Contractor discovers a cyber incident that affects a covered contractor information system or the covered defense information residing therein, or that affects the contractor's ability to perform the requirements of the contract that are designated as operationally critical support and identified in the contract, the Contractor shall—

(i) Conduct a review for evidence of compromise of covered defense information, including, but not limited to, identifying compromised computers, servers, specific data, and user accounts. This review shall also include analyzing covered contractor information system(s) that were part of the cyber incident, as well as other information systems on the Contractor's network(s), that may have been accessed as a result of the incident in order to identify compromised covered defense information, or that affect the Contractor's ability to provide operationally critical support; and

(ii) Rapidly report cyber incidents to DOD at http://dibnet.DOD.mil.

(2) *Cyber incident report.* The cyber incident report shall be treated as information created by or for DOD and shall include, at a minimum, the required elements at http://dibnet.DOD.mil.

(3) *Medium assurance certificate requirement.* In order to report cyber incidents in accordance with this clause, the Contractor or subcontractor shall have or acquire a DOD-approved medium assurance certificate to report cyber incidents. For information on obtaining a DOD-approved medium assurance certificate, see http://iase.disa.mil/pki/eca/Pages/index.aspx.

(d) *Malicious software.* When the Contractor or subcontractors discover and isolate malicious software in connection with a reported cyber incident, submit the malicious software to DOD Cyber Crime Center (DC3) in accordance with instructions provided by DC3 or the Contracting Officer. Do not send the malicious software to the Contracting Officer.

(e) *Media preservation and protection.* When a Contractor discovers a cyber incident has occurred, the Contractor shall preserve and protect images of all known affected information systems identified in paragraph (c)(1)(i) of this clause and all relevant monitoring/packet capture data for at least 90 days from the submission of the cyber incident report to allow DOD to request the media or decline interest.

(f) *Access to additional information or equipment necessary for forensic analysis.* Upon request by DOD, the Contractor shall provide DOD with access to additional information or equipment that is necessary to conduct a forensic analysis.

(g) *Cyber incident damage assessment activities.* If DOD elects to conduct a damage assessment, the Contracting Officer will request that the Contractor provide all of the damage assessment information gathered in accordance with paragraph (e) of this clause.

(h) *DOD safeguarding and use of contractor attributional/proprietary information.* The Government shall protect against the unauthorized use or release of information obtained from the contractor (or derived from information obtained from the contractor) under this clause that includes contractor attributional/proprietary information, including such information submitted in

accordance with paragraph (c). To the maximum extent practicable, the Contractor shall identify and mark attributional/proprietary information. In making an authorized release of such information, the Government will implement appropriate procedures to minimize the contractor attributional/proprietary information that is included in such authorized release, seeking to include only that information that is necessary for the authorized purpose(s) for which the information is being released.

(i) *Use and release of contractor attributional/proprietary information not created by or for DOD.* Information that is obtained from the contractor (or derived from information obtained from the contractor) under this clause that is not created by or for DOD is authorized to be released outside of DOD—

(1) To entities with missions that may be affected by such information;

(2) To entities that may be called upon to assist in the diagnosis, detection, or mitigation of cyber incidents;

(3) To Government entities that conduct counterintelligence or law enforcement investigations;

(4) For national security purposes, including cyber situational awareness and defense purposes (including with Defense Industrial Base (DIB) participants in the program at 32 CFR part 236); or

(5) To a support services contractor ("recipient") that is directly supporting Government activities under a contract that includes the clause at 252.204-7009, Limitations on the Use or Disclosure of Third-Party Contractor Reported Cyber Incident Information.

(j) *Use and release of contractor attributional/proprietary information created by or for DOD.* Information that is obtained from the contractor (or derived from information obtained from the contractor) under this clause that is created by or for DOD (including the information submitted pursuant to paragraph (c) of this clause) is authorized to be used and released outside of DOD for purposes and activities authorized by paragraph (i) of this clause, and for any other lawful Government purpose or activity, subject to all applicable statutory, regulatory, and policy based restrictions on the Government's use and release of such information.

(k) The Contractor shall conduct activities under this clause in accordance with applicable laws and regulations on the interception, monitoring, access, use, and disclosure of electronic communications and data.

(l) *Other safeguarding or reporting requirements.* The safeguarding and cyber incident reporting required by this clause in no way abrogates the Contractor's responsibility for other safeguarding or cyber incident reporting pertaining to its unclassified information systems as required by other applicable clauses of this contract, or as a result of other applicable U.S. Government statutory or regulatory requirements.

(m) *Subcontracts*. The Contractor shall—

(1) Include this clause, including this paragraph (m), in subcontracts, or similar contractual instruments, for operationally critical support, or for which subcontract performance will involve covered defense information, including subcontracts for commercial items, without alteration, except to identify the parties. The Contractor shall determine if the information required for subcontractor performance retains its identity as covered defense information

and will require protection under this clause, and, if necessary, consult with the Contracting Officer; and

(2) Require subcontractors to—

(i) Notify the prime Contractor (or next higher-tier subcontractor) when submitting a request to vary from a NIST SP 800-171 security requirement to the Contracting Officer, in accordance with paragraph (b)(2)(ii)(B) of this clause; and

(ii) Provide the incident report number, automatically assigned by DOD, to the prime Contractor (or next higher-tier subcontractor) as soon as practicable, when reporting a cyber incident to DOD as required in paragraph (c) of this clause.

8.0 CONTRACT TRANSITION AND KNOWLEDGE TRANSFER

The purpose of this section is to address the minimum requirements for transition of the contract from the incumbent (exiting) contractor to the suceeding contractor.

8.1 Successor Contractor Transition Phase-In

To minimize any decreases in productivity and to prevent possible negative impacts on additional services, the contractor shall have personnel employed in each Functional Area (FA) during the not to exceed 30 calendar day transition phase-in period. During the phase-in period, the contractor shall become familiar with performance requirements in order to commence full performance of services immediately following the end of the transition period. Upon completion of phase-in, the Government will physically transfer all Government-provided equipment, materials, property and COTS products to the incoming contractor for which at this point forward, the contractor shall account for and maintain. The contractor shall jointly work with and assume responsibility from the incumbent work-force to ensure continuity of operations. The new contractor shall ensure personnel are available to accomplish all PWS tasks without the aid of the incumbent contractor work-force on 01 October 2019.

8.2 Incumbent Contractor Transition Phase-Out (OPTIONAL)

The incumbent Contractor recognizes that the services under this contract are vital to the Government and shall be continued without interruption until the last day of performance of the contract. The Contractor shall provide for knowledge transfer to facilitate successful transition of duties and responsibilities from the incumbent Contractor to the successor Contractor as well as to Government designated third parties as facilitated by the Government.

The incumbent contractor shall develop a Phase-Out Transition Plan for transition to a successor contractor, and deliver the plan to the COR within (30) calendar days of execution of this optional task.

If exercised, the Government will inform the contractor to provide a price proposal at least 90 days prior to the contractor's last date of performance on this contract. The Government and the incumbent Contractor will negotiate the price for this work. The Government will provide the incumbent Contractor a modification to the contract funding the negotiated work before performance begins.

Deliverable: Phase-Out Transition Plan within (30) calendar days of execution of this optional task

8.2.1 Phase-Out Transition Plan::
The incumbent contractor shall provide the Government with a **Phase-Out Transition Plan** detailing how all tasks will be transferred to the successor. The incumbent contractor retains responsibility for work performed in accordance with the PWS until the end of the transition period.

Phase-Out Transition Plan will include but not be limited to:

1. A formal turnover plan of all CE/GovCloud Infrastructure documents, hardware, software and GFE.

2. The plan shall
    a. Detail the prescribed processes for hand-off of hardware, software, and Government Furnished equipment (GFE)
    b. Identify specific models, versions, configurations, current manuals and instructions for each task item
    c. Timing of the turnover to minimally impact CE/GovCloud operations
    d. Ensure the succeeding contractor is involved in processing all help desk requests, service requests, and change requests, and sustaining and maintaining the CE/GovCloud during the transition period
3. Hand-off procedures.
4. Contingency strategy for CE/GovCloud Infrastructure recovery should any part of it fail during turnover.
5. List of outstanding issues, problems, and change requests pertaining to the issues and current state of the CE/GovCloud operating environments.
6. List of closeout activities for the transition period.
7. List of current projects and their statuses.

8.2.2 Transition Execution

The Government will at its discretion determine the date to initiate the approved Phase-Out Transition Plan. This section addresses the minimum requirements for turnover or transition of CE/GovCloud Infrastructure support and process knowledge, documentation, and equipment from the incumbent Contractor to the successor Contractor. The transition period will be 30 days. This transition should occur with as little disruption to operations as possible and may be shortened at Government discretion.

8.2.2.2 Knowledge Transfer

Contractor shall provide the CE/GovCloud Infrastructure support Machine images to the successor Contractor's program and technical staff clearly define the CE/GovCloud Infrastructure's current state. This transfer shall occur with as little disruption to CE/GovCloud hosted system operation at turnover as possible. The contractor shall support and allow the succeeding contractor to have hands-on Machine images with all CE/GovCloud infrastructure hardware and software at a minimum of seven (7) calendar days after the initiation of the transition period.

8.2.2.3 Exit Requirements

Upon direction by the COR, the contractor shall organize all documents and files from this contract effort in which the government has rights, store them on the shared drives or portable media as designated by the COR, and provide a file plan outlining the file structure. All work related documents and files along with the file plan shall be delivered to the COR. Status for each technology utilized in the CE/GovCloud shall be documented, to include recent, current, and pending actions and shall be delivered to the COR at least 5 business days prior to the effective closeout date of the contract. In addition, the contractor shall provide a complete list of network server and appliance, database, backup and storage server and appliance user-ids /password used in conjunction with sustaining CE/GovCloud Infrastructure. The contractor shall provide a list of all badges, vehicle passes, and Government software access permissions of all individuals currently on the task. This list shall be provided at least 5 business days prior to the effective closeout date of the contract. All badges and vehicle passes shall be delivered to the COR on the effective closeout date of the contract. The contractor shall transfer to the Government all intellectual and real property belonging to the Government, which was generated, purchased on behalf of, or provided by the Government for the performance of the work within this contract. Some examples would be code or scripts used to perform automated system backups, the monitoring of system processes, web development, code to check for security concerns, etc. The contractor acknowledges that anything developed at the expense of the Government during the period of performance is the property of the Government. Electronic copies of the scripts shall be submitted to the Government for baseline control. The contractor shall ensure that no logistics or contract data is corrupted, changed, or altered in a manner that would adversely impact the Government.

APPENDICES:

A	ACRONYMS
B	APPLICABLE DOCUMENTS
C	CE/GOVCLOUD HOSTEDAPPLICATIONS
D	SAMPLE TASK LIST
E	HISTORICAL WORKLOAD
F	NON-DISCLOSURE AGREEMENT
G	WORKFORCE CERTIFICATION REQUIREMENTS

Appendix A

ACRONYMS

Acronym	Definition
G2	Security Division
G6	Information Management Division
ACOR	Alternate Contract Officer Representative
AIS	Automated Information System
AMC	Air Mobility Command
API	Automated Program Interface
ATC	Authorization to Connect
ATCTS	Army Training & Certification Tracking System
ATO	Authorization to Operate
AT	Antiterrorism
CAC	Common Access Card
CCB	Configuration Control Board
CE	Centralized Enclave
CCT	Change Control Tool
CD	Compact Disc
CDE	Common Development Environment
CDP	Customs Document Portal
CFE	Contractor Furnished Equipment
CI	Counter Intelligence
CIET	Carrier In-transit Visibility (ITV) Entry Tool
CIL	Critical Information List
CIO	Chief Information Officer
CJCS	Chairman of the Joint Chiefs of Staff
CM	Configuration Management
CMP	Configuration Management Plan
CMR	Contractor Management Report
COI	Community of Interest
COOP	Continuity of Operations Plan
COR	Contracting Officer Representative
COTR	Contracting Officer Technical Representative
COTS	Commercial off the shelf
DISCO	Defense Industrial Security Clearance Office
CWE/SANS	Common Weakness Enumeration/System Admin, Audit, Network, Security Institute
DM	Data Maintenance
DMDB	Detention Management Database
DIACAP	DOD Information Assurance Certification and Accreditation Process
DISA	Defense Information Systems Agency
DOD	Department of Defense
DODAF	DOD Architecture Framework
DODI	Department of Defense Instruction
DRE	Disaster Recovery Exercise
DSS	Defense Security Service
DTEB	Defense Transportation Electronic Board
DTS	Defense Transportation Systems
DVD	Digital Video Disc
DWCA	Defense Workforce Certification Application
EA	Enterprise Architecture
EDI	Electronic Data Interchange

EET	Enterprise EDI Team
EIP	Enterprise Infrastructure Program
E-GOV	Electronic Government
eMASS	Enterprise Mission Assurance Support Service
EO	Executive Order
ESB	Electronic service bus
ETA	Electronic Transportation Acquisition
ETAV	Electronic Tool Asset Visibility Tool
ETL	Extract-transform-load
FCL	Facility Clearance Level
FOIA	Freedom of Information Act
FOUO	For Official Use Only
FPCON	Force Protection Condition
FPR	Fortify Report
FSC	Federal Service Code
FSO	Facility Security Officer
FTE	Full Time Employee
GFE	Government Furnished Equipment
GFI	Government Furnished Information
GIG	Global Information Grid
GIS	Geographic Information System (GIS)
HBSS	Host Based Security System
IA	Information Assurance
IASO	Information Assurance Security Officer
IAVA	Information Assurance Vulnerability Assessments
IAVM	Information Assurance (IA) Vulnerability Management
IAW	In Accordance With
IAWIP	Information Assurance Workforce Improvement Program
IA&ISP	Information Assurance and Industrial Security Plan
IMA	Information Management Area
IPv6	Internet Protocol version 6
ISDDC	Integrated Mission Support for Surface Deployment & Distribution Command
IT	Information Technology
ITV	In-transit Visibility
JIE-T	Joint Information Environment - Transportation
JPAS	Joint Personnel Adjudication System
LEW	Levy Exemption Waiver
LDAP	Lightweight Directory Access Protocol
LOB	Lift on Board Portal
MAC	Mission Assurance Category
MSC	Military Sealift Command
MSR	Monthly Status Report
NACLC	National Agency Check with Local Credit
OCCA	Ocean Cargo Clearing Authority
ODC	Other Direct Costs
OPM	Office of Personnel Management
OPSEC	Operations Security
OSD	Office of the Secretary of Defense
OSD (AT&L)	Office of the Secretary of Defense for Acquisition Training & Logistics
OWASP	Open Web Application Security Project
PAT	Pipeline Asset Tool

PM	Program Manager
PMI	Project Management Institute
PMO	Program Management Office
PMR	Program Management Review
POC	Point of Contact
PPSM	Ports, Protocols, and Services Management
PWS	Performance Work Statement
RMDB	Reconciliation Management Database
SAFB	Scott Air Force Base
SCCM	System Center Configuration Manager
SDDC	Military Surface Deployment and Distribution Command
SDK	Software Developer Kit
SDS	Service Delivery Summary
SFTP	Secure File Transfer Protocol
SME	Subject Matter Expert
SMO	Security Management Office
SOA	Service Oriented Architecture
SOP	Standard Operating Procedure
SSC	Security Service Center
SSRB	Source System Review Board
ST&E	Security Test and Evaluation
STIG	Security Technical Implementation Guide
STP	Security Test Plan
TA	Trusted Agent
TA	Technical Advisories
TARP	Threat Awareness and Reporting Program
TCC	Transportation Component Command
TCJ6	Command, Control, Communications and Computer Systems Directorate
TPA	Trading Partner Agreement
UIC	Unit Identification Code
US	United States
US-CERT	United States Computer Emergency Readiness Team
USTRANSCOM	United States Transportation Command
VPC	Virtual Private Cloud
VPN	Virtual Private Network
WBS	Work Breakdown Structure
WSUS	Windows Server Update Services
WSDL	Web Service Description Language
XML	Extensible Markup Language
XSD	XML Schema Definitions

Appendix B

APPLICABLE DOCUMENTS

Federal and DOD Regulations

Clinger-Cohen Act (CCA) of 1996

DOD Directive 1100.22, Policy and Procedures for Determining Workforce Mix

DOD Directive 8000.1, Management of DOD Information Resources and Information Technology

DOD Instruction 5158.06, Distribution Process Owner

DOD Instruction 8115.01, Information Technology Portfolio Management

DOD Instruction 8115.02, Information Technology Portfolio Management Implementation

E-Government Act of 2002 (Public Law 107-347)

Federal Acquisition Reform Act (Division D of Public Law 104-106)

Federal Information Security Management Act (FISMA) of 2002

Information Technology Management Reform Act (Division E of Public Law 104-106)

Paperwork Reduction Act (Public Law 104-13, Chapter 35 of title 44, United States Code)

DOD Directive (DODD) 8500.1, Information Assurance (IA)

DOD Instruction 8500.2, Information Assurance (IA) Implementation

DODD 8570.01, Information Assurance Training, Certification, and Workforce Management

DOD 8570.01-M, Information Assurance Workforce Improvement Program

CJCS Manual 6510.01A, Information Assurance (IA) and Computer Network Defense (CND) Volume I (Incident Handling Program)

DODI 8520.2, Public Key Infrastructure (PKI) and Public Key (PK) Enabling

DODI 8551.1, Ports, Protocols, and Services Management (PPSM)
DODI 8510.01 DOD Information Assurance Certification and Accreditation Process (RMFRMF/RMF)

Any modification to above mentioned Policy or Guidance

Army Best Business Practices

USTRANSCOM Instructions

USTRANSCOM Instruction 33-16, Management of United States Transportation Command (USTRANSCOM) Computer Assets

USTRANSCOM FAR Supplement 5552.204-9000, Notification of Government Security Activity and Visitor Group Security Agreements

Appendix C

SDDC GovCloud Currently Hosted Application as of 1 October 2019

Applications supported by CE

- Applications hosted:
  - *Integrated Mission Support for Surface Deployment & Distribution Command (ISDDC)
    -- Common Electronic Data Interchange(CEDI)

    -- Axway EDI translator
    -- Pipeline Asset Tool (PAT)
  -
  - *Integrated Booking Systems (IBS)
    -- IBS Container Management Module (CMM)
    -- IBS Carrier Analysis and Rate Evaluation(CARE II)
    -- IBS Commercial Sealift Solutions (IBSCSS)
    -- IBS Electronic Shipper System (IBSESS)
    -- IBS Ocean Carrier Interface (IBSOCI)
    -- IBS One-Time-Only (IBSOTO)
    -- IBS Requirements Forecasting & Rate Analysis Module (RFRAM)
    -- IBS Web Vessel Schedule (IBSWEBVS)
  - * Global Freight Management (GFM)
    -- Training Simulator (GFMSIM)
    -- Customer Added Value Suite (CAVS)
    -- Discrepancy Identification Shipment (DIS)
    -- Freight Acquisition Shipping Tool (FAST)
    -- Freight Carrier Registration Program (FCRP)
    -- In-Transit Visibility (ITV)
    -- Rate Quotation
    -- Shipper's Export Declaration (SED)
    -- Small Package Express (SPE)
    -- Spot Bid
  - *
  - * Transportation Financial Management System-SDDC (TFMS-M)
  - * Defense Table of Official Distances (DTOD)
  - * Electronic Transportation Acquisition (ETA)
  - * Integrated Computerized Deployment System (ICODES)
    -- *Single Load Planner (SLP)*
    -- *Terminal Management Module (TMM)*
    -- *Conveyance Builder (CB)*
    -- *Conveyance Estimator (CE)*
    -- *Collaborative Information Workspace (CIW)*
    -- *Data Cleanser (DC)*
    -- *Information Repository (IR)*
    -- *Breakbulk Tool*
    -- *Conveyance Repository (CR)*
    -- *Data Manager*
    -- *Hand Held Terminal (HHT) Administrator*
    -- *Transportability Analysis Reports Generator (TARGET)*

  - * Legacy Transportation Operational Personal Property Standard System (TOPS)
  - * Web-Enabled TOPS (ETOPS)
  - * SafteyNet
  - * Installation Out loading Capability Collection (IOCC)
  - Bidding Interface Delivery Solicitation (BIDS) and other web services
  - * Joint Equipment Characteristics Database system (JECD)

  - ArcGIS/TGIS
  - * AMCADRE (CATS)
  - Air Carrier Analysis Support System
  - Serena Business Mashups
  - Serena Dimensions
  - Service Oriented Architecture (SOA)
  - Splunk – IA logging
  - File Transfer Management (FTM)
  - Fortify

- Applications utilizing CE Storage and Backup capability:
  - All applications hosted in CE environments

- CE is currently backing up over 85 Terabytes (TB) weekly
- Over 90TB space is allocated

CE Hardware Overview

- Database layer servers:
  - Enterprise M5000
  - Enterprise M9000 (2)
- Application and Web layer servers
  - Enterprise M4000
  - Dell R805, R905 and R815
  - SPARC T4
- SAN Storage
  - Netapp 6080, 3240, 2020 and 3120
  - SUN 7320
- Backup
  - DXI 8500
  - DXI 7500
  - DXI 6702

- Network
  - Cisco 4507 Catalyst
  - F5 load balancers 6900s and 8900s
  - Cisco 2960, 3750
  - Cisco Nexxus 5010

Fiber Network

- Brocade 48000
- Brocade 4900

Technologies Utilized by CE

- Solaris 10/11 with virtualization (Global and Non-Global Zones)
- Windows 2008 Advanced Server with virtualization (VMWare)
- VERITAS Clustering
- F5 load balancing
- NETAPP Storage with redundancy
- Commvault enterprise backup
- Sun Java web/app servers
- Oracle Database and Oracle app servers
- Cognos Application Server
- Informatica Power Center
- VM ware
- VEAM backup and replication

- MSSQL database
- MSIIS web services
- Microsoft clustering Silver Peak WAN accelerators
- EM7 system monitoring and ticketing
- Solar winds

**Targeted Systems to Plan Migration into CE

- Installation Out-loading Capability Collection (IOCC)
- ArcGIS/TGIS

.

Appendix D

Sample Task List
(This is a sample of tasks and subtasks historically used to maintain the CE; however, this does not represent an all-inclusive list of tasks for this PWS effort.)

Backups -

Commvault backup and recovery software:

Rotate tapes weekly
Check job status on backup reports daily
Configure disk libraries on appropriate media agents
Configure Virtual Tape Libraries
Create backup jobs
Create backup storage policies
Install backup client agents
Manage retention on backup storage policies
Monitor status of disk library ingest
Create disk library replication jobs
Monitor disk library replication
Create backup job schedule policies
Manage VTL scratch pools for spares
Install and configure media agents
Create/Edit backup job reports
Manage agent licensing
Apply CommVault patches weekly
Apply Commvault Service packs as needed
Manage media locations
Run data aging jobs
Configure run schedules on backup jobs
Troubleshoot backup failures
Create user accounts
Create client groups
Assign client servers to groups
Recover files, folders as needed
SOP creation/maintenance
configuration of backup policies post install
perform and test restores of files on VMs/Physicals

Windows Servers Server Maintenance

Requesting and renewing certs
hardware maintenance (NICs, memory)

hardware moves
troubleshooting agent issues
perform scheduled maintenance during ASIs
Major Minor Mod Checklist
degauss HDs
NIC configuration
burn/export 2008R2 international standards organization (ISO)
validate information for IA team
mitigate vulnerabilities
Apply monthly MS security patches
Install application software (i.e. Java)
Configure IP parameters
Configure DNS settings
Configure advanced NIC settings (i.e. jumbo frames)
Cable server
Install antivirus software
Install HBSS software agents
Install Splunk agents
Manage local security policy settings
Manage local accounts by creating, deleting, disabling accounts as needed)
Manage Windows event logs
Assign permission to file system folders
Apply STIG settings in local security policy
Apply IAVA directed system configurations
Maintain windows hosts file
Configure accounts and network access per DIS STIG's
Configure password policies on server per DISA STIG
Configure network protocols on server
Configure SNMP service to allow monitoring by EM7
Configure SNMP traps to send to EM7
Configure services to use proper account
Configure Microsoft Windows Update Services Server (WSUS) to pull down patches
Configure Servers to point to the WSUS server for monthly patching
Approve monthly Microsoft patches
Place servers into WSUS groups
Troubleshoot network/connectivity errors
Monitor system performance
Dump traffic using wire shark as needed
PowerShell scripting
Visual Basic scripting
Configure clusters

Add resources to clusters
Document SOPs
Migration of user data

EM7 Performance Monitoring and Reporting
Configure ticketing settings
Configure notification settings
Configure alerts
Configure system backup
Create custom events
Configure web content monitors
Configure DB monitors
Configure Organizations
Configure SNMP credentials
Add/Remove User accounts
Assign user rights
Discover devices to monitor
Create custom applications/MIBS
Track server performance
Configure and run reports
Patch device as needed
Monitor live Events
Respond to alerts
Resolve tickets
Place servers in maintenance mode as needed
Update Knowledge store documentation
Define device thresholds
Service Request assignments
First response to SRs. SR elevation if required
Server creation and maintenance
User account creation and maintenance
Configure notifications
Run at least monthly reports
add servers to EM7 for monitoring/notification

Hardware Management & Inventory
Plan for future hardware needs
Research specifications of hardware currently in use
Research specifications of future hardware
Create CIPS requests for any hardware removed or installed into datacenter
Maintain rack inventory & elevations
Label servers and cables

Maintain a CAT 6, Twinax and fiber cut sheet
Packing and shipping of hardware
Server maintenance (hard drives, cards, memory, PSU)
Schedule equipment pickups with organization logistic teams
Schedule equipment drop-offs with organization logistic teams
Coordinate equipment intake window with datacenter management
Record equipment make/model/serial information
Create Server names with standard enterprise Machine imaging conventions
Unbox equipment, check packing list for items included.
Prepare devices for rack mounting
Placing classification stickers on hardware
Storage of misc. spare equipment
Coordinate with vendors for faulty part replacements
Running cable under 1575 floors
Coordinate with IMA maintenance lead
Obtain market research for maintenance

Database management
Install Oracle database software
Install Oracle Fusion middleware software
Install Oracle 12c Cloud Control software
Install Oracle Application Express software
Configure Oracle database software
Configure Oracle Fusion middleware software
Configure Oracle 12c Cloud Control software
Configure Oracle Application Express software
Monitor and maintain Oracle products
Create Oracle databases
Upgrade databases
Install security patches
Start databases as needed
Shutdown databases as needed
Start Oracle application servers
Stop Oracle application servers
Manage and maintain storage structures for 30+ databases
Create users
Assign system privileges to users
Assign object privileges to users
Create roles
Assign system privileges to roles

Assign object privileges to roles
Assign roles to users
Assign Oracle passwords as needed
Change Oracle passwords as needed
Create profiles
Manage and maintain profiles
Create views
Manage and maintain views
Create triggers
Manage and maintain triggers
Create indexes
Manage and maintain indexes
Create constraints
Manage and maintain constraints
Create functions, procedures, and packages as needed
Manage and maintain functions, procedures, and packages as needed
Create sequences as needed
Manage and maintain sequences as needed
Create tables and views
Manage and maintain tables and views
Create Oracle database jobs
Schedule Oracle database jobs
Create and maintain other database objects as needed
Design and plan database backup strategy
Configure database backups according to strategy
Schedule database backups
Proactively monitor the condition of the database
Take preventive or corrective actions, as required
Monitor database performance
Tune database performance as required
Stop APEX listeners as needed
Start APEX listeners as needed
Configure APEX listeners
Maintain APEX listeners
Compile Oracle Forms and Reports as needed
Deploy applications to the Oracle Application Server
Create database listeners
Configure database listeners
Start database listeners
Stop database listeners

Monitor database logs for anomalies
Monitor listener logs for anomalies
Monitor application server logs
Determine database space requirements
Work with SAs to allocate storage for databases
Monitor database growth
Assign ports for new database listeners
Identify Oracle Wallet requirements
Request Oracle Wallets as needed
Apply Oracle Wallets
Patch all Oracle products as required
Monitor database backups through COMMVAULT
Configure database backups in COMMVAULT to support backup strategy
Maintain database backups
Work with customers on all database related issues
Participate in strategy meetings with customers as required
Identify database related network issues
Work with network administrators to resolve database related network issues
Identify database related operating system (OS) issues
Work with system administrators to resolve database related OS issues
Identify Security Technical Implementation Guide (STIG) database requirements
Test over 60 databases for STIG compliance
Resolve any STIG findings
Develop scripts to support STIG testing
Develop scripts to support recurring database monitoring tasks
Maintain database related OS users
Change database related OS user passwords according to policy
Migrate Oracle databases into the CE database environments, i.e. Training, Staging, Prod & COOP
Work with EIP technical staff to identify Oracle database COOP requirements
Develop and implement Oracle database Disaster Recovery Plan

CIW Power Chute Install

Install the network interface card for the APC UPS unit
Configure the interface card with necessary information
Ensure the network interface is up and ready for communication
Install the Power Chute software on the windows servers
Ensure the client GUI comes up on the server to talk with the UPS
Make all the configuration changes necessary to establish communications with the UPS
Ensure the UPS is recognized and talking with the windows server
Install the Power Chute software on the Solaris server

Ensure the client GUI comes up on the server to talk with the UPS
Make all the configuration changes necessary to establish communications with the UPS
Ensure the UPS is recognized and talking with the Solaris server
Install the VMA software on the windows virtual server
Ensure the client GUI comes up on the server to talk with the UPS
Make all the configuration changes necessary to establish communications with the UPS
Ensure the UPS is recognized and talking with the master windows server
Install the VMA control software on the server
Configure the software to gracefully take down all VM's when needed
Configure the software to bring all the VMs back up when needed
Configure all the graceful shutdown down timings
Configure an UPS response to each type power emergency listed
Ensure each server has the time configured that it needs to shutdown
Ensure none of the shutdown timings conflict with other shutdowns
Configure all the timings for bringing the systems back up
Test the completed installation.
Periodically go to vendors site to check for updated software versions
Update any documentation to compensate for any upgrades or updates to the software

F5 BIG IP Switch Management

Account creation/deletion
Virtual service creation/deletion
Load balancer pool creation
Protocol profile modification
Health monitor creation
Load balancer rule creation
Network address translation
Packet dumps
Performance monitoring
Certificate management
Manage F5 licensing
iRule TCL scripting
Perl scripting for custom monitors
Installing hotfixes and image releases
High availability configuration
Import SSL certificates
SSL offloading configuration
Create nodes to represent real IP addresses
Application Policies
XML Profiles

Anomaly detection
Application security reports
Troubleshoot connectivity issues
Create SNAT for internal hosts

Switch Maintenance

Awareness of IOS version vulnerabilities
IOS updates
Install/remove network hardware
Hardware maintenance (ports, memory)
Install SFP modules
Hardware moves
Perform scheduled maintenance during ASIs

Switch Management/administration

Port configuration
Port activation
Port assignment & tracking
Port descriptions
Vlan assignment & tracking
Ensure DISA STIG compliance
Maintain configuration standards
Administer access control lists
SNMPv3 configuration
AAA configuration settings
Access control lists
Redundant connectivity
Maintain emergency admin accounts
Major Minor Mod Checklist
Configure logging
Configure Radius groups
Troubleshoot network/connectivity errors
Configure emergency accounts
Enforce password policies per DISA STIG
Configure SNMP service for monitoring
Configure SNMP traps
Configure SNMP Access Control Lists (ACLs)
Configure NTP service
Configure NTP ACLs
Spanning tree configuration

Backups - VEEAM

Monitor backup proxy snapshots
Add/Remove VM's from jobs
Create backup proxy servers
Create backup targets on enterprise storage
Configure email for job reporting
Configure storage options on backup jobs
Configure backup type on backup jobs
Configure CBT (Change Block tracking) on backup jobs
Configure application-aware settings on backup jobs
Configure guest file system indexing settings on backup jobs
Configure run schedules on backup jobs
Troubleshoot backup failures

Quantum DXI

Configure access to web GUI
Periodically change administrator password
Join to domain
Configure IP settings
Configure NTP time source
Configure DNS settings
Configure fiber channel access to devices
Configure NAS shares as backup targets
Monitor available space
Configure space reclamation jobs
Monitor deduplication ratio's
Monitor free block pool space for deduplication
Configure appliance NIC's for use
Open service requests to replace faulty disks
Work with vendor support to complete unit performance evaluation

SQL Server

Install and configure MS SQL Server software
Configure server settings within SQL Server (i.e. AWE, Processor affinity)
Create databases
Manage storage for database servers
Create database backup jobs
Install and configure MS SQL Server backup agents
Perform restore of databases

Perform database maintenance tasks using DBCC libraries
Create and delete SQL server accounts
Monitor backup jobs for problems
Monitor database log file system sizes
Monitor database log backups
Monitor tempdb size
Monitor SQL Server management logs
Delete databases
Monitor database performance using SQL Monitor/SQL Profiler
Create SQL Server Witness & mirror servers
Configure SQL Server mirroring
Rebuild database indexes as needed
Configure linked servers
Shrink database physical files as required
Perform mirror failover and failback
SQL cluster creation and maintenance

Web Server
Install IIS web server role
Configure IIS settings
Add a Virtual Directory
Add an Application
Add IIS website
Configuring Authentication in IIS 7.0
Create IIS application pools
Configuring Recycling Settings for an Application Pool
Configuring Connection Strings in IIS 7
Configuring Machine Keys in IIS 7
Configuring Connection Strings in IIS 7
Configuring Machine Keys in IIS 7
Update web content
Tune application pools
Request web certificates
Register web certificates with PKI authority
Install web certificates
Package websites using Web Deployment Tool V2
Website deployment using Web Deployment Tool V2
ColdFusion administration
CGI administration
Configure handler mappings

Inetpub permissions
ODBC configurations
Start or Stop an Application Pool
Data source Name (DSN) creation

F5

Account creation/deletion
Virtual service creation/deletion
Load balancer pool creation
Protocol profile modification
Health monitor creation
Load balancer rule creation
Network address translation
Packet dumps
Performance monitoring
Certificate management
Manage F5 licensing
iRule TCL scripting
Perl scripting for custom monitors
Installing hotfixes and image releases

IP assignments & auditing

update/verify IPs
exchange Ip's
EM7
IP spreadsheets
Solar Winds updates
audit accomplished and information provided upon request
validate virtual/physical information in F5

Network

Maintain physical and logical topology architecture diagrams
Maintain equipment rack elevation diagrams
Assign and track CE IP Addresses
Track switch & patch panel port density, usage and availability
Ensure Cisco Switches to comply with DISA STIG
Provide day to day enclave network support
Provide future planning for network infrastructure
Configure and maintain Solar Winds for enterprise management
Work with vendors for evaluation of products for future needs

Coordinate ASI's for upgrades and maintenance
F5 management/administration
Switch management/administration
Manage switch administrator access (RADIUS)
VPN user authentication management/administration
NTP management
SNMP configuration & management
Install and management equipment network cabling
Vlan assignment & management
Maintain Network Time Machine (NTM) for packet capture analysis
Network troubleshooting and fault isolation and resolution
Respond to daily CE trouble tickets
Provide best business practices security to enclave
Develop and implement technical solution for JIE-T migration
Input and track vulnerabilities of all network assets in VMS
Coordinate internal & external agencies for troubleshooting
Retina scanning
Firewall management/administration
Proxy server management/administration
VPN management/administration
Provide Firewall maintenance and Access Control Lists maintenance
Manage Coop Network Environment
Remote Access solution and support
NAC integration
COOP connectivity re-engineering
Engineering and implement Out of Band Management (OOBM) network

Solaris
research, plan, design, implement and maintain the Oracle OS software
performance monitoring and testing
maintain all centralized file systems located on storage
Virtualize all Solaris zones
install, configure, maintain ssh, ssl, sudo, pam, auto mounts, NTP, mail, snmp, syslog, and auditing
monitor all used SMF services for enabled status and clear or mitigate any deviations
troubleshoot all communication issues with server to end device
identify and document firewall requests
engineer, install, and configure jumpstart
Jumpstart all new servers based on a highly hardened standardized image
Build all zones by cloning a highly hardened standardized zone
perform all performance tuning involved to maximize performance with databases

interface management
identify and document all NAT and load balanced requests
identify and mitigate and CPU spikes
identify and mitigate any disk sizing issues
install, configure and maintain ZFS file systems.
perform ZFS snapshots
manage ZFS pools
test and implement all OS and application patches and updates.
Replace faulty equipment (drives, power supplies)
Update drivers to hardware and interfaces
retain audit logs per STIG guidance
Maintain all local user accounts and permissions
build and maintain all LDAP accounts and permissions
build and maintain all RSA users accounts and permissions
Build and deploy servers
Develop solutions to meet customer needs
Add and modify ldap users, devices,
Install, configure, maintain RSA software
Install, configure, maintain Nagios (adding hosts, services, users as needed)
Monitor all hosts for connectivity - correct as needed
Monitor defined services on all hosts for functionality - correct as needed
install, upgrade, configure and maintain Digi console devices
set up Lights out management
configure XSCF users and settings
upgrade XSCF

Veritas

plan, engineer, implement, upgrade and maintain Multipathing, Volume manager, and cluster services
design and build service groups for failover
integrate client, storage and failover operation into cluster services
constantly monitor all cluster services processes
research and mitigate any service failure
integrate application operations to cluster services
resize volume manage disks and volumes
mount both file and block storage
maintain heartbeat networks
implement and maintain I/o fencing
install, configure and maintain vxfs file systems

EFT - Windows

Create project accounts
Create groups
Create feed users
Maintain, upgrade the EFT software
Create and update power shell scripts
Help users connect
Monitor file transfers
Troubleshoot connection errors
Use EFT to pull files from the Unix server
Create Event rules to help in moving, appending the filename, uploading and downloading the files
Create bursting rules
Working to Jail the entire EFT feeds that have more than one feed
Maintain EFT groups to sort through data
Run reports to find, troubleshoot, fix issues
Maintain the Virtual file system on the server
Maintain the IP ban list
Test new release of the software, and work with the customers during upgrades
Work all customer issues as they arise.
Maintain the database of all the connections and errors for EFT

FTM - Unix
Create project accounts
Create feed users
Maintain the jail application
Monitor disk space
Maintain Scripts to move files, permissions, accounts, find large files, put files etc...
Patch the system
Upgrade packages on the UNIX OS such as OpenSSH, java etc....

ICODES warfile deployments
Have the customer fill out a service request for deploying the file
Have the customer email the file
Save the file the customer sends to a location
Login to the Glassfish Web GUI for the server environment pertaining to the file being deployed (stage/prod)
Bring up the warfile deployment window
Put in the parameters to meet the file, along with the saved location of the file
Have the software upload and deploy the file

Call the customer and verify a successful deployment
Perform all the same steps in the recovery site environment

NTM
Packet capture
Packet analysis
Traffic dumps

Retina Scanning
Develop target lists
Initiate scans
Interpret results
Upload to VMS

VPN
Maintain hardware
User permissions

OOBM Network
Engineer
Research solutions
Implementation
Maintain
Install client hardware

NAC
Product research
NAC integration

Monitoring/Troubleshoot
Switch port connectivity
Switch CPU loads
Trouble tickets

Diagrams/Documentation
Physical connectivity diagrams
Logical architecture diagrams
Equipment rack elevation diagrams
Switch port usage and availability
Patch panel port usage and availability

Patch panel labeling
Track vulnerabilities of all network assets in VMS

VMWare

Deploy VM's from template for new server requests
Updating of template to keep up with current patches and STIG configurations
Apply patches to ESXi hosts
Configure vSwitch settings
Configure data stores
Grant/Revoke access to accounts/groups for VCenter
Adjust resource allocations to VM's
Add/Remove disk space to VM's
Add/Remove NIC to VM's
Manage licenses in VCenter
Create Vlans on vSwitches
Configure physical NIC to vSwitches
Configure failover settings for redundancy on vSwitches
Configure HA settings
Configure and maintain DRS settings
Scan hosts for patching needs using Update Manager
Monitor system alarm events and take corrective action
Manage snapshots on virtual machines
Build ESXi hosts
Monitor system workload to insure DRS is operating properly
Monitor high resource use VM's using VEEAM monitor to correct resource allocations
Monitor snapshot usage/age using VEEAM Monitor
Keep VM template updated with latest STIG settings and patches
Create program resource pools
Configure each programs VMs to utilize their resource pool
Manage resources within a resource pool
Manage resources within an Application
Configure ESXi Clusters for each environment
Convert physical machines into VMs
Troubleshoot storage, network, HA, VM issues
Cloning of VMs

Active Directory

Install Domain Controller role on member servers
Install DNS role on Domain Controllers
Configure AD domain controller DNS settings

Add forward lookup zones
Add reverse lookup zones
Add hosts to DNS zones
Remove hosts from DNS zones
Configure AD domain controller DNS settings
Configure zone transfers
Configure secondary DNS zones
Configure DNS record scavenging
Configure root hints
Monitor replication between domain controllers
Create AD domain user accounts
Create AD domain user groups
Create and deploy Group Policy Objects (GPO)
Configure a domain NTP time source
Join Servers to domain
Create domain program groups (EIP, ETA and IBS etc.)
Place servers into domain program groups
Edit GPOs as STIG guidance changes
Scheduling tasks
Unlock accounts
Delete inactive accounts

RSA

Install RSA
RSA console configuration
Token imports
Account creation
User group creation
User group assignment
Agent creation in console
Agent installation on target server
Agent configuration on target server
Token assignment
Authentication troubleshooting
Report creation
manipulating user groups
run user account reports at least monthly and provide to IA
remove accounts as required
update SOP
updated authentication agents in the RSA console

train users on account authentication procedures
troubleshoot user authentication problems

Avocent DS View / KVM Systems
Mount KVM switch into Rack
Mount KVM monitor/keyboard unit into Rack
Rename KVM target host names
Configure IP settings
Configure and rename individual server port settings
Install cables from KVM to servers
Build Windows based server to house the web server
Install DS View web management software
Configure IP settings on web management software
Create user accounts for web software
Monitor hardware issues with KVM
Configure devices for two-form authentication with RSA

Server Deployment
deploy VMs
configure network adapters
join to domain
perform post installation steps
install required software
add to SUS & DNS
install application software
AV installs for IA
Splunk installations
audit AV updates to ensure servers within IA requirements

CAC Enable application servers
verify username
add data to cert2user file on server
restart service
verify application is up

Manage Orphaned Files on the FTM server
run PowerShell scripts to monitor for orphaned files
utilize EFT software to identify user account associated w/ orphaned file
move orphaned file manually using PowerShell
monitor outbound file transfers

Manage Service accounts - Windows

create and maintain AD accounts for Prod, Stage, COOP, Training
conduct SQL server installs using service accounts
provide password expiry notifications daily

Manage Service accounts - Solaris

creation
PW management
group management
permissions
check crontabs during acct maintenance
provide password expiry notifications daily

IP Migration task

Network IP Migration Effort
Notify Program Managers and server administrators regarding IP conflicts on server
Configuration and arrange ASI effort
Put in CCB request for ASI

Inventory

Monthly HW Inventory checks in Bldg. 1575
update Excel and Visio documents as equipment move/change occur

Security

Create an SRR directory on the new server
Install the SRR software
Run SRR script
Run Manual Review
Answer all questions
Run SR DB Update script
Run Review Findings Report
Create the findings report
Attach the report to a word document
Fix any findings from the report
Note any residual findings
Document the findings with justification for IA
Create POA&M for any documented findings
Periodically check for any SRR updates
Note any differences between the new and old versions

Periodically check for any STIG updates
Check for the differences in the new vs. the old versions
Note whether the differences effect our systems
Direct any questions regarding a STIG change to IASE
Request the RETINA scan be ran
Fix any findings from the report
Document any residual findings with justification for IA
Create POA&M for any documented findings
Request a rescan until all findings are fixed or have to be justified
Check for any IAVA's
Read the IAVA documentation to see what area of software is affected
Create a report of finding to develop a fix plan of action
Check on vendors sites for an appropriate patch/firmware upgrade
Direct any IAVA related questions to US CYBERCOM
Justify any findings on a VMS report from IA.
Report to IA what our plan of action will be on any new findings
Create an ASI request for both staging and production environments
Report to the CCB on any new findings with the fix action plan
Report to IA on the date we plan on implementing a fix to any findings
Test any fixes on our test servers
Implement the fix in the various environments
Verify the fix didn't break anything
Repair anything that was broken as a result of an implemented fix

Web

Install Web server software
Install Web instances
Configure instance parameters
Create pass-through
Install IP address
Deploy Web instances
Start/stop the instances
Create web instance database
Set up the database password
Request Web certificates
Send over the cert request to our Level 1 personnel
Install Web certificates
Check for Software upgrades
Vet any software upgrades through the CCB process
Inform IA of any plans for upgrade

Complete the software change form (for any software version changes)
Check for IAVA's
Read the IAVA documentation to see how the web software is affected
Create a report of finding to develop a fix plan of action
Check on vendors sites for an appropriate patch/firmware upgrade
Direct any IAVA related questions to US CYBERCOM
Justify any findings on a VMS report from IA.
Report to IA what our plan of action will be on any new findings
Report to the CCB on any new findings with the fix action plan
Report to IA on the date we plan on implementing a fix to any findings
Test any fixes on our database servers
Implement the fix in the various environments
Verify the fix didn't break anything
Repair anything that was broken as a result of an implemented fix

Firewall Management
Administer access control lists
Create/delete rules
Ensure proper routing

Solar Winds
Configure alerting
Configuration backup
Configuration updates
Performance monitoring
Customized reports
Schedule status polling
Schedule configuration backups

Cabling @ 1575

Cut to length
Labeling
Fabrication
Termination
Testing
Installation
Patch panel management
Maintain Cut sheets
Management

Storage management

install storage OS
update storage OS to meet security and feature needs
configure storage OS
install new storage system components
install new drive arrays
replace failed drives
configure aggregates
configure volumes
configure LUNS
configure NFS shares
configures CIFS shares
provision LUNS
configure iSCSI
monitor storage performance
plan storage growth
grow volumes as needed
grow LUNS as needed
offline unused LUNS
offline unused volumes
destroy unused LUNS
destroy unused volumes
troubleshoot performance issues
troubleshoot access issues
mask LUNS to hosts
create vfilers
add resources to vfilers
document storage configuration
document storage connectivity

install storage management software

configure storage management software

patch storage management software

configure replication

start replication processes

monitor replication processes

stop replication for validation

configure storage event management

ensure all configurations are supportable

Engineer storage solutions and implement (currently every task is performed in a similar capacity with Netapp and Oracle ZFS storage)

Maintain and upgrade storage collector software

Maintain a clustered, HA environment

Engineer, design, and implement Vfilers

STIG all storage devices and maintain the vendor security best practices to ensure a secure device

Install and properly cable all Collectors and shelves

implement and/or run all snap mirror, volcopy, ndmpcopy, snapshot capability

Evaluate, plan, and engineer all new software and hardware for each vendor and implement with minimal downtime

create and maintain correct access levels for storage user accounts

create and parse out aggregates

evaluate aggregation location for, build, add/delete, grow/reduce volumes

Build and increase sized for Luns

build and map groups to block storage

manage qtrees

manage NFS exports

manage CIFS exports

Disk management and replacement

implement and maintain LACP on interfaces to double bandwidth

Clone or snap mirror volumes to be used in various environments

manage fractional reserve

update collector firmware and OS

update shelf firmware

update disk firmware

install, configure, and maintain all vendor managing and monitoring software for the storage devices

install, configure, and optimize the vendor client software to ensure connectivity

install and configure Multipathing on the storage and client device

support snmp push and pull operations for storage monitoring and log collection

install, maintain, troubleshoot Fibre channel and ISCI connections

Task management

Weekly activity report

weekly meeting with COR
weekly team priority meeting
identify all purchasing requirements
up channel priority environment improvements
down channel COR priorities
De-conflict priorities between teams and staff
ensure COR timelines are meet
ensure action reports are filed
attend all required meetings (migration, engineering, priority determination)
create CE documentation as required
provide oversight and reporting of all other tasks
provide input for IPRs
Provide government advice on obtaining market research for all purchases
continually help maintain maximum staff productivity
help identify and implement cost saving for the government
create reports as needed
create documents as needed
provide project management leadership
recommend staff augmentation / changes to meet customer needs
coordinate new employee in-processing
plan hardware refreshes
plan software updates
coordinate license management issues

Server Decommissioning

De-Configure client in Commvault
Add an CE Calendar event 30 days in future to remove backups & VMWare disk
Set date to remove from vSphere in the notes section of the VM.
Login to VEEAM Ent Server, start VEEAM backup , click jobs, locate backup job, right click, properties, click on Virtual machines, highlight VM in question, click remove

Remove from WSUS [NOT SOLARIS]

Remove from EM7, both device and asset (if there is an asset)

Remove from \\eipcommvault\c$\SysinternalsSuite\servernames.txt (make sure not to leave any gaps in the script) [NOT SOLARIS]

Remove from \\eippwfs01\C$\SysinternalsSuite\servernames.txt (make sure not to leave any gaps in the script) [NOT SOLARIS]

Remove from DNS

- -Visionapp
- -Domain Controllers
- -EIPCOMMVAULT(Primary)

Remove from RSA Console

Remove from Solar winds

Remove from IPFirst.xls
Validate IP addresses to ensure they are not in use
-Search the F5 entries for any links (validate that a virtual does not have multiple physicals)
-Validate IP addresses with the requestor
Notify IMN (Cassandra Hollins) for IP tracking.
Remove from inventory in Visionapp.
(Submit CCB request for the following 2
Remove any load balancer configurations
Remove any firewall rules (SDDC-SAFB-FIREWALL)
[If virtual]
Remove from inventory in vSphere. After 30 days remove from disk

- -Power off the server
- -make note of Data Store (and annotate on EIP Calendar event)
- -Remove from Inventory

[If physical]
Remove label from physical machine at 1575
Rename dongle on Avocent switch to OLD-SERVERNAME—row-.rack
Execute the 'pull names from appliance' in DS view to retrieve the updated dongle name for the DS view interface dongle name for
Remove any switch configuration turn off ports

FC network -
Engineer, plan, and manage a Fibre channel (FC) network
Run all fiber optic cable needed from the storage device to the Fibre channel switch
Run all fiber optic cable from the client to the Fibre channel switch
install, configure and optimize all HBAs on the storage and client devices
perform all configuration, upgrades, aliases, and zoning on the Fibre channel switch
Ensure redundancy throughout the FC network
Troubleshoot any optical communication problems
install fiber switches
install fiber switch OS
configure fiber switch
create FC mappings
manage hosts within fiber switch
update fiber connectivity spreadsheet

Appendix E

HISTORICAL WORKLOAD*

Task Area 1: Contract Level and Project Management, 960 hours
Task Area 2: CE Sustainment, 31,020 hours
Task Area 3: CE Enhancements, 18,330 hours
Task Area 4: Configuration Management, 940 hours
Task Area 5: IA Support, 960 hours

*The Historical Workload is for the duration of one Fiscal Year and may not necessarily based on the current fiscal year.

APPENDIX F

Non-Disclosure agreement and agreement to disclose potential conflicts of interest for contract employees on the United States Transportation Command (USTRANSCOM) contracts.

Template NDA
Contractor Personnel

APPENDIX G: WORKFORCE CERTIFICATION REQUIREMENTS

Part I – Information Assurance Certification Requirements

(From DOD 8570.01-M, Table C3.T3 – IAT Level I Functions and Table C10.T3 - IASAE Level I Functions)

Contract Task	DOD 8570.01-M IA Function	IAT I	IAT II	IASAE I
Task 2, 3 & 4	T-I.4, T-I.7, T-I.13, T-I.14 T-II.2, T-II.3, T-II.8, T-II.9,T-II.17, T-II.23, T-11.26, T-II.29	X	X	
Task 5,6 - CM	T-I.7, T-I.13, T-II.9, T-II.24, T-II.29	X	X	