NETCENTS-2 SOLUTIONS
AIR FORCE INTRANET CONTROL SUPPORT

Executive Summary

Purpose

The intent of this acquisition is to acquire services supporting the 26th Network Operations Squadron (26 NOS) and its mission to operate, manage and defend the Air Force portion of the Department of Defense Information Network (DODIN).

Mission

The 26th Network Operations Squadron (26 NOS) operates the AFINC weapon system and the Department of Defense (DoD) Joint Regional Security Stacks (JRSS). The AFINC provides Air Force (AF) enterprise-level network management, optimized communications and defensive measures at the Air Force Information Network (AFIN) Gateway System (AFNGS) and SIPRNET Hydra Sentinel nodes. (Hydra Sentinel nodes are referred to as SIPRNET gateways). The AFINC operates and manages all Service Delivery Point (SDP) routers for Non-Secure Internet Protocol Router Network (NIPRNET) and Secret Internet Protocol Router Network (SIPRNET); operates and manages all AF routers and all AF circuits that have connectivity to the Air Force NIPRNET gateways and SIPRNET Hydra Sentinel nodes; and operates the AF portion of the JRSS. Additionally, the AFINC operates the Common User virtual private network (VPN) mesh tying the components of the AFs intranet together and protecting AF network traffic through encryption as it traverses public infrastructure.

The AFINC provides the AF with robust network communications by operating and maintaining the health and status of the Air Force NIPRNET gateways, SIPRNET Hydra Sentinel nodes, Integrated Management Suites (IMS), Joint IMS (JIMS), SDP routers, JRSS Agency\Base, and AF Wide Area Network and long-haul circuits, and provides a vital tactical cyberspace defense capability which, at a minimum, blocks known malicious traffic at the AF perimeter to ensure uninterrupted network integrity, reliability, availability, and confidentiality for the warfighter. The AFINC maintains the AF Enterprise Firewall, JRSS, Domain Name, electronic mail filtering and Web Proxy services at the outer most network boundary. The AFINC handles remote management of the AF NIPRNET gateways, JRSS, and SIPRNET Hydra Sentinel nodes, directing traffic across newly established Defense Information Systems Agency (DISA) circuits, and managing all of the connections at the AF external router. The AFINC also provides Incident Response capabilities in support of defense, network, mission application incidents, and contingency operations.

The 26 NOS delivers cyberspace situational awareness (SA) to AF leadership and all mission partners by providing 24/7/365 status of the AFIN, the Air Force portion of the DODIN and Defensive Cyber Operations (DCO) postures of the underlying infrastructure. The AFINC actively develops and maintains a proactively oriented deny-by-default posture, executes countermeasures in preparation for and response to a hostile cyber attack, analyzes AFIN performance, issues temporary network addresses and domains to Combat Communications Squadrons, and coordinates network maintenance. Specifically, the AFINC conducts network operations, management and defense of the AF NIPRNET gateways, SIPRNET Hydra Sentinel nodes, Integrated Management System (IMS), Joint IMS (JIMS), JRSS, firewalls, Service Delivery Point (SDP) routers, web proxy servers, E-mail relays, domain name servers, and their supporting network components.

NETCENTS-2 NetOps and Infrastructure F&O
AIR FORCE INTRANET CONTROL SUPPORT

1. Purpose

The intent of this acquisition is to acquire services supporting the 26th Network Operations Squadron (26 NOS) and its mission to operate, manage and defend the Air Force portion of the Department of Defense (DoD) Information Network (DODIN).

2. Scope

The mission of the 26 NOS is to provide mission assurance to the warfighter through the operation, management, and defense of DODIN. In the execution of its mission, the 26 NOS operates, manages, and defends the Non-classified Internet Protocol (IP) Router (NIPR) Network Gateways and the Secret Internet Protocol (IP) Router (SIPR) Network equivalents; all Service Delivery Point (SDP) routers on both NIPR and SIPR; the Integrated Management Suite (IMS) out-of-band (OOB) management networks; the Joint Regional Security Stacks (JRSS) Joint Management System (JMS) OOB management network; unit AFNet workstations, printers, and servers; training lab environment; the external Domain Name System (DNS) for the AF (both af.mil and af.smil.mil); NIPR and SIPR JRSS; and the underlying workstations, servers, storage networks, and network devices that are required to do so. Specifically, contractor support is required for Persistent Network Operations, Defensive Global Information Grid (GIG) Operations (DGO), AF Domain Management and Network Analysis and Troubleshooting.

3. Requirement/Description of Services

3.1 Singularly Managed Infrastructure with Enterprise Level Security (SMI-ELS) Infrastructure Implementation and Operation

3.1.1 Singularly Managed Infrastructure (SMI)

The contractor shall provide services and solutions utilizing industry best practices, innovative solutions, emerging technologies, and lessons learned to realize a SMI that brings together at the middleware layer disparate networks and communications capabilities into a consistent AF enterprise-wide Information Technology (IT) capability.   The SMI shall support all AF mission requirements, and share data through federation with other infrastructure environments across the DoD, Federal agencies and Joint and Coalition environments. The contractor shall provide the capabilities for Core Enterprise Services (CES), transport layers, metadata environments, cloud environments, enclaves, Communities of Interest (COIs) and federation that make an SMI possible.

3.1.1.1 Core Enterprise Services

The contractor shall provide services and solutions that provide infrastructure capabilities to execute and manage content delivery services that deliver information to the warfighter and operational end user. CES will include but not be limited to storage management, messaging, transaction management, workflow management, search and discovery, directory services and service execution through an application server capability for control and management of multiple services. CES will provide monitoring for Quality of Service (QoS) and governance of configuration and contract management to ensure a stable environment. The contractor shall ensure these solutions use the DoD CES when and wherever possible and deliver AF-specific CES as required to augment the DoD CES to fulfill the AF mission.

3.1.1.2 Enclaves

The contractor shall provide services and solutions to identify a logical partitioning of the network and its information assets into capabilities-based enclaves. In the SMI-ELS Concept Document, enclaves are defined as virtual or physical collections of hardware, software (including services), network and users that share common features, such as: authentication, authorization, trust, account directories and policies. The contractor shall provide services and solutions to enable the establishment of trust relationships and inter-enclave credentialing through which enclaves can interoperate and control the direction and nature of information exchanges, allowing the execution of multi-enclave service threads. The contractor shall provide services and solutions to facilitate migration of legacy enclave environments to enclaves compliant with the SMI-ELS Concept Document.

3.1.1.3 Federation

The contractor shall provide services and solutions that facilitate federation—a set of minimal agreements between enclave layer components which enable interaction between enclaves to take place transparently. The contractor shall provide federation capabilities within single domains and across multiple domains. Where applicable, the contractor shall provide federation capabilities across other domains within the DoD and Intelligence Community (IC) to share mission-critical information. The contractor shall establish federated naming and authentication between enclaves to enable discovery across them in accordance with applicable guidance, policy and direction. Contractor services and solutions shall adhere to core specifications, standards and technologies, such as Public Key Infrastructure (PKI), Security Assertion Markup Language (SAML), Java Message Service (JMS) and Web Services (WS-*), etc. (* denotes the assurance standards of Web Services like Trust, Security, etc. See paragraph 3.1.2.1)

3.1.1.4 Metadata Environments (MDEs)

MDEs include the generation, consumption and management of metadata to enable the operational user to discover authoritative and aggregated data and support automated mediation where appropriate. The contractor shall provide services and solutions that help generate and manage metadata and MDEs. The contractor shall maximize the use of Government-approved commercial-off-the-shelf (COTS) products when and where appropriate. Metadata are characteristics or attributes of information assets, describing the type of information asset, its structure or syntax and its content or semantics, plus a wide range of other attributes that assist users in finding, managing and consuming information contained in assets. The contractor shall develop and sustain a MDE to be used in the discovery of information by end users and other services, the management of information assets for storage, retention and records management; and security authorization and access control. All metadata shall be created in accordance with the DoD Discovery Metadata Specification (DDMS) as appropriate. The contractor shall develop MDEs in accordance with the DoD Enterprise Architecture (EA) Data Reference Model or IC Architecture Reference Model as appropriate. The contractor shall develop a federated query capability to enable end users to discover and exploit mission services to gain mission essential information. Federated queries shall access MDEs within enclaves to determine where information resides and how to access it. The MDE is characterized by the components and services it provides.

3.1.1.4.1 Metadata Components

The MDE comprises the following components: Metadata Registry (MDR), Metadata Catalog and Service Registry.

3.1.1.4.1.1 Metadata Registry

The contractor shall develop and support a MDR to hold metadata definitions for the various types of metadata in a persistent store that is accessible during runtime operations. The contractor shall develop the capability for the MDE to use metadata from the MDR to tag instances of information assets with metadata values to support discovery, lifecycle management, storage management and categorization of the individual information assets. The contractor shall develop and support the capability for the MDR to track releasable information about individual artifacts and components of those artifacts where applicable. The metadata registry shall store COI vocabularies and other metadata artifacts, describing the concepts and terminology required for information exchange within a COI. The vocabularies will be used by Authoritative Data Sources (ADS) to format exposed information assets and by the semantic discovery capability to allow users to find information assets and the services that deliver those assets. The contractor shall make it possible for vocabularies and other metadata artifacts registered in the AF MDE to become available through the DoD MDR or IC MDR using federation. The contractor shall manage metadata that enables users to discover and consume information provided by mission capabilities implemented as services. (CDRL: A023-Metadata Registry)

3.1.1.4.1.2 Metadata Catalog

The contractor shall develop and support Metadata Catalogs that include metadata to describe individual information assets and that link those assets to the content delivery service that provides the asset to the end user. The metadata shall include the format of the information asset as delivered by the service, expressed as an eXtensible Markup Language (XML) schema, Portable Document Format (PDF) or other Government approved format and adhering to the vocabulary prescribed by the COI that governs that information asset. Metadata shall also include the tags necessary to support the DDMS. (CDRL: A024-Metadata Catalog)

3.1.1.4.1.3 Service Registry

The contractor shall leverage existing service registry and provide support for a Service Registry where all services are registered and stores information about implemented services, service interfaces and the ports and bindings involved. The Service Registry shall also track the identities and credentials of services within the enterprise Cyber Security infrastructure. The Service Registry shall support the invocation of services to deliver information assets once selected by an end user or another requesting service. Metadata Catalog entries shall point to services registered in the Service Registry, where the AFINC infrastructure will be able to invoke the service to deliver the information asset to the requestor. The Service Registry shall enable the information stored in it to be federated with other DoD or IC service registries. (CDRL: A025-Metadata Service Registry)

3.1.1.4.2 Metadata Environment Services

MDE services include the following: MDE Infrastructure Services, MDE Lifecycle Management, Discovery Services and MDE Federation.

3.1.1.4.2.1 MDE Infrastructure Services

The contractor shall provide infrastructure services to support MDEs. These services and solutions include, but are not limited to, Cyber Security, messaging, application hosting, storage management and other core enterprise services. The contractor shall provide standard repository management services and solutions to support authorized administrative personnel in the creation, update, retrieval and deletion of items within the MDE.

3.1.1.4.2.2 Metadata Lifecycle Management

Metadata Lifecycle Management includes the following services: Metacards and Asset Registration, Automated Metadata Population Services (AMPS), Versioning and Indexing.

3.1.1.4.2.2.1 Metacards and Asset Registration

The contractor shall provide services and solutions that support the manual or automatic population of metacards for registered assets in a structure that is compliant with DDMS or IC standards most current version and is in correlation with one or more COI vocabularies. The contractor shall provide services and solutions that support registering infrastructure services as assets, including but not limited to, the following:

1. Services developed to support COI business processes (e.g., content exposure, aggregation and presentation).
2. Service interfaces based on one or more XML schemata or other Government approved format.
3. Vocabulary artifacts that describe COI domain knowledge. This includes Web Ontology Language (OWL) representations of knowledge and XML Schema Definition (XSD) representations of message types.
4. Information assets that are instances of authoritative content. This includes unstructured text documents, images, binary large object (BLOB) fields in databases and any other assets that qualify as requiring accountability of their content.

3.1.1.4.2.2.2 Automated Metadata Population Service

The contractor shall develop and support an AMPS to automatically create the metadata for an information asset or service. AMPS shall automatically create metacards for registration in the Metadata Catalog. Users shall be able to invoke AMPS during registration of their assets to create metacards. AMPS shall be available as a service that can be invoked automatically during creation of an asset or in large scale metadata creation. AMPS shall be capable of tagging information assets defined by XML schemas as payloads coming from content delivery services so that services can be registered in the MDE and invoked upon discovery by an end user. (CDRL: A026- Automated Metadata Population Service (AMPS))

3.1.1.4.2.2.3 Versioning

The contractor shall provide tools and services that will deliver version control of all metadata artifacts. These services will include but not be limited to capabilities that maintain different versions of the metadata artifacts such as metacards, ontologies and indexes; manage and control deprecation of artifacts such as COI vocabularies; provide publication to consumers of versioning activities; ensure the application of the correct versions of the artifacts to other metadata services such as discovery, indexing and automated metadata generation and maintain histories and activity logs of metadata artifact versioning activities.

3.1.1.4.2.2.4 Indexing

The contractor shall provide tools and services that will deliver indexing capabilities to support discovery and management of information assets. These services will include but not be limited to the indexing of metacards using keywords, concepts and other indexing schemes; the application of the ontologies generated from COI vocabularies to the indexing of artifacts; the generation of the indexes either from metadata artifacts such as XSDs and Web Services Description Languages (WSDLs) or directly from information assets in other formats such as documents, emails or presentations. The services will also include capabilities that will maintain the indexes as metadata artifacts subject to the same constraints for versioning that are applied to the metadata artifacts to which the index references.

3.1.1.4.2.3 Semantic Discovery Services

The contractor shall provide services and solutions that support a semantic discovery capability that is based on vocabularies constructed by COIs. Semantic discovery users will be able to discover information based on their own preferred vocabulary and automatically navigate across other users' vocabularies to find information relevant to each query. The semantic discovery capability will support both users seeking mission critical information as well as developers responsible for implementing new information capabilities for those users. The semantic discovery capability will pass DDMS metacard contents, rather than asset content, directly to consumers with delivery service invocation instructions which will be activated by consumers as required. The semantic discovery capability will federate with other DoD and IC Components and their information assets through the Joint DoD/DNI Federated Search Specification.

3.1.1.4.2.4 Federation of MDEs

The contractor shall provide services and solutions that support the federation of MDEs. Federation of MDEs will direct discovery queries to the right enclaves and, using the Information Assurance (IA) infrastructure, access information and services across enclaves. The federation of MDEs will include the capability for MDEs to broadcast information requests and queries across all enclaves, if direct requests are not possible. The federation of MDEs will support the mutual exchange of metadata to share reference data and support roll-up of summary metadata for the purposes of discovery and metadata management.

3.1.2 Enterprise Level Security (ELS)

3.1.2.1 Cyber Security Architecture

The contractor shall provide services and solutions to realize a Cyber Security architecture that permeates all components and operations. The contractor shall deliver information architecture services that conform to the Air Force Enterprise Architecture along with adherence to DoD and federal standards for Cyber Security, using role-based, policy-based or attribute-based controls, and managing trusted relationships between network enclaves. The contractor shall support the conformance with the 2-way authentication and end to end security stipulated by SMI-ELS and the AF Cyber Security Enterprise Architecture.

The contractor shall provide services and solutions in support of a Cyber Security architecture that delivers but is not limited to the following five categories of security services: confidentiality, integrity, availability, authenticity and non-repudiation. The contractor shall provide services and solutions to use the Cyber Security architecture to protect information consumed and generated by mission services. The contractor shall provide the capability of delivering these services at a level commensurate with the information assets being protected.

The contractor shall provide infrastructure capabilities that enable AFINC solutions to implement IA in accordance with Web Services (WS) assurance standards below.

WS-Security
WS-SecureConversation
WS-SecurityPolicy
WS-Trust
XML Signature
XML Encryption
XML Key Management (XKMS)

The contractor shall provide Cyber Security architecture, services, and solutions as stipulated by IC standards or other US, Allied, and Partner standards as specified in this Task Order (TO).

3.1.2.1.1 Confidentiality

The contractor shall provide confidentiality security services that prevent unauthorized disclosure of data, both while at rest and during transit.

3.1.2.1.2 Integrity

The contractor shall provide integrity security services that prevent unauthorized modification of data, both while at rest and in transit, and detection and notification of unauthorized modification of data.

3.1.2.1.3 Availability

The contractor shall provide availability services that ensure timely, reliable access to data and information services for authorized users.

3.1.2.1.4 Authenticity

The contractor shall provide authenticity services that ensure the identity of a subject or resource is the one claimed. The contractor shall ensure that authenticity applies to entities such as users, processes, systems, and information.

3.1.2.1.5 Non-Repudiation

The contractor shall provide non-repudiation services that ensure actions within the AF, DoD, or IC AFINC service invocations, information queries, etc., are attributable to the entity or entities that invokes them.

3.1.2.2 Cyber Security Services

The contractor shall provide services and solutions to implement and conduct IA operations such as, but not limited to, identity management, identity authentication, threat analyses and certification and accreditation.

The contractor shall ensure that all the requirements meet the DoD Cyber Security Risk Management Framework (RMF) and DoDI 8500.2, Intelligence Community directive (ICD) 503, or the most current standards and guidance that are applicable. This includes Certification and Accreditation (C&A) activities. The contractor shall provide applications services that are in compliance with and support DoD, USAF, or IC PKI policies as applicable.   The contractor shall support activities to make applications PK-enabled (PKE) in order to achieve standardized, PKI-supported capabilities for digital signatures, encryption, identification, and authentication. The contractor shall assist in defining user and registration requirements to Local Registration Authorities (LRAs). The contractor shall provide solutions that meet confidentiality, data integrity, authentication, and non-repudiation requirements. Contractor solutions shall comply with National Institute for Standards and Technologies (NIST) and Federal Information Processing Standards (FIPS) and applicable IC standards.

The contractor shall ensure that all infrastructure deliverables comply with the Defense Information Systems Agency (DISA) Security Technical Implementation Guide (STIG) and Computer Network Defense (CND), which includes the need for source code scanning, the DISA Database STIG, and a Web Penetration Test to mitigate vulnerabilities associated with Structured Query Language (SQL) injections, cross-site scripting, and buffer overflows. The contractor shall also support activities and meet the requirements of DoDI 8520.02, Public Key

Infrastructure (PKI) and Public Key (PK) Enabling, in order to achieve standardized, PKI-supported capabilities for biometrics, digital signatures, encryption, identification and authentication.

3.1.2.2.1 Identity Management

The contractor shall provide services and solutions to accomplish identity management to enable users and applications to discover one another and utilize services provided by entities using methods such as the negotiated collaborative approach. The contractor shall also provide capabilities to selectively monitor interactions and manage all active identities to include user, services, machines and services identity based on PKI.

The contractor shall provide services and solutions to accomplish lifecycle entity identity management from user creation to user revocation. Entities are defined as both human and non-human users possessing accounts within the enterprise. The contractor shall support user creation (identity confirmation, credentialing, and enrollment), user management (provisioning across single or multiple systems and services, automated provisioning workflow and self-service), user access (identification, authentication and authorization) and user revocation (de-provisioning and disablement). The contractor shall enable the de-provisioning process through automated account disablements and token revocation. The contractor shall provide access controls with rights, roles and privileges. The contractor shall provide the capability for all accounts to comply with FIPS 196, or other specified standard in this TO, by using approved methods of authentication such as, but not limited to, the following:

1. PKI based authentication.
2. One-Time Password (OTP) Tokens.
3. Biometrics with PIN or password.

3.1.2.2.2 Threat Analysis

The contractor shall conduct comprehensive threat analyses for Network Defense of AFINC Cyber Security architecture in support of DoDIN Network Defense.

3.1.2.3 Enabling Security Capabilities

The contractor shall provide the following enabling capabilities to facilitate Warfighter access to critical mission capabilities:

1. Ensure all interactions between people, machines, and services are verified using security policy.

2. Conduct confirmed two-way authentication using DoD-PKI and Federal Bridge credentials or applicable IC PKI and bridge.

3. Authorize access to data based on groups and roles.

4. Monitor and log all activities to provide for both real time assessment and historical analysis.

5. Use automated tools to analyze and detect anomalous behavior using real time/logged information to preclude and prevent internal attacks on AF information and computing resources.

6. Delegate roles and groups based on policy.

7. Mediate graduated access to data for various types of users.

8. Enable efficient cross-domain information sharing across networks operating at different classification levels (e.g., SIPRNET and NIPRNET).

9. Operate, maintain and configure point to point, VPN and bulk encryption for network and long-haul circuits.

10. Provide encryption to the base campus SIPRNET connectivity.

3.1.3 Enterprise Service Management

The contractor shall provide services and solutions to accomplish Singularly Managed SMI-ELS service level management. The contractor shall provide operation and maintenance of the SMI-ELS infrastructure including, but not limited to, network monitoring, long haul circuit administration, load balancing, information archival and backup, disaster recovery and Continuity of Operations (COOP). The contractor shall provide lifecycle management of services for both requestors of services and service providers. The contractor shall establish processes to inform users of the availability of new versions of services. The contractor shall analyze bandwidth utilization and conduct trend analyses of communications circuits and hardware resource utilization for all supported systems. The contractor shall request circuit upgrades for threshold levels that meet or exceed Government requirements and load balance redundant circuits.

3.1.4 SMI-ELS Architecture Documentation

The contractor shall document the SMI-ELS within the AF Enterprise Architecture (EA). The contractor shall document the Metadata Environment in the DoD EA Data Reference Model (DRM). The contractor shall document the standards and protocols that the AF will enforce in the DoD EA Technical Reference Model (TRM). The contractor shall develop DoD Architecture Framework (DoDAF) products or products adhering to other architectural guidelines as specified. The contractor shall support process improvement events, such as Air Force Smart Operations for the 21st Century (AFSO21), to address SMI-ELS processes and issues. The contractor shall document AFSO21 products and engineered processes in the Process Reference Model (PRM) and DoD EA System Reference Model (SRM).

3.2 Network Services and Solutions

The contractor shall provide services and solutions that enable Network Operations and Network Infrastructure capabilities. Networks as defined in this section are for data, voice and video.

3.2.1 Network Operations

The contractor shall provide services and solutions that enable Network Operations (NetOps) to operate and defend the DoD Information Network (DoDIN) to ensure information superiority. DoDIN network operations refer to land, air, and space networks across multiple levels of security. The contractor shall provide capabilities that support the essential tasks, Situational Awareness (SA), and Command and Control (C2) that comprise the operational framework that comprises NetOps. The contractor shall support the following essential NetOps tasks: DoDIN Enterprise Management (EM), DoDIN Network Defense (DoDNetD), and DoDIN Web Content Management. The contractor shall provide services and solutions that help the Government attain the following desired effects in its management of the DoD Information Network (DoDIN):

1. Assured System and Network Availability that ensures uninterrupted availability and protection of system and network resources. This includes providing for graceful degradation, self-healing, fail-over, diversity and elimination of critical failure points.
2. Assured Information Protection of information in storage, at rest, while it is passing over networks, including from the time it is stored and catalogued until it is distributed to users, operators and decision makers.
3. Assured Information Delivery of information to users, operators and decision makers in a timely manner.

3.2.1.1 DoDIN Enterprise Management (EM)

The contractor shall provide services and solutions that enable Enterprise Management. This shall include traditional systems and network management (Fault Management, Configuration Management, Accounting Management, Performance Management, Identity and Access Management, and Security Management), as well as information and infrastructure protection. It shall also encompass the DoDIN information technology (IT) services management and consist of the many elements and processes needed to communicate across the full spectrum of the DoDIN, including, but not limited to, the following:

1. Enterprise Application Services and Services Management
2. Enterprise Information Management
3. Network Management and Enterprise Services
4. Fault Management
5. Vulnerability Scanning and Patch Management

3.2.1.1.1 Enterprise Application Services and Service Management

The contractor shall provide services and solutions that enable service management and the management of enterprise application services, including, but not limited to, the following:

1. Monitoring and measuring application and service health and performance.
2. Reporting and visualizing key application and service QoS metrics.
3. Complying with Memorandums of Agreement/Understanding (MOA/MOUs) between 26 NOS and other organizations.
4. Managing application and service lifecycles.
5. Provisioning applications and services.
6. Logging and auditing application and service activities.
7. Anticipating application and service problems and sending alert notifications.
8. Pinpointing the root cause of application or service problems and allocating resources to correct the problems.
9. Automating failover and load balancing.
10. Mediation services transforming service messages and performing content based routing.
11. Correlating enterprise service messages for business transaction tracking.

3.2.1.1.2 Enterprise Information Management

The contractor shall provide services and solutions that enable and support information management services, including, but not limited to, the following:

1. Collaboration Services
2. Continuity of Operations
3. Disaster Recovery

4. Data Storage
5. Storage Area Network (CDRL: A011-Monthly Storage Report)
6. Network Attached Storage
7. Back-Up/Archive/Restore (CDRL: A012-Monthly Off-Site Status Report)
8. Records Management

3.2.1.1.3 Network Management and Enterprise Services

The contractor shall provide services and solutions that accomplish Network Management for enterprise activities such as, but not limited to, the following:

1. Automation and Enforcement of Network Policy
2. Operation of Network Sensors
3. Monitoring and Analysis of Network Behavior
4. Network Performance Analysis and Tuning
5. Network Counter Measures
6. Network Boundary Management and Control
7. Network Security Access
8. Network Service Orchestration
9. Execution of INFOCON
10. Load Balancing
11. Vulnerability Analysis and Response
12. Application and Content Management
13. Resource Virtualization
14. Information Lifecycle Management
15. Security Management Service
16. IT Service Virtualization
17. Service/Security Management and Provisioning
18. Domain Security
19. Cross-Domain Security
20. Content and Service Staging
21. Federated Content Discovery
22. Application, System, Services and Data Hosting
23. Producer to Consumer Availability of Service
24. Configuration and Change Management
25. Asset Management
26. Network Configuration Management
27. Patch Management

3.2.1.1.4 Fault Management

The contractor shall work with 26 NOS mission partners and 26 NOS work centers to perform fault-detection, fault-isolation, and recovery/resolution (FDIR) services. The contractor shall troubleshoot, resolve, and document status of network incidents and faults to maintain service levels IAW DoD, AF regulations, and 26 NOS Operation Instructions regarding Incident Management.

3.2.1.1.5 Vulnerability Scanning and Patch Management

The contractor shall perform vulnerability scanning, remediation, reporting, and patch management for systems managed by the 26 NOS IAW CTO 08-005, Scanning Remediation; 26 NOS instructions and regulations. (CDRL A005: Weekly Vulnerability Status Reports)

The contractor shall install current anti-virus software, updates, patches, and definitions on every computer, information system, network, and stand-alone computing devices including all Legacy, AFNET, IMS and Area 52 workstations IAW guidance received.

3.2.1.2 DoDIN Network Defense (ND)

The contractor shall provide services and solutions that enable DoDIN Network Defense, including, but not limited to, the following:

3.2.1.2.1 Cyber Security (CS)

Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This shall include, but not be limited to, providing for restoration of information systems by incorporating protection, detection, and reaction capabilities. IA services shall include, but not be limited to:

1. Assured Information Sharing and Management
2. Access Control
3. Cross-Domain Security
4. Information Environment Protection
5. Certification and Accreditation
6. Risk Analysis
7. IA Awareness
8. Auditing
9. Communication Security (COMSEC)
10. Operation Security (OPSEC)
11. Information Protection
12. Authentication
13. Resource Protection
14. Federated Identity Management
15. Virtual Private Networking
16. Network Protection
17. Filtering
18. Intrusion Detection and Prevention
19. Cryptographic Services
20. Key and Certificate Services
21. Insider Threat Protection
22. Anomalous Behavior Detection
23. Time Compliance Network Order (TCNO)
24. Air Force Computer Emergency Response Team (AFCERT)
25. Security Technical Implementation Guide (STIG) Compliance

3.2.1.2.2 Computer Network Defense (CND)

Defensive measures to protect, monitor, analyze, detect and respond to unauthorized activity with DoD information systems and computer networks and defend information, computer and networks from disruption, denial, degradation or destruction. This shall include, but not be limited to, the employment of IA capabilities in response to CND alert or threat information and the capability to predict, analyze and defend against new attack vectors. (CDRL: A005-Weekly Vulnerability Status Reports)

3.2.1.2.3 Computer Network Defense Response Actions (CND RA)

Deliberate, authorized defensive measures or activities that protect and defend DoD computer systems and networks under attack or targeted for attack by adversary computer systems/networks. The contractor shall also rapidly and accurately implement TTPs and NetOps directed Information Operations Condition (INFOCON) changes and provide command and control on the progress and completion.

3.2.1.2.4 Weapons and Tactics (W&T)

Actions taken to prevent, remediate or mitigate risks resulting from network infrastructure vulnerabilities that in turn maximize the mission effectiveness of 26 NOS forces through mission planning, critical self-analysis, and the implementation of tactics. Ultimately, the W&T program yields tacticians who think about tactics, techniques and procedures (TTP) in a structured way, are committed to continuous learning about the AFINC weapon system and the threat, and sharpen their peers and themselves through critical self-analysis. The contractor shall provide solutions and services that enable Weapons and Tactics Development and Implementation. This position requires a TS/SCI clearance. Reference AFSPCI 10-415, Weapons and Tactics Program. (CDRL: A007-Trip Report)

3.2.1.2.5 Intelligence Analysis

Intelligence analysis is a cognitive capability—both art and science—applying tools, judgements, processes, and tradecraft to data and information to create and deliver new intelligence, insights, and knowledge, with the goal of providing decision advantage to commanders, decision makers, and intelligence customers. The contractor shall discover, assess, explain, anticipate and deliver information, products and services provide mission assurance IAW AFI 14-133, Intelligence Analysis. The contractor shall provide solutions and services that enable intelligence analysis for events impacting the AFIN. This position requires a TS/SCI clearance. The contractor shall:

1. Facilitate Requests for Information (RFI) and Production Requirements (PR) processes for the 26 NOS.
2. Coordinate with Cyberspace operators to produce questions and provide operational details for tactical cyberspace responses.
3. Participate in Tactics Review Board (TRB) meetings, answering questions, providing information, seeking clarification, and gathering information for the government.
4. Provide data usable for course of action (COA) development and analysis, mission analysis during tactical mission planning, readiness training, and force protection tasks.
5. Liaise with Training (PWS paragraph 3.2.1.4.7) to provide mission qualification training on intelligence support, processes, and integration into the 26 NOS mission and maintain training modules for mission qualification and specialized training.
6. Prepare threat data for analysis and provide to 26 NOS leadership and AFINC operators.
7. Provide adversary cyberspace TTP analysis to local tactic review forums.
8. Provide situation briefs, tactical intelligence reports, cyberspace threat intelligence reports, and cyberspace malware and forensic reports.
9. Complete guidance checklists, update on-line databases, and validate Higher Headquarters guidance.
10. Provide Operational Preparation of the Environment (OPE) products focused on tactical tasks execution, tactical mission planning, and readiness training. (CDRLs: A028-Tactical Intelligence Reports, A029-Cyberspace Threat Intelligence Report, A030-Cyberspace Malware and Forensics Reports)

3.2.1.2.6 Exercise Management and Planning

The contractor shall provide solutions and services that support 26 NOS exercise management, planning and participation:

1. Provide execution support for a minimum of ten (10) consecutive joint, national or combined exercises.
2. Plan, coordinate, facilitate, and attend exercise related events, to include planning conferences, after action activities and exercise “hot washes”.
3. Manage activities and various other local actions related to training and exercises support.
4. The contractor shall know and understand the unit’s Mission Essential Tasks (METs) and derived Unit Training Objectives (UTOs), to include measures of effectiveness (MOE) and measures of performance (MOP), to incorporate personnel and capabilities into Master Scenario Events List (MSEL) activities.
5. The contractor shall develop and present information briefs, in-progress reviews, and papers to support exercise design, exercise training objectives in Joint Training Information Management System (JTIMS), exercise agreements, scenario development, exercise control, and Operation/Fires/Targeting IAW AFI 10-204, Participation in Joint and National Exercises.
6. The contractor shall coordinate with higher, adjacent, and coalition force planners and analysts.
7. The contractor shall support exercise execution and the implementation of exercise storylines and/or vignettes including all exercise Master Storyline Events.
8. The contractor shall create lessons learned using the Joint Lessons Learned Information System (JLLIS).
9. The contractor shall support development and synchronization of the exercises within the Joint Exercise Life Cycle (JELC).
10. The contractor shall understand Joint Operational Planning and Execution System (JOPES) to include drafting and releasing messages.
11. The contractor shall develop and recommend scenarios and/or scenario injects during planning cycle when creating the MSEL.
12. The contractor shall be proficient with the JELC, supporting joint, national and combined exercises.
13. The contractor shall have experience with computer network operations, information assurance, offensive cyberspace operations, defensive cyberspace operations, DoDIN operations, signals intelligence, collection management, Cyberspace threat analysis, and/or technical operations.
14. The contractor shall conduct follow-on actions (e.g., prepare after action, trip and lessons learned reports) for response training and exercise events.(CDRL: A007-Trip Report; CDRL: A002-After Action Report)
15. The contractor shall possess excellent writing, briefing, coaching, and leadership skills.
16. This position requires travel and TS/SCI clearance.

3.2.1.3 DoDIN Web Content Management

The contractor shall provide services and solutions to develop and administer web sites that enable Web Content Management and help ensure information is available to users on the DoDIN to accomplish their mission. Capabilities shall include, but not be limited to, those that enable the following core services areas:

3.2.1.3.1 Web Content Discovery

The ability to quickly search for information throughout the DoDIN. The contractor shall provide the capability for operational staffs to search across multiple sources from one place using a web crawler and web browser, vice making several attempts. Once products are located, the Content Delivery service shall permit users to pull in needed products.

3.2.1.3.2 Web Content Delivery

Delivery of requested information to DoDIN users. The contractor shall provide the capability for timely delivery of items across multiple, heterogeneous communication systems with delivery and read receipt notifications, providing assured delivery of information products.

3.2.1.3.3 Content Storage

The contractor shall provide and support physical and virtual places to host data on the network throughout the DoDIN with varying degrees of persistence.

3.2.1.3.4 Content Management

The contractor shall provide services and solutions that provide Network Operations Centers with capabilities such as, but not limited to, the following:

1. The ability to optimize the flow and location of information over the DoDIN by positioning and repositioning data and services to optimum locations on the DoDIN in relation to the information producers, information consumers, and the mission requirements.
2. The ability to ensure that the DoDIN is optimally delivering the information required by DoDIN users in accordance with information delivery priorities.
3. The visibility of information flowing across the DoDIN and of those systems used to store, catalog, discover, and transport information.
4. Tools to view information flows and access, determine impact to network capacity, and ensure user profiles are being satisfied with a reasonable quality of service.
5. The capability to prioritize information requirements, determine the sources responsible for providing that information, and stage information content throughout the DoDIN in support of a given operation.
6. The ability to track and maintain knowledge of various requests and user profiles for information.
7. The ability to coordinate changes in operating parameters of DoDIN assets.
8. The ability to review and validate the user-profile database.

3.2.1.4 Network Operations Enabling Capabilities

The contractor shall provide services and solutions that accomplish or provide the following enabling capabilities:

3.2.1.4.1 Distributed Network Connectivity

Robust, redundant data paths and nodes with both physical and logical diversity to maximize effectiveness and eliminate single points of failure.

3.2.1.4.2 High Availability/Logical Redundancy

Plans and capabilities to enable uninterrupted NetOps operations with seamless transfer of operations, especially network C2, following outages at any key NetOps sites. These shall include, but not be limited to, fully redundant backup and restoral capabilities with automatic failover that is transparent to users.

3.2.1.4.3 Information Management and Exchange

Automated tools and processes to facilitate the exchange of information and to aid operators in visualizing network operations and events, to facilitate rapid event characterization and information exchange and to keep pace with rapidly changing networks.

3.2.1.4.4 Standardization

Standardization of configurations, processes and applications across the enterprise to facilitate centralized management, enhance security through configuration control and save manpower in certification and accreditation, patch implementation, hardware/software upgrades and asset tracking.

3.2.1.4.5 Risk Management

A multi-faceted and global approach for risk management on applications currently residing on the network and new applications waiting to be fielded. This approach shall assess the benefits of adding the application to the network and any security risks it may introduce, the ability to execute corrective actions or configuration control measures and the potential effect any change would have on network configuration, services, or other applications. This process shall apply across Major Commands (MAJCOMs) and include arbitration processes in the event of a conflict between the intended user and others. Solutions shall follow Government approved standards such as the DoD Enterprise Service Management Framework (DESMF).

3.2.1.4.6 Department of Defense (DOD) Enterprise Service Management Framework (DESMF)

Tools, tactics, techniques and procedures for accomplishing ITSM across the AF enterprise to provide higher service quality and availability levels, improve alignment between service provider and mission areas, and improve management of changes to ensure security and capability of the information enterprise. The contractor shall provide solutions and services that enable ITSM practices according to DoDI 8440.01, DoD Information Technology Service Management (ITSM) and DESMF Edition III. (CDRLs: A010-AFNet Baseline; A013-Asset Management Database Report; A014-Interdependency Diagrams and Charts; A016-Monthly Warranty Report; A017-Software Inventory Report)

3.2.1.4.7 System Administration

Set up, configure, develop, maintain, tune, upgrade, troubleshoot and support 26 NOS managed networks with various operating systems such as, but not limited to, Windows and Linux. The contractor shall provide services to include, but not limited to, the following:

1. PKI Key Management
2. Scripting Language Programming to include, but not limited to: Tcl, Perl, Shell
3. Capacity Planning
4. Performance and Resource Optimization
5. Cloud Computing
6. Server Virtualization
7. Enterprise Security Management

3.2.1.4.8 Database Management

Perform database management to include but not limited to, installs, upgrades, patches, rebuilds, data recovery, and backups.

3.2.1.4.9 Account Management

Perform account management to include but not limited to creation, auditing, modification, disabling, archiving, and deleting users' accounts and providing means to unlock SIPR tokens for 26 NOS local network.

3.2.1.4.10 Network Address Management

Management and maintenance of the AF Internet Protocol (IP) and DNS space using IPv4 and IPv6 addressing schemes; administer Tactical IP (TACIP) addresses and provide DNS services for deployed unit exercises and real world contingencies; maintain authoritative control of af.mil and af.smil.mil domains for the Air Force. The contractor shall develop a plan to migrate from IPv4 to IPv6. (CDRL: A033-IPv6 Migration Plan).

3.2.1.5 Network Command and Control

The contractor shall provide services and solutions that enable network command and control, including, but not limited to, the following:

1. The consolidation of network SA services and solutions that integrate C2 capabilities, eliminate the need for scheduled manual reporting and provide the warfighter with on-demand, real-time operational status of networks, core services and applications directly serving or influencing his or her Area of Responsibility.

2. Rapid characterization and response to anomalous activity, including, but not limited to, “low and slow” network probe and exploitation efforts and implement appropriate defensive actions or countermeasures.

3. Trend analysis and correlation of network incidents (e.g., probes, intrusions and virus outbreaks), outages and degradation events.

4. Rapid implementation of security countermeasures by facilitating the coordination of network restoration priorities and actions after an intrusion or adverse network event.

5. Coordination and reallocation of limited resources (e.g., bandwidth, frequencies) in response to multiple and/or conflicting warfighter requirements.

3.3 Enterprise Solutions and Integration

Services and solutions to upgrade existing technology or integrate new technology into the AFIN. The contractor shall perform system engineering, provide implementation plans and develop Rehearsal of Concept (ROC) drills.

3.3.1 Systems Engineering

The contractor shall employ disciplined systems engineering processes to accomplish the following to include, but not limited to: research, planning, architecting, design, technical reviews, implementation plans, technical analysis, integrated risk management, configuration management, interface management, decision analysis, systems management, test and evaluation, verification and validation. These systems engineering solutions shall follow industry standard engineering processes and use commercial best practices in accordance with AFI 20-101, Integrated Life Cycle Management.

The contractor shall enable system solutions to integrate with the AF enterprise architecture. The contractor shall conduct assessments and analyses of existing architecture to determine and document corrective measures and proposed technology insertions that enable the capabilities and requirements of this TO. The contractor shall report how the new system will meet and support SMI-ELS and AF EA. The contractor shall develop documentation and training that enable lessons learned to be socialized within the organization and across other DoD organizations. The contractor shall provide reengineering capabilities to examine structures, systems and roles for the purpose of executing a ground-up redesign for achieving long-term, full-scale integration required for the DoDIN.

Types of support and services provided by the contractor shall include, but not be limited to: Email Hygiene, Server and Storage Area Network Administration, Security Boundary Administration, Configuration/Release Management (i.e. Security/Patch Administration, etc.), Data Analysis, Network Infrastructure Management and Administration, Certification and Accreditation (i.e. Security Scanning, etc.), and Event Management (e.g. Authorized Service Interruptions (ASIs).

3.3.2 Design/Integration Reviews

The contractor shall conduct design and integration reviews in compliance with disciplined system engineering processes. There may be a formal or informal preliminary and final design reviews. The contractor shall report impacts on the issues such as costs, return on investment, schedule dependencies and recommend functional and technical solutions. The contractor shall identify integration issues and problems such as requirements definition, architecture and policy/standards compliance and engineering guidelines compliance. The contractor shall enable convergence with data systems and/or collaborative tools as specified and required in this TO.

3.3.3 Implementation Plans (Rehearsal of Concept (ROC) DRILLS)

The contractor shall develop schedules and implementation plans with definable deliverables, including parallel operations where required, identification of technical approaches and a description of anticipated results associated with delivery of infrastructure capabilities. The implementation plans shall include, but not be limited to: hardware, software, facilities, materials, definable deliverables, documentation strategy and plans, schedule, site requirements, site implementation details, risks, contingencies, verification, validation and recommendations (e.g., network architecture, site architecture, topology and configuration) for the implementation with considerations of on-site failover and continuity of operations. The contractor shall operate and maintain prototype applications, infrastructures, models and databases to determine optimal solutions for integration concepts and problems integral to the integration process. (CDRL: A008-System Implementation Plan)

3.4 General Requirements

3.4.1 Business Relations

3.4.1.1 The contractor shall work with the Contracting Officer Representative (COR), the authorized Government representative, to accomplish Government requirements, goals, and mission objectives as efficiently and effectively as possible. This shall include sharing or coordinating information resulting from the work required within this PWS or previous Government efforts and working as a team to perform tasks in concert.

3.4.1.2 The contractor shall ensure minimum duplication of effort in the execution of all work specified within this PWS and build upon work previously accomplished by the Government, the contractor, or other contractors to the fullest extent practical.

3.4.1.3 The contractor shall successfully integrate and coordinate all activity needed to execute the requirement.

3.4.1.4 The contractor shall cooperate, support, and interface with 26 NOS military, Government civilians, and other contractors for completion of all tasks.

3.4.1.5 The contractor shall function with the Government as a single, comprehensive team to raise the level of proficiency and effectiveness of the entire team thereby providing mission assurance to the AF through the operation, maintenance, and defense of the AF network enclave.

3.4.1.6 The contractor shall attend meetings to recommend implementable courses of actions, address emerging capabilities, provide status updates, and participate in the development of Plan of Action and Milestones (POA&Ms).

3.4.1.7 The contractor shall maintain, update, and create meeting minutes for ensuring continuity of knowledge and operations. (CDRL A001: Meeting Minutes)

3.4.1.8 The contractor shall maintain, update, and create After Action Reports for ensuring continuity of knowledge and operations. (CDRL A002: After Action Report)

3.4.1.9 The contractor shall provide a Weekly Activity Report (WAR). The WAR should include current significant accomplishments, issues and problems for the current week. (CDRL A003: Weekly Activity Report)

3.4.1.10 The contractor shall provide a Quarterly Contract Summary Report. The Quarterly Contract Summary Report shall provide a summary of all significant accomplishments and work performed by Contractor for the current quarter. (CDRL A004: Quarterly Contract Summary Report)

3.4.1.11 The contractor shall adhere to the latest version or successor to any policies listed in this PWS.

3.4.1.12 The contractor shall manage the timeliness, completeness, and quality of problem identification.

3.4.1.13 The contractor shall complete and comply with information requests from the 26 NOS IA program.

3.4.1.14 The contractor shall obtain, at a minimum, Mission Ready (MR) status on an AFINC crew position, through in house training, within 90 days of contract start date.

3.4.2 Contract Administration and Management

The following subsections specify requirements for contract management, contract administration, personnel administration, and Common Access Cards (CACs).

3.4.2.1 Contract Management

3.4.2.1.1 The contractor shall establish clear organizational lines of authority and responsibility to ensure effective management of the resources assigned to the requirement.

3.4.2.1.2 The contractor shall maintain continuity between the support operations at 26 NOS Maxwell AFB-Gunter Annex in Alabama, the Alternating Operating Location (AOL), and the contractor's corporate offices.

3.4.2.1.3 The contractor shall be responsible for any subcontract management necessary to integrate work performed on this requirement and shall be responsible and accountable for subcontractor performance on this requirement.

3.4.2.1.4 The contractor shall manage work distribution to ensure there are no Organizational Conflict of Interest (OCI) considerations. Contractors may add subcontractors to their team after notification to the Contracting Officer (CO) or COR.

3.4.2.1.5 The contractor shall submit a Program Management Plan at contract start date to the CO or other designated Government representative. The contractor shall provide updates to the plan within three (3) business days of personnel changes or updates. The Program Management Plan shall include, but not be limited to, the following (CDRL A006: Program Management Plan):

1. Current listing of employees to include employees' name, social security number, and level of security clearance. The list shall be validated and signed by the company Facility Security Officer (FSO).
2. Process for recruitment and retention of personnel to include incentives, if any.
3. Overall organizational structure of positions at the primary location and AOL to meet the requirements in Section 3.0 of the PWS and a practical approach for ensuring AOL personnel are integrated into the 26 NOS daily mission IAW PWS Section 3.0.
4. Subcontracting and teaming arrangements, if any.
5. Procedures for ensuring surge support IAW PWS para 3.4.4.3.3.
6. Procedures for ensuring a Site POC or authorized Contractor Representative IAW PWS para. 3.4.2.2.
7. Process for ensuring requirements of the PWS and DD254 are maintained while filling vacancies and during short and long-term personnel absences.
8. Process for maintaining employee certifications required in this PWS.
9. Continuation of Mission Essential Services Plan IAW PWS Section 4.9.

3.4.2.2 Contract Administration

3.4.2.2.1 The contractor shall establish processes and assign appropriate resources and infrastructure to effectively administer this PWS.

3.4.2.2.2 The contractor shall respond to Government requests for contractual actions within one (1) business day and provide requested information or action within three (3) business days if not otherwise stated.

3.4.2.2.3 The contractor shall have a single point of contact between the Government and contractor personnel assigned to support this contract.

3.4.2.2.4 The contractor shall assign work effort and maintain proper and accurate time keeping records of personnel assigned to work on the requirement.

3.4.2.2.5 The contractor shall match personnel skills to the work or task with a minimum of under/over employment of resources.

3.4.2.3 Personnel Administration

3.4.2.3.1 The contractor shall provide a plan to their employees so they know what to do during designated Government non-work days or other periods where Government offices are closed due to weather or security conditions.

3.4.2.3.2 The contractor shall maintain the currency of their employees' certifications and job skills by providing initial and recurring training as required to meet the PWS requirements.

3.4.2.3.3 The contractor shall make necessary travel arrangements for employees when work is required at a location other than Gunter Annex or the AOL. (Reference PWS Paragraph 3.4.5)

3.4.2.3.4 The contractor shall provide administrative support to employees in a timely fashion (time keeping, leave processing, pay, emergency needs).

3.4.2.4 Common Access Card (CAC)

3.4.2.4.1 Primary Location

Contractors shall be identified with a contractor CAC marked by a green stripe. When required, contractor personnel shall comply with local security policies to wear their CAC in the standardized manner, clearly visible attached to the torso of the exterior garment above the belt and below the shoulders. Except when in use (i.e. inserted in a computer CAC reader) or when in controlled areas requiring other credentials as the primary method of identification. To access any Government base, the contractor shall present their CAC upon demand. The contractor will coordinate with the COR to obtain CAC. The contractor shall coordinate with the 26 NOS Security Officer to obtain a facility entry badge by completing an AF Form 2586 (Unescorted Entry Authorization Certificate). This badge will allow entry into buildings/rooms were contractors are assigned to work.

3.4.2.4.2 AOL

Contractors shall be identified with a contractor CAC marked by a green stripe. When required, contractor personnel shall comply with local security policies to wear their CAC in a standardized manner, clearly visible attached to the torso of the exterior garment above the belt and below the shoulders. Except when in use (i.e. inserted in a computer CAC reader) or when in controlled areas requiring other credentials as the primary method of identification. Contractors shall be identified by their Air Force Intelligence Surveillance and Reconnaissance Agency (AFISRA) Form 325 (Green Badge) clearly visible attached to the torso of their exterior garment above the belt and below the shoulders when present within the TOP SECRET Sensitive Compartmented Information Facility (SCIF) as proof of proper clearance to remain unescorted within the SCIF. The AFISRA Form 325 is marked with name, CONTRACTOR, and contract expiration date. Upon exit from controlled areas the contractor shall conceal their credentials (Green Badge) from plain view. To access any Government base and certain facilities, the contractor shall present their CAC upon demand. The contractor and Contractor Special Security Officer will coordinate with the COR for CAC and Green Badge issue.

3.4.3 Contractor Personnel, Disciplines, and Specialties

3.4.3.1 Contractor Personnel

3.4.3.1.1 The contractor shall not employ any person for work on this contract if such an employee is identified to the contractor by the CO as a potential threat to the health, safety, security, general well-being, or operational mission of the installation and its population. During the performance of this PWS, the COR will notify the CO of contractor personnel that pose a potential threat with behavior that disrupts the good order and discipline demanded of persons working in the unique, controlled environment staffed with active duty military, Government civilians and numerous diverse contractor personnel.

3.4.3.1.2 The contractor shall ensure that its employees are able to fluently read, write, speak and understand the English language to the extent necessary in the performance of the work.

3.4.3.1.3 The contractor shall not employ any person who is an employee of the United States (US) Government if employing that person would create an OCI. Additionally, the contractor shall not employ any person who is an employee of the Department of the Air Force, unless such has been approved according to DOD 5500.7-R, Joint Ethics Regulation.

3.4.3.1.4 Contractor employees shall identify themselves as contractor personnel by introducing themselves or being introduced as contractor personnel and displaying distinguishing badges or other visible identification for meetings with Government personnel (see paragraph 3.4.2.4). In addition, contractor personnel shall appropriately identify themselves as contractor employees in telephone conversations and in formal and informal written correspondence.

3.4.3.2 Contractor Disciplines and Specialties

3.4.3.2.1 The contractor shall accomplish the assigned work in this PWS by employing and utilizing qualified personnel with appropriate combinations of education, training, certifications, and enterprise network experience.

3.4.3.2.2 The contractor shall obtain appropriate DoDD 8140 certifications for supporting the 26 NOS IAW DoDD 8140, Cyber Workforce, prior to contract start date and maintain certifications throughout life of the contract at contractor's expense except where noted otherwise in this PWS.

3.4.3.2.3 The contractor shall obtain appropriate certifications detailed within Appendix 4 of the this PWS for each functional area prior to contract start date and maintain certifications throughout life of the contract at contractor's expense except where noted otherwise in this PWS.

3.4.3.2.4 The contractor shall ensure adequate levels of technically certified personnel are spread throughout work areas and shifts.

3.4.4 Work Location and Work Hours

Work Locations: The contractor shall perform the PWS requirements at the primary and alternate operating location (AOL). The COR will notify the Site POC or Contractors Representative concerning any changes in work location.

3.4.4.1 Primary Operating Location

The contractor performance required by this PWS includes contractor manning on all shifts, 24x7x365 days a year including holidays, at the primary operating location (except where noted in the PWS). The performance of work described in this PWS may also necessitate contractor personnel traveling to various contractor, subcontractor, and Government facilities in the continental US (CONUS) and abroad. The contractor may work extended hours past their shift, with prior approval of the CO, to ensure timely completion of work at no additional cost to the Government.

3.4.4.2 Alternate Operating Location

3.4.4.2.1 The contractor performance required by this PWS includes contractor manning between the hours of 0700L and 2300L Monday - Friday with the capability to recall personnel to duty within one hour in the event of a mission transfer to the AOL. The contractor shall be on-call when the AOL is not physically manned.

3.4.4.2.2 In the event the AOL plan is activated, the contractor shall transition from day to day AOL operations and provide 100% coverage within 24 hours. Staffing includes requirements in this PWS.

3.4.4.2.3 The contractor shall execute operations and contingency plans for the 26 NOS ensuring operations failover to AOL IAW 26 NOS policies and procedure and network operations resume without impact to AOL and Primary location.

3.4.4.2.4 The contractor team at the AOL must be able to seamlessly assume the Current Operations mission for the 26 NOS without disruption of mission coverage.

3.4.4.2.5 The contractor shall coordinate with the Government to determine the required AOL support. Additionally, the contractor will determine which of its personnel are required to deploy to the AOL in support of operations.

3.4.4.2.6 The contractor shall support AOL documentation revision efforts.

3.4.4.2.7 The performance of work described in this PWS may also necessitate contractor personnel traveling to various contractor, subcontractor, and Government facilities in the CONUS and abroad.

3.4.4.2.8 The contractor may work extended hours past their shift, with prior approval of the CO, to ensure timely completion of work at no additional cost to the Government.

3.4.4.3 Other Work Hours

3.4.4.3.1 Overtime and Holidays

Overtime and holidays are not reimbursed by the Government under the terms of the contract as it is included within the price proposed; therefore, changes shall be negotiated solely between the contractor and its employees IAW applicable labor laws.

3.4.4.3.2 Surge Hours

Surge requirements may require additional work hours due to downward-directed tasks affecting the 26 NOS core mission or emergency circumstances that may require the implementation of emergency action plans. The contractor shall be capable of supplying any normal contract requirements at the same time as any surge requirement.

3.4.4.3.3 Emergency Services

On occasion, services may be required to support an activation or exercise of contingency plans. In the event of an emergency, contractor personnel are considered essential personnel for purposes of any instruction regarding the activation or contingency plan. Announcements will normally be disseminated by local television and radio stations.

3.4.4.3.4 Base Closures Due to Emergencies:

From time to time, the Center or Base Commander may decide to close all or part of a base in response to an unforeseen emergency or similar occurrence. Such emergencies include adverse weather such as snow, ice, tornados, earthquakes, or a base disaster such as a gas leak or fire. Contractor personnel are considered essential personnel for purposes of any instruction regarding the emergency. Base closure announcements will normally be disseminated by local television and radio station.

3.4.5 Travel / Temporary Duty (TDY)

Travel off-site to Government facilities or other contractor facilities may be required and as specified in the PWS. All travel requirements (including plans, agenda, itinerary, or dates) shall be pre-approved by the Government (subject to local policy procedures), and is on a strictly cost reimbursable basis. Costs for travel shall be billed IAW the regulatory implementation of Public Law 99-234 and FAR 31.205-46 Travel Costs (subject to local policy & procedures). The contractor shall submit trip reports within three (3) business days of return from travel. (CDRL A007: Trip Report)

3.4.6 Continuation of Essential DoD Contractor Services During Crisis

The performance requirements in this TO are considered mission essential and shall be accomplished at the same level of performance during periods of crises, IAW Defense FARS (DFARS) 237.76.
3.4.6.1The contractor shall provide support during contingencies, exercises, heightened operations, and adverse weather or security closures in the accomplishment of section 3 performance requirements.

3.4.7 Base Closures Due to Emergencies

From time to time, the Center of Base Commander may decide to close all or part of a base in response to an unforeseen emergency or similar occurrence. Such emergencies include adverse weather such as snow, or ice, "an act of God such as tornado or earthquake, or a base disaster such as a gas leak or fire. Contractor personnel are essential personnel for purposes of any instruction regarding the emergency. Base closure announcements will normally be disseminated by local television and radio station.

3.4.8 Contingency

3.4.8.1 Continuity of Operations Plan

3.4.8.1.1 The contractor shall maintain and update plans for catastrophic events, non-catastrophic events and work stoppages that covers each 26 NOS location (CDRL: A031 - Continuity of Operations Plan).
3.4.8.1.2 The contactor shall maintain and update Emergency Resource Shutdown Plans (ERSPs) for all 26 NOS controlled AFIN servers and services ensuring updates are incorporated whenever changes occur IAW local guidance (CDRL: A032- Emergency Resource Shutdown Plan).

3.4.8.2 Real World Events

3.4.8.2.1 The contractor shall implement contingency operations IAW the Continuity of Operations Plan (COOP) for real world events and travel to COOP locations as required.
3.4.8.2.2 The contractor shall execute the ERSP for servers and services at all AFIN locations.
3.4.8.2.3 The contractor shall draft after action reports supporting contingency situations that may require no-notice recall of contractor personnel to augment shifts and enhance operational continuity in times of national emergency or international crisis as determined by higher Government authority and the Crew Commander (CC) or Operations Controller (OC)/Crew Chief.

3.4.8.3 Enterprise-Level Disaster Recovery

3.4.8.3.1 The contractor shall maintain and update existing COOP facilities.
3.4.8.3.2 The contractor shall document new equipment, facilities, services and systems in the COOP and performing modifications if needed.
3.4.8.3.3 The contractor shall evaluate and recommend pros and cons for cold, warm, or hot COOP sites.
3.4.8.3.4 The contractor shall maintain and update disaster recovery, continuity, contingency plans for Government approval.
3.4.8.3.5 The contractor shall maintain, update and document procedures for disaster recovery.
3.4.8.3.6 The contractor shall work with every operational area to assure fail-over with no mission gap.

3.5 Non-Personal Services

The Government shall neither supervise contractor employees nor control the method by which the contractor performs the required tasks. Under no circumstances shall the Government assign tasks to, or prepare work schedules for, individual contractor employees. It shall be the responsibility of the contractor to manage its employees and to guard against any actions that are of the nature of personal services, or give the perception of personal services. If the contractor believes that any actions constitute, or are perceived to constitute personal services, it shall be the contractor's responsibility to notify the Contracting Officer (CO) immediately.

4. Contractual Requirements

4.1 Performance Reporting

The contractor’s performance will be monitored by the Government and reported in Contractor Performance Assessment Reporting (CPARs). Performance standards shall include the contractor’s ability to:

4.1.1 Provide quality products and customer support.
4.1.2 Provide timely and accurate reports.
4.1.3 Meet the standards identified in the Service Delivery Summary (para 4.2.1) and appendix 7.

4.2 Program Management

The contractor shall identify a Program Manager who shall be the primary representative responsible for all work awarded under this contract, participating in Program Management Reviews and ensuring all standards referenced herein are adhered to.
The contractor shall assign one of the full-time, Department of Defense Directive (DoDD) 8570.01-M certified employees as site lead and at least two additional full-time, DoDD 8570.01-M certified employees as alternate site leads for each shift. *NOTE: DoDD 8570 is being replaced by DoDD 8140. The contractor shall comply with this guidance once it is made available. The Government expects the primary and alternate site lead(s) to be an additional duty. These positions serve as the primary interface with Government. The primary and alternate site lead(s) are expected to work on different shifts. A site lead, primary or alternate(s), shall be on site and available during all shifts to meet with COR or Government shift lead to discuss program and/or technical issues. The site lead shall attend scheduled staff meetings, as requested by the COR.

4.2.1 Services Delivery Summary

The Services Delivery Summary (SDS) will be in accordance with AFI 20-101, Integrated Life Cycle Management and FAR Subpart 37.6, Performance-Based Acquisition. Reference Appendix 7 for Performance Threshold Standards.

PWS Paragraph	Performance Threshold Heading
3.1 Singularly Managed Infrastructure with Enterprise Level Security (SMI-ELS) Infrastructure Implementation and Operation	
3.1.1 Singularly Managed Infrastructure (SMI)	Network Infrastructure: Items 1-12 Enterprise Services: 13-18
3.1.1.1 Core Enterprise Services	Network Infrastructure: Items 1-12 Enterprise Services: Items 13-18 System Administration: Items 19-28 Database Administration: Items 29-36 VoSIP: Item 37

	Cable Installation & Maintenance: Item 38 Performance Management: Items 39-42 Metadata Management: items 43-45
3.1.1.2 Enclaves	Network Infrastructure: Items 1-12
3.1.1.3 Federation	Network Infrastructure: Items 1-12 Enterprise Services: Items 13-18 System Administration: Items 19-28 Database Administration: Items 29-36 VoSIP: Item 37 Cable Installation & Maintenance: Item 38 Performance Management: Items 39-42 Metadata Management: items 43-45
3.1.1.4 Metadata Environments	Metadata Management: items 43-45
3.1.1.4.1 Metadata Components	Metadata Management: items 43-45
3.1.1.4.1.1 Metadata Registry	Metadata Management: items 43-45
3.1.1.4.1.2 Metadata Catalog	Metadata Management: items 43-45
3.1.1.4.1.3 Service Registry	Metadata Management: items 43-45
3.1.1.4.2 Metadata Environment (MDE) Services	Metadata Management: items 43-45
3.1.1.4.2.1 MDE Infrastructure Services	Network Infrastructure: Items 1-12 Performance Management: Items 39-42 Metadata Management: items 43-45
3.1.1.4.2.2 Metadata Lifecycle Management	Metadata Management: items 43-45
3.1.1.4.2.2.1 Metacards and Asset Registration	Metadata Management: items 43-45
3.1.1.4.2.2.2 Automated Metadata Population Service	Metadata Management: items 43-45
3.1.1.4.2.2.3 Versioning	Metadata Management: items 43-45
3.1.1.4.2.2.4 Indexing	Metadata Management: items 43-45
3.1.1.4.2.3 Semantic Discovery Services	Metadata Management: items 43-45
3.1.1.4.2.4 Federation of MDEs	Metadata Management: items 43-45
3.1.2 Enterprise Level Security (ELS)	Network Infrastructure: Items 1-12 Enterprise Services: Items 13-18 System Administration: Items 19-28 Database Administration: Items 29-36 VoSIP: Item 37 Performance Management: Items 39-42
3.1.2.1 Cyber Security Architecture	Network Infrastructure: Items 1-12 Enterprise Services: Items 13-18 System Administration: Items 19-28 Database Administration: Items 29-36 VoSIP: Item 37 Performance Management: Items 39-42
3.1.2.1.1 Confidentiality	Network Infrastructure: Items 1-12 Enterprise Services: Items 13-18 System Administration: Items 19-28 Database Administration: Items 29-36 VoSIP: Item 37 Performance Management: Items 39-42
3.1.2.1.2 Integrity	Network Infrastructure: Items 1-12

	Enterprise Services: Items 13-18 System Administration: Items 19-28 Database Administration: Items 29-36 VoSIP: Item 37 Performance Management: Items 39-42
3.1.2.1.3 Availability	Network Infrastructure: Items 1-12 Enterprise Services: Items 13-18 System Administration: Items 19-28 Database Administration: Items 29-36 VoSIP: Item 37 Performance Management: Items 39-42
3.1.2.1.4 Authenticity	Network Infrastructure: Items 1-12 Enterprise Services: Items 13-18 System Administration: Items 19-28 Database Administration: Items 29-36 VoSIP: Item 37 Performance Management: Items 39-42
3.1.2.1.5 Non-Repudiation	Network Infrastructure: Items 1-12 Enterprise Services: Items 13-18 System Administration: Items 19-28 Database Administration: Items 29-36 VoSIP: Item 37 Performance Management: Items 39-42
3.1.2.2 Cyber Security Service	Network Infrastructure: Items 1-12 Enterprise Services: Items 13-18 System Administration: Items 19-28 Database Administration: Items 29-36 VoSIP: Item 37 Performance Management: Items 39-42
3.1.2.2.1 Identity Management	Network Infrastructure: Items 1-12 Enterprise Services: Items 13-18 System Administration: Items 19-28 Database Administration: Items 29-36 VoSIP: Item 37 Performance Management: Items 39-42
3.1.2.2.2 Threat Analysis	Network Infrastructure: Items 1-12 Enterprise Services: Items 13-18 System Administration: Items 19-28 Database Administration: Items 29-36 VoSIP: Item 37 Performance Management: Items 39-42
3.1.2.3 Enabling Security Capabilities	Network Infrastructure: Items 1-12 Enterprise Services: Items 13-18 System Administration: Items 19-28 Database Administration: Items 29-36 VoSIP: Item 37 Performance Management: Items 39-42
3.1.3 Enterprise Service Management	Enterprise Services: Items 13-18 System Administration: Items 19-28 Database Administration: Items 29-36

3.1.4 SMI-ELS Architecture Documentation	Enterprise Services: Items 13-18 Cable Installation & Maintenance: Item 38
3.2 Network Services and Solution	
3.2.1 Network Operations	Network Infrastructure: Items 1-12 Enterprise Services: Items 13-18 System Administration: Items 19-28 Database Administration: Items 29-36 VoSIP: Item 37 Cable Installation & Maintenance: Item 38 Performance Management: Items 39-42
3.2.1.1 DoDIN Enterprise Management	Network Infrastructure: Items 1-12 Enterprise Services: Items 13-18
3.2.1.1.1 Enterprise Application Services and Service Management	Network Infrastructure: Items 1-12 Enterprise Services: Items 13-18 System Administration: Items 19-28
3.2.1.1.2 Enterprise Information Management	Enterprise Services: 13-18 System Administration: Items 19-28
3.2.1.1.3 Network Management and Enterprise Services	Enterprise Services: Items 13-18 VoSIP: Item 37
3.2.1.1.4 Fault Management	Network Infrastructure: Items 1-12
3.2.1.1.5 Vulnerability Scanning and Patch Management	
3.2.1.2 DoDIN Network Defense	
3.2.1.2.1 Cyber Security	Network Infrastructure: Items 1-12 Enterprise Services: Items 13-18
3.2.1.2.2 Computer Network Defense (CND)	Network Infrastructure: Items 1-12 Enterprise Services: Items 13-18
3.2.1.2.3 CND Response Actions (RA)	Network Infrastructure: Items 1-12 Enterprise Services: Items 13-18
3.2.1.2.4 Weapons and Tactics	
3.2.1.2.5 Intelligence Analysis	
3.2.1.2.6 Exercise Management and Planning	
3.2.1.3 DoDIN Web Content Management	System Administration: Items 19-28 Database Administration: Items 29-36
3.2.1.3.1 Web Content Discovery	
3.2.1.3.2 Web Content Delivery	
3.2.1.3.3 Content Storage	
3.2.1.3.4 Content Management	
3.2.1.4 Network Operations Enabling Capabilities	
3.2.1.4.1 Distributed Network Connectivity	Cable Installation & Maintenance: Item 38
3.2.1.4.2 High Availability/Logical Redundancy	
3.2.1.4.3 Information Management and Exchange	
3.2.1.4.4 Standardization	
3.2.1.4.5 Risk Management	
3.2.1.4.6 Department of Defense (DoD) Enterprise Service Management Framework (DESMF)	

3.2.1.4.7 System Administration	System Administration: Items 19-28
3.2.1.4.8 Database Management	Database Administration: Items 29-36
3.2.1.4.9 Account Management	
3.2.1.4.10 Network Address Management	
3.2.1.5 Network Command and Control	Network Infrastructure: Items 1-12
3.3 Enterprise Solutions and Integration	
3.3.1 Systems Engineering	
3.3.2 Design/Integration Reviews	
3.3.3 Implementation Plans (ROC Drills)	

4.2.2 Task Order (TO) Management

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

4.2.3 Configuration and Data Management

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

4.2.4 Records, Files and Documents

All physical records, files, documents and work papers, provided and/or generated by the Government and/or generated for the Government in performance of this PWS, maintained by the contractor which are to be transferred or released to the Government or successor contractor, shall become and remain Government property and shall be maintained and disposed of IAW AFMAN 33-363, Management of Records; AFI 33-364, Records Disposition – Procedures and Responsibilities; the Federal Acquisition Regulation, and/or the Defense Federal Acquisition Regulation Supplement, as applicable. Nothing in this section alters the rights of the Government or the contractor with respect to patents, data rights, copyrights, or any other intellectual property or proprietary information as set forth in any other part of this PWS or the NetOps and Infrastructure Solutions contract of which this PWS is a part (including all clauses that are or shall be included or incorporated by reference into that contract).

4.3 Security Management

4.3.1 Safeguarding Classified Information

The contractor shall transmit and deliver classified material/reports IAW the National Industrial Security Program Operations Manual (NISPOM) and the National Industrial Security Program Operating Manual (DoD 5220.22-M). These requirements shall be accomplished as specified in the TO. All Classified Contracts must have at a minimum, the Clause 52.204-2 Security Requirement, incorporated into the contract.

Each base will follow its own classified process IAW with the proscribed Federal guidance of the NISPOM and FAR "Subpart 4.4 along with DD Form 254. When transmitting classified information ensure all classified information is properly sanitized and/or degaussed of all sensitive/classified information IAW AFSSI 5020.

4.3.2 DD Form 254

Overarching security requirements and Contractor access to classified information shall be as specified in the basic DD Form 254, which will be further identified in the DD Form 254, as required. All contractor personnel with access to unclassified information systems, including e-mail, shall have at a minimum a favorable National Agency Check (NAC).

4.3.3 Visitor Group Security Agreement

The contractor shall sign a Contractor Visitor Group Security Agreement to protect classified information involved in performance under this contract or Task Order. The Agreement will outline responsibilities in the following areas: Contractor security supervision; Standard Practice Procedures; access, accountability, storage, and transmission of classified material; marking requirements; security education; personnel security clearances; reports; security checks; security guidance; emergency protection; protection of government resources; DD Forms 254; periodic security reviews; and other responsibilities, as required.

4.3.4 Personnel Security

The contractor shall follow the security requirements outlined in the contract DD Form 254, Department of Defense Security Classification Specification.

4.3.4.1 Gunter AFB Security Requirements

Contractor personnel working on-site must possess a final U.S. Government issued SECRET security clearance. Contractor personnel supporting PWS paragraphs 3.2.1.2.4, 3.2.1.2.5, 3.2.1.2.6 and 3.4.8 shall possess TOP SECRET security clearances.

4.3.4.2 AOL Security Requirements

Contractor personnel working on-site must possess a final U.S. Government issued TOP SECRET security clearance and be Director of Central Intelligence Directive (DCID) 6/4 eligible with a current SSBI. Any contractor personnel deploying to the AOL in support of the 26 NOS mission shall possess a TOP SECRET security clearance.

4.3.5 OPSEC Operations Security

The contractor shall comply with Operations Security requirements contained in AFI 10-701 and AFIOC Sup 1 to AFI 10-701, to include all current Critical Information (CI) listings.

4.3.6 Information Systems Security

The contractor's unclassified Information System (IS) shall comply with AFI 33-200, IA MANAGEMENT, Chapter Three, AF IA Policy. Classified IS shall comply with DOD 5220.22-M, National Industrial Security Program Operating Manual (NISPOM), Chapter Eight "Information Security". Sensitive Compartmented Information (SCI) IS shall also comply with Intelligence

Community Directive (ICD) 503, Intelligence Community Information Technology Systems Security Risk Management, Certification and Accreditation.

Contractor personnel and any other expert level support personnel shall be certified at IAT Level I DoDD 8750 Certification IAW DoD 8570.01-M, Information Assurance Workforce Improvement Program. Contractor personnel shall sign an acceptance of responsibilities statement complying with the DoDD 8570, Appendix 4. *NOTE: DoDD 8570 is being replaced by DoDD 8140. The contractor shall comply with this guidance once it is made available.

4.3.7 Physical Security

The contractor shall be responsible for safeguarding all Government property provided for contractor use. At the close of each work period, Government facilities, property, and materials shall be secured.

4.4 Protection of System Data

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

4.5 Travel Requirements

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

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

4.6 Contractor Manpower Reporting

The contractor shall report ALL contractor labor hours (including subcontractor labor hours) required for performance of services provided under this contract for the AFINC via a secure data collection site. The contractor is required to completely fill in all required data fields using the following web address http://www.ecmra.mil. Reporting inputs will be for the labor executed during the period of performance during each Government fiscal year (FY), which runs October 1 through September 30. While inputs may be reported any time during the FY, all data shall be reported no later than October 31 of each calendar year, beginning with 2015. Contractors may direct questions to the help desk at: http://www.ecmra.mil.

4.7 Safety and Environmental Requirements

4.7.1 Safety

4.7.1.1 General Safety

The contractor shall conform to the safety requirements contained in the contract for all activities related to the accomplishment of the work.

The contractor shall take such additional immediate precautions as the CO may reasonably require for safety and mishap prevention purposes.

The contractor shall develop and provide at the start of the orientation period or the start of the first operational performance period a safety plan for the protection of Government facilities and property and to provide a safe work environment for contractor personnel.

The contractor shall provide protection to Government property to prevent damage during the period of time the property is under the control or in possession of the contractor.

The safety provisions of this contract, shall apply to any subcontracts/subcontractors. The contractor shall include a clause in each applicable subcontract requiring the subcontractor's cooperation and assistance in accident reporting and investigation.

4.7.1.2 Safety Mishap Notification

The contractor shall notify the COR or 67 CW Safety Office (67 CW/SE) within one hour of all mishaps or incidents. A written report of the mishap/incident shall be sent within three calendar days to the COR, who will forward it to the 67 CW Safety Office. For information not available at the time of initial written report, the contractor shall provide the remaining information no later than 20 calendar days after the mishap, unless extended by 67 CW Safety Office.

If requested by the COR, Installation Safety Office, or Incident Commander, the contractor shall immediately secure the mishap scene/damaged property and impound pertinent maintenance and training records, until released by the Safety Office or other appropriate authority. If the Government elects to conduct an investigation of the accident/mishap, the contractor shall cooperate fully and assist government personnel in the conduct of investigation until the investigation is completed.

Mishap notifications shall contain, as a minimum, the following information:

a. Contract, Contract Number, Name and Title of Person(s) Reporting
b. Date, Time and exact location of accident/incident
c. Brief Narrative of accident/incident (Events leading to accident/incident)
d. Cause of accident/incident, if known
e. Estimated cost of accident/incident (material and labor to repair/replace)
f. Nomenclature of equipment and personnel involved in accident/incident
g. Corrective actions (taken or proposed)
h. Other pertinent information

4.7.1.3 Safety Program Procedures, Qualifications, Facilities and Equipment

The contractors Safety Program shall clearly define procedures, personnel qualifications, facilities and required equipment necessary to fulfill AFI 91-203, Air Force Consolidated Occupational Safety Instruction.

4.7.1.4 Conservation of Utilities

The contractor shall instruct employees in utilities conservation practices. The contractor shall be responsible for operating under conditions which prevent the waste of utilities which include the following:

a. Lights shall be used only in areas where and when work is actually being performed.
b. Mechanical equipment controls for heating, ventilation, and air conditioning systems shall not be adjusted by the contractor or by contractor employees unless authorized.
c. Water faucets or valves shall be turned off after the required use has been accomplished.
d. Government telephones shall be used only for official government business.

4.8 Housekeeping

The contractor shall keep the work areas clean and orderly in compliance with federal, state, local health, fire, and safety standards.

4.8.1 Refuse Collection

The Government will provide dumpsters for refuse and provide dumpster collection service. The contractor shall take personal refuse to the nearest authorized refuse dumpster. The Government will provide containers for the collection of recycling materials. All discarded work product must be 100% shredded or bagged in approved and appropriately labeled burn bag security containers IAW 67CW OPSEC Plan dated 21 Dec 15.

4.9 Continuation of Essential Contractor Services During Crisis

IAW DoDI 1100.22 and IAW Defense Federal Acquisition Regulation Supplement (DFARS) 237.76, all contractor personnel under this task order are considered to be mission essential at the primary location and AOL. The contractor shall be required to continue to perform at the same level during national crisis. (CDRL A021: Mission Essential Services Plan)

4.9.1The contractor shall identify to the Government any employees working under this task order having military mobilization recall commitments.

4.9.2 The contractor shall notify the CO upon activation or recall of any such personnel.

4.10 Contractor Transition

4.10.1 In the event the follow-on contract is awarded to other than the incumbent, the incumbent Contractor shall provide all necessary support to the Government and the successful offeror to ensure an orderly transition and minimize any impact on the entire operation.

4.10.2 The incumbent Contractor recognizes that the services provided by this contract are vital to the Government's overall effort and continuity shall be maintained at a consistently high level without interruption; that upon expiration of this contract, a successor, either the Government or another Contractor, may continue these services; that the successor, be it the Government or another Contractor, shall require assistance from the Contractor and the Contractor shall give his/her best efforts and cooperation in order to effect an orderly and efficient transition from his/her operation to a successor. The incumbent Contractor shall provide a comprehensive transition plan not later than 90 calendar days prior to expiration of this contract unless otherwise directed by the CO. The transition plan shall include provisions for incumbent Contractor actions to assist and coordinate with the Government and the successor Contractor in the changeover of all functions on the contract performance start date. (CDRL: A034-Transition Plan)

4.10.3 Utilizing the Transition Plan. The Contractor shall work in concert with the incumbent during normal duty hours at the primary and alternate operating locations during the transition period. During this time, the Contractor shall familiarize themselves with the AFNET environment, the AFINC weapon system and all processes and procedures regarding the operation and maintenance of such.

5. Quality Processes

As a minimum, the prime contractor shall be appraised at ISO 9001:2008 or ISO/IEC 20000-1:2011 or CMMI for Services Level 4 (or higher) using the SEI SCAMPI, a method by an SEI-authorized lead appraiser, or comparable documented systems engineering processes, for the entire performance period of the contract, inclusive of options. Formal certifications must be held at the prime contractor’s organizational level performing the contract. If not ISO certified or SEI appraised, acceptable comparable System Engineering processes shall be maintained for the entire performance period of the contract, inclusive of options. These processes include: requirements management; configuration management; development of specifications; definition and illustration of architectures and interfaces; design; test and evaluation/verification and validation; deployment and maintenance. The Government reserves the right to audit and/or request proof of these comparable quality processes for the entire performance period of the contract, inclusive of options.

In addition, small business companion contract awardees that elect to take advantage of provisions outlined in clause H139 must comply with the quality processes requirements. This means that at the time of award and as a minimum, the prime contractor shall be appraised at ISO 9001:2008 or ISO/IEC 20000-1:2011 or CMMI for Services Level 4 (or higher) using the Software Engineering Institute’s (SEI) SCAMPI A method by an SEI-authorized lead appraiser and must be held at the prime contractor’s organizational level performing the contract for the entire performance period of the contract, inclusive of options. Evidence of comparable Systems Engineering (SE) processes will not be accepted.

APPENDIX 1: NETOPS AND INFRASTRUCTURE SOLUTIONS STANDARDS & REFERENCES

Purpose:
The following table of specifications, standards, policies and procedures represent documents and standards that are required for this contract. The list below is not all-inclusive and the most current version of the document in the AF Standard Center of Excellence Repository (SCOER) at the time of task order issuance will take precedence. Web links are provided wherever possible.

NETWORK OPERATIONS AND INFRASTRUCTURE SOLUTIONS (COMPLIANCE)			
Standard		URL	Description
1.	AFI 10-206 Operational Reporting	http://static.e-publishing.af.mil/production/1/af_a3/publication/afi10-206/afi10-206.pdf	This instruction implements Air Force Policy Directive (AFPD) 10-2, Readiness. It applies to all US Air Force Major Commands (MAJCOM), Air National Guard (ANG), Air Force Reserve Command (AFRC), Field Operating Agencies (FOA), and Direct Reporting Units (DRU). Prior to mobilization/activation AF, ANG, and AFRC units will address the HQ AF Service Watch Cell (AFSWC) on all applicable record copy Air Force Operational Reports (AF OPREP-3). It establishes and describes the Air Force Operational Reporting System. It explains the purpose and gives instructions for preparing and submitting these reports. Refer recommended changes and questions about this publication to AF/A3O, 1480 Air Force Pentagon, Washington, D.C. 20330-1480, Office of Primary Responsibility (OPR) using the AF Form 847, Recommendation for Change of Publication. MAJCOMs are authorized to supplement this Air Force Instruction (AFI) instead of repeating instructions in separate directives.

NETWORK OPERATIONS AND INFRASTRUCTURE SOLUTIONS (COMPLIANCE)			
Standard		URL	Description
2.	AFI 10-208 Air Force Continuity of Operations (COOP) Program.	http://static.e-publishing.af.mil/production/1/af_a3_5/publication/afi10-208/afi10-208.pdf	This Instruction implements Air Force Policy Directive (AFPD) 10-2, Readiness, and is consistent with AFPD 10-8, Homeland Security. It describes policy and requirements for implementing DODI 3020.42, Defense Continuity Plan Development, and DODI O-3020.43, Emergency Management and Incident Command of the Pentagon Facilities; DODI O-3000.08 Balanced Survivability Assessments (BSAs);and O-DODI 5110.11, Raven Rock Mountain Complex (RRMC).
3.	AFI 10-601 Operational Capability Requirements Development	http://static.e-publishing.af.mil/production/1/af_a3_5/publication/afi10-601/afi10-601.pdf	The primary intent of this instruction is to facilitate timely development and fielding of affordable and sustainable operational systems needed by the combatant commander. The primary goal is to fulfill stated defense strategy needs with effects based, capabilities-focused materiel and non-materiel solutions. These solutions must be well integrated to provide suitable, safe, and interoperable increments of capability that are affordable throughout the life cycle.
4.	AFI 10-701 Operations Security (OPSEC)	http://static.e-publishing.af.mil/production/1/af_a3_5/publication/afi10-701/afi10-701.pdf	This publication provides guidance for all Air Force personnel (military and civilian) and supporting contractors in implementing, maintaining and executing OPSEC programs. It describes the OPSEC process and discusses integration of OPSEC into Air Force plans, operations and support activities.

NETWORK OPERATIONS AND INFRASTRUCTURE SOLUTIONS (COMPLIANCE)			
Standard		**URL**	**Description**
5.	AFI-1604 Air Force Information Security Program	http://static.e-publishing.af.mil/production/1/saf_aa/publication/afi16-1404/afi16-1404.pdf	This publication implements Air Force Policy Directive (AFPD) 16-14, Security Enterprise Governance; Department of Defense (DoD) Directive 5210.50, Management of Serious Security Incidents Involving Classfied Information, DoD Instruction (DoDI) 5210.02, Access and Dissemination of RD and FRD, DoDI 5210.83, DoD Unclassified Controlled Nuclear Information (UCNI), DoD Manual (DoDM) 5200.01, DoD Information Security Program, Volume 1, Volume 2, Volume 3, and Volume 4; and DoDm 5200.45, Instructions for Developing Security Classification Guides.
6.	AFI 31-501 Personnel Security Program Management	http://static.e-publishing.af.mil/production/1/saf_aa/publication/afi31-501/afi31-501.pdf	Use this instruction with the DOD Regulation 5200.2-R and AFPD 31-5 to implement the personnel security program. This instruction requires collecting and maintaining information protected by the Privacy Act of 1974 authorized by Executive Orders 9397, 9838, 10450, 11652, and 12968; and 5 United States Code (U.S.C.) 7513, 7532, 7533; 10 U.S.C. 8013.

NETWORK OPERATIONS AND INFRASTRUCTURE SOLUTIONS (COMPLIANCE)			
Standard		URL	Description
7.	AFI 32-10112 Installation Geospatial Information and Services (Installation GI&S)	http://static.e-publishing.af.mil/production/1/af_a4_7/publication/afi32-10112/afi32-10112.pdf	This instructions convey guidance and procedures allowing commanders and Air Force professionals to maintain a flow of timely geospatial information with due regard for national security, accuracy, and privacy. Describe Geospatial Information and Services (GI&S) support for the installation and facilities mission, hereafter referred to as the GeoBase Program or GeoBase. Explain the organization and execution of the GeoBase Program for all levels of command. GI&S is the key platform for cross functional integration, and to that end this AFI provides guidance for those organizations seeking to integrate with the Geo-Base Service. Provide guidance and procedures for all Air Force military and civilian personnel that perform or utilize GeoBase functions, products or systems, including those in the Air National Guard and U.S. Air Force Reserve. This instruction is not intended to overlap or supersede GI&S guidance found in AFI 14-205, Geospatial Information and Services, 4 May 2004. Ensure that all records created as a result of processes prescribed in this publication are maintained in accordance with AFMAN 37-123, Management of Records and disposed of in accordance with the Air Force Records Disposition Schedule (RDS) located at https://afrims.amc.af.mil/. The use of the name or mark of any specific manufacturer, commercial product, commodity, or service in this publication does not imply endorsement by the Air Force.

NETWORK OPERATIONS AND INFRASTRUCTURE SOLUTIONS (COMPLIANCE)			
Standard		URL	Description
8.	AFI 33-332 Air Force Privacy And Civil Liberties Program	http://static.e-publishing.af.mil/production/1/saf_cio_a6/publication/afi33-332/afi33-332.pdf	Records that are retrieved by name or other personal identifier of a U.S. citizen or alien lawfully admitted for permanent residence are subject to Privacy Act requirements and are referred to as a Privacy Act system of records. The Air Force must publish SORNs in the Federal Register, describing the collection of information for new, changed or deleted systems to inform the public and give them a 30 day opportunity to comment before implementing or changing the system.
9.	AFI 33-364 Records Disposition Procedures and Responsibilities	http://static.e-publishing.af.mil/production/1/saf_cio_a6/publication/afi33-364/afi33-364.pdf	Records Disposition Procedures
10.	AFI 17-140 AFGM2016-01 AFI 33-401 Air Force Architecting	http://static.e-publishing.af.mil/production/1/saf_cio_a6/publication/afi17-140/afi17-140.pdf	This Air Force Instruction (AFI) implements Air Force Policy Directive (AFPD) 33-4, *Enterprise Architecting*. This instruction describes the federation of Air Force architectures and its concept for federated architecture development, its associated business rules, governance, and the roles and responsibilities for appropriate Air Force organizations.

NETWORK OPERATIONS AND INFRASTRUCTURE SOLUTIONS (COMPLIANCE)			
Standard		URL	Description
11.	AFI 17-220 AFGM to AFI 33-580 AFI 33-580 Spectrum Management	http://static.e-publishing.af.mil/production/1/saf_cio_a6/publication/afi17-220/afi17-220.pdf	This instruction establishes guidance and procedures for Air Force-wide management and use of the electromagnetic spectrum and implements Department of Defense Instruction (DoDI) 4650.01, Policy and Procedures for Management and Use of the Electromagnetic Spectrum; DoDI 8320.05, Electromagnetic Spectrum Data Sharing; National Telecommunications and Information Administration (NTIA) Manual of Regulations and Procedures for Federal Radio Frequency Management; Air Force Policy Directive (AFPD) 33-5, Warfighting Integration; and the procedures established by the Joint Staff J65A United States Military Communications-Electronics Board (USMCEB).
12.	AFI 17-210 Cyberspace RADIO MANAGEMENT	http://static.e-publishing.af.mil/production/1/saf_cio_a6/publication/afi17-210/afi17-210.pdf	This standard specifies requirements for types of land mobile radios, frequency ranges and encryption standards. It provides requirements processing, validation, and handling procedures for classified and unclassified Personal Wireless Communication Systems (PWCS), and training. It provides procedures for the management, operation, and procurement of commercial wireless service for all PWCS.

NETWORK OPERATIONS AND INFRASTRUCTURE SOLUTIONS (COMPLIANCE)

Standard		URL	Description
13.	AFI 36-2201 Air Force Training Program	http://static.e-publishing.af.mil/production/1/af_a1/publication/afi36-2201/afi36-2201.pdf	This Air Force Instruction (AFI) applies to Total Force – Active Duty, Air Force Reserve, Air National Guard (ANG), and Department of Air Force Civilian. Ensure that all records created as a result of processes prescribed in this publication are maintained in accordance with AFMAN 33-363, Management of Records, and disposed of in accordance with the Air Force Records Disposition Schedule (RDS) located at https://www.my.af.mil/afrims/afrims/afrims/rims.cfm. Refer recommended changes and questions about this publication to the Office of Primary Responsibility (OPR) using the AF IMT 847, Recommendation for Change of Publication; route AF IMT 847s from the field through Major Commands (MAJCOMS) publications/forms managers.
14.	AFI 99-103 Capabilities-Based Test And Evaluation	http://static.e-publishing.af.mil/production/1/af_te/publication/afi99-103/afi99-103.pdf	It describes the planning, conduct, and reporting of cost effective test and evaluation (T&E) programs as an efficient continuum of integrated testing known as seamless verification. The overarching functions of T&E are to mature system designs, manage risks, identify and help resolve deficiencies as early as possible, and ensure systems are operationally mission capable (i.e., effective and suitable). The Air Force T&E community plans for and conducts integrated testing as an efficient continuum known as seamless verification in collaboration with the requirements and acquisition communities.

NETWORK OPERATIONS AND INFRASTRUCTURE SOLUTIONS (COMPLIANCE)			
Standard		URL	Description
15.	AFMAN 1701 AFGM to AFMAN 33-152 User Responsibilities and Guidance for information Systems	http://static.e-publishing.af.mil/production/1/saf_cio_a6/publication/afman17-1201/afman17-1201.pdf	This instruction implements Air Force Policy Directive (AFPD) 33-1, Information Resources Management, AFPD 33-2, Information Assurance (IA) Program, and identifies policies and procedures for the use of cyberspace support systems/services and compliance requirements of Secretary of the Air Force, Chief of Warfighting Integration and Chief Information Officer (SAF/CIO A6) managed programs. These programs ensure availability, interoperability, and maintainability of cyberspace support systems/services in support of Air Force mission readiness and warfighting capabilities. This manual applies to all Air Force military, civilians, contractor personnel under contract by the Department of Defense (DOD), and other individuals or organizations as required by binding agreement or obligation with the Department of the Air Force. This manual applies to the Air National Guard (ANG) and the Air Force Reserve Command (AFRC).

NETWORK OPERATIONS AND INFRASTRUCTURE SOLUTIONS (COMPLIANCE)			
Standard		**URL**	**Description**
16.	AFMAN 17-1203 AFGM to AFMAN 33-153 Information Technology (IT) Asset Management (ITAM)	http://static.e-publishing.af.mil/production/1/saf_cio_a6/publication/afman17-1203/afman33-153.pdf	This Air Force Manual (AFMAN) implements Executive Order (E.O.) 13103, Computer Software Piracy and Air Force Policy Directives (AFPD) 33-1, Cyberspace Support and supports AFPD 33-2, Information Assurance (IA) Program; AFPD 63-1/20-1, Integrated Life Cycle Management; and AFPD 10-6, Capabilities-Based Planning & Requirements Development. This AFMAN provides the overarching guidance and direction for managing IT hardware and software. The hardware management guidance identifies responsibilities for supporting Air Force (AF) IT hardware (IT assets) and maintaining accountability of Personal Wireless Communications Systems (PWCS) including cellular telephones and pagers. The software management guidance identifies responsibilities for management of commercial off-the-shelf (COTS) and AF-unique software acquired/developed by the AF (other than software internal to a weapon system; see AFPD 63-1/20-1, Integrated Life Cycle Management).
17.	AFMAN 17-1301 AFGM to AFMAN 33-282 Computer Security (COMPUSEC)	http://static.e-publishing.af.mil/production/1/saf_cio_a6/publication/afman17-1301/afman17-1301.pdf	This AFMAN implements Computer Security in support of AFPD 33-2, Information Assurance Program and AFI 33-200, IA Management Computer Security (COMPUSEC) is defined within the IA Portion of AFI 33-200.

NETWORK OPERATIONS AND INFRASTRUCTURE SOLUTIONS (COMPLIANCE)

Standard		URL	Description
18.	AFMAN 33-363 Management of Records	http://static.e-publishing.af.mil/production/1/saf_cio_a6/publication/afman33-363/afman33-363.pdf	This manual implements Department of Defense (DoD) Directive (DoDD) 5015.2, DoD Records Management Program, and Air Force Policy Directive (AFPD) 33-3, Information Management. It establishes the requirement to use the Air Force Records Information Management System (AFRIMS); establishes guidelines for managing all records (regardless of media); and defines methods and the format for record storage, file procedures, converting paper records to other media or vice versa, and outlines the minimum to comply with records management legal and policy requirements.
19.	AFPD 33-3 Information Management	http://static.e-publishing.af.mil/production/1/saf_cio_a6/publication/afpd33-3/afpd33-3.pdf	This policy directive establishes Air Force policy for the management of information assets (all forms of data and content), across all AF information sources, as both a strategic resource and corporate asset supporting the warfighter during mission and support operations.
20.	DoDI 8510.01 - DoD Risk Management Framework (RMF) for DoD Information Technology	http://www.dtic.mil/whs/directives/corres/pdf/851001_2014.pdf	Provides procedural guidance for the reciprocal acceptance of authorization decisions and artifacts within DoD, and between DoD and other federal agencies, for the authorization and connection of information systems (ISs). Revised from 2007 version on 12 March 2014.

NETWORK OPERATIONS AND INFRASTRUCTURE SOLUTIONS (COMPLIANCE)

Standard		URL	Description
21.	DoDI 8500.01 – Cyber Security (CS)	http://www.dtic.mil/whs/directives/corres/pdf/850001_2014.pdf	The purpose of the Defense Cybersecurity program is to ensure that IT can be used in a way that allows mission owners and operators to have confidence in the confidentiality, integrity, and availability of IT and DoD information, and to make choices based on that confidence
22.	DoDI 8551.01 – Ports, Protocols and Services Management	http://www.dtic.mil/whs/directives/corres/pdf/855101p.pdf	
23.	CJCSI 6211.02D – Defense Information Systems Network (DISN) Responsibilities	http://www.dtic.mil/cjcs_directives/cdata/unlimit/6211_02a.pdf	This instruction establishes policy and responsibilities for the connection of information systems (ISs) (e.g., applications, enclaves, or outsourced processes) and unified capabilities (UC) products to the DISN provided transport (including data, voice, and video) and access to information services transmitted over the DISN (including data, voice, video, and cross-domain).
24.	DFARS 252.227-7013 Rights in Technical Data Non-Commercial Items	http://farsite.hill.af.mil/reghtml/regs/far2afmcfars/fardfars/dfars/Dfars252_227.htm#P696_47162	Provides guidelines for rights in technical data on non-commercial items

NETWORK OPERATIONS AND INFRASTRUCTURE SOLUTIONS (COMPLIANCE)			
Standard		URL	Description
25.	Department of Defense Architecture Framework (DoDAF) Ver2.02 Aug 2010	http://dodcio.defense.gov/Library/DoD-Architecture-Framework/	The Department of Defense Architecture Framework (DoDAF), Version 2.0 is the overarching, comprehensive framework and conceptual model enabling the development of architectures to facilitate the ability of Department of Defense (DoD) managers at all levels to make key decisions more effectively through organized information sharing across the Department, Joint Capability Areas (JCAs), Mission, Component, and Program boundaries. The DoDAF serves as one of the principal pillars supporting the DoD Chief Information Officer (CIO) in his responsibilities for development and maintenance of architectures required under the Clinger-Cohen Act. DoDAF is prescribed for the use and development of Architectural Descriptions in the Department. It also provides extensive guidance on the development of architectures supporting the adoption and execution of Net-centric services within the Department.
26.	DFARS 252.227-7014 Rights in Non-commercial Computer Software	https://www.gpo.gov/fdsys/pkg/CFR-2011-title48-vol3/pdf/CFR-2011-title48-vol3-sec252-227-7014.pdf	Guidance on rights in technical data and computer software small business innovation research (SBIR) program.

NETWORK OPERATIONS AND INFRASTRUCTURE SOLUTIONS (COMPLIANCE)

Standard		URL	Description
27.	DFARS 252.227-7015 Technical Data Commercial Items	https://www.gpo.gov/fdsys/pkg/CFR-2011-title48-vol3/pdf/CFR-2011-title48-vol3-sec252-227-7015.pdf	Provides the Government specific license rights in technical data pertaining to commercial items or processes. DoD may use, modify, reproduce, release, perform, display, or disclose data only within the Government. The data may not be used to manufacture additional quantities of the commercial items and, except for emergency repair or overhaul and for covered Government support contractors, may not be released or disclosed to, or used by, third parties without the contractor's written permission.
28.	DFARS 252.227-7017 Identification and Assertion of Use, Release, or Disclosure Restrictions	http://farsite.hill.af.mil/reghtml/regs/far2afmcfars/fardfars/dfars/Dfars252_227.htm#P1182_92447	Provides requirements for the identification and assertion of technical data.
29.	DoD 5220.22-M, National Industrial Security Program Operating Manual	http://www.dss.mil/documents/odaa/nispom2006-5220.pdf	Provides baseline standards for the protection of classified information released or disclosed to industry in connections with classified contracts under the National Industrial Security Program.
30.	DoD Manual 5200.01, DoD Information Security Program: Overview, Classification, and Declassification, V1-V4	http://www.dtic.mil/whs/directives/corres/pdf/520001_vol1.pdf	The purpose of this manual is to implement policy, assign responsibilities, and provide procedures for the designation, marking, protection, and dissemination of controlled unclassified information (CUI) and classified information, including information categorized as collateral, sensitive compartmented information (SCI), and Special Access Program (SAP).

NETWORK OPERATIONS AND INFRASTRUCTURE SOLUTIONS (COMPLIANCE)			
Standard		URL	Description
31.	TIA/EIA-TSB-72, Centralized Optical Fiber Cabling Guidelines	http://www.tiaonline.org/	Must be purchased. ANSI/TIA/EIA-568-B series standard incorporates and refines the technical content of TSB67, TSB72, TSB75, TSB95 and TIA/EIA-568-A-1, A-2, A-3, A-4 and A-5.
32.	DoD Mobile Application Strategy	http://archive.defense.gov/news/dodmobilitystrategy.pdf	It is intended to align the progress of various mobile device pilots and initiatives across DoD under common objectives, ensuring that the warfighter benefits from such activities and aligns with efforts composing the Joint Information Environment.
33.	DoD CIO Net-Centric Data Strategy	http://dodcio.defense.gov/Portals/0/Documents/Net-Centric-Data-Strategy-2003-05-092.pdf	This Strategy lays the foundation for realizing the benefits of net centricity by identifying data goals and approaches for achieving those goals. To realize the vision for net-centric data, two primary objectives must be emphasized: (1) increasing the data that is available to communities or the Enterprise and (2) ensuring that data is usable by both anticipated and unanticipated users and applications. (Source: Department of Defense Net-Centric Data Strategy, DoD CIO, 9 May 2003

NETWORK OPERATIONS AND INFRASTRUCTURE SOLUTIONS (COMPLIANCE)

Standard		URL	Description
34.	DoD CIO Net-Centric Services Strategy	http://dodcio.defense.gov/Portals/0/documents/DoD_NetCentricServicesStrategy.pdf	The DoD Net-Centric Services Strategy (NCSS) [R1313] builds upon the DoD Net-Centric Data Strategy's (May 2003) goals of making data assets visible, accessible, and understandable. The NCSS establishes services as the preferred means by which data producers and capability providers can make their data assets and capabilities available across the DoD and beyond. It also establishes services as the preferred means by which consumers can access and use these data assets and capabilities.
35.	DoDD 5205.02E, Operations Security (OPSEC) Program	http://www.dtic.mil/whs/directives/corres/pdf/520502e.pdf	Underscores the importance of OPSEC and how it is integrated as a core military capability within Information Operations (IO) that must be followed in daily application of military operations.
36.	DoDD 8000.01 Management of the Department of Defense Information Enterprise	http://www.dtic.mil/whs/directives/corres/pdf/800001p.pdf	Provides direction on creating an information advantage for DoD personnel and mission partners, and establishing and defining roles for CIOs at various levels within the Department of Defense

NETWORK OPERATIONS AND INFRASTRUCTURE SOLUTIONS (COMPLIANCE)			
Standard		URL	Description
37.	DoDD 8100.02, Use of Commercial Wireless Devices, Services, and Technologies in the DoD Global Information Grid (GIG)	http://www.dtic.mil/whs/directives/corres/pdf/810002p.pdf	Establishes policy and assigns responsibilities for the use of commercial wireless devices, services, and technologies in the DoD Global Information Grid (GIG) (DoD Directive 8100.1, "Global Information Grid (GIG) Overarching Policy," September 19, 2002). Directs the development and use of a Knowledge Management (KM) process to promote the sharing of wireless technology capabilities, vulnerabilities, and vulnerability mitigation strategies throughout the Department of Defense. Promotes joint interoperability using open standards throughout the Department of Defense for commercial wireless services, devices, and technological implementations.
38.	DoDI 1100.22 Policy and Procedures For Determining Workforce Mix	http://www.dtic.mil/whs/directives/corres/pdf/110022p.pdf	Provides manpower mix criteria and guidance for risk assessments to be used to identify and justify activities that are inherently Governmental (IG); commercial (exempt from private sector performance); and commercial (subject to private sector performance).
39.	AFI 63-101/20-101, Integrated Life Cycle Management	http://static.e-publishing.af.mil/production/1/saf_aq/publication/afi63-101_20-101/afi63-101_20-101.pdf	It identifies elements of Air Force systems engineering (SE) practice and management required to provide and sustain, in a timely manner, cost-effective products and systems that are operationally safe, suitable, and effective.

NETWORK OPERATIONS AND INFRASTRUCTURE SOLUTIONS (COMPLIANCE)			
Standard		URL	Description
40.	DoDI 3222.03, DoD Electromagnetic Environmental Effects (E3) Program	http://www.dtic.mil/whs/directives/corres/pdf/322203p.pdf	Reissue DoD Directive (DoDD) 3222.3 (Reference (a) as a DoD instruction (DoDI) in accordance with the authority in DoDD 5144.02 (Reference (b)). The mission of the DoD E3 IPT is to promote communication, coordination, commonality, and synergy among the DoD Components for E3-related matters.
41.	DoDD 5230.24, Distribution Statements on Technical Documents	http://www.dtic.mil/whs/directives/corres/pdf/523024p.pdf	This instruction updates policies and procedures for marking technical documents, including production, engineering, and logistics information, to denote the extent to which they are available for distribution, release, and dissemination without additional approvals or authorizations.
42.	AFI 33-200, Air Force Cybersecurity Program Management	http://static.e-publishing.af.mil/production/1/saf_cio_a6/publication/afi33-200/afi33-200.pdf	This AFI provides general direction for implementation of IA and management of IA programs according to AFPD 33-2. Compliance ensures appropriate measures are taken to ensure the availability, integrity, and confidentiality of Air Force ISs and the information they process. Using appropriate levels of protection against threats and vulnerabilities help prevent denial of service, corruption, compromise, fraud, waste, and abuse.
43.	AFI 17-101 AFGM to AFI 33-210, AF Certification and Accreditation (C&A) Program (AFCAP)	http://static.e-publishing.af.mil/production/1/saf_cio_a6/publication/afi17-101/afi17-101.pdf	AF C&A program guidance

NETWORK OPERATIONS AND INFRASTRUCTURE SOLUTIONS (COMPLIANCE)			
Standard		URL	Description
44.	DODI 8330.01 Interoperability of Information Technology (IT), Including National Security Systems (NSS)	http://www.dtic.mil/whs/directives/corres/pdf/833001p.pdf	Establishes policy, assigns responsibilities, and provides direction for certifying the interoperability of IT and NSS pursuant to sections 2222, 2223, and 2224 of Title 10, United States Code (Reference (c)). Establishes a capability-focused, architecture-based approach for interoperability analysis. Establishes the governing policy and responsibilities for interoperability requirements development, test, certification and prerequisite for connection of IT, including NSS (referred to in this instruction as "IT"). Defines a doctrine, organization, training, materiel, leadership and education, personnel, facilities, and policy (DOTMLPF-P) approach to enhance life-cycle interoperability of IT. Establishes the requirement for enterprise services to be certified for interoperability. Incorporates and cancels DoDD 4630.05, DoDI 4630.8, and DoD Chief Information Officer (CIO) memorandum (References (d), (e), and (f)).
45.	AFMAN 17-1202 AFGM to AFMAN 33-145 Collaboration Services and Voice Systems Management	http://static.e-publishing.af.mil/production/1/saf_cio_a6/publication/afman17-1202/afman17-1202.pdf	It establishes procedures and guidance for Collaboration Services including electronic collaboration and management of Video Teleconferencing (VTC) resources to include systems, equipment, personnel, time, and money and provides the directive guidance for Air Force VTC and voice systems management activities.

NETWORK OPERATIONS AND INFRASTRUCTURE SOLUTIONS (COMPLIANCE)			
Standard		URL	Description
46.	DoDI 8520.02 Public Key Infrastructure (PKI) and Public Key (PK) Enabling	http://www.dtic.mil/whs/directives/corres/pdf/852002p.pdf	This instruction establishes and implements policy, assign responsibilities, and prescribe procedures for developing and implementing a DoD-wide PKI and enhancing the security of DoD information systems by enabling these systems to use PKI for authentication, digital signatures, and encryption.
47.	Installation Energy Management	http://www.dtic.mil/whs/directives/corres/pdf/417011p.pdf	ENERGY STAR is a joint program of the U.S. Environmental Protection Agency and the U.S. Department of Energy helping us all save money and protect the environment through energy efficient products and practices. It was enacted by Executive Order 13423 and governed by FAR 23.704.

NETWORK OPERATIONS AND INFRASTRUCTURE SOLUTIONS (COMPLIANCE)			
Standard		URL	Description
48.	Federal Information Security Management Act (FISMA) 2002	http://www.dhs.gov/federal-information-security-management-act-fisma	FISMA was enacted as part of the E-Government Act of 2002 to “provide a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support Federal operations and assets,” and also to “provide for development and maintenance of minimum controls required to protect Federal information and information systems.” FISMA requires Federal agencies to: •designate a Chief Information Officer (CIO), •delegate to the CIO authority to ensure compliance with the requirements imposed by FISMA, •implement an information security program, •report on the adequacy and effectiveness of its information security policies, procedures, and practices, •participate in annual independent evaluations of the information security program and practices, and •develop and maintain an inventory of the agency’s major information systems. FISMA requires the Director of the Office of Management and Budget (OMB) to ensure the operation of a central Federal information security incident center. FISMA makes the National Institute of Standards and Technology (NIST) responsible for “developing standards, guidelines, and associated methods and techniques” for information systems used or operated by an agency or contractor, excluding national security systems.

NETWORK OPERATIONS AND INFRASTRUCTURE SOLUTIONS (COMPLIANCE)			
Standard		URL	Description
49.	FedRAMP Security Controls for Cloud Service Providers	http://cloud.cio.gov/document/fedramp-security-controls	The attachment at the link contains a listing for the FedRAMP low and moderate baseline security controls, along with additional guidance and requirements for Cloud Service Providers. Those controls, guidance, and requirements are key standards for NetOps vendors to meet for any Cloud-related task orders that might have issues on NetOps.
50.	Homeland Security Presidential Directive 12 (HSPD 12)	http://www.dhs.gov/homeland-security-presidential-directive-12	Federal law signed by George Bush that directed promulgation of a Federal standard for secure and reliable forms of identification for Federal employees and contractors. Part two provides detailed specifications that will support technical interoperability among PIV systems of Federal departments and agencies. NIST has been designated as the approval and testing authority to certify products. FIPS 201 implements this policy.
51.	ICD 503, IT Systems Security, Risk Management, Certification and Accreditation	http://www.dni.gov/files/documents/ICD/ICD_503.pdf	This Intelligence Community Directive (ICD) establishes Intelligence Community (IC) policy for information technology systems security risk management, certification and accreditation. This ICD focuses on a more holistic and strategic process for the risk management of information technology systems, and on processes and procedures designed to develop trust across the intelligence community information technology enterprise through the use of common standards and reciprocally accepted certification and accreditation decisions.

NETWORK OPERATIONS AND INFRASTRUCTURE SOLUTIONS (COMPLIANCE)			
Standard		URL	Description
52.	IEEE/EIA 12207.0 Standard for Information Technology	http://IEEE.org	IEEE/EIA 12207.0, "Standard for Information Technology – Software Life Cycle Processes", is a standard that establishes a common framework for software life cycle process. This standard officially replaced MIL-STD-498 for the development of DoD software systems in May 1998.[1] Other NATO nations may have adopted the standard informally or in parallel with MIL-STD-498.This standard defines a comprehensive set of processes that cover the entire life-cycle of a software system—from the time a concept is made to the retirement of the software. The standard defines a set of processes, which are in turn defined in terms of activities. The activities are broken down into a set of tasks. The processes are defined in three broad categories: Primary Life Cycle Processes, Supporting Life Cycle Processes, and Organizational Life Cycle Processes.

NETWORK OPERATIONS AND INFRASTRUCTURE SOLUTIONS (COMPLIANCE)			
Standard		URL	Description
53.	AFI 17-100 AFGM to AFI 33-115 Air Force Information Technology (IT) Service management	http://static.e-publishing.af.mil/production/1/saf_cio_a6/publication/afi17-100/afi17-100.pdf	This Air Force instruction (AFI) implements Air Force Policy Directive (AFPD) 33-1, Information Resources Management. It sets forth policies regarding the official or authorized use of Government-provided electronic messaging systems on both Non-secure Internet Protocol Router Network (NIPRNet) and SECRET Internet Protocol Router Network (SIPRNet). It identifies the c(DMS) as the core-messaging system of record for the Air Force. It provides the roles, standards, and guidance relating to the messaging classes used by the Air Force: organizational DMS High Grade Service (HGS), and Simple Mail Transfer Protocol (SMTP) electronic mail (E-mail) messaging. This instruction applies to all Air Force organizations, personnel, Air National Guard, Air Force Reserve Command, and contractors regardless of the information classification transmitted or received. This instruction provides guidance to differentiate between record and non-record E-mail.
54.	ISO/IEC 20000	http://www.iso.org/iso/home.html	ISO/IEC 20000 is an international standard for IT Service Management (ITSM). It allows IT organizations to ensure the alignment between ITSM processes and their overall organization strategy. It requires the service provider to plan, establish, implement, operate, monitor, review, maintain and improve a service management system (SMS). ISO/IEC 20000 consist of 5 separate documents, ISO/IEC 20000-1 through 20000-5

NETWORK OPERATIONS AND INFRASTRUCTURE SOLUTIONS (COMPLIANCE)			
Standard		URL	Description
55.	ITU Recommendation H.320, Narrow-band Visual Telephone Systems and Terminal Equipment	http://www.itu.int/rec/T-REC-H.320	International Telecommunication Union recommendation that DoD requires for VTC and DISN Video Services equipment must meet. This standard sets BONDING (Bandwidth on Demand) algorithms to ensure bandwidth in proper increments. This included with FTR 1080B-2002.

NETWORK OPERATIONS AND INFRASTRUCTURE SOLUTIONS (COMPLIANCE)			
Standard		URL	Description
56.	CJCSI 6212.01F Interoperability and Supportability of Information Technology and National Security Systems	https://acc.dau.mil/CommunityBrowser.aspx?id=738675	Establishes policies and procedures for developing, coordinating, reviewing, and approving Information Technology (IT) and National Security System (NSS) Interoperability and Supportability (I&S) needs. Establishes procedures to perform I&S Certification of Joint Capabilities Integration and Development System (JCIDS) Acquisition Category (ACAT) programs/systems. Establishes procedures to perform I&S Certification of Information Support Plans (ISPs) and Tailored ISPs (TISPs) for all ACAT, non-ACAT and fielded programs/systems. Defines the five elements of the Net-Ready Key Performance Parameter (NR-KPP). Provides guidance for NR-KPP development and assessment. Establishes procedures for the Joint Interoperability Test Command (JITC) Joint Interoperability Test Certification. Adds the requirement from Joint Requirements Oversight Council Memorandum (JROCM) 010-08, 14 January 2008, “Approval to Incorporate Data and Service Exposure Criteria into the Interoperability and Supportability Certification Process” for reporting of data and service exposure information as part of I&S submissions.
57.	DODI 5015.02 DoD Records Management Program	http://www.dtic.mil/whs/directives/corres/pdf/501502p.pdf	Establishes policy and assigns responsibilities for the management of DoD records in all media, including electronic

NETWORK OPERATIONS AND INFRASTRUCTURE SOLUTIONS (COMPLIANCE)			
Standard		URL	Description
58.	Section 508 of the Rehabilitation Act of 1973	http://www.opm.gov/html/508-textOfLaw.asp	On August 7, 1998, President Clinton signed into law the Rehabilitation Act Amendments of 1998 which covers access to federally funded programs and services. The law strengthens section 508 of the Rehabilitation Act and requires access to electronic and information technology provided by the Federal Government. The law applies to all Federal agencies when they develop, procure, maintain, or use electronic and information technology. Federal agencies must ensure that this technology is accessible to employees and members of the public with disabilities to the extent it does not pose an "undue burden." Section 508 speaks to various means for disseminating information, including computers, software, and electronic office equipment. It applies to, but is not solely focused on, Federal pages on the Internet or the World Wide Web.

NETWORK OPERATIONS AND INFRASTRUCTURE SOLUTIONS (COMPLIANCE)

Standard		URL	Description
59.	DODD 8100.02 Use of Commercial Wireless Devices, Services, and Technologies in the DoD Information Network (DODIN)	http://www.dtic.mil/whs/directives/corres/pdf/810002p.pdf	Establishes policy and assigns responsibilities for the use of commercial wireless devices, services, and technologies in the DoD Global Information Grid (GIG) (DoD Directive 8100.1, "Global Information Grid (GIG) Overarching Policy," September 19, 2002). Directs the development and use of a Knowledge Management (KM) process to promote the sharing of wireless technology capabilities, vulnerabilities, and vulnerability mitigation strategies throughout the Department of Defense. Promotes joint interoperability using open standards throughout the Department of Defense for commercial wireless services, devices, and technological implementations.
60.	DODD 8100.1 Department of Defense Information Network (DoDIN) Overarching Policy	http://www.acq.osd.mil/ie/bei/pm/ref-library/dodd/d81001p.pdf	Establishes policy and assigns responsibilities for GIG configuration management, architecture, and the relationships with the Intelligence Community (IC) and defense intelligence components.

NETWORK OPERATIONS AND INFRASTRUCTURE SOLUTIONS (COMPLIANCE)			
Standard		URL	Description
61.	DODI 8320.02 Sharing Data, Information, and Information Technology (IT) Services in the Department of Defense	http://www.dtic.mil/whs/directives/corres/pdf/832002p.pdf	Establishes policies and responsibilities to implement data sharing, in accordance with Department of Defense Chief Information Officer Memorandum, “DoD Net-Centric Data Strategy,” May 9, 2003, throughout the Department of Defense. Directs the use of resources to implement data sharing among information capabilities, services, processes, and personnel interconnected within the Global Information Grid (GIG), as defined in DoD Directive 8100.1, “Global Information Grid (GIG) Overarching Policy,” September 19, 2002.
62.	Security Technical Implementation Guides (STIGs)	http://iase.disa.mil/stigs/Pages/index.aspx	The Security Technical Implementation Guides (STIGs) are the configuration standards for DoD IA and IA-enabled devices/systems. The STIGs contain technical guidance to 'lock down' information systems/software that might otherwise be vulnerable to a malicious computer attack.

NETWORK OPERATIONS AND INFRASTRUCTURE SOLUTIONS (COMPLIANCE)			
Standard		URL	Description
63.	Title 44 USC Section 3542	https://www.gpo.gov/fdsys/pkg/USCODE-2011-title44/pdf/USCODE-2011-title44-chap35-subchapIII-sec3542.pdf	(2)(A) The term “national security system” means any information system (including any telecommunications system) used or operated by an agency or by a contractor of an agency, or other organization on behalf of an agency— (i) the function, operation, or use of which— (I) involves intelligence activities; (II) involves cryptologic activities related to national security; (III) involves command and control of military forces; (IV) involves equipment that is an integral part of a weapon or weapons system; or (V) subject to subparagraph (B), is critical to the direct fulfillment of military or intelligence missions; or (ii) is protected at all times by procedures established for information that have been specifically authorized under criteria established by an Executive order or an Act of Congress to be kept classified in the interest of national defense or foreign policy. (B) Subparagraph (A)(i)(V) does not include a system that is to be used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications).

NETWORK OPERATIONS AND INFRASTRUCTURE SOLUTIONS (COMPLIANCE)

Standard		URL	Description
64.	Security Technical Implementation Guides (STIGs) CJCSI 6510.01F Information Assurance (IA) AND Support To Computer Network DEFENSE (CND)	http://www.dtic.mil/cjcs_directives/cdata/unlimit/6510_01.pdf	The Security Technical Implementation Guides (STIGs) and the NSA Guides are the configuration standards for DOD IA and IA-enabled devices/systems. Since 1998, DISA Field Security Operations (FSO) has played a critical role enhancing the security posture of DoD's security systems by providing the Security Technical Implementation Guides (STIGs). The STIGs contain technical guidance to "lock down" information systems/software that might otherwise be vulnerable to a malicious computer attack. DISA FSO is in the process of moving the STIGs towards the use of the NIST Security Content Automation Protocol (S-CAP) in order to be able to “automate” compliance reporting of the STIGs.
65.	CNSSI 1253: Security Categorization and Controls Selection for National Security Systems	http://disa.mil/Services/DoD-Cloud-Broker/~/media/Files/DISA/Services/Cloud-Broker/cnssi-security-categorization.pdf	Instruction serves as a companion document to NIST SP 800-53 for organizations that employ NSS.
66.	NIST SP 500-292: Cloud Computing Reference Architecture	http://disa.mil/Services/DoD-Cloud-Broker/~/media/Files/DISA/Services/Cloud-Broker/nist-cloud-ref-architecture.pdf	Overview of the five major roles & responsibilities using the Cloud Computing Taxonomy.
67.	NIST SP 800-146: Cloud Computing Synopsis & Recommendations	http://disa.mil/Services/DoD-Cloud-Broker/~/media/Files/DISA/Services/Cloud-Broker/nist-cloud-synopsis.pdf	NIST explains the cloud computing technology and provides recommendations for information technology decision makers.

NETWORK OPERATIONS AND INFRASTRUCTURE SOLUTIONS (COMPLIANCE)			
Standard		URL	Description
68.	NIST SP 800-145: Definition of Cloud Computing	http://disa.mil/Services/DoD-Cloud-Broker/~/media/Files/DISA/Services/Cloud-Broker/NIST-SP800145-DefinitionofCloudComputing.pdf	NIST provides a baseline for what cloud computing is and how to best use cloud computing. The services and deployment models are defined within this document.
69.	NIST SP 800-53: Security and Privacy Controls for Federal Information Systems and Organizations	http://disa.mil/Services/DoD-Cloud-Broker/~/media/Files/DISA/Services/Cloud-Broker/NIST-SP80053-SecurityandPrivacyControls.pdf	Guidelines for selecting and specifying security controls for organizations and information systems supporting the executive agencies of the federal Government to meet requirement FIPS Publication 200.
70.	Best Practices for Acquiring IT as a Service	http://disa.mil/Services/DoD-Cloud-Broker/~/media/Files/DISA/Services/Cloud-Broker/Creating-Effective-Cloud-Computing-Contracts-for-the-Federal-Government.pdf	Guidance on the implementations of shared services as well as navigate through the complex array of issues that are necessary to move to a shared service environment.
71.	Department of Defense Chief Information Officer Cloud Computing Strategy	http://dodcio.defense.gov/Portals/0/Documents/Cloud/DoD%20Cloud%20Computing%20Strategy%20Final%20with%20Memo%20-%20July%205%202012.pdf	This strategy is to enable the Department to increase secure information sharing and collaboration, enhance mission effectiveness, and decrease costs using cloud services.
72.	CNSSI 4009: National Information Assurance (IA) Glossary	https://www.cnss.gov/CNSS/openDoc.cfm?hulX3mO7fF1F/DGRf3R81A==	This revision of CNSSI 4009 incorporates many new terms submitted by the CNSS Membership. Most of the terms from the 2006 version of the Glossary remain, but a number of them have updated definitions in order to remove inconsistencies among the communities.
73.	Executive Order 13526: Classified National Security Information	https://www.ise.gov/resources/document-library/executive-order-13526-classified-national-security-information	This order prescribes a uniform system for classifying, safeguarding, and declassifying national security information, including information relating to defense against transnational terrorism.

NETWORK OPERATIONS AND INFRASTRUCTURE SOLUTIONS (COMPLIANCE)			
Standard		URL	Description
74.	Designation of the Defense Information Systems Agency as the Department of Defense Enterprise Cloud Service Broker	http://www.disa.mil/Services/DoD-Cloud-Broker/~/media/Files/DISA/Services/Cloud-Broker/disa-designation-memo.pdf	This memorandum establishes Defense Information Systems Agency (DISA) as the DoD Enterprise Cloud Service Broker.
75.	Interim Guidance Memorandum on Use of Commercial Cloud Computing Services	http://www.disa.mil/services/dod-cloud-broker/~/media/files/disa/services/cloud-broker/interim-guidance-memo-on-use-of-commerical-cloud-computing-services.pdf	This Memorandum serves to reinforce existing policy and processes, and is in effect for all DoD networks and systems.
76.	DoD Instructions, 8500 Series	http://www.dtic.mil/whs/directives/corres/ins1.html	DoD Issuances
77.	FIPS 199: Standards for Security Categorization of Federal Information and Information Systems	http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf	This publication is to develop standards for categorizing information and information systems.
78.	NIST SP 800-59: Guideline for Identifying an Information System as a National Security System	http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-59.pdf	The purpose of these guidelines is to assist agencies in determining which, if any, of their systems are national security systems as defined by FISMA and are to be governed by applicable requirements for such systems, issued in accordance with law and as directed by the President.

NETWORK OPERATIONS AND INFRASTRUCTURE SOLUTIONS (COMPLIANCE)

Standard		URL	Description
79.	NIST SP 800-66, Revision 1: An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule	http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-66r1.pdf	This Special Publication summarizes the HIPAA security standards and explains some of the structure and organization of the Security Rule. The publication helps to educate readers about information security terms used in the HIPAA Security Rule and to improve understanding of the meaning of the security standards set out in the Security Rule.
80.	NIST SP 800-88, Revision 1: Draft: Guidelines for Media Sanitization	http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf	This guide will assist organizations and system owners in making practical sanitization decisions based on the categorization of confidentiality of their information.
81.	NIST SP 800-122: Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)	http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-122.pdf	This document provides guidelines for a risk-based approach to protecting the confidentiality of PII. The recommendations in this document are intended primarily for U.S. Federal Government agencies and those who conduct business on behalf of the agencies, but other organizations may find portions of the publication useful.
82.	NIST SP 800-144: Guidelines on Security and Privacy in Public Cloud Computing	http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-144.pdf	The primary purpose of this report is to provide an overview of public cloud computing and the security and privacy considerations involved. It describes the threats, technology risks, and safeguards surrounding public cloud environments, and their treatment. It does not prescribe or recommend any specific cloud computing service, service arrangement, service agreement, service provider, or deployment model.

NETWORK OPERATIONS AND INFRASTRUCTURE SOLUTIONS (COMPLIANCE)			
Standard		URL	Description
83.	NIST SP 800-37, Revision 1: Guide for Applying the Risk Management Framework to Federal Information Systems	http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r1.pdf	The purpose of this publication is to provide guidelines for applying the Risk Management Framework to federal information systems to include conducting the activities of security categorization, security control selection and implementation, security control assessment, information system authorization, and security control monitoring.
84.	Defense Information Systems Agency, the Security Technical Implementation Guide (STIG)	http://iase.disa.mil/stigs/Pages/index.aspx	The Security Technical Implementation Guides (STIGs) are the configuration standards for DoD IA and IA-enabled devices/systems. The STIGs contain technical guidance to 'lock down' information systems/software that might otherwise be vulnerable to a malicious computer attack.

NETWORK OPERATIONS AND INFRASTRUCTURE SOLUTIONS (COMPLIANCE)			
Standard		URL	Description
85.	Cloud Computing Security Requirements Guide (SRG), Version 1	http://iase.disa.mil/cloud_security/Documents/u-cloud_computing_srg_v1r1_final.pdf	The 15 December 2014 DoD CIO memo regarding Updated Guidance on the Acquisition and Use of Commercial Cloud Computing Services defines DoD Component responsibilities when acquiring commercial cloud services. The memo allows components to responsibly acquire cloud services minimally in accordance with the security requirements outlined in Federal Risk and Authorization Management Program (FedRAMP) and this Security Requirement Guide (SRG). DISA previously published the concepts for operating in the commercial cloud under the Cloud Security Model. Version 1 defined the overall framework and provided initial guidance for public data. Version 2.1 added information for Controlled Unclassified Information. This document, the Cloud Computing Security Requirements Guide, SRG, documents cloud security requirements in a construct similar to other SRGs published by DISA for the DoD. This SRG incorporates, supersedes, and rescinds the previously published Security Model.
86.	Class Deviation - Contracting for Cloud Services (DFARS 239.99/252.239-7999)	http://www.acq.osd.mil/dpap/policy/policyvault/USA001321-15-DPAP.pdf	New requirements for contracting officers to follow in contracts, task orders, and delivery orders in acquisitions for, or that may involve cloud computing services.

NETWORK OPERATIONS AND INFRASTRUCTURE SOLUTIONS (COMPLIANCE)			
Standard		URL	Description
87.	Unified Capabilities Requirements 2013 (UCR 2013)	http://www.disa.mil/Network-Services/UCCO/Archived-UCR	This document specifies technical requirements for certification of approved products supporting voice, video, and data applications services to be used in Department of Defense networks to provide end-to-end Unified Capabilities (UC).
88.	Updated Guidance on the Acquisition and Use of Commercial Cloud Computing Services	http://www.doncio.navy.mil/Download.aspx?AttachID=5555	This memo clarifies and updates DoD guidance when acquiring commercial cloud services.
89.	NSTISSAM TEMPEST 2-95	http://en.wikipedia.org/wiki/RED/BLACK_concept	Also known as Red/Black Installation Guidance, it requires commercial telecommunications products that process classified information to be certified by the NSA Certified TEMPEST Products Program and addresses considerations for facilities where national security information is processed. The red/black concept refers to the careful segregation in cryptographic systems of signals that contain sensitive or classified plaintext information (red signals) from those that carry encrypted information, or cipher text (black signals). In NSA jargon, encryption devices are often called blackers, because they convert red signals to black. TEMPEST standards spelled out in NSTISSAM Tempest/2-95 specify shielding or a minimum physical distance between wires or equipment carrying or processing red and black signals.

NETWORK OPERATIONS AND INFRASTRUCTURE SOLUTIONS (COMPLIANCE)			
Standard		URL	Description
90.	AFMAN 17-1303 AFGM to AFMAN 33-285 Cybersecurity Workforce Improvement Program	http://static.e-publishing.af.mil/production/1/saf_cio_a6/publication/afman17-1303/afman17-1303.pdf	This rewrite identifies cybersecurity baseline certification requirements for the AF cybersecurity workforce; stipulates minimum certification requirements for various cyber roles and risk management positions; sets qualifications criteria; clarifies the cybersecurity-coding position process; and codifies the waiver policy for baseline certification requirements.
91.	AFGM 2015-33-01, End-of-Support Software Risk Management	http://static.e-publishing.af.mil/production/1/saf_cio_a6/publication/afgm2015-33-01/afgm2015-33-01.pdf	This Guidance Memorandum supersedes AFGM 2014-33-03, Microsoft Windows XP End-of-Life, and highlights current policies and SAF/CIO A6 authorities to mitigate cybersecurity vulnerabilities introduced by unsupported software. Compliance with this Memorandum is mandatory.
92.	Business and Enterprise Systems (BES) Process Directory	https://acc.dau.mil/bes	The BES Process Directory (BPD) is a life cycle management and systems engineering process based on the Integrated Defense Acquisition, Technology, and Logistics Life Cycle Management System; as tailored for Information Technology (IT) systems via the Defense Acquisition Process Model for Incrementally Fielded Software Intensive Programs
93.	DoDI 8540.01 Cross Domain (CD) Policy	http://www.dtic.mil/whs/directives/corres/pdf/854001p.pdf	Establishes policy, assigns responsibilities, and identifies procedures for the interconnection of information systems (ISs) of different security domains using CD solutions (CDSs) in accordance with the authority in DoD Directive (DoDD) 5144.02

NETWORK OPERATIONS AND INFRASTRUCTURE SOLUTIONS (COMPLIANCE)			
Standard		URL	Description
94.	DFARS: Network Penetration Reporting and Contracting for Cloud Services	https://www.federalregister.gov/articles/2015/08/26/2015-20870/defense-federal-acquisition-regulation-supplement-network-penetration-reporting-and-contracting-for	DoD is issuing an interim rule amending the DFARS to implement a section of the National Defense Authorization Act for Fiscal Year 2013 and a section of the National Defense Authorization Act for Fiscal Year 2015, both of which require contractor reporting on network penetrations. Additionally, this rule implements DoD policy on the purchase of cloud computing services.
95.	DoDD 8140.01 Cyberspace Workforce Management	http://www.dtic.mil/whs/directives/corres/pdf/814001_2015_dodd.pdf	Reissue and renumber DoDD 8570.01 to update and expand establish polices and assigned responsibilities for managing the DoD cyberspace workforce.
96.	DODI 4650.10 Land Mobile Radio (LMR) Interoperability and Standardization	http://www.dtic.mil/whs/directives/corres/pdf/814001_2015_dodd.pdf	Reissue and renumber DoDD 8570.01 to update and expand establish polices and assigned responsibilities for managing the DoD cyberspace workforce.
97.	AFI 11-260, Tactics Development Program.	http://static.e-publishing.af.mil/production/1/af_a3_5/publication/afi11-260/afi11-260.pdf	
98.	Air Force Instruction (AFI) 11-415, Weapons and Tactics Programs	http://static.e-publishing.af.mil/production/1/af_a3/publication/afi11-415/afi11-415.pdf	
99.	AFSPCI 10-415, Weapons and Tactics Programs	http://static.e-publishing.af.mil/production/1/afspc/publication/afspci10-415/afspci10-415.pdf	
100.	AFSPCI 10-260, Tactics Development Program	http://static.e-publishing.af.mil/production/1/afspc/publication/afspci10-260/afspci10-260.pdf	

APPENDIX 2 – DELIVERABLES AND STANDARDS

Deliverables

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

Applicable Documents and Standards

CDRL	CDRL TITLE	CDRL DESCRIPTION
A001	Meeting Minutes	The Contractor shall provide a Meeting Minutes in Memorandum format no later than 48hrs after meetings.
A002	After Action Report	The Contractor shall provide an After Action Report. The reports shall provide a brief overview of the event (i.e., exercise, installation) addressing who, what, why, where, when, and how of the event.
A003	Weekly Activity Report	The WAR should include current significant accomplishments, issues and problems for the current week.
A004	Quarterly Contract Summary Report	The report shall provide summary of all significant accomplishments and work performed by Contractor for current quarter.
A005	Weekly Vulnerability Status Reports	The report will provide a summary of all open Security Technical Implementation Guide (STIG) findings identified per week and status of remediation.
A006	Program Management Plan	The Contractor shall provide a Program Management Plan at contract start date and provide updates to the plan within three business days of personnel changes or updates.
A007	Trip Report	A detailed trip report shall be provided no later than 5 working days after completion of travel by Contractor.
A008	System Implementation Plan	The plan should include description and purpose of upgrades, steps to minimize adverse impact to organization missions.
A009	Preventive Maintenance Inspection (PMI) Schedule	The Contractor shall provide a Weekly Preventive Maintenance Inspection (PMI) Schedule.
A010	AFNet Baseline	The baseline will provide diagrams, database input and information export detailing system, software, hostname, application, relationship to connecting devices and function.

A011	Monthly Storage Report	The report should at minimum include consumption trends, remaining storage available, allocated usage data.
A012	Monthly Off-Site Status Report	The Off-site backup should include a copy of this report in off-site container with date delivered and POC who conducted delivery.
A013	Asset Management Database Report	The report should include hardware, warranty info, dates, locations, serial numbers, and ITAM account association.
A014	Interdependency Diagrams and Charts	The report should provide database input and information export detailing system, software, hostname application, relationship to connecting devices and function.
A015	Overdue Change Request Report	The report should include Change Request database export detailing at minimum, team, POC, summary, report date, last modified date and category.
A016	Monthly Warranty Report	The report should include all hardware warranties due to expire within 6 months.
A017	Software Inventory	The Contractor shall provide a monthly report documenting all software due to expire within 6 months and all software licensed to the 26 NOS.
A018	Ad Hoc Reports	The Contractor shall provide the unit with a Weekly Ad Hoc Report.
A019	All Circuit Utilization Report	The Contractor shall provide the unit with a Weekly All Circuit Utilization Report.
A020	Tool Feature Training Plan	This document will provide the operators a comprehensive view on how to perform all tasks associated with the tool.
A021	Mission Essential Services Plan	Plan describing how contractor will continue to perform mission critical services during periods of crisis.
A022	Quality Control Plan	The contractor must provide an acceptable Quality Control Plan in Contractor Format.
A023	Metadata Registry	The Contractor shall develop and support a MDR to hold metadata definitions for the various types of metadata in a persistent store that is accessible during runtime operations.
A024	Metadata Catalog	The Contractor shall develop and support Metadata Catalogs that include metadata to describe individual information assets and link those assets to the content delivery service that provides the asset to the end user.
A025	Metadata Service Registry	The contractor shall leverage existing service registry and provide support for a Service Registry where all services are registered and stores information about implemented services, service interfaces and the ports and bindings involved.
A026	Automated Metadata Population Service (AMPS)	The contractor shall develop and support an AMPS to automatically create the metadata for an

		information asset or service.
A027	A&A Package	The contractor must provide a monthly eMass A&A control review and update for all Plan of Action and Milestones of managed networks
A028	Tactical Intelligence Report	The Contractor shall provide a Tactical Intelligence Report that provide and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation.
A029	Cyberspace Threat Intelligence Report	The Contractor shall provide a Cyberspace Threat Intelligence Reports to protect, monitor, analyze, detect and respond to unauthorized activity with DoD information systems and computer networks.
A030	Cyberspace Malware and Forensics Report	The contractor shall provide a Cyberspace Malware and Forensics Report that discover, assess, explain, anticipate and deliver information, products and services provide mission assurance.
A031	Continuity of Operations Plan	The contractor shall maintain and update plans for catastrophic events, non-catastrophic events and work stoppages that covers each 26 NOS location.
A032	Emergency Resource Shutdown Plan	The contactor shall maintain and update Emergency Resource Shutdown Plans (ERSPs) for all 26 NOS controlled AFIN servers and services ensuring updates are incorporated whenever changes occur IAW local guidance.
A033	IPV6 Migration Plan	The contractor shall provide a plan to migrate the AFNet and AFIN to an IPv6 addressing scheme.
A034	Transition Plan	The contractor shall provide a plan that details its transition efforts to ensure an orderly transition and minimize any impact on the entire operation.
A035	Top Five Problem Report	The contractor shall provide a monthly report that identifies the problems that have caused multiple incidents.
A036	Impact Reduction Report	The contractor shall provide a monthly report detailing the workarounds that have been implemented to reduce the impact of incidents associated with the Top Five Problems.

APPENDIX 3: ACRONYMS

ACRONYM	Meaning in This Document
26 NOS	26 Network Operations Squadron
ACAT	Acquisition Category
ADS	Authoritative Data Sources
AF	Air Force
AFCAP	Air Force Certification and Accreditation Program
AFCERT	Air Force Computer Emergency Response Team
AFI	Air Force Instruction
AFMAN	Air Force Manual
AFPD	Air Force Policy Directive
AFRC	Air Force Reserve Command
AFRIMS	Air Force Records Information Management System
AFSO21	Air Force Smart Operations for the 21st Century
AFSPCI	Air Force Space Command Instruction
AFSWC	Headquarters Air Force Service Watch Cell
AMPS	Automated Metadata Population Services
ANG	Air National Guard
ASI	Authorized Service Interruption
AT	Anti-Terrorism
BES	Business and Enterprise Systems
BLOB	Binary Large Object
BMC	Basic Mission Capable
BPD	Business and Enterprise Systems Process Directory
BSA	Balanced Survivability Assessments
C&A	Certification and Accreditation
C2	Command and Control
CD	Cross Domain
CDRL	Contract Data Requirements List
CDS	Cross Domain Solutions
CES	Core Enterprise Services
CIO	Chief Information Officer
CND	Computer Network Defense
CND RA	Computer Network Defense Response Actions
COA	Course of Action
COI	Communities of Interest
COMPUSEC	Computer Security
COMSEC	Communications Security
COOP	Continuity of Operations
COTS	Commercial off the Shelf
CPAR	Contractor Performance Assessment Reporting
CS	Cyber Security

ACRONYM	Meaning in This Document
CT	Continuation Training
CUI	Controlled Unclassified Information
DD Form	Department of Defense Form
DDMS	Department of Defense Discovery Metadata Specification
DESMF	Department of Defense Enterprise Service Management Framework
DFARS	Defense Federal Acquisition Regulation Supplement
DGO	Defensive Global Information Grid (GIG) Operations
DISA	Defense Information Systems Agency
DISN	Defense Information Support Network
DMS	Defense Message System
DNS	Domain Name System
DoD	Department of Defense
DoDAF	Department of Defense Architecture Framework
DoDD	Department of Defense Directive
DoDI	Department of Defense Instruction
DODIN	Department of Defense Information Network
DoDM	Department of Defense Manual
DoDNetD	Department of Defense Information Network Network Defense
DOTMLPF-P	Doctrine, Organization, Training, Materiel, Leadership and Education, Personnel, Facilities, and Policy
DRM	Data Reference Model
DRU	Direct Reporting Units
E.O.	Executive Order
E3	Electromagnetic Environmental Effects
EA	Enterprise Architecture
ECA	External Certification Authority
EITDR	Enterprise Information Technology Data Repository
ELS	Enterprise Level Security
EM	Enterprise Management
F&O	Full and Open
FedRAMP	Federal Risk and Authorization Management Program
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
FOA	Field Operating Agency
FSO	Facility Security Officer
GI&S	Geospatial Information and Services
GIG	Global Information Grid
GTG-F	Global Information Grid Technical Guidance Federation
HGS	High Grade Service
HIPAA	Health Insurance Portability and Accountability Act
HSPD	Homeland Security Presidential Directive
I&S	Interoperability and Supportability
IA	Information Assurance
IC	Intelligence Community

ACRONYM	Meaning in This Document
ICD	Intelligence Community Directive
IG	Inherently Governmental
IMS	Integrated Management Suite
INFOCON	Information Operations Condition
IO	Information Operations
IP	Internet Protocol
IPv6	Internet Protocol Version 6
IQT	Initial Qualification Training
IS	Information System
ISP	Information Support Plan
IT	Information Technology
ITAM	Information Technology Asset Management
ITSM	Information Technology Service Management
JCA	Joint Capability Area
JCIDS	Joint Capabilities Integration and Development System
JELC	Joint Exercise Life Cycle
JITC	Joint Interoperability Test Command
JLLIS	Joint Lessons Learned Information System
JMS	Joint Management System
JOPES	Joint Operational Planning and Execution System
JROCM	Joint Requirements Oversight Council Memorandum
JRSS	Joint Regional Security Stacks
JTIMS	Joint Training Information Management System
KM	Knowledge Management
LMR	Land Mobile Radio
LRA	Local Registration Authority
MAJCOM	Major Command
MDE	Metadata Environment
MDR	Metadata Registry
MET	Mission Essential Task
MOA	Memorandums of Agreement
MOE	Measure of Effectiveness
MOP	Measure of Performance
MOU	Memorandums of Understanding
MQT	Mission Qualification Training
MR	Mission Ready
MSEL	Master Scenario Events List
NACI	National Agency Check Inquiry
NCSS	Net-Centric Services Strategy
ND	Network Defense
NESI	Net-Centric Enterprise Solutions for Interoperability
NetOps	Network Operations
NHO	New Hire Orientation
NIPR	Non-secure Internet Protocol Routing

ACRONYM	Meaning in This Document
NIPRNet	Non-Secure Internet Protocol Router Network
NISPOM	National Industrial Security Program Operating Manual
NIST	National Institute for Standards and Technologies
NR-KPP	Net-Ready Key Performance Parameter
NSS	National Security Systems
NTIA	National Telecommunications and Information Administration
ODC	Other Direct Cost
OMB	Office of Management and Budget
OOB	Out of Band
OPE	Operational Preparation of the Environment
OPR	Office of Primary Responsibility
OPREP	Operational Report
OPSEC	Operations Security
OTP	One-Time Password
OWL	Web Ontology Language
PDF	Portable Document Format
PII	Personally Identifiable Information
PK	Public Key
PKE	Public Key Enabled
PKI	Public Key Infrastructure
PR	Production Requirements
PRM	Process Reference Model
PSI	Personnel Security Investigation
PWCS	Personal Wireless Communication Systems
QoS	Quality of Service
RDS	Records Disposition Schedule
RFI	Requests for Information
RMF	Risk Management Framework
ROC	Rehearsal of Concept
RRMC	Raven Rock Mountain Complex
RT	Requalification Training
S	Secret
S/SCI	Secret Sensitive Compartmented Information
SA	Situational Awareness
SAF/CIO	Secretary of the Air Force Chief Information Officer
SAML	Security Assertion Markup Language
SAP	Self-Assessment Program
SB	Small Business
SBIR	Small Business Innovation Research
S-CAP	Security Content Automation Protocol
SCI	Sensitive Compartmented Information
SCOER	Standard Center of Excellence Repository
SDP	Service Delivery Point
SDS	Services Delivery Summary

ACRONYM	Meaning in This Document
SE	Systems Engineering
SEI	Software Engineering Institute
SIPR	Secret Internet Protocol Routing
SIPRNet	Secret Internet Protocol Routing Network
SISSU	Security, Interoperability, Supportability, Sustainability and Usability
SME	Subject Matter Expert
SMI	Singularly Managed Infrastructure
SMI-ELS	Singularly Managed Infrastructure with Enterprise Level Security
SMQ	Special Mission Qualified
SMS	Service Management System
SMTP	Simple Mail Transport Protocol
SQL	Structured Query Language
SRG	Security Requirement Guide
SRM	System Reference Model
SSL	Secure Socket Layer
STIG	Security Technical Implementation Guide
T&E	Test and Evaluation
TCNO	Time Compliance Network Order
TISP	Tailored Information Support Plan
TO	Technical Order
TRB	Tactics Review Board
TRM	Technical Reference Model
TS	Top Secret
TS/SCI	Top Secret Sensitive Compartmented Information
TLS	Transport Layer Security
TTP	Tactics Techniques and Procedures
U.S.C.	United States Code
UC	Unified Capabilities
UCNI	Unclassified Controlled Nuclear Information
UCR	Unified Capabilities Requirement
USMCEB	United States Military Communications-Electronics Board
UTO	Unit Training Objective
VTC	Video Teleconference
W&T	Weapons and Tactics
WEPTAC	Weapons and Tactics
WS	Web Services
WSDL	Web Services Description Languages
XKMS	Extensible Markup Language Key Management
XML	Extensible Markup Language
XSD	Extensible Markup Language Schema Definition

APPENDIX 4: DODIN OPERATIONS CERTIFICATION REQUIREMENTS

NOTE: PWS Paragraph references include sub-paragraphs where applicable.

System Administration Certifications				
Vendor	Minimum	Preferred	Reach Back Capability	PWS Paragraph References
VMWare	VMware Certified Professional 6 - Data Center Virtualization (VCP6-DCV)	VMware Certified Advanced Professional 6 – Data Center Virtualization Deploy (VCAP6-DCV Deploy)	VMware Certified Advanced Professional 6 – Data Center Virtualization Deploy (VCAP6-DCV Deploy)	3.1.1; 3.2.1.1; 3.2.1.2.1; 3.2.1.2.2; 3.2.1.2.3; 3.2.1.4; 3.2.1.5
Microsoft	Microsoft Certified Solutions Associate (MCSA): Windows Server 2012 **OR** MCSA: Windows Server 2016	Microsoft Certified Solutions Expert (MCSE): Server Infrastructure **OR** Microsoft Certified Solutions Expert (MCSE) Cloud Platform and Infrastructure	Microsoft Certified Solutions Expert (MCSE) Cloud Platform and Infrastructure	3.1.1; 3.2.1.1; 3.2.1.2.1; 3.2.1.2.2; 3.2.1.2.3; 3.2.1.4; 3.2.1.5
Microsoft	MCSA: Windows Server 2012 **OR** MCSA: Windows Server 2016	1. MCSE: Productivity Solutions Expert 2. MCSE: Data Management and Analytics	1. MCSE: Productivity Solutions Expert 2. MCSE: Data Management and Analytics	3.1.1; 3.2.1.1; 3.2.1.2.1; 3.2.1.2.2; 3.2.1.2.3; 3.2.1.4; 3.2.1.5
Microsoft	MCSA: Windows Server 2012 **OR** MCSA: Windows Server 2016	Microsoft Certified Technology Specialist (MCTS): Administering and Deploying System Center 2012 Configuration Manager (SCCM)		3.1.1; 3.2.1.1; 3.2.1.2.1; 3.2.1.2.2; 3.2.1.2.3; 3.2.1.4; 3.2.1.5
Storage Certifications				
Vendor	Minimum	Preferred	Reach Back Capability	PWS References
Dell EMC NetApp	1. EMC Storage Administrator (EMCSA) Specialist: SAN Specialty 2. NetApp Certified Data Administrator (NCDA) Professional, ONTAP	NetApp Certified Implementation Engineer (NCSE) – SAN Specialist, ONTAP **OR** NetApp Certified Implementation Engineer (NCSE) – Data Protection Specialist **OR** NetApp Certified Implementation Engineer (NCSE) – SAN	NetApp Certified Support Engineer (NCSE) Professional	3.1.1; 3.2.1.1; 3.2.1.2.1; 3.2.1.2.2; 3.2.1.2.3; 3.2.1.4; 3.2.1.5

		Specialist, Data ONTAP 7-Mode **OR** NetApp Certified Implementation Engineer (NCSE) – SAN Specialist, E-Series		
Disaster Recovery Certifications				
Vendor	Minimum	Preferred	Reach Back Capability	PWS References
Veritas	1. Veritas Certified Specialist (VCS): Administration of Veritas Backup 2. VCS: Administration of NetBackup and Appliances 3. VCS: Administration of Veritas Backup Exec	Veritas Certified Professional: Data Protection		3.1.1; 3.2.1.1; 3.2.1.2.1; 3.2.1.2.2; 3.2.1.2.3; 3.2.1.4; 3.2.1.5
Linux Certifications				
Vendor	Minimum	Preferred	Reach Back Capability	PWS References
Red Hat	Red Hat Certified System Administrator (RHCSA)	Red Hat Certified Engineer (RHCE)		3.1.1; 3.2.1.1; 3.2.1.2.1; 3.2.1.2.2; 3.2.1.2.3; 3.2.1.4; 3.2.1.5
Web Developer Certifications				
Vendor	Minimum	Preferred	Reach Back Capability	PWS References
Microsoft	Microsoft Technology Associate (MTA): Software Development Fundamentals	Microsoft Certified Solutions Developer (MCSD): App Builder **OR** MCSA Web Applications		3.1.1; 3.2.1.1; 3.2.1.2.1; 3.2.1.2.2; 3.2.1.2.3; 3.2.1.3; 3.2.1.4; 3.2.1.5
Database Administrator Certifications				
Vendor	Minimum	Preferred	Reach Back Capability	PWS References
Microsoft	MCSA: SQL Server 2012/2014	MCSE: Data Management and Analytics		3.1.1; 3.2.1.1; 3.2.1.2.1; 3.2.1.2.2; 3.2.1.2.3; 3.2.1.3; 3.2.1.4; 3.2.1.5
Configuration Management Certifications				
Vendor	Minimum	Preferred	Reach Back Capability	PWS References

N/A	ITIL Intermediate – Service Strategy ITIL Intermediate – Service Design ITIL Intermediate – Service Transition ITIL Intermediate – Service Operation ITIL Intermediate – Continual Service Improvement	ITIL Intermediate - Operational Support and Analysis ITIL Intermediate - Planning, Protection, and Optimization ITIL Intermediate - Release, Control, and Validation ITIL Intermediate - Service Offerings and Agreements	ITIL Master	3.1; 3.2; 3.3
Infrastructure Certifications				
Vendor	Minimum	Preferred	Reach Back Capability	PWS References
Cisco	Cisco Certified Network Associate (CCNA): Routing and Switching	Cisco Certified Network Professional (CCNP): Routing and Switching	Cisco Certified Internetwork Expert (CCIE): Routing and Switching	3.1.1; 3.2.1.1; 3.2.1.2.1; 3.2.1.2.2; 3.2.1.2.3; 3.2.1.4; 3.2.1.5
Host Base Security System (HBSS) Certifications				
Vendor	Minimum	Preferred	Reach Back Capability	PWS References
DISA	1. HBSS Admin 2. HBSS Reviewer 3. HBSS Analyst 4. HBSS Auditor			3.1.1; 3.2.1.1; 3.2.1.2.1; 3.2.1.2.2; 3.2.1.2.3; 3.2.1.4; 3.2.1.5
DNS Certifications				
Vendor	Minimum	Preferred	Reach Back Capability	PWS References
N/A	Certified DNS/BIND Professional (DNS/CP) DNSSEC Professional	Certified DNSSEC Expert (DNS/CDE)	Certified DNSSEC Expert (DNS/CDE) Certified IPv6 Associate (IPv6/CA)	3.1.1; 3.2.1.1; 3.2.1.2.1; 3.2.1.2.2; 3.2.1.2.3; 3.2.1.4; 3.2.1.5
Infoblox	Core Network 2016 Advanced Services Expert Accreditation	Core Network 2016 Expert Services Expert Accreditation	Core Network 2016 Expert Services Expert Accreditation	3.1.1; 3.2.1.1; 3.2.1.2.1; 3.2.1.2.2; 3.2.1.2.3; 3.2.1.4; 3.2.1.5
Routing and Firewall Certifications				
Vendor	Minimum	Preferred	Reach Back Capability	PWS References

CISCO	Cisco Certified Network Professional (CCNP): Routing and Switching		Cisco Certified Internetwork Expert (CCIE): Routing and Switching	3.1.1; 3.2.1.1; 3.2.1.2.1; 3.2.1.2.2; 3.2.1.2.3; 3.2.1.4; 3.2.1.5
Juniper	Juniper Networks Certified Professional Enterprise Routing and Switching (JNCIP-ENT)		Juniper Networks Certified Expert Enterprise Routing and Switching (JNCIE-ENT)	3.1.1; 3.2.1.1; 3.2.1.2.1; 3.2.1.2.2; 3.2.1.2.3; 3.2.1.4; 3.2.1.5
CISCO	CCNA: Security	CCNP: Security	CCNP: Security	3.1.1; 3.2.1.1; 3.2.1.2.1; 3.2.1.2.2; 3.2.1.2.3; 3.2.1.4; 3.2.1.5
Palo Alto	Palo Alto Networks Certified Network Security Engineer (PCNSE) 7		Palo Alto Networks Certified Network Security Engineer (PCNSE) 7	3.1.1; 3.2.1.1; 3.2.1.2.1; 3.2.1.2.2; 3.2.1.2.3; 3.2.1.4; 3.2.1.5
Global Information Assurance Certification (GIAC)	GIAC Certified Perimeter Protection Analyst (GPPA)		GIAC Certified Perimeter Protection Analyst (GPPA)	3.1.1; 3.2.1.1; 3.2.1.2.1; 3.2.1.2.2; 3.2.1.2.3; 3.2.1.4; 3.2.1.5
Web Proxy Certifications				
Vendor	Minimum	Preferred	Reach Back Capability	PWS References
BlueCoat	Blue Coat Certified ProxySG Administrator (BCCPA)	Blue Coat Certified Proxy Professional (BCCPP)	Blue Coat Certified Proxy Professional (BCCPP)	3.1.1; 3.2.1.1; 3.2.1.2.1; 3.2.1.2.2; 3.2.1.2.3; 3.2.1.4; 3.2.1.5
Traffic Management Certifications				
Vendor	Minimum	Preferred	Reach Back Capability	PWS References
F5	1. F5 Certified Technology Specialist (F5-CTS) – Local Traffic Manager (LTM) 2. F5-CTS-Global Traffic Manager (GTM)		F5 Certified Solution Expert (F5-CSE)	3.1.1; 3.2.1.1; 3.2.1.2.1; 3.2.1.2.2; 3.2.1.2.3; 3.2.1.4; 3.2.1.5

	3. F5-CTS-Application Security Manager (ASM) 4. F5-CTS- Access Policy Manager (APM)			
Network Analysis Certifications				
Vendor	Minimum	Preferred	Reach Back Capability	PWS References
Splunk	Splunk Certified Admin	Splunk Certified Architect	Splunk Certified Architect	3.1.1; 3.2.1.1; 3.2.1.2.1; 3.2.1.2.2; 3.2.1.2.3; 3.2.1.4; 3.2.1.5
Riverbed (one from Minimum and one from Preferred)	1. Riverbed Certified Solutions Associate (RCSA)-Wan Optimization (W) Blueprint 2. RCSA-Network Performance Management (NPM) Blueprint 3. RCSA-Application Performance Management (APM) Blueprint 4. RCSA-Hyper-Converged Branch (HCB) Blueprint 5. RCSA-Network Planning and Configuration Management (NPCM) Blueprint	1. Riverbed Certified Solutions Professional (RCSP)-W Blueprint 2. RCSP-NPM Blueprint 3. RCSP-APM Blueprint 4. RCSP-HCB Blueprint	1. Riverbed Certified Solutions Professional (RCSP)-W Blueprint 2. RCSP-NPM Blueprint 3. RCSP-APM Blueprint 4. RCSP-HCB Blueprint	3.1.1; 3.2.1.1; 3.2.1.2.1; 3.2.1.2.2; 3.2.1.2.3; 3.2.1.4; 3.2.1.5
InfoVista	InfoVista Certified Administrator (IVCA)	Certified Developer (IVCD) 4.2	Certified Developer (IVCD) 4.2	3.1.1; 3.2.1.1; 3.2.1.2.1; 3.2.1.2.2; 3.2.1.2.3; 3.2.1.4; 3.2.1.5

Hewlett Packard Enterprise	1. HP Accredited Technical Professional (ATP) - ArcSight Security V1 2. HP ASE-ArcSight Logger V1	1. Hewlett Packard Accredited Solutions Expert (HP ASE) - ArcSight Analyst V1 2. HP Master ASE - ArcSight Security V2	1. Hewlett Packard Accredited Solutions Expert (HP ASE) - ArcSight Analyst V1 2. HP Master ASE - ArcSight Security V2	3.1.1; 3.2.1.1; 3.2.1.2.1; 3.2.1.2.2; 3.2.1.2.3; 3.2.1.4; 3.2.1.5
WireShark	Wireshark Certified Network Analyst (WCNA)			3.1.1; 3.2.1.1; 3.2.1.2.1; 3.2.1.2.2; 3.2.1.2.3; 3.2.1.4; 3.2.1.5
IBM	IBM Certified Associate - Tivoli Netcool/OMNIbus V7.4			3.1.1; 3.2.1.1; 3.2.1.2.1; 3.2.1.2.2; 3.2.1.2.3; 3.2.1.4; 3.2.1.5
Other Network Industry Certifications				
Vendor	Minimum	Preferred	Reach Back Capability	PWS References
Red Seal	1. RedSeal Network Expert 2. RedSeal Security Expert	1. RedSeal Network Administrator 2. RedSeal Security Administrator	1. RedSeal Network Administrator 2. RedSeal Security Administrator	3.1.1; 3.2.1.1; 3.2.1.2.1; 3.2.1.2.2; 3.2.1.2.3; 3.2.1.4; 3.2.1.5
Lancope	Cisco Stealthwatch Advanced Tuning (SWAT)	Cisco Stealthwatch Proactive Hunting and Detection (PHD)	Cisco Stealthwatch PHD	3.1.1; 3.2.1.1; 3.2.1.2.1; 3.2.1.2.2; 3.2.1.2.3; 3.2.1.4; 3.2.1.5

APPENDIX 5: AFINC WEAPON SYSTEM TOOLS

TOOL	DESCRIPTION
26 NOS DASHBOARD or similar	An SNMP poller written by 26 NOS support contract staff that serves as the information source for the Dashboard tool that is displayed on the data wall for the operators.
ArcSight or similar	Tool used for log collection.
Bluecoat Director or similar	Tool is used to manage Bluecoat Proxies.
CACTI or similar	Web-based RRDTool Bandwidth and CPU monitoring application that uses SNMP to poll network devices.
Cascade or similar	Tool used for WAN optimization, log collection and NetFlow collection.
CISCO ACS or similar	Used for TACACS+ and Radius Authentication
CISCO Security Manager or similar	Tool used to manage a wide range of Cisco security devices, gain visibility across the network deployment, and share information with other essential network services.
Cisco UCS or similar	MPLS deployment and configuration tool.
CSG Data Orchestrator	Situational Awareness
eHealth or similar	SNMP based tool used to monitor all network devices on the 26 NOS network (CPU utilization, BW utilization, CPU temperature, errors, discards, etc).
Gigamon GigaVUE	Tool used for network visibility.
Infoblox Manager or similar	Enterprise DNS manager.
Lancope StealthWatch or similar	Tool to manage Joint Information Management Suite (JIMS).
Logman/logwatch or similar	This tool displays a scrolling log on the data wall for the operators
Nagios or similar	Agentless Server Monitoring.
Netcool or similar (InfoVista/Spectrum)	IBM manager of managers (MOM) which receives traps from various tools for a "single pane of glass" view.
NetIQ or similar	Agent based server monitoring
NetQoS or similar	Cisco-developed tool that collects Netflow technology.
Netwitness	
Nominum Manager or similar	Enterprise DNS manager.
Panorama or similar	Tool used for Palo Alto Management and Palo Alto Log collection.
Quest Password Manager or similar	The tool automatically updates network device passwords and securely stores them and is used to remotely manage all network tools.
RedHat/Linux Software Update	
RedSeal	Tool used to obtain network visibility and identify attack risks and non-compliance.
Remedy	Trouble Ticket System.
Retina or similar	Tool used for vulnerability scanning.

SCAT or similar	UNIX vulnerability management.
Microsoft SCCM or similar	Tool used for Windows patching.
Solarwinds Application Manager or similar	IT Management tool where the following modules are in use currently: Server & Application Monitor; Network Performance Monitor; IP Address Manager; IP Control Bundle; Network Configuration Manager; and Server and Application Monitor.
Sourcefire Defense Center or Similar (Bro/Fidelis/InQuest)	Tool used to centrally manage hundreds of appliances and analyze events, automate threat prevention updates, configure policies, and generate reports and custom dashboards.
Splunk or similar	Tool used to search through the logs of various systems that are logging to our syslog collectors.
Lancope StealthWatch (Argus) or similar	Tool user to add/remove interfaces that need to be monitored/ create /schedule custom reports.
Tipping Point	Assist Troubleshooting ability.
VMware VCenter or similar	Tool used to manage VMware environments.
Veritas or similar	Tool used for data recovery and back up.

APPENDIX 6: AFINC WEAPON SYSTEM EQUIPMENT

DEVICES	TYPE OF NETWORK	NUMBER OF DEVICES SUPPORT
NIPR ROUTERS		
Gateway/IMS Routers	NIPR	50
SDP Routers	NIPR	203
ADX Routers	NIPR	38
DECC Routers	NIPR	18
AMC Routers	NIPR	13
JRSS Routers	NIPR	234
MISC Routers	NIPR	31
MISC Switches	NIPR	116
TOTAL NIPR ROUTERS		**703**
SIPR ROUTERS		
SDP Routers	SIPR	242
C2 NODES Routers	SIPR	2
JRSS Routers	SIPR	160
MISC Routers	SIPR	37
MISC Switches	SIPR	16
TOTAL SIPR ROUTERS		**457**
TOTAL ROUTERS SUPPORTED		**1160**
NIPR INFRASTRUCTURE DEVICES		
Switches	NIPR	51
Environmental Monitors	NIPR	18
SRLCO	NIPR	18
KVM	NIPR	42
UPS	NIPR	20
NTP	NIPR	18
ACS Appliance	NIPR	2
TOTAL NIPR INFRASTRUCTURE DEVICES		**169**
SIPR INFRASTRUCTURE DEVICES		
Switches	SIPR	13
Routers	SIPR	2
NTP	SIPR	1
ACS Appliance	SIPR	2
SRLCO	SIPR	1
TOTAL SIPR INFRASTRUCTURE DEVICES		**19**
TOTAL INFRASTRUCTURE DEVICES SUPPORTED		**188**
NIPR SYSTEM ADMINISTRATION DEVICES		
IMS Servers	NIPR	96
Gateway Servers	NIPR	288
IMS Workstations	NIPR	172

TOTAL NIPR SYSTEM ADMINISTRATION DEVICES		**556**
SIPR SYSTEM ADMINISTRATION DEVICES		
Servers	SIPR	49
26 NOS IS Servers	SIPR	43
SIPR Workstations	SIPR	140
AOL Workstations	SIPR	9
TOTAL SIPR SYSTEM ADMINISTRATION DEVICES		**241**
TOTAL SYSTEM ADMINISTRATION DEVICES		**797**
DNS OPS NIPR DEVICES		
NOMINUM Authoritative Name Server Masters	NIPR	2
NOMINUM Authoritative Name Servers	NIPR	16
NOMINUM Vantios Caching Name Servers	NIPR	32
EMAIL Gateways	NIPR	44
EMAIL Gateway Control Centers	NIPR	10
TOTAL NIPR DNS OPS DEVICES		**104**
DNS OPS SIPR DEVICES		
Domain Name Servers	SIPR	3
TOTAL SIPR DNS OPS DEVICES		**3**
TOTAL DNS DEVICES SUPPORTED		**107**
VoSIP Devices		
CUCM Servers	SIPR	5
PHONES CONFIGURED	SIPR	551
TOTAL VoSIP DEVICES		**556**
TOTAL VoSIP DEVICES SUPPORTED		**556**
NIPR NETWORK SECURITY DEVICES		
PALO ALTO	NIPR	70
PANORAMA	NIPR	2
BLUECOAT Director	NIPR	2
BLUECOAT Proxies	NIPR	69
BLUECOAT AV (ANTIVIRUS)	NIPR	68
BLUE COAT SSL Visibility Appliance	NIPR	1
SSL Encryptor/Decryptor	NIPT	104
Load Balancers	NIPR	344
ASA (Adaptive Security Device)	NIPR	53
TOTAL NIPR NETWORK SECURITY DEVICES		**713**
SIPR NETWORK SECURITY DEVICES		
PALO ALTO	SIPR	128
PANORAMA	SIPR	1
ASA (Adaptive Security Device)	SIPR	18
TOTAL SIPR NETWORK SECURITY DEVICES		**147**
TOTAL NETWORK SECURITY DEVICES		**860**
TOTAL NETWORK DEVICES SUPPORTED		**3668**

APPENDIX 7: PERFORMANCE THRESHOLD STANDARDS

Item #	Performance Requirements	Performance Threshold	Surveillance Methods
NETWORK INFRASTRUCTURE SUPPORT			
1	Network availability	At least 99.9% availability for the base portion of the JRSS. The network should not experience downtimes, planned or unplanned, that exceed 1 minute, 26 seconds in day; 10 minutes, 5 seconds in a week; 43 minutes, 50 seconds in a month; and 8 hours, 45 minutes, 57 seconds in a year.	Automated Reports, Random Sampling, 100% Inspection, Periodic Inspection, QAE monthly review of contractor metrics
2	Circuit Utilization	Balance bandwidth within +/- 20% of each redundant circuit.	Automated Reports, Random Sampling, 100% Inspection, Periodic Inspection, QAE monthly review of contractor metrics
3	Backbone or Infrastructure Return to Service	Service (i.e. network, point-to-point, VPN, bulk encryption connectivity, etc.) restored within two (2) hours of notification, automated (i.e. Solarwinds or Nagios) or otherwise (i.e. phone or person)	Automated Reports, Random Sampling, 100% Inspection, Periodic Inspection, QAE monthly review of contractor metrics
4	Server availability	At least 99.9% availability. The server should not experience downtimes, planned or unplanned, that exceed 1 minute, 26 seconds in day; 10 minutes, 5 seconds in a week; 43 minutes, 50 seconds in a month; and 8 hours, 45 minutes, 57 seconds in a year.	Automated Reports, Random Sampling, 100% Inspection, Periodic Inspection, QAE monthly review of contractor metrics
5	Availability of Mission Critical Servers	Maintain critical system availability by conducting synthetic transactions -- system connectivity will be >99%	Automated Reports, Random Sampling, 100% Inspection, Periodic Inspection, QAE monthly review of contractor metrics
6	System availability	Ensure at least 99.9% system availability for all systems in the AFIN/AFNet. The system should not experience downtimes, planned or unplanned, that exceed 1 minute, 26 seconds in day; 10 minutes, 5 seconds in a week; 43 minutes, 50 seconds in a month; and 8 hours, 45 minutes, 57 seconds in a year.	Automated Reports, Random Sampling, 100% Inspection, Periodic Inspection, QAE monthly review of contractor metrics

7	System Return to Service	Restored within 4 hours of notification, at least 95% of the time	Automated Reports, Random Sampling, 100% Inspection, Periodic Inspection, QAE monthly review of contractor metrics
8	Core Network Device Performance	a. Ensure network devices have the bandwidth to support a failover and handle total traffic from multiple Service Delivery Points (SDPs). b. Ensure primary and secondary SDPs are load balanced with utilization below 50%. c. Ensure routing devices maintain a packet loss of <4%. d. Identify and resolve degraded routing within 30 minutes of alert, at least 90% of time.	
9	Network perimeter defense	Implement firewall ruleset changes within 2 hours of receipt of change requirement. Track and report monthly number of attempted/successful unclassified/classified network penetrations.	Automated Reports, Random Sampling, 100% Inspection, Periodic Inspection, QAE monthly review of contractor metrics
10	Accuracy of the network architecture drawings	All changes to network architecture drawings shall be updated within one week of approved change.	Automated Reports, Random Sampling, 100% Inspection, Periodic Inspection, QAE monthly review of contractor metrics
11	Perform TCNOs/TCTOs and NOTAMS as directed	a. Changes shall successfully deploy to 80% of the machines on first try. A POA&M shall be submitted within three (3) days of deployment for remediation of the remaining 20%. b. Systems shall be compliant with requirements and completed IAW TCNOs, TCTOs, and NOTAMs. d. Track and complete TCNO implementation within 30 days of receipt or by the indicated TCNO closeout date, whichever is sooner, unless an AFCERT TCNO extension is coordinated and approved in advance.	Automated Reports, Random Sampling, 100% Inspection, Periodic Inspection, QAE monthly review of contractor metrics
12	Network and system outages	Schedule and coordinate any outages IAW 26 NOS local job guides.	Automated Reports, Random Sampling, 100% Inspection, Periodic Inspection,

			QAE monthly review of contractor metrics
ENTERPRISE SERVICES			
13	Configuration Management database updates and accuracy	a. The Configuration Management Database (CMDB) shall be updated with new systems or software within 2 duty days of installation/implementation. b. Configuration management database includes all systems and software and a 98% accuracy rate is maintained at all times.	Automated Reports, Random Sampling, 100% Inspection, Periodic Inspection, QAE monthly review of contractor metrics
14	IA incident reporting/response action	Provide initial response to incidents within 15 minutes of identification during normal duty hours.	Automated Reports, Random Sampling, 100% Inspection, Periodic Inspection, QAE monthly review of contractor metrics
15	IA INFOCON action	Implement INFOCON related actions within 2 hours of notification of a change in the INFOCON level.	Automated Reports, Random Sampling, 100% Inspection, Periodic Inspection, QAE monthly review of contractor metrics
16	Problem Management Resolution	a. Identify problems that have caused multiple incidents and create a Top Five Problem report by the 3rd of every month for the previous month. (CDRL: A035 - Top Five Problem Report) b. Implement workarounds that reduce and/or eliminate the impact of incidents associated with the previous month's top five problems and create a report detailing impact reduction by the first day of each quarter of the FY (October, January, April, and July). (CDRL: A036-Impact Reduction Report) c. Initiate changes that reduce the number of incidents associated with the previous month's top five problems and reduce and/or eliminate the backlog of outstanding problems.	Automated Reports, Random Sampling, 100% Inspection, Periodic Inspection, QAE monthly review of contractor metrics
17	Asset Management: Hardware and Software Inventory Accuracy	a. Ensure that asset information is current and accurate to include the tracking, reporting, and disposal, as required, of resources and general-purpose computer assets, vendor coordination and administering licenses for System Software and	Automated Reports, Random Sampling, 100% Inspection, Periodic Inspection, QAE monthly review of contractor metrics

		maintenance agreements of the assets. b. IT system inventories include all systems and software and a 98% accuracy rate is maintained at all times c. Inventory database 95% accurate w/10 day correction period on average for audits throughout the period	
18	Application Maintenance	Between 95 percent and 98 percent of scheduled upgrades and/or maintenance are executed according to schedule For non-mission critical applications, between 80 percent and 90 percent of requests for unscheduled software maintenance are responded to within 48 hours For critical mission applications, 95 percent and 100 percent of requests are responded to within 2 hours	Automated Reports, Random Sampling, 100% Inspection, Periodic Inspection, QAE monthly review of contractor metrics
SYSTEM ADMINISTRATION			
19	Storage Management	a. Restore systems to requested good configuration upon request. b. Maintain at least (1) year of backed up information. c. Transport mission critical data to an offsite Government storage facility and store for a period of one (1) calendar year. d. The storage environment is available 99.9% monthly. The environment should not experience downtimes, planned or unplanned, that exceed 1 minute, 26 seconds in day; 10 minutes, 5 seconds in a week; 43 minutes, 50 seconds in a month; and 8 hours, 45 minutes, 57 seconds in a year. e. Storage usage and capacity does not exceed 90%.	Automated Reports, Random Sampling, 100% Inspection, Periodic Inspection, QAE monthly review of contractor metrics
20	Enterprise Storage Utilization	< 20% free space left on a logical storage partition (the logical partition can still be increased) > 90% free space for a logical partition that has been there for over 3 months (so there is logical space that could be better allocated) < 35 % on a physical storage partition	Automated Reports, Random Sampling, 100% Inspection, Periodic Inspection, QAE monthly review of contractor metrics

21	Disaster Recovery	a. Nightly backups to be completed 99% of the time. b. Tests of the disaster recovery be completed on schedule 99% of the time	Automated Reports, Random Sampling, 100% Inspection, Periodic Inspection, QAE monthly review of contractor metrics
22	Spare Disks	No spares (or RAID sets are running “one disk down”)	Automated Reports, Random Sampling, 100% Inspection, Periodic Inspection, QAE monthly review of contractor metrics
23	“Hot” Disks	Hot Disk utilization is double the average utilization rate.	Automated Reports, Random Sampling, 100% Inspection, P, QAE monthly review of contractor metrics eriodic Inspection
24	Image Management	Create, test, and document a new image within 10 days from receipt of request from Government.	Automated Reports, Random Sampling, 100% Inspection, Periodic Inspection, QAE monthly review of contractor metrics
25	Configuration	a. Configure a system within 2 working days from receipt of request. b. "Field test" at least15% of configurations for one month after implementation.	Automated Reports, Random Sampling, 100% Inspection, Periodic Inspection, QAE monthly review of contractor metrics
26	Quantitative: Customer	a. Average synthetic transaction performance variance is less than 30% b. Run sample transactions to set a throughput base line then measure variance	Automated Reports, Random Sampling, 100% Inspection, Periodic Inspection, QAE monthly review of contractor metrics
27	Application Availability	a. Maintain weekly operational availability 99.9% or higher. The environment should not experience downtimes, planned or unplanned, that exceed 1 minute, 26 seconds in day; 10 minutes, 5 seconds in a week; 43 minutes, 50 seconds in a month; and 8 hours, 45 minutes, 57 seconds in a year. b. Constantly monitor operational requirements and application availability to detect potential problems before failure	Automated Reports, Random Sampling, 100% Inspection, Periodic Inspection, QAE monthly review of contractor metrics

28	Consolidated server operations: Perform system administrative and maintenance function for the consolidated application servers.	Maintain weekly operational availability 99.9% or higher. The environment should not experience downtimes, planned or unplanned, that exceed 1 minute, 26 seconds in day; 10 minutes, 5 seconds in a week; 43 minutes, 50 seconds in a month; and 8 hours, 45 minutes, 57 seconds in a year.	Automated Reports, Random Sampling, 100% Inspection, Periodic Inspection, QAE monthly review of contractor metrics
DATABASE ADMINISTRATION			
29	Backbone or Infrastructure Return to Service	Workstations, peripherals, communications devices, and operating system/application software are restored within 2 hours	Automated Reports, Random Sampling, 100% Inspection, Periodic Inspection, QAE monthly review of contractor metrics
30	Database Administration: Individual patches and requisite patches per database	Based on Elapsed; Same Business Day as signoff by customer completed within Availability SLRs	Automated Reports, Random Sampling, 100% Inspection, Periodic Inspection, QAE monthly review of contractor metrics
31	Database Administration: Service packs and updates to “dot” releases	Based on Elapsed; Same Business Day as signoff by customer completed within Availability SLRs	Automated Reports, Random Sampling, 100% Inspection, Periodic Inspection, QAE monthly review of contractor metrics
32	Database Administration: Version or major release updates	Based on elapsed time; Within 5 Business Days of signoff by customer. Required downtime is outside of the normal Availability SLRs	Automated Reports, Random Sampling, 100% Inspection, Periodic Inspection, QAE monthly review of contractor metrics
33	Database Administration: Instance Creation and Refresh	Based on elapse time; Create=2BusinessDays Refresh = 1 Business Day	Automated Reports, Random Sampling, 100% Inspection, Periodic Inspection, QAE monthly review of contractor metrics
34	Database Administration: Create End-User ID, Grants, Revokes, Create table space, other data definition requests	Based on elapse time: 2hours(1–5requestsdaily) 4hours(6–10requestsdaily) 2BusinessDays>10daily Based on a per-database request	Automated Reports, Random Sampling, 100% Inspection, Periodic Inspection, QAE monthly review of contractor metrics
35	Database Administration: Schema changes and	Based on elapse time: 1 Business Day Based on a per-database request	Automated Reports, Random Sampling, 100% Inspection,

	stored procedures		Periodic Inspection, QAE monthly review of contractor metrics
36	Database Administration: Performance tuning and maintenance	Based on elapse time: Proactive monitoring and preemptive intervention to maintain required performance levels Two hours to respond to ad hoc requests	Automated Reports, Random Sampling, 100% Inspection, Periodic Inspection, QAE monthly review of contractor metrics
VoSIP			
37	Secure/Non-Secure VTC support	Secure/non-secure VTCs are available and operational with real time video and intelligible audio 95% of the time.	Automated Reports, Random Sampling, 100% Inspection, Periodic Inspection, QAE monthly review of contractor metrics
CABLE INSTALLATION & MAINTENANCE SERVICES			
38	Intra-Building Cable Support, and Cable Plant: Perform quality Government approved system modifications.	No more than one deviation per month from applicable unit or EIA/TIA performance standards for the applicable medium modified.	Automated Reports, Random Sampling, 100% Inspection, Periodic Inspection, QAE monthly review of contractor metrics
PERFORMANCE MANAGEMENT SERVICES			
39	Proactive Network Monitoring	Identify 100% of major system or network outages with network management tools	Automated Reports, Random Sampling, 100% Inspection, Periodic Inspection, QAE monthly review of contractor metrics
40	Incident/Problem Management Escalation : Timely and appropriate notification of disruption of network services or emergency/unscheduled outages	Notify crew commander immediately of an outage on any operational system	Automated Reports, Random Sampling, 100% Inspection, Periodic Inspection, QAE monthly review of contractor metrics
41	Summarization of network anomalies or degradation	Provide monthly reports	Automated Reports, Random Sampling, 100% Inspection, Periodic Inspection, QAE monthly review of contractor metrics
42	Circuit thresholds	Provide monthly reports	Automated Reports, Random Sampling, 100% Inspection,

			Periodic Inspection, QAE monthly review of contractor metrics
METADATA MANAGEMENT			
43	Metadata Environment (MDE) Development	a. Develop the MDE within six months of contract start date. b. Develop MDEs in accordance with the DoD Enterprise Architecture (EA) Data Reference Model or IC Architecture Reference Model.	Automated Reports, Random Sampling, 100% Inspection, Periodic Inspection, QAE monthly review of contractor metrics
44	Metadata Creation	Create metadata in accordance with the DoD Discovery Metadata Specification (DDMS) as appropriate.	Automated Reports, Random Sampling, 100% Inspection, Periodic Inspection, QAE monthly review of contractor metrics
45	Metadata Management	Ensure metadata is complete, accurate, and available to be queried at a moment’s notice.	Automated Reports, Random Sampling, 100% Inspection, Periodic Inspection, QAE monthly review of contractor metrics