NETCENTS-2 SOLUTIONS
Network Operations (NetOps) and Infrastructure
Full and Open Performance Work Statement (PWS)

29 October 2015

Revised 12 July 2017

PERFORMANCE WORK STATEMENT (PWS)
NETWORK OPERATIONS (NetOps) AND INFRASTRUCTURE SOLUTIONS

1. NETCENTS-2 INTRODUCTION

1.1 NETCENTS-2 Goal

The goal of the overall NETCENTS-2 program is to support missions that require voice, data, and video communications, information services, solutions, and products to deliver the right information, in the right format, to the right place, at the right time – efficient in peace, effective in war, and ensuring success across the spectrum of operations. NETCENTS-2 supports the IT lifecycle to include legacy operational and sustainment activities, re-engineering of legacy capabilities into target architectures and environments, and future service-oriented capabilities. NETCENTS-2 is an enabler to meet Air Force IT transformation goals to allow for innovation with the ability to more rapidly provision and field capabilities. NETCENTS-2 enables the ability to segregate aspects of full system lifecycles into more granular components that can be composed into integrated capabilities for the warfighter. Furthermore, NETCENTS-2 enables different solution providers to participate over the course of the program lifecycle. For example, the solution providers for development may be different from those that accomplish deployment, operation, and support.

1.2 NETCENTS-2 Scope

The NETCENTS-2 ID/IQ contracts will provide a wide range of IT Network-centric and Telephony products, services and solutions covering the full spectrum of netcentric operations and missions, including existing legacy infrastructure, networks, systems and operations as well as emerging requirements based on the AF Chief Information Officer's (CIO's) SOA construct. The contracts will provide Network-Centric Information Technology, Networking, and Security, Voice, Video and Data Communications, system solutions and services to satisfy the Combat Support (CS), Command and Control (C2), and Intelligence Reconnaissance and Surveillance (ISR) Air Force and Department of Defense (DoD) requirements worldwide. These contracts will provide users the capabilities to find, access, collaborate, fuse, display, manage, and store information on the Department of Defense (DoD) Information Network (DoDIN). AF sites may include commercial-off-the-shelf (COTS) National Security Systems (NSS), intelligence data handling equipment, C2 equipment, Local Area Networks (LAN), Wide Area Networks (WAN), secure and non-secure video, voice and data systems, and/or mission equipment. The equipment processes information of varying security classifications and may include sites that are Sensitive Compartmented Information Facilities (SCIFs).

All effort supported under this contract shall be provided in accordance with Department of Defense, United States Air Force, or DOD Intelligence Information Systems (DoDIIS), and National Security Agency standards as applicable to the task order. Efforts under this contract will support industry best practices when not proscribed by aforementioned standards.

1.3 NETCENTS-2 Acquisition Strategy

NETCENTS-2 consists of various related IDIQ contracts in an effort to meet the above-stated goals. There are functions where performance on one task order may limit, because of dependencies or type of activity (e.g., support to the Government), work on other task orders. Total solutions will potentially be composed of combinations of subsets of the contract. NETCENTS-2 comprises the following suite of contracts:

1. Netcentric Products – COTS products to support the network

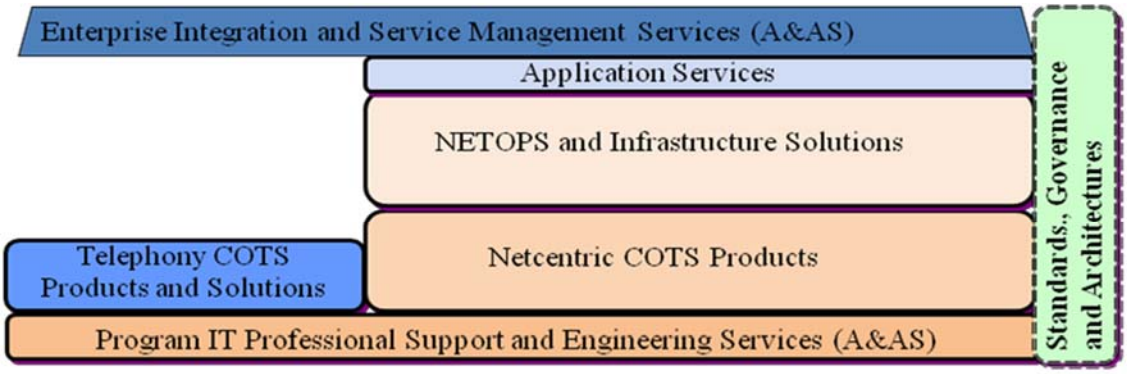
2. NetOps and Infrastructure Solutions – Solutions to support network operations, core enterprise services, and infrastructure development and operations (includes legacy Telephony)

3. Application Services - Services to sustain, migrate, integrate, re-engineer, and expose Mission Applications for secure access by authorized users, by establishing web and netcentric services, to include help desk, testing and operational support, in legacy and netcentric enterprise environments

4. Enterprise Integration and Service Management (A&AS) - Enterprise level integration/portfolio management activities

5. IT Professional Support and Engineering Services Advisory and Assistance Services (A&AS)

The NETCENTS-2 contracts enable the delivery of products, services and solutions that adhere to the AF Enterprise Architecture (AF EA) and complement each other as depicted in Figure 1.



2

Figure 1. Relationship of Contract Areas

1.4 Air Force IT Challenge

Currently, the Air Force has multiple, disparate and sub-optimized collections of computing and communications resources. Each set of resources is managed independently, resulting in costly and inefficient redundancy. Different networks, multiple computing centers, and stove-pipe systems all make it difficult for end users to access consistent and relevant information in a timely manner, allocate resources to respond to demand, and consequently make timely and informed decisions.

1.5 NETCENTS-2 Solution

NETCENTS-2 is a vehicle enabling the IT lifecycle to include legacy operational and sustainment activities, migration of legacy systems, and future service-oriented capabilities. NETCENTS-2 provides a streamlined, enterprise-supported contract vehicle that enables the consolidation of many existing base-level contracts for Operations and Maintenance (O&M) activities. In addition, NETCENTS-2 supports the re-engineering and modernization of legacy systems through the rapid, incremental delivery of solutions, enabling improved day-to-day operations and warfighting mission execution. NETCENTS-2 provides a contract vehicle for the acquisition of the components, such as infrastructure, services, resources and activities, required to implement service-oriented capabilities.

To support the re-engineering of legacy systems and future service-oriented capabilities, the AF has created a set of information sharing business rules called the Singularly-Managed Infrastructure (SMI) and Enterprise Level Security (ELS) (SMI-ELS). SMI-ELS is not a technical solution or specific product, instead it guides a business model informed by governance and architecture that affects all aspects of a Doctrine, Organization, Training, Materiel, Leadership and education, Personnel and Facilities (DOTMLPF) solution for the effective implementation of a secure Net-Centric Data Strategy (NCDS). SMI-ELS gives form to processes such as architecture and acquisition; technical solutions such as networks, vocabulary- based web services, applications, data repositories, and computing infrastructures; and force transformation, to drive Air Force systems and users into higher degrees of information and knowledge- based operations.

The NETCENTS-2 scope of work directly supports SMI-ELS objectives, as follows:

1. SMI: The Singularly Managed Infrastructure will place AF core service computing and communications resources under a single enterprise-wide management construct. This does not mean consolidating resources into a single physical location for management purposes. Many high-end computing platforms, like those used to run simulations, may have internal management constructs as their resources are not shared across the enterprise. However, any interaction between these localized collections and any other computing resources will fall under the SMI construct. Likewise, not all communications (i.e., Military Strategic Tactical Relay (MILSTAR) satellites) may be individually managed under the SMI concept, but the overall capability delivered by these resources will adhere to SMI concepts. The SMI will operate over existing physical locations, with some adaptation of those physical locations based on business case analyses, to manage all computing resources from the enterprise perspective. Existing data centers, such as the MAJCOM Computing Centers, will be integrated into the SMI and the management of the resources within those Centers will be subject to the SMI processes and procedures.

2. ELS: The Enterprise Level Security will enable authorized users to locate, access, and utilize information from authoritative sources regardless of the location of the data as long as information security guidelines stipulated are met.

NETCENTS-2 also provides the contract vehicle to support the development of vocabulary-based web services, content delivery and presentation services, and new mission applications that operate in netcentric enterprise environments and exploit SOA infrastructures.

This contract provides the services management support required by SMI-ELS. Service Management (SM) ensures that: (1) agreed upon services are delivered when and where they are supposed to be delivered and (2) services operate as agreed upon. Using NETCENTS-2 contract vehicles, portfolio managers implement SM with a focus on risk mitigation and policies that require built-in closed-loop governance mechanisms.

1.6 Governance

The services and solutions delivered under NETCENTS-2 in support of Air Force operations will be subject to the oversight of an Air Force enterprise level governance structure and set of processes. The governance processes will employ systems engineering fundamentals, ensure adherence to the Air Force Enterprise Architecture, and be implemented along with the normal reviews in the acquisition process. The governance structure has three tiers, strategic, operational, and tactical, where policy will be set at the strategic level, reviews for compliance and technical rigor will be done at the operational level, and contract mechanics will be handled at the tactical level. Further explanation of the governance structure is explained in the User's Guide.

2. CONTRACT PURPOSE

The purpose of this contract is to provide Network Operations (NetOps), Infrastructure, and Service Oriented Architecture (SOA) implementation and transformation services and solutions to the United States AF (USAF) and Department of Defense (DoD) agencies at locations inside the contiguous United States (CONUS), outside the contiguous United States (OCONUS) and in war zone areas. The services and solutions provided will address the development, acquisition, integration, test, deployment, and sustainment of Air Force (AF) infrastructure and network operations, production, research and development, and Command, Control, Communications, Computers (C4) and, Intelligence, Surveillance, Reconnaissance (ISR) mission capabilities. The proposed solutions shall be in compliance with existing DoD, USAF, and Intelligence Community (IC) standardization and interoperability policies. Technology refreshment and system evolution within this contract will track proven, accepted, and available leading edge technology within industry.

This contract supports the Department of Defense Information Network (DoDIN) architecture, Defense Information Infrastructure (DII), IC Information Sharing environments, and AF and Defense Communications Systems infrastructure for computer and telecommunications network mission areas. Solutions and services provided under this contract will help the DoD and IC achieve information superiority as called for in Joint Vision 2020 and will promote adherence to the Systems Engineering Process (SEP) as specified in the DoD 5000-series.

2.1 Contract Goal

The goal of this contract is to provide a full range of innovative, reasonably priced, world-class information technology services and solutions to support the full spectrum of netcentric operations and missions. It will help our warfighters be efficient in peace and effective in war while providing them the right information in the right format to the right place at the right time. NETCENTS-2 will support USAF, DoD, and other Federal Agency customers that work in transitory, static, and deployed locations throughout the world. The netcentric services and solutions provided will combine with joint and interagency assets and capabilities from land, sea, air, space, and cyberspace components, as well as coalition and allied capabilities, to create an interoperable force capability.

2.2 Contract Scope

This contract will provide a wide range of services and solutions covering existing legacy infrastructure, networks, systems and operations as well as emerging requirements. and guidance provided by the IC Information sharing Executive (ISE) and AF Chief Information Officer's (CIO) . The contracts will provide Network-Centric Information Technology, Networking, and Security, Voice, Video and Data Communications, system solutions and services to satisfy the Combat Support (CS), Command and Control (C2), and Intelligence Reconnaissance and Surveillance (ISR) Air Force and Department of Defense (DoD) requirements worldwide. This NetOps contract will provide users the capabilities to find, access, collaborate, fuse, display, manage, and store information on the Department of Defense (DoD) Information Network (DoDIN) and IC Information sharing environment as applicable. Other services include, but are not limited to, wireless devices/capabilities, Personal Digital Assistants (PDAs) to include Blackberries and information intensive data applications (e.g. video-teleconferencing, imagery, modeling, simulation, streaming video, web-enabled weapon systems and applications, information management, Everything over IP (EoIP), and Voice over IP (VoIP). This contract will support the transformation of AF global-level command and control and administration of Information Technology (IT) resources from base-level Network Control Centers (NCC), MAJCOM Coordination Centers (MCCC), MAJCOM Network Operations Security Centers (NOSC), and Network Operations Divisions (NOD) and Network Security Divisions (NSD) to regionally consolidated Area Processing Capabilities (APC), Enterprise Service Units (ESU), Integrated NOSCs (I-NOSC) and Enterprise Service Desks (ESD).

Through this contract vehicle, customers can acquire network infrastructure system solutions, operations, and maintenance, as well as systems management, configuration management, and NetOps Core IT services (e.g., e-mail, storage, and directory services). System solutions shall follow disciplined System

Engineering Processes and shall include, but not be limited to: establishment of the SOA Singularly Managed Infrastructure with Enterprise Level Security (SMI-ELS), including Metadata Environments (MDEs), Enclaves, Federation and Enterprise Management of the AF Architecture; Network Operations including (DoDIN) Web Content Management, (DoDIN) Enterprise Management (EM) and DoDIN Network Defense (DoDNetD); and Network Infrastructure Messaging and Site Preparation and Installation services. This contract will provide NetOps services and solutions support to establish, operate, and maintain the network and SOA infrastructure required to provide netcentric capabilities and traditional network operations.

2.3 Netcentric Strategies, Standards, and the Use of This Contract by Other Agencies and Departments

Specific standards, guidance, and applicable documents within this contract are written with the intent of accomplishing Air Force netcentric strategies. These strategies will evolve over time and, when appropriate, the AF will revise and replace standards accordingly. The contractor shall conform to Air Force strategies and visions and adhere to associated standards. Other agencies and departments are encouraged to use this contract for the same purpose and may specify and substitute other standards, guidance, and applicable documents within their task orders that are appropriate to provide solutions tailored to meet their netcentric strategies. AF functional communities may be required by law or other National guidance to meet non-AF standards and guidance; in these cases the mandated standards and guidance will be identified in individual task orders.

The Air Force reserves the right to restrict use of this contract and to disallow DoD and other Federal Agencies from using this contract.

3. REQUIREMENTS

The contractor shall provide a wide range of services and solutions that support existing legacy infrastructure, networks, systems, and operations, as well as evolving the infrastructure, networks, systems and operations to comply with the AF enterprise architecture.

3.1 SMI-ELS Infrastructure Implementation and Operation

3.1.1 Singularly Managed Infrastructure (SMI)

The contractor shall provide services and solutions to realize a SMI that brings together at the middleware layer disparate networks and communications capabilities into a consistent AF enterprise-wide 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, enclaves, Communities of Interest (COIs), and federation that make an SMI possible.

3.1.1.1 Core Enterprise Services (CES)

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 exploit the DoD CES when and wherever possible, and deliver AF-specific CES as required to augment the DoD CES to fulfill the AF mission.

Notes: Cyber Security (CS) related services, while part of Core Enterprise Services, are listed separately in the Enterprise Level Security section. Transport layer capabilities are covered in the Network Operations section and deliver the physical infrastructure upon which middleware and services operate, including physical plants and network operations capabilities.

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 collections of hardware, software (including services), networks, 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 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 PKI, SAML, JMS, and WS-*, etc.

3.1.1.4 Metadata Environments

Metadata environments 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 Metadata Environments (MDEs). The contractor shall maximize the use of 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 metadata environment 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 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, Metadata Catalog and Service Registry.

3.1.1.4.1.1 Metadata Registry

The contractor shall develop and support a Metadata Registry (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, life cycle 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 ADS's 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 Metadata Registry or IC Metadata Registry using federation. The contractor shall manage metadata that enables users to discover and consume information provided by mission capabilities implemented as services.

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 XML schema, 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 Department of Defense Discovery Metadata Specification (DDMS).

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 SOA 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.

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, but is not limited to, 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, but is not limited to, unstructured text documents, images, 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 (AMPS)

The contractor shall develop and support an Automated Metadata Population Service (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.

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 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 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 an 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 exploit 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 SOA solutions to implement IA in accordance with WS assurance standards. WS standards will be defined at the task order level, but the expected ones are:

WS-Security
WS-Secure Conversation
WS-Security Policy
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 Parner standards as specified in TO.

3.1.2.1.1 Confidentiality

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

3.1.2.1.2 Integrity

The contractor shall provide integrity security services that prevent unauthorized modification of data, both while stored 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 SOA service invocations, information queries, etc., are attributable to the entity 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 Public Key Infrastructure (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.

As specified by the Task Order, the contractor shall provide Commercial-Off-The-Shelf (COTS) IA and IA-enabled products IAW AFI 33-200, Cyber Security or other specified guidance. These products must be National Security Telecommunications and Information Systems Security Policy Number 11 (NSTISSP-11) compliant, requiring them to be validated by accredited labs under the National Cyber Security Partnership (NCSP) Common Criteria Evaluation and Validation Scheme or National Institute of Standards and Technology (NIST) Federal Information Processing Standards (FIPS) Cryptographic Module Validation Program (CMVP) or IC standards as applicable.

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 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 life-cycle entity identity management from user creation to user revocation, as depicted in Figure 2. Entities are defined as both human and non-human users possessing accounts within the enterprise. The contractor shall support user creation (identity confirmation, credentialing, 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 Federal Information Protection Standard (FIPS) 196, or other specified standard in TO, by using approved methods of authentication such as, but not limited to, the following:

Public Key Infrastructure (PKI) based authentication.
One-Time Password Tokens.
Biometrics with PIN or password.

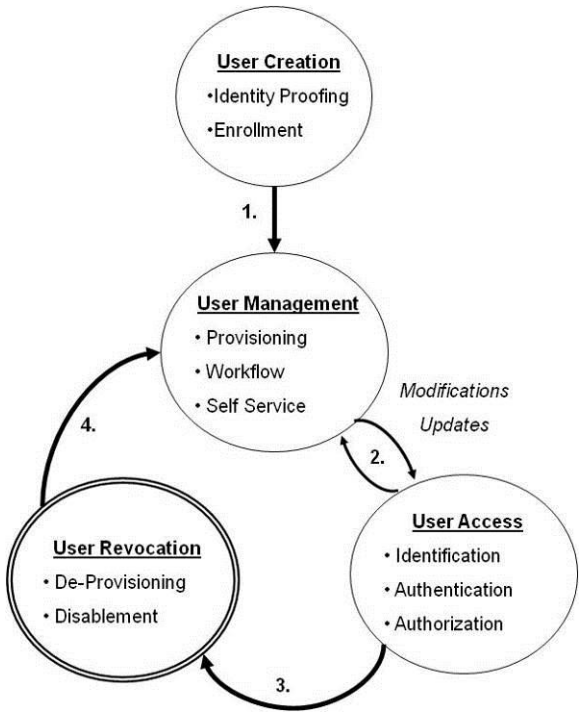


Figure 2: Enterprise Entity Lifecycle

3.1.2.2.2 Threat Analysis

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

3.1.2.2.3 Certification and Accreditation

The contractor shall provide services and solutions to help address the risks associated with AF network convergence into an interoperable enterprise and accomplish the certification and accreditation (C&A) of the AF SOA infrastructure. The contractor shall follow the DoD Cyber Security Risk Management

Framework (RMF) or ICD 503 to accomplish the infrastructure C&A as applicable. In order to satisfy DoD system security documentation requirements, the contractor shall register the SOA infrastructure in the Enterprise Information Technology Data Repository (EITDR), and complete the Security, Interoperability, Supportability, Sustainability and Usability (SISSU) checklist, as described in the IT LEAN Reengineering and SISSU Guidebook, v5.0, 4 April 2007. The contractor shall accredit the SOA infrastructure so that it can be leveraged by individual mission services. TOs for classified network support will identify when alternative registries and C&A guidance is applicable.

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 2-way authentication using DOD-PK I 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 Air Force 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, NIPRNET, and JWICS)
9. Operate, maintain, and configure point to point, VPN, and bulk encryption for network and longhaul circuits
10. Provide encryption to the base campus SIPRNet connectivity.
11. Provide SCI network security capabilities as specified in TOs.

3.1.3 Enterprise Service Management

The contractor shall provide services and solutions to accomplish SMI-ELS service level management. The contractor shall provide operation and maintenance of the SMI-ELS infrastructure including, but not limited to, network monitoring, load balancing, information archival and backup, disaster recovery, Continuity of Operations (COOP), and enterprise support desk (ESD). The ESD shall support users encountering issues in accessing mission capabilities.

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 version of services.

The contractor shall provide enterprise service management to SCI networks as specified in TOs.

3.1.4 SMI-ELS Architecture Documentation

The contractor shall document the Singularly Managed Infrastructure with Enterprise Level Security (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 architecture guidelines as specified in task orders. The contractor shall support process improvement events, such as 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).

The contractor shall develop, document, and register SCI architectures and artifacts per TO directions. The contractor shall document engineering processes and process improvement activities and artifacts per TO directions for SCI systems and networks.

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 comprise 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, and Security Management), as well as information and infrastructure protection. It shall also encompass the DoDIN's information technology (IT) services management and consist of the many elements and processes needed to communicate across the full spectrum of the DoDIN, including the following:

1. Enterprise Services Management
2. Systems Management
3. Network Management
4. Satellite Communications Management
5. Electromagnetic Spectrum Management

3.2.1.1.1 (Not in the original) Enterprise Messaging and Directory Services

The contractor shall provide services and solutions that enable directory services, e-mail and organizational messaging in accordance with Enterprise Architecture..

3.2.1.1.2 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. Monitoring and enforcing service level agreement (SLA) compliance
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

3.2.1.1.3 Enterprise Information Management

The contractor shall provide services and solutions that enable 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
6. Network Attached Storage
7. Back-Up/Archive
8. Records Management

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:

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:

a. Assured Information Sharing and Management
b. Access Control
c. Cross-Domain Security
d. Information Environment Protection
e. Certification and Accreditation
f. Risk Analysis
g. Cyber Security Awareness
h. Auditing
i. Emanations Security (EMSEC) /TEMPEST for TS or SCI environments
j. Communication Security (COMSEC)
k. Operation Security (OPSEC)
l. Information Protection
m. Authentication

n. Resource Protection
o. Federated Identity Management
p. Virtual Private Networking
q. Network Protection
r. Filtering
s. Intrusion Detection and Prevention
t. Cryptographic Services
u. Key and Certificate Services
v. Insider Threat Protection
w. Anomalous behavior detection
x. Time Compliance Network Order (TCN))
y. Computer Incident Response Team (CIRT)
z. Air Force Computer Emergency Response Team (AFCERT)
aa. Telecommunications Monitoring and Assessment Program (TMAP)

1. 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, analysis and defend against new attack vectors..

2. 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 JTF-GNO and NetOps directed Information Operations Condition (INFOCON) changes and provide Command and control on the progress and completion.

3. Defense Critical Infrastructure Protection (CIP) – Actions taken to prevent, remediate, or mitigate the risks resulting from critical infrastructure vulnerabilities. Actions shall include, but not be limited to, changes in tactics, techniques, or procedures; adding redundancy; selection of another asset; isolation or hardening; guarding; etc.

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:

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.

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. 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.

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:

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.

2. Continuity of Operations (COOP) – 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 capabilities with automatic failover that is transparent to users.

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. Operate the Base Information Transfer System and Official Mail Center. Provide Privacy ACT, Freedom of Information Act (FOIA), and record management training.

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

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 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 Information Technology Infrastructure Library (ITIL) framework.

6. Change Management – Tools, tactics, techniques and procedures for accomplishing change management across the AF enterprise to help implement network operational concepts.

7. Training – Resources need to provide training such as training materials, instructors and facility.

8. System Administrator- Set up, configure, develop, maintain, troubleshoot, and support internal and external networks.
9. Database Management- Perform loads, upgrade, patches, data recovery, backups, and maintain active directory.
10. Account Management – Create, delete, and modify voice, data, and video accounts and provides means to unlock Common Access Card (CAC).

3.2.1.5 Network Command and Control (C2)

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 situational awareness (SA) services and solutions that integrate command and control (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.

3.2.1.6 Network Management and Enterprise Services

The contractor shall provide services and solutions that accomplish Network Management for AF Network Operation Center (AFNOC)/ Integrated Network Operations and Security Center (I-NOSC) 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. Asset management to include Equipment Management

The contractor shall provide services and solutions that accomplish Network Management and Support for the Enterprise Support Unit (ESU) and the Enterprise Service Desk (ESD) anticipated activities such as, but not limited to, the following:

1. Network configuration management
2. Load balancing
3. Vulnerability analysis and response
4. Application and content management
5. Continuity of Operations (COOP) management
6. Resource virtualization
7. Information lifecycle management
8. Service Orchestration
9. Virtualized IT service support
10. Help Desk/Call Center
11. Security Management Service

The contractor shall provide services and solutions that accomplish Enterprise Services to support Network Operations such as, but not limited to, the following:

1. Information technology (IT) service virtualization
2. IT Support
3. Service/security management and provisioning
4. Domain security
5. Cross-domain security
6. Collaboration (video teleconference)
7. Content and service staging
8. Federated content discovery
9. Application, system, services and data hosting
10. Development of applications for database or web pages
11. Producer to consumer availability of service
12. Configuration and change management

TOs from other agencies, departments, or AF functional communities for the same purpose may be issued. These TOs may specify and substitute other standards, guidance, and applicable within their TO to provide solutions tailored to meet their network management and enterprise services strategies

3.2.2 Network Infrastructure

The contractor shall provide services and solutions in support of transport layer capabilities to deliver the physical infrastructure upon which the SOA middleware and services operate, including, but not limited to, messaging capabilities and site preparation and installation services. Support of the transport layer includes the AF's Information Transport System (ITS) which is the engineering, installation, and sustainment of the high-performance, survivable fiber optic backbone to include "wired" and "wireless" networks.

3.2.2.1 Messaging

The contractor shall provide messaging capabilities allowing separate, uncoupled applications to reliably communicate asynchronously. The messaging system architecture generally replaces the client/server model with a peer-to-peer relationship between individual components, where each peer can send and receive messages to and from other peers. The contractor shall provide delivery pathways, such as Web services, HyperText Transfer Protocol (HTTP) or HyperText Transfer Protocol Secure (HTTPS) connections, or other links, as needed to support content delivery and presentation service requests. The contractor shall tag and register delivery pathways as necessary. The contractor shall support other data

transport pathways, such as File Transfer Protocol (FTP) and Open DataBase Connectivity (ODBC), for legacy systems and databases.

The contractor shall provide messaging services including, but not limited to, the design and/or implementation of: messaging architecture; point-to-point distribution of messages; publish-subscribe distribution of messages; message producer; message consumer; one-way interaction between a message producer and a message provider; request-reply interaction between a message producer and a message consumer; and connectivity between an application and a messaging provider.

The contractor shall provide messaging services that encompass, but are not limited to, provision of federated, distributed, and fault-tolerant enterprise messaging capabilities; message publishing and subscribing, peer-to-peer messaging and queuing; support for the configuration of QoS parameters for a published message, including the priority, precedence, and time-to-live (TTL); provision of guaranteed delivery to disconnected users or applications; development of Online Asynchronous Processing (OLAP) and real or near real-time enterprise data reporting capabilities.

3.2.2.2 Site Preparation and Installation Services

The contractor shall perform site preparation and installation activities to support implementation of required services and solutions under this contract at any AF, DoD, or other Federal Agency location.

3.2.2.2.1 Requirements Analysis and Conceptual Design

The contractor shall perform requirements analyses and conceptual designs at required locations. During this process, the contractor shall collect all the information to complete a requirements analysis and conceptual design. The contractor shall survey, evaluate, and provide technical advice concerning all existing infrastructures, communications, power, Heating, Ventilation and Air Conditioning (HVAC), and environmental aspects of the site. The contractor shall provide an implementation plan, in accordance with the task order, reflecting the strategy, schedule, and recommendations (e.g., site architecture, topology, and configuration) for the implementation with considerations of on-site failover and continuity of operations. The Government will provide applicable information, as available, such as existing/projected user network resources and locations, GFE, base support requirements, and other written information related to specific implementation for each task order to establish the unique characteristics of each site. Access to Government facilities will be provided and interviews shall be coordinated with Government points of contact specified in the task order.

Types of support and services provided by the contractor shall include, but not be limited to: Email, Server and Storage Area Network Administration, Security Boundary Administration, Print Management, Configuration/Release Management (i.e. Security/Patch Administration, etc), Mobile/Remote User Services Support and Administration, Network Infrastructure Management and Administration, Certification and Accreditation (i.e. Security Scanning, etc), Directory Services, and Event Management.

The contractor shall possess reach back capabilities to obtain expertise that may not be immediately available onsite and the ability to surge in times of crisis.

The contractor is required to deliver all services and solutions provided under this contract described below. The contractor shall design, develop, install, document and test custom solutions and their infrastructures. The contractor shall enable system solutions to integrate with: Air Traffic Control, Land Mobile Radio, Command Post Switches, Defense Red Switch (DSR), Defense Red Switch Network (DRSN), Giant Voice, Enhanced 911, Cell Systems, Base Altering Systems and Crash Nets, and any other systems specifically identified in the task order.

3.2.2.2.2 Site Survey

The contractor shall perform site surveys at required locations. The findings of the site survey and any actions required in preparation for system installation shall be documented.

3.2.2.2.2.1 Systems Engineering

The contractor shall provide systems engineering solutions for the analysis, design, integration, installation, testing, and life-cycle support of new and upgraded systems associated with delivery of infrastructure capabilities as defined by the AF enterprise architecture. The contractor shall employ disciplined systems engineering processes in accomplishing contract taskings, using commercial best practices in accordance with of AFI 63-101/20-101, Integrated Life Cycle Management, for systems engineering processes in planning, architecting, requirements development and management, design, technical management and control, technical reviews, technical measurements, integrated risk management, configuration management, data management, interface management, decision analysis, systems management, inspections and maintenance, sources of supply maintenance and repair, and test and evaluation, verification and validation. These systems engineering solutions shall follow industry standard engineering processes and may include but not be limited to: Technical assessments of all user requirements, integration of all GFE and Contractor Furnished Equipment (CFE) as proposed, hardware and software information, network applications, system design, training (COTS or customized)(initial and recurring), maintenance and support, system interface studies and control documents, network integration and test plans, cost analysis/trade-off studies, engineering change proposals, Voice Switching System (VSS) facility and systems/applications studies, VSS call detail recording and traffic measurement data analysis, engineering support (digital transmission/switching equipment) to Government engineers. 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.

Task orders may further refine the systems engineering processes according to MAJCOM or functional policies and practices. The contractor shall employ the principles of open technology development described in the DoD Open Technology Development Guidebook and in Net-Centric Enterprise Solutions for Interoperability (NESI) body of knowledge, and systems engineering activities used in developing contractor solutions shall adhere to open architecture designs for hardware and software, and employ a modular open systems architecture approach. The contractor's systems engineering planning and design activities shall also adhere to the DoD's Information Sharing and Net Centric Strategies published by the DoD CIO and the engineering body of knowledge and lesson's- learned accumulated in NESI. TOs may require adherence to other governmental standards.

3.2.2.2.2.2 System Upgrade/Update Support

The contractor shall provide system upgrade support and future planning associated with delivery of infrastructure capabilities as defined by the AF enterprise architecture.. The contractor shall maintain currency with the design and development of systems similar to those implemented in the VSS, and discuss recommended changes or strategies with the Government. The contractor shall identify current or anticipated problem areas relating to telephony hardware and software systems and present technical issues of interest or value to the Government regarding VSS.

The contractor shall provide information regarding technology advancement to the Government and support new telecommunications products and solutions as they are approved by the DoD JITC and introduced into the VSS network. These newly emerging solutions must adhere to AF or IC security requirements as they pertain to voice telecommunications assets prior to installation.

3.2.2.2.2.3 Post-Cutover Support

Each solution shall include a warranty as specified in Section I, Clause 52.246-17. In addition to FAR Clause 52.246-17, the following additional requirements apply: Users shall have highly reliable and maintainable telephony products and system solutions to interoperate with the described environment. Components shall be maintainable and expandable by the user without voiding the warranty coverage.

In addition to any OEM warranty coverage, three types of post cutover operation and maintenance support shall be provided: System Support, Workmanship Support, and Construction Support. The contractor shall provide for restoration of the system and repair of equipment in a timeframe specified as required by this contract, unless stated otherwise in the task order. The means to transport equipment and repair personnel both to and from the Government site is the responsibility of the contractor. The contractor shall provide technical support, software support, and hardware replacement for failed components, engineering support, and maintenance services necessary to ensure active management, reliable operations, and rapid restoration. These technical support services shall include Tier II to Original Equipment Manufacturer (OEM) level support as required based on the need to achieve problem resolution. All technical support shall be provided by certified technical personnel fluent in the English language. If the Offeror is alerted to a degradation or failure, the Offeror shall provide immediate support to the operational user to identify, troubleshoot, and remedy the problem. The Offeror shall execute all hardware repair actions necessary to return the affected system to full operational capability. If the failed equipment is no longer under any alternative warranty support, the Offeror shall provide replacement equipment. Technical support shall be provided on a continuous, as-needed basis twenty-four (24) hours per day, 365 days per year for systems, peripherals, applications, and devices deployed. The contractor shall provide toll free, email, DSN, and PSTN access capabilities to contact requesting support for support issues.

3.2.2.2.3 Design/Integration Reviews

The contractor shall conduct design and integration reviews if required in the task order and in compliance with disciplined system engineer processes. This may be a formal or informal preliminary and final design reviews.

The contractor shall provide a single source of integration management for worldwide support, planning and sustainment of dissimilar manufacturer's switching systems, applications and peripheral equipment related to the VSS. The contractor shall identify cross functional applications and technical issues from selected symbiotic functional areas and document the opportunities for resolving the issues. 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 the task order.

3.2.2.2.3.1 Prototypes

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 prototype results associated with delivery of infrastructure capabilities as defined by the AF DoD or applicable IC enterprise architecture.. 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.

3.2.2.2.3.2 Preliminary Design/Integration Review (PDR)

During the PDR, the contractor shall present initial draft system design associated with delivery of infrastructure capabilities as defined by the enterprise architecture for Government review.
The draft documents to be reviewed shall include those specified in the Task Order. Examples may include the system requirements, the final Site Survey Report, System Design, Installation Specification (IS), Engineering Drawings and Installation Plan. This review shall include a list of recommended long-lead time items that the Government must order and have available at the time of system installation. This review shall be in sufficient detail to ensure technical understanding of the following: mission and requirements analysis, identification of all equipment and software to be integrated and to be used in the development of the design, and the scope and schedule of the work to be performed.

3.2.2.2.3.3 Final Design/Integration Review (FDR)

During the FDR, the Contractor shall present final system design documentation associated with delivery of infrastructure capabilities as defined by the enterprise architecture for Government review. The documents shall consist of those identified in the Task Order. Upon Government approval of the FDR documentation, the Contractor will be authorized to proceed with the installation. If discrepancies are identified, the Contractor shall correct all discrepancies and another FDR may be required at the discretion of the Government.

3.2.2.2.4 Site Preparation

As part of an overall system design and installation, the contractor may be required to perform site preparation support as required by the IS and approved by the Government Contracting Officer. The Government may, at its option, perform any portion or all of the requirements documented in the site survey report. Base civil engineering functions (or equivalent) will be used whenever possible. The contractor shall work with the base Quality Assurance Personnel (QAP) to accept civil engineering functions (or equivalent) as being in accordance with the approved implementation plan prior to beginning work. The final IS shall specify what site preparation the Government will perform and what site preparations the contractor will perform.

3.2.2.2.4.1 Pre-Installation Briefing

As required by the task order, the contractor shall present pre-installation briefings at the user sites. These briefings shall include the implementation strategy, installation schedule, verification that all allied support is completed and the site is ready for installation, and discussions of any potential problem areas. Additional pre-installation briefings may be held, as required by the Government.

3.2.2.2.4.2 Government Support

The Government will furnish facilities and utilities to the Contractor, including light, heat, ventilation, electric current, and outlets for use by installation personnel as required and stated in Task Orders. These facilities and utilities will be provided as specified in the Site Survey Report. These facilities will be readied prior to arrival of Contractor personnel and be provided at no cost to the Contractor. The Contractor shall provide required temporary utilities, which are not readily available in the work area. The Contractor shall coordinate, through the on-site QAP, any requirement before temporary disconnection of a utility. The Contractor shall submit a request in writing to the on-site QAP fourteen (14) days in advance of the necessity of utility disconnection.

3.2.2.2.4.3 Installation

The contractor shall engineer, install, configure, modify, relocate, or remove Communication and Information (C&I) systems for operational use. The systems and equipment installations or modifications must comply with established architectures. The contractor shall perform validation and verification testing on the system, assist users in configuring the system to meet their system requirements, and provide all applicable operating manuals/system management guides. Further, the contractor shall provide pre-cutover and post-cutover on-site training IAW with task orders. The government will identify personnel who will receive this training. The training shall provide for in-depth hands-on maintenance, operations and database administration.

3.2.2.2.4.4 Inside Plant

The contractor shall, (as required by each task order), install and configure of all the components for inside plant (e.g., power, groundings, HVAC, racks, fiber optic distribution panels, equipment, internal cabling, comm. closet, etc). The contractor shall install and test all cable and components IAW accepted industry standards, unless superseded by a Government approved IS indicated within the task order. Electrical

and communications cable, conduits, and circuits shall be installed IAW the National Electric Code (NEC). The contractor shall clearly label each end of every individual cable in accordance with the floor plans or engineering drawings. The contractor shall provide attached labels that are durable and legible. For any deviations to the specific installation specification, the contractor shall submit a proposal to the contracting officer for approval.

3.2.2.2.4.5 Outside Plant

The contractor shall, as required by each task order, install and configure of all the components for outside plant (e.g., fiber, manholes, duct, building entries, trenching, digging, constructions, external cabling, etc). The contractor shall install and test all cable and components IAW accepted industry standards, unless superseded by a Government approved IS indicated within the task order. Electrical and communications cable, conduits, and circuits shall be installed IAW the National Electric Code (NEC). The contractor shall clearly label each end of every individual cable in accordance with the floor plans or engineering drawings. The contractor shall provide attached labels that are durable and legible. For any deviations to the specific installation specification, the contractor shall submit a proposal to the contracting officer for approval. The contractor's design should not include aerial cable unless the Government has approved specific site exceptions. When use of aerial cable is approved, installation and test shall be IAW accepted industry standards, unless superseded by a Government approved IS indicated within the task order.

3.2.2.2.4.6 Tools and Testing Support

The contractor shall provide all tools, installation materials, and test equipment required to perform any required product installation and maintenance as called for by the task order. All tools and test equipment shall remain the property of the contractor. Any damage caused by the contractor to existing site facilities or equipment which might occur during site preparation, installation, testing or cutover of the system will be repaired at the expense of the contractor unless otherwise directed by the Government. The site shall be restored to the original condition which existed prior to the event unless otherwise directed. The Task Order will specify testing and inspection requirements. The contractor shall demonstrate that the system design meets the reliability/availability/maintainability requirements of the task order. Mean Time Between Failure data will be used to calculate the reliability/availability/maintainability of the system. The calculations shall be based on all of the equipment installed in the network. The contractor shall be capable of performing reliability, availability, and maintainability analyses of components, isolated sub-networks and the entire system.

3.3 Dynamic Test Environment

The contractor shall provide tools and services to support the design, implementation, and operation of a dynamic test environment. The dynamic test environment will enable applications developers to deploy their applications and services into the infrastructure and test the operation of those applications and the effect of those applications on other fielded capabilities.

3.3.1 Design

The contractor shall provide tools and services to support the design of the dynamic test environment. This will include but not be limited to defining concepts for dynamic testing;
Articulating processes and procedures for conducting dynamic testing; architecting the test environment; evaluating and selecting products and technologies for the test environment.

3.3.2 Implementation

The contractor shall provide tools and services to implement the dynamic test environment. This will include but not limited to configuring the products and technologies required by the design of the test environment; installing those products and technologies in location designated by the design; developing

capabilities necessary to fully integrate the products and technologies with each other and with existing infrastructure capabilities; integrating the products, technologies and developed capabilities with existing infrastructure capabilities to configure the test environment; and developing and executing test procedures to ensure the proper functioning of the test environment.

3.3.3 Operation

The contractor shall provide tools and services to operate the dynamic test environment. This shall include but not be limited to developing operating procedures, user guides, training materials, and other documentation to ensure to correct use of the test environment by users; developing administrative and management processes and documentation to ensure proper operation of the test environment in support of end users; monitoring the operation of the test environment to ensure users are achieving their test objectives; conducting performance evaluations of the test environment; and scheduling and executing technology refreshes and other activities to ensure the ongoing operation of the test environment.

3.4 Communication Operations and Maintenance (O&M)

The contractor shall provide services and solutions that accomplish O&M that include, but not limited to the following:

1. Operations and Telephony Infrastructure to include telephone customer support
2. Meteorological and Navigational Aids (METNAV)
3. Land Mobile Radios (LMR)
4. Personal Wireless Communication Systems (PWCS)
5. Video Teleconferencing (VTC)
6. Satellite Communications (SATCOM)
7. Air Traffic Control and Landing Systems (ATCALS)
8. Radar
9. Computer Systems Control (Tech Control) including but not limited to Circuit Management, Circuit Management Office, and Telecommunications Manager
10. Electronic Communication Management
11. Visual Imagery and Intrusion Detection
12. Deployment Manager
13. Antennas

3.5 General Requirements

The contractor shall meet the following requirements throughout the life of this contract, independent of ID/IQ task orders. All services and solutions provided under this contract shall conform to the guidelines detailed in the following paragraphs.

3.5.1 ~~Contractors Use of NETCENTS-2~~ Products ~~Contract~~

The contractor ~~shall~~ may obtain all products and associated peripheral equipment required by each individual task order from the NETCENTS-2 Products contract. The Contractor shall ensure that services, solutions and products meet the standards identified in the AF Standard Center of Excellence Repository (SCOER) located at http://www.netcents.af.mil/contracts/netcents-2/netops/documents/index.asp. The contractor shall adhere to requirements in the following paragraphs when providing products. These paragraphs describe general product requirements, types of products that are considered to comprise each of the product categories, and guidelines for product support.

3.5.1.1 General Product Requirements

All products provided under this contract shall conform to the guidelines detailed in the following paragraphs.

3.5.1.1.1. Hardware and Associated Software and Peripherals.

All hardware delivered under this contract shall include associated software and associated peripherals required for operations (such as controllers, connectors, cables, drivers, adapters, etc.) as provided by the Original Equipment Manufacturer (OEM). This is true only if the applicable OEM provides such items with the product itself.

3.5.1.1.2. Information Assurance (IA) Technical Considerations.

The contractor shall ensure that all applicable Commercial-Off-The-Shelf (COTS) IA and IA-enabled products comply with AFI 33-200, Information Assurance. These products must be Committee on National Security Systems Policy 11 (CNSSP-11) compliant, requiring them to be validated by accredited labs under the National Information Assurance Partnership (NIAP) Common Criteria Evaluation and Validation Scheme or National Institute of Standards and Technology (NIST) Federal Information Processing Standards (FIPS) Cryptographic Module Validation Program (CMVP).

3.5.1.1.3. Authorized Resellers.

The contractor shall be an authorized reseller, as defined by the Original Equipment Manufacturer (OEM), of new and refurbished/remanufactured equipment for OEMs proposed under this contract. If the OEM does not have authorized resellers the contractor may procure directly from the OEM or utilize other legitimate distribution channels to provide the required products. Any channel relationships with their OEM partners (gold, silver, etc) will be represented in the best pricing offered. Delivery orders may restrict the use of specific OEMs or identify required OEMs.

3.5.1.1.4. Technical Refresh

In order to ensure new design enhancements and technological updates or advances, the contractor shall offer, under this contract, hardware and software components available to the contractor's commercial customers. Furthermore, the contractor shall make available any commercially available updates to the hardware and software provided under this contract. If such updates are available to other customers without charge, then they shall also be made available to the Government without additional charge. The contractor will ship these updates to existing customers who have acquired the hardware/software being updated under this contract. Vendor commercial product offerings shall include “state of the art” technology, i.e., the most current proven level of development available in each product category.

3.5.1.1.5. Products.

The contractor shall provide all products, peripherals, and associated peripheral equipment as required by each individual delivery order. The “products” are commercial items as defined by FAR 2.101. All documentation, software, and user guides that are commercially packaged with the product shall be provided to the Government. All proposed products must be compliant with the Trade Agreements Act of 1979 (TAA). In accordance with DFARS 252.225-7021, the Trade Agreements Certificate at DFARS 252.225-7020 shall be provided as requested by the Ordering Contracting Officer for any end item offered in response to any RFQ issued under this contract. Please note that Federal Acquisition Regulation (FAR) paragraph 25.103(e) includes an exemption from the Buy American Act (BAA) for acquisition of information technology that are commercial items. If further clarification is required contact the Contracting Officer or submit your questions to www.netcents.af.mil. The contractor shall ensure that products meet the standards identified in the AF Standards Center of Excellence Repository (SCOER) located at netcents.af.mil.

3.5.1.1.6. Standards and Certifications

Certifications, specifications, standards, policies and procedures are listed in the Products Standards document in AF Standards of Excellence Repository section of the NETCENTS-2 Products website: (http://www.netcents.af.mil/contracts/netcents-2/products/documents/index.asp). The referenced certifications, specifications, standards, policies and procedures represent possible constraints that may be placed on individual contract delivery orders. Individual delivery orders may impose additional standards to those required at the contract level. The referenced list is not all-inclusive and the most current version of the document at the time of delivery order issuance will take precedence. Other documents required for execution of tasks issued under NETCENTS-2 will be cited in the relevant Delivery Order. Web links are provided wherever possible.

3.5.1.1.6.1. Quality Certification

The contractor shall be ISO 9001:2008 (or higher), or ISO/IEC 20000 (or higher) certified for the entire performance period of the contract, inclusive of options. This certification must be held at the organizational level of the legal entity performing the contract.

3.5.1.2. Specific Product Categories

The following paragraphs describe the types of products that are considered to comprise each of the product categories. The list of sub-categories with associated baseline performance specifications are found in Section J, Attachment 4 of this document and will be updated annually. The contractor shall provide ALL of the equipment items in ALL product categories unless modified by delivery orders.

3.5.1.2.1. Networking Equipment.

The contractor shall provide networking equipment such as network devices, appliances, switches, hubs, gateways, routers, firewalls, bridges, repeaters, wireless networking devices, microwave radios (data, voice, video), Land Mobile Radios (LMR), satellite communications terminals, adapters, associated cables, interface cards, multiplexers, Voice over IP (VoIP), modems, cabinets, converters, test equipment (including, but not limited to, sensors, probes, data collectors, and user emulation analysis tools), proxies, network security appliances and Global Positioning System (GPS) timing systems.

3.5.1.2.2. Servers/Storage.

The contractor shall provide network servers, such as low-end servers (tower, rack-mount), medium-end servers (tower, rack-mount, blade), high-end servers (tower, rack-mount, blade), operating systems including, but not limited to, Exchange Server; Microsoft SMS Server; Windows Server; Linux Enterprise; Red Hat Linux Enterprise; Open VMS; Unix; Unix; Netware; Solaris; Unixware/OpenServer; VMware; Network Attached Storage (NAS), Storage Area Networking (SAN) devices; hard drive/tape drive array, external hard drives, optical drives, CD, DVD, Tape Storage Media; portable storage devices, and various JBODs (Just a Bunch of Disks/Drives) configuration. Unless modified by delivery orders, all Microsoft network infrastructure role-based servers, including File Servers, Print Servers, Outlook Web Access Servers, Exchange Servers, SharePoint Servers and SQL 2005 servers, must comply with the AF Standard Server Configuration (SSC) which is managed by the 754th ELSG/DON Air Force Enterprise Configuration Management Office (AFECMO).

3.5.1.2.3. Peripherals.

The contractor shall provide any components that directly support the proposed platforms such as various processors with different clock rates, memory modules and upgrades, video cards, network interface cards, interface adapter cards, expansion bay, internal cables, processor/motherboard upgrades, keyboard/mouse, memory cards, power strips, USB hubs, card readers, speakers, external connection cables, expansion chassis, monitors, power adapters, Wi-Fi adapters, faxes, printers, scanners, peripherals (including monitors), Uninterruptible Power Supplies (UPS), Power Distribution Units (PDU), Surge Suppressors, power strips, USB hubs, card readers, computer speakers, touch pads, data terminals, cameras (Web, Network, Wireless), power adapters/cords, antennas, computer switches, Keyboard/Video/Mouse (KVM) switches, printers (multi-function, laser, inkjet, color/BW, line matrix, plotter), scanners, standard and touch-screen monitors, keyboards/mice, port replicators, computer (display/input) terminals, disc back-up and replication equipment, message archivers, patch panels, warranty variations, and operating systems/licenses when not covered or provided under other existing Government enterprise agreements.

3.5.1.2.4. Multimedia.

The contractor shall provide all types of multimedia devices, such as multi-functional, standalone displays (e.g., plasma screens, HDTVs), video devices, DVD/VCR players, Video Teleconferencing (VTC) equipment (projectors, speakers, microphones, video converters/transmitters, etc.), text devices, audio devices, devices that produce still images, animation, video, and interactive media.

3.5.1.2.5. Software.

The contractor shall supply commercial software products, sold independently of hardware, related to netcentric mission areas such as Network Management, Network Defense, Server Virtualization, Collaboration, Security, Geo-based, E-learning, Database Performance Tuning, Database Warehousing, and Web Development. Other types of software required may include, but not be limited to, storage, database, messaging, backup/recovery, archiving, compliance, provisioning, patch management, asset management, data visualization, business analytics, information assurance and development tools, and Virtualization software management tools.
Unless modified by delivery orders, in situations where the purchase of new COTS software is needed to satisfy the requirements of a particular delivery order, the customer shall first be required to review and utilize (if available) the DoD's Enterprise Software Initiative (ESI) source. The listing of COTS software available from DoD ESI sources can be viewed on the web at http://www.esi.mil. In the event that the software required is not available to the customer through a DoD ESI source, the customer will be authorized to obtain the software through this contract or other authorized contracts. The DoD is expected to award new ESI vehicles throughout the life of the NETCENTS-2 contract.

3.5.1.2.6. Identity Management/Biometric Hardware and Associated Software.

The contractor shall supply identity management/biometric products and associated software, such as Electronic Fingerprint Images, Iris Images, Face Recognition, Hand Geometry, Speaker Recognition (telephony based and web based), Multi-modal Biometric Jump Kit, Smart Card Reader (fingerprint), Fingerprint Reader, Palm Vein Authentication, and Public Key Infrastructure (PKI) / Common Access Card (CAC) devices.

3.5.1.3. Product Support Requirements

The contractor shall adhere to the following requirements when providing products under this contract.

3.5.1.3.1. Product Delivery Capability.

The contractor shall deliver the quantities of Network-Centric products to meet ordinary as well as fluctuating (war-time, Terrorist Tempo, Ops Tempo) government requirements in accordance with prescribed delivery schedules stipulated in individual delivery orders. Delivery of products will be to CONUS, OCONUS, and remote locations as identified below. For AOR's and/or remote sites that do not permit commercial deliveries, the vendor's delivery capabilities must be in accordance with AFI 24-203, Preparation and Movement of Air Force Cargo, 13 April 2007. Additional delivery terms or schedules, such as ship-in-place, expedited shipping or shipping to APO/FPO addresses, shall be negotiated between the Contractor and the Ordering Contracting Officer (OCO) at the Delivery Order level. The contractor shall have the capability to simultaneously deliver large volumes of products to multiple locations worldwide.
1. CONUS: The 48 contiguous states, Alaska, Hawaii, and the District of Columbia.
2. Named OCONUS: Germany, Italy, Japan, Korea, Belgium, Turkey, Puerto Rico, United Kingdom, and the Netherlands.
3. Remote OCONUS: those locations that are not listed under CONUS or Named OCONUS.

The following table sets forth the performance parameters for deliveries:

Timeframe	CONUS	OCONUS	Remote OCONUS
Routine	NLT 30 calendar	NLT 45 calendar	NLT 45 calendar
Critical	NLT 3 calendar days	NLT 5 calendar days	NLT 10 calendar
Emergency/War	Within 24 hours	Within 48 hours	Within 72 hours

Table 1. Delivery Performance Parameters

3.5.1.3.1.1. Delivery Delays

Contractors are required to meet the timeframes stated in this paragraph unless Department of Commerce approval and/or review activities prevent the contractor from meeting these timeframes. In the event that the contractor determines they are unable to achieve the stated timeframes, the contractor shall notify the Contracting Officer within two (2) business days of such determination, or immediately upon such determination if operating under the Emergency/War Tempo timelines.

3.5.1.3.1.1.1. Items on Backorder

In their response to a Request for Quote (RFQ), the contractor shall provide notification, if applicable, that a particular item is on backorder, the expected lead-time to fulfill the order, etc. It shall be implicit that a response to an RFQ with no items identified on backorder, is a declaration that the items are available at the time of quote submission.

3.5.1.3.1.1.2. Installation.

In the rare instances where installation services are required, the contractor shall provide installation support related to the applicable products(s) as defined in the delivery order. In those instances, the DD Form 254 (DEPARTMENT OF DEFENSE CONTRACT SECURITY

CLASSIFICATION SPECIFICATION)
requirements will be addressed in the individual delivery order and only at the security level necessary.

3.5.1.3.1.1.3. Warranty.

The contractor shall provide any OEM pass through warranty and standard commercial warranties applicable to the products being purchased at no cost. This shall apply to new, refurbished and remanufactured equipment. Additionally, extended warranties may be purchased as defined in each delivery order.

3.5.1.3.1.1.4. Customer Support.

The prime contractor shall provide 24x7 live telephone support during the warranty period to assist in isolating, identifying, and repairing software and hardware failures, or to act as liaison with the manufacturer in the event that the customer requires assistance in contacting or dealing with the manufacturer.

3.5.1.3.1.1.5. Product Maintenance.

The contractor shall provide associated maintenance and upgrades to include spares/parts and emergency support worldwide, during the warranty period, or as required in delivery orders.

3.5.1.3.1.1.6. Special Asset Tagging

When required and defined by the Delivery Order, the contractor shall provide special asset tags IAW DODI8320.04, Item Unique Identification (IUID) Standards for Tangible Personal Property, to include Unique Identification (UID) tagging requested by non-DoD customers.

3.5.1.3.1.1.7. Radio Frequency Identification (RFID)

When required and defined by the Delivery Order, the contractor shall provide RFID tagging IAW DoD Radio Frequency Identification (RFID) Policy, 30 July 2004 or most current version. RFID tagging is mandatory for deliveries as follows:
1. Major end items (items with an acquisition cost of $5000 or more) delivered to the sites identified in Attachment 3 of the RFID policy; and
2. All shipped cases, pallets, and items with a UID tag.

3.5.1.3.1.1.8. Software Tagging

When required and defined by the Delivery Order, commercial off-the-shelf software items shall support International Standard for Software Tagging and Identification, ISO/IEC 19770-2, Software Tags when designated as mandatory by the standard.

3.5.1.3.1.1.9. TEMPEST Requirements

TEMPEST is the codename referring to investigations and studies of compromising emanations. Compromising Emanations are defined as unintentional intelligence-bearing signals which, if intercepted and analyzed, may disclose the information transmitted, received, handled, or otherwise processed by any information-processing equipment and analyzed, may disclose the information transmitted, received, handled, or otherwise processed by any information-processing equipment. When required and defined by the Delivery Order, the contractor shall provide

commercially available TEMPEST-compliant communications and information processing devices.

3.5.1.3.1.1.10 Remanufactured/Refurbished Products

Any product offering that is remanufactured or refurbished shall be clearly identified as such by the contractor. Remanufactured products shall have the OEM or factory certification if available for that product.

3.5.2 Enterprise Software Initiative

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

Solutions task order Contracting Officer will authorize the contractor to use existing enterprise licenses or ESI vehicles for task orders issued under this contract. Task orders may be modified as applicable to meet IC or other functional community requirements.

3.5.3 Software License Management

When required at the task order level, the contractor shall provide maintenance and support to control the entire asset life-cycle, from procurement to retirement, which includes applications, license agreements as well as software upgrades. The contractor shall provide asset inventory and services that track the financial aspects of an asset to include cost and depreciation, contract management, leases, maintenance agreements and service contracts. The contractor shall provide support summary information to include the general terms and conditions, benefits, strategic and tactical directions, license ordering information, internal billing process, pricing and deployment and support of the products included in the agreement. The contractor shall support common practices for ordering assets, tracking orders and assets, and tagging the assets. The contractor shall support application installation, operations, customer support, training, maintenance, sustainment, and configuration control, to include the procurement of supporting software licenses. (paragraph added)

3.5.4 Hardware

All hardware provided in support of solutions under this contract shall include all software and associated hardware required for operations (such as controllers, connectors, cables, drivers, adapters, etc.) as provided by the OEM.

3.5.5 Software Support

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

3.5.6 Government Furnished Equipment

Under some task orders, the Government will provide products acquired under this contract, other contracts, and GFE identified in site specific task orders. The contractor's design shall incorporate existing systems/subsystems to the maximum extent possible, based on cost/technical tradeoff analysis conducted during the engineering process to ensure security and resource sharing of both Government Furnished Equipment (GFE) and Contractor Furnished Equipment (CFE).

3.5.7 Host Nation Installations

As specified by the task order, the contractor shall use commercial telephone industry installation standards as documented in TL9000 compliant procedures for accomplishment of all installation work unless otherwise prohibited by host nation regulations and/or standards. The contractor shall determine if any host nation restrictions are applicable to any installation. The contractor shall be responsible for compliance with all host nation labor, safety, and environmental laws, regulations, and standards applicable at each installation location. If any additional permits or regulations apply, the contractor shall inform the Government and provide a proposal to initiate the appropriate documentation upon approval from the Government.

3.5.8 Tools and Test Equipment

Unless specified otherwise in the Task Order, the contractor shall provide all tools and test equipment required to perform any required product installation and maintenance as called for by the task order. All tools and test equipment shall remain the property of the contractor.

3.5.9 Warranty

Each product shall include a warranty as specified in Section I, Clause 52.246-17. In addition to FAR Clause 52.246-17, the following additional requirements apply: Users shall have highly reliable and maintainable network-centric products and system solutions to interoperate with the described environment. Components shall be maintainable by the user without voiding the warranty coverage. Components, which are expandable, shall be expandable by the user without voiding the warranty coverage provided the Government adheres to standard commercial practices in accomplishing the additions. Four types of warranty shall be provided:

1. System Warranty
2. Workmanship Warranty
3. Construction Warranty
4. Equipment Warranty

The warranty program shall provide for restoration of the system and repair of equipment in a timeframe specified in this contract, unless stated otherwise in the Task Order. The Contractor shall provide means to transport equipment and bear transportation charges and responsibility for equipment and repair personnel under warranty while in transit both to and from the Government site.

3.5.9.1 System Warranty

Unless specified otherwise in the Task Order, the Contractor shall provide a minimum one-year system warranty (some customers may require two or more years of warranty) to include coverage of all equipment supplied, installed, and integrated by the Contractor associated with delivery of infrastructure capabilities as defined by the AF enterprise architecture.. The system warranty shall ensure the full operational use of the system (CFE and GFE). The Contractor shall provide to the Government a 24-hour a day, 7-day a week point of contact for the system warranty. The system warranty shall begin at the time the final system DD Form 250 is signed by an authorized Government representative. The system warranty shall provide fault diagnosis, hardware and software repair, replacement, or redesign. The Contractor shall be responsible for diagnosing any problems, identifying malfunctioning equipment, and removing the equipment for repair. Prior approval shall be obtained from the authorized Government site representative before any GFE is removed from the system. Actual repair of malfunctioning GFE will be the responsibility of the Government, unless stated otherwise in the Task Order. The system warranty shall include transportation for both Contractor personnel and equipment to and from the specific site. The system warranty shall provide for a return to service any malfunctioning CFE component or applications within 48 clock hours CONUS, 96 clock hours OCONUS after notification by the authorized Government site representative unless stated otherwise by the Task Order. Costs for system warranty will be included within each Task Order proposal provided by the contractor as required by the Task Order.

In lieu of a system proposal that includes a traditional warranty, the Customer and Contractor may agree to a basic system proposal plus a block of hours for Contractor Maintenance Support Services. For many Contractors and Customers, this strategy has proven advantageous since traditional system warranties can be voided by today's dynamically changing networks forcing the Customer to maintain the network in a static environment during the warranty period. In addition, support is limited to a much narrower scope with a traditional system warranty whereas a Contractor Support Services contract is much more flexible in solving problems as they arise within the entire Network-Centric environment.

3.5.9.2 Workmanship Warranty

Unless specified otherwise in the Task Order, the Contractor shall provide a minimum one year workmanship warranty (some customers may require two or more years of warranty) on all work provided

or integrated under this contract. The warranty shall ensure the full operational use of the system (CFE and GFE). The Contractor shall provide to the Government a 24-hour a day, 7 day a week point of contact for the workmanship warranty. The workmanship warranty shall begin at the time the final system DD Form 250 is signed by an authorized Government representative. The workmanship warranty shall provide fault diagnosis, hardware and software repair, replacement, or redesign. The Contractor shall be responsible for diagnosing and fault isolation of any problems, identifying the poor workmanship causing the problem and affecting an acceptable industry standard repair. Prior approval shall be obtained from the authorized Government site representative before any GFE is removed from the system. Actual repair of malfunctioning GFE will be the responsibility of the Government. The workmanship system warranty shall include transportation for both Contractor personnel and bits, pieces, and parts to and from the specific site and the actual repair. The workmanship warranty shall provide for a return to service any malfunctioning CFE component or applications within 48 clock hours CONUS, 96 clock hours OCONUS after notification by the authorized Government site representative unless stated otherwise by the Task Order.

3.5.9.3 Construction Warranty

Unless specified otherwise in the Task Order, the Contractor shall provide a minimum one-year construction warranty (some customers may require two or more years of warranty) on all work provided or integrated under this contract. The warranty shall ensure the full operational use of all work. The Contractor shall provide to the Government a 24-hour a day, 7-day a week point of contact for the construction warranty. The construction warranty shall begin at the time the final system DD Form 250 is signed by an authorized Government representative. The construction warranty shall provide fault diagnosis, repair, replacement, or redesign. The Contractor shall be responsible for diagnosing and fault isolation of any degradation problems, identifying the poor construction-ship causing the problem and affecting an acceptable industry standard repair. Prior approval shall be obtained from the authorized Government site representative or Government QAP before affecting any repair. The construction warranty shall include transportation for Contractor personnel, bits, pieces, and parts to and from the specific site and the actual repair. The construction warranty shall provide for a return to service any degrading component or area within 48 clock hours CONUS, 96 clock hours OCONUS after notification by the authorized Government site representative unless stated otherwise by the Task Order.

3.5.9.4 Equipment Warranty

Unless specified otherwise in the Task Order, the Contractor shall provide standard, OEM pass through, extended or otherwise warranties for the periods specified in the Task Order for all hardware and software products, for both CONUS and OCONUS Government sites located worldwide. Repairs shall be accomplished within 48 clock hours CONUS, 96 clock hours OCONUS of receipt of the equipment warranty trouble call, unless stated otherwise by the Task Order, when the Contractor is performing the warranty repair. The warranty shall also provide for repair or replacement of equipment and repair and distribution of updated software to all users who purchased the software from this contract. Warranty coverage commences on the date of acceptance in block 21B of the DD Form 250, Commercial Invoice dated and signed, or SF 1449 dated and signed.

The Contractor shall provide a worldwide warranty repair solution capability for systems with qualified maintenance repair personnel and leverage existing OEM support infrastructures to the greatest extent possible. Repairs shall be performed at a time required by the Task/Delivery Order/Delivery Order or as coordinated by the Government QAP. The Contractor shall provide a 24-hour, 7-day a week warranty repair point of contact to receive calls from the Government. The Contractor shall provide the capability for toll-free telephone access for obtaining technical warranty repair support assistance from worldwide locations. The Contractor shall provide the tools, equipment and consumables required for personnel to complete their duties. The Contractor shall not invalidate the warranty provided on components purchased under this contract when the Government elects to perform user self maintenance and/or self-installation during the warranty period. Note: The Government will perform routine user-maintenance for all equipment both during and after the warranty period using separately orderable spare parts and/or repaired parts from this contract. The Government will only be liable for any damage to the equipment that results from Government Maintenance or additions to equipment that did not adhere to stand commercial practice. At

no additional charge to the Government, the Contractor shall furnish, for hardware purchased under this contract, all repairs (labor and parts) for the duration of the warranty period. At a minimum, repair during the warranty period shall be equivalent to standard per-call maintenance during the principal period of maintenance (PPM) as specified in this PWS. The Government, at its option, may order additional repair coverage during the warranty period. The Governments purchase of additional repair coverage will be specified in details by the task order.

All parts replaced during the warranty period, in an unclassified environment, shall become the property of the Contractor. However, in classified environments the Government will maintain title of certain items. These items typically will be broken storage devices/mediums. All other parts may be returned to the contractor and the government will have up to 30 days to relinquish possession of the part.

The warranty shall not apply to maintenance required due to the fault or negligence of the Government. If Government negligence results in a repair call (either for equipment under warranty or per call maintenance), the maximum repair time shall not apply and the Government will pay the price per hour specified in the contract for the hours rendered to complete the repair.

Only new or reconditioned parts shall be provided for repairs. If reconditioned parts are provided, the reconditioned parts shall carry the same warranty provisions as originally provided by the Contractor for new parts.

The Contractor guarantees to repair at no charge any malfunction which reoccurs within 90 calendar days of the initial repair. Warranty of Repair is a separate warranty from those described elsewhere in the contract.

If the Contractor elects to replace the malfunctioning hardware, the Contractor shall either provide the Government with a permanent replacement which shall contain a unique serial number or shall provide the Government with a temporary replacement with a unique serial number. If the Contractor elects to repair the malfunctioning hardware, the Contractor shall repair and return the repaired hardware to the Government at which time the temporary replacement shall be surrendered to the Contractor at the contractor’s expense.

3.6 Maintenance

Unless specified otherwise in the Task Order, the contractor shall provide a worldwide maintenance solution capability (on-site and on-site per-call) for systems provided under this contract with qualified maintenance personnel, leveraging existing OEM support infrastructures to the greatest extent possible. Maintenance shall be performed at a time required by the task order or as coordinated by the Government QAP. The contractor shall provide a maintenance POC 24-hours-a-day, 7-days-a-week to receive calls from the Government. The specific maintenance requirements will be included in the task order and may include maintenance on systems/equipment not purchased under this contract. The contractor shall provide the capability for toll-free telephone and e-mail access for obtaining technical maintenance support assistance from worldwide locations. The contractor shall provide remote engineering and technical support via telephone or other remote system capabilities to assist maintenance personnel, analyze software, hardware, system problems and provide problem resolutions. This support may consist of routine maintenance, testing, diagnostic fault isolation, problem resolution, activation of features and/or equipment, software configurations and general information on features or capabilities of equipment. All requests for remote maintenance services shall be acted upon immediately upon receipt of the request and logged for inclusion in a service ticket status log of some type. The requesting unit shall be notified of the current status of corrective actions for hardware and software related problems that cannot be immediately corrected. The contractor shall provide the tools, equipment and consumables required for personnel to complete their duties.

3.6.1 Per-Call Maintenance/Standard Per-Call Maintenance (SPCM)

Unless specified otherwise in the Task Order, the contractor shall provide the Government with on-site per-call maintenance at the Government location for all cable plant and non-cable plant items. One instance of a per-call maintenance visit shall include the repair of all units identified at the time the Government notification call to the vendor was placed. The minimum charge per-call shall not exceed one (1) labor hour. The maximum charge per-call shall not exceed any limitations (labor and parts) indicated by the Government at the time of the maintenance call without prior approval from the designated Government official and as funded in the applicable task order. Hourly rate charges shall commence when the contractor representative reports to the Government site representative indicated in the call. Outside the Principal Period of Maintenance (OPPM) is defined as all time other than the PPM. If a call is placed during the OPPM or, if the Government wants the weekend/holiday time to count toward time to repair, then the OPPM rate may be applicable. The OPPM rate shall be applicable only if specifically requested by the Government at the time of the maintenance call and approved by the contracting officer.

3.6.2 Contractor Provided Non-Cable Plant, Non-Switching System SPCM

Unless specified otherwise in the Task Order, the contractor shall have, from the time of notification of equipment failure(s), a maximum of 8 hours to respond and 48 hours to complete the repair(s) or replace (at the user's site) the malfunctioning system(s) or components for CONUS or 16 hours to respond and 96 hours to complete the repair(s) or replace (at the user's site) the malfunctioning system(s) or components for OCONUS, unless otherwise stated in the task order.

3.6.3 Government Owned Equipment Non-Cable Plant, Non-Switching System SPCM

Unless specified otherwise in the Task Order, the contractor shall maintain the non-cable plant and non-switching systems (i.e., microwave radios, UPS equipment, multiplexers, antennas, LAN/CAN/MAN/WAN equipment, VTC equipment, phones, land mobile radios (LMR) Air Traffic Control and Landing Systems (ATCALS) and Meteorological and Navigational Aid (METNAV)) and those provided by the contractor under this contract. The contractor shall have, from the time of notification of equipment failure(s), a maximum of 8 hours to respond and 48 hours to complete the repair(s) or replace (at the user's site) the malfunctioning system(s) or components for CONUS or 16 hours to respond and 96 hours to complete the repair(s) or replace (at the user's site) the malfunctioning system(s) or components for OCONUS, unless otherwise stated in the task order.

3.6.4 Switching System SPCM

Unless specified otherwise in the Task Order, the contractor shall have, from the time of notification of equipment failure(s), a maximum of 4 hours to respond and 24 hours to complete the repair(s) or replace (at the user's site) the malfunctioning system(s) or components for CONUS or 8 hours to respond and 72 hours to complete the repair(s) or replace (at the user's site) the malfunctioning system(s) or components for OCONUS, unless otherwise stated in the task order (i.e., non-ISDN/ISDN capable, DSS, etc.).

3.6.5 Cable Plant Maintenance

Unless specified otherwise in the Task Order, the contractor shall have, from the time of notification of equipment failure(s), a maximum of 2 hours to respond and 8 hours to complete the repair(s) or temporarily replace or patch the malfunctioning components for CONUS or 4 hours to respond and 12 hours to complete the repair(s) or temporarily replace or patch the malfunctioning components for OCONUS, unless otherwise stated in the task order. This maintenance shall include inside and outside cable plant maintenance. If the Government cannot provide drawings identifying placement of both inside and outside cable components to be maintained, then the Government will order a cable-plant survey via task order using the applicable labor categories; the contractor shall not be held accountable for any repair timeframes until the Government provides such drawings. The contractor shall also provide, on a pre-

scheduled basis, preventative and routine maintenance required for optimized usage and life of the existing cable plant on a per-call basis. Within 24 hours of a repair or patch that restores service using a temporary repair, the contractor shall provide the Government with a draft list for components that were temporarily repaired until permanent replacements could be obtained. In this event, the contractor shall provide a firm-fixed-price proposal to the user for installation of the components identified in the draft list.

3.6.6 Rapid Response Per-Call Maintenance (RRPCM)

For RRPCM, the contractor shall have a maximum time of 2 hours from the time of notification of failure(s) to respond, unless stated otherwise in the task order. Repair time shall be within 12 hours.

3.6.7 System Maintenance

Unless specified otherwise in the Task Order, the contractor shall provide all supplies, parts, tools, and test equipment required for maintenance of the system and be responsible for total system maintenance.

3.6.8 Maintenance Charges

The per-call maintenance charge may include the CLIN labor rate, travel and ODCs, and transportation of any equipment, as applicable. Replaced faulty parts shall remain the property of the Government.

3.6.9 Maintenance Alternative

The Government may select maintenance alternative (standard or rapid per call response) with the issuance of a task order. The Government shall have the option to change the type of maintenance by giving the contractor thirty (30) days notice and a contract modification. Any change in type of maintenance will not be considered a partial termination of the task order for the convenience of the Government.

3.6.10 Relocation and Removal

The contractor shall relocate and remove systems as specified in the task order. The contractor shall be responsible for storage, staging and deployment of any equipment and materials provided as part of awarded task orders unless otherwise mutually agreed upon by the contractor and the Government. If removal of equipment and/or material is necessary, the contractor shall be responsible for disposal and shall comply with all applicable industry rules and regulations. Any equipment removal and/or disposal shall be coordinated with a designated official at the host base communications squadron.

3.7 Surge Requirements

Surge requirements include greater than expected requirements/workload for existing services within the scope of Task Orders awarded. Normally, surge requirements are of short duration, from one to six months. An example of a surge requirement is additional help desk or system maintenance support personnel required to handle temporarily increased workloads because of war or contingency. Surge requirements shall be accomplished as required under the Task Order.

3.8 Unified Capabilities Requirements (UCR)

Unless specified otherwise in the Task Order, the contractor shall report to the government through quarterly PMRs, how each solution awarded meets the Unified Capabilities Requirements (UCR). Detail shall include, but not be limited to the applicable MILDEP Service Level Architecture requirements. For example, vendor

shall report how each awarded solution that is implemented at a United States Air Force Installation meets the United States Air Force i-TRM Architecture requirements. Similar report requirements including the ConstellationNet Architecture may also be requested at the Task Order level.

3.9 Special Asset Tagging

When required and defined by the Delivery/Task Order, the contractor shall provide special asset tags IAW DODI8320.04, Item Unique Identification (IUID) Standards for Tangible Personal Property, to include Unique Identification (UID) tagging requested by non-DoD customers.

4. CONTRACT REQUIREMENTS

The following contract requirements are applicable to all Task Orders.

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:

1. Provide quality products, incidentals and customer support;
2. Meet customer's agreed-upon timelines for scheduled delivery of items, warranty, and/or incidental services: Emergency/critical, Maintenance/Warranty – 24 x 7 x 365, and remote OCONUS, OCONUS vs. CONUS response times;
3. Provide satisfactory product repairs or advance replacement, as appropriate;
4. Provide timely and accurate reports;
5. Respond to the customer's requests for proposals and configuration assistance as identified in each delivery order;
6. Meet subcontracting goals.

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.

4.2.1 Services Delivery Summary

The contractor's performance at the contract level will be assessed quarterly by a process that measures success towards achieving performance objectives as defined in Table 1 below. The contractor will be responsible for delivering applicable performance data in a formal report titled Contractor Performance Report (Exhibit A, CDRL A004). The performance metrics reporting will be in accordance with AFI 63-124, Performance Based Services Acquisition and FAR Subpart 37.6, Performance-Based Acquisition. Service Level Agreements will be defined in each task order.

Desired Outcome		Performance Objective	Performance Threshold	
Overall Outcome	Specific Outcomes		Target	Tolerance
Compliance with NetOps and Infrastructure Solutions support requirements (delivery, quality)	Ensure compliance with NetOps and Infrastructure Solutions deliverables requirements	Deliver the NetOps and Infrastructure Solutions w/ predetermined outcomes and on time	Documentation submitted IAW CDRL A001 verifies the task order was completed on time	98% of the time

Compliance with NetOps and Infrastructure Solutions support requirements (delivery, quality)	Ensure compliance with NetOps and Infrastructure Solutions Customer Support requirements	Customer Support Availability for NetOps and Infrastructure Solutions provided under contract	24x7 Live Customer Support assistance is provided if required by task order	98% of the time
Compliance with NetOps and Infrastructure Solutions support requirements (delivery, quality)	Ensure completed task orders are invoiced and submitted to the Government in a timely manner.	Invoices are received by the Government from the contractor within 30 calendar days of completion of task order.	Documentation submitted IAW CDRL A001 verifies invoices were submitted on time	99% of the time
Compliance with NetOps and Infrastructure Solutions support requirements (delivery, quality)	Ensure delivery of all CDRLs by the contractor within the timeframe identified	Completed on time or ahead of schedule	CDRLs are delivered as identified	98% of the time
Compliance with NetOps and Infrastructure Solutions support requirements (delivery, quality)	Ensure adherence to quality requirements of all CDRLs by the contractor	Quality CDRLs (conforming to design, specification or requirements) are delivered according to performance parameters	Quality CDRLs are delivered as identified	98% of the time
Compliance with NetOps and Infrastructure Solutions Requirements	Ensure NetOps and Infrastructure Solutions provided by the contractor are fulfilled within the timeframe identified by the task order	Task orders are completed on time or ahead of schedule	Documentation submitted IAW CDRL A001 verifies task order was completed on time	98% of the time
Compliance with Small Business Subcontracting Requirements	Contractor meets small business requirements	SB requirements listed in Clause H133 or in the Subcontracting Plan, whichever is greater, are met	Documentation submitted, Exhibit A, CDRL A005, verifies SB requirements were met	100% of the time

Table 1. Minimum Required Performance Metrics

4.2.2 Task Order Management.

The contractor shall establish and provide a qualified workforce capable of performing the required tasks. The workforce may include a project/task order manager who will oversee all aspects of the task order. The contractor shall use key performance parameters to monitor work performance, measure results, ensure delivery of contracted product deliverables and 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 task order 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 Task Order Proposals. The contractor shall provide the Government with electronic access to this data, including access to printable reports. The contractor shall have an approved property control system IAW FAR 45, DFARS 245, and approved procedures to document and track all GFM and Government Furnished Equipment (GFE). The contractor shall provide as-built documentation including, but not limited to, drawings and diagrams of the solution provided under each Task Order identifying specific cards in a chassis/shelf. The as-built documentation shall also include layout drawings, power drawings/specifications, floor plans and engineering specifications generated in support of the installation of the system. Documentation shall also include equipment listing with serial/model numbers, and manufacturer specifications.

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 Network Operation (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).

4.2.5 Security Management

4.2.5.1 Transmission of Classified Material

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 Task Order.

4.2.5.2 Personnel Security.

Individuals performing work under these task orders shall comply with applicable program security requirements as stated in the task order. NETCENTS-2 will support the following levels of security: Unclassified; Unclassified, But Sensitive; Secret (S); Secret Sensitive Compartmented Information (S/SCI); Top Secret (TS); and Top Secret Sensitive Compartmented Information (TS/SCI)

Certain task orders may require personnel security clearances up to and including Top Secret, and certain task orders may require all employees to be United States citizens. The security clearance requirements will depend on the security level required by the proposed task order. The task orders may also require

access to sensitive compartmented information (SCI) for which SCI eligibility will be required. Contractors shall be able to obtain adequate security clearances prior to performing services under the task order. The Contract Security Classification Specification (DD Form 254) will be at the basic contract and task order level and will encompass all security requirements. All contractors located on military installations shall also comply with Operations Security (OPSEC) requirements as set forth in DoD Directive 5205.02, Operations Security Program and AFI 10-701, Operations Security. In accordance with DoD 5200.2-R, Personnel Security Program (Jan 87), DoD military, civilian, consultants, and contractor personnel using unclassified automated information systems, including e-mail, shall have, at a minimum, a completed favorable National Agency Check plus Written Inquiries (NACI).
The types of Personnel Security Investigations (PSI) required for the contractor vary in scope of investigative effort depending upon requirements of the Government and/or conditions of the contract/task order. In cases where access to systems such as e-mail is a requirement of the Government, application/cost for the PSI shall be the responsibility of the Government. In cases where access to systems is as a condition of the contract/task order, application/cost for the appropriate PSI shall be the responsibility of the contractor. In such instances the contractor shall diligently pursue obtaining the appropriate PSI for its employees prior to assigning them to work any active task order. Acquisition planning must consider antiterrorism (AT) measures when the effort to be contracted could affect the security of operating forces (particularly in-transit forces), information systems and communications systems IAW DoD Instructions 2000.16 Anti Terrorism Standards.

4.2.5.3 Protection of System Data

Unless otherwise stated in the task order, the contractor shall protect system design-related documents and operational data whether in written form or in electronic form via a network in accordance with all applicable policies and procedures for such data, including DOD Regulations 5400.7-R and 5200.1-R to include latest changes, and applicable service/agency/ combatant command policies and procedures. The contractor shall protect system design related documents and operational data at least to the level provided by Secure Sockets Layer (SSL)/Transport Security Layer (TSL)-protected web site connections with certificate and or userid/password-based access controls. In either case, the certificates used by the Contractor for these protections shall be DoD or IC approved Public Key Infrastructure (PKI) certificates issued by a DoD or IC approved External Certification Authority (ECA) and shall make use of at least 128-bit encryption.

4.2.6 On-Site Task Approval Process

The contractor shall, for CONUS tasks (7-day notice) and for OCONUS tasks (14-day notice), notify the on-site QAP in writing before a requirements analysis/conceptual design visit, site survey, and other on-site tasks are to be performed. The following information must be provided; Names of Employees, SSAN, Security Clearance, Location, Project Number, On/About Date Planned for On-Site Work, Anticipated Duration of Visit, Support Required.

4.2.7 Travel Requirements

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

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

4.2.8 Other Direct Cost (ODC)

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

5. DELIVERABLES

The Government requires all deliverables that include Scientific and Technical Information (STINFO), as determined by the Government, be properly marked IAW DoD Directive 5230.24 and AFI 61-204 prior to initial coordination or final delivery. Failure to mark deliverables as instructed by the government will result in non-compliance and non-acceptance of the deliverable. The contractor 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.

The contractor shall provide reports identified below. The format for each can be found in Section J, Exhibit A.

CDRL A001: Delivery Order Status Report (DOSR),
CDRL A002: Fiscal Year Order and Financial Status,
CDRL A003: Annual Execution Review to AFPEO/CM
CDRL A004: Contractor Performance Report
CDRL A005: Small Business Subcontracting Report
CDRL A006: Contractor Manpower Reporting(CDRL A006 was added)
CDRL B001: Small Business Participation

Manpower Reporting(A006)

The contractor shall report ALL contractor labor hours (including subcontractor labor hours) required for performance of services provided under this contract for NETOPS F&O via a secure data collection site. The contractor is required to completely fill in all required data fields at http://www.ecmra.mil.

Reporting inputs will be for the labor executed during the period of performance for each Government fiscal year (FY), which runs 1 October through 30 September. While inputs may be reported any time during the FY, all data shall be reported no later than 10 October* of each calendar year. Contractors may direct questions to the CMRA help desk.

Uses and Safeguarding of Information: Information from the secure web site is considered to be proprietary in nature when the contract number and contractor identity are associated with the direct labor hours and direct labor dollars. At no time will any data be released to the public with the contractor name and contract number associated with the data.

6. ELECTRONIC ORDERING

The vast majority of NETCENTS-2 products, services, or solutions will be procured using Requests for Quotes (RFQs) and Requests for Proposals (RFPs). The contractor shall establish a web site that is interoperable (electronically and procedurally) with the NETCENTS Portal, its follow-on (e.g., AFWAY II), or equivalent, within 30 working days after contract award to manage, report, and provide indicative data/status on all delivery orders, RFQs, and RFPs. The contractor shall maintain an operable interface with the current Government system and any future replacement system or changes to the existing system. While the plan is for AFWAY II to be available before NETCENTS-2 contract award, current

Government capabilities may initially require NETCENTS-2 customers to follow a link on the legacy AFWAY system to get to the legacy NETCENTS Portal which will provide links to contractors' NETCENTS-2 web sites. Within 40 work days of NETCENTS-2 Contracting Officer announcement of the availability of AFWAY II, the contractor shall establish a working business-to-business (B2B) or Global Exchange (GEX) service interface through DISA with associated secure communications protocols and certificates or key-based authentication as required to communicate securely with NETCENTS-2 via AFWAY II. As the Government anticipates improving the web-based NETCENTS reporting capabilities and processes in the future, NETCENTS-2 contractors shall adjust and comply with Government efforts to standardize and modernize Government e-commerce capabilities in order to establish and improve interactive solicitation (pre and post award) processes and reporting. General policies and procedures will be established and published by the NETCENTS-2 PMO and shall be followed by the Contractor when transmitting, receiving, and processing NETCENTS-2 business documents.

7. QUALITY PROCESSES

As a minimum, the prime contractor shall be appraised at ISO 9001:2000 or ISO 9001:2008 or ISO/IEC 20000 or CMMI Development Level 2 (or higher) using the Software Engineering Institute's (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 offeror's organizational level performing the contract. If not ISO certified or SEI appraised, acceptable comparable Systems Engineering (SE) 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.

8. APPLICABLE DOCUMENTS AND STANDARDS

The following certifications, specifications, standards, policies and procedures in Table 2 represent documents and standards that may be placed on individual contract task orders. Individual task orders may impose additional standards to those required at the contract level. The list below is not all-inclusive and the most current version of the document in the AF Standard Center of Excellence Repository (SCOER) referenced in section 3.5.1 at the time of task order issuance will take precedence. Other documents required for execution of tasks issued under NETCENTS-2 will be cited in the relevant Task Order, such as specific FIPS, NIST, or MIL-Standards. Web links are provided wherever possible.

(Table was added)

NETWORK OPERATIONS AND INFRASTRUCTURE SOLUTIONS (COMPLIANCE)		
Standard	**URL**	**Description**

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_5/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.
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.

NETWORK OPERATIONS AND INFRASTRUCTURE SOLUTIONS (COMPLIANCE)			
Standard		**URL**	**Description**
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.
5.	AFI 31-401 Information Security Program management	http://static.e-publishing.af.mil/production/1/saf_aa/publication/afi31-401/afi31-401.pdf	This publication implements Air Force Policy Directive (AFPD) 31-4, Information Security. It prescribes and explains how to manage and protect unclassified controlled information and classified information. Use this instruction with Executive Order (EO) 12958, as amended, Classified National Security Information, 25 March 2003; Office of Management and Budget (OMB), Information Security Oversight Office (ISOO) Directive Number 1, Classified National Security Information, Executive Order 12829, National Industrial Security Program (NISP), DOD Manual 5220.22, National Industrial Security Program Operating Manual, January 1995; and, Department of Defense (DOD) 5200.1-R, Information Security Program, 14 Jan 97, for the management of the Air Force Information Security Program. Additional references include DOD Instruction (DODI) 5240.11, Damage Assessments, 23 Dec 91; DOD Directive (DODD) 5210.83, Unclassified Controlled Nuclear Information (UCNI), 15 Nov 91; Air Force Policy Directive (AFPD) 31-4, Information Security. This instruction is applicable to contractors as prescribed in AFI 31-601, Industrial Security Program. All these references are listed at the end of each paragraph where applicable. This instruction is not to be used as a stand-alone document. HQ USAF/XOS-F is delegated approval authority for revisions to this AFI.
6.	AFI 31-501 Personnel Security Program Management	http://static.e-publishing.af.mil/production/1/af_a4_7/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.
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

NETWORK OPERATIONS AND INFRASTRUCTURE SOLUTIONS (COMPLIANCE)			
Standard		**URL**	**Description**
10.	AFI 33-401 Air Force Architecting	http://static.e-publishing.af.mil/production/1/saf_cio_a6/publication/afi33-401/afi33-401.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.
11.	AFI 33-580 Spectrum Management	http://static.e-publishing.af.mil/production/1/saf_cio_a6/publication/afi33-580/afi33-580.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 33-590 Radio Management	http://static.e-publishing.af.mil/production/1/saf_cio_a6/publication/afi33-590/afi33-590.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 61-204 Disseminating Scientific And Technical Information	http://static.e-publishing.af.mil/production/1/saf_aq/publication/afi61-204/afi61-204.pdf	This instruction updates the procedures for identifying export-controlled technical data and releasing export-controlled technical data to certified recipients and clarifies the use of the Militarily Critical Technologies List. It establishes procedures for the disposal of technical documents.
15.	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 sys-tem 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**
16.	AFMAN 33-152 User Responsibilities and Guidance for information Systems	http://static.e-publishing.af.mil/production/1/saf_cio_a6/publication/afman33-152/afman33-152.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).
17.	AFMAN 33-153 Information Technology (IT) Asset Management (ITAM)	http://static.e-publishing.af.mil/production/1/saf_cio_a6/publication/afman33-153/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).

NETWORK OPERATIONS AND INFRASTRUCTURE SOLUTIONS (COMPLIANCE)			
Standard		**URL**	**Description**
18.	AFMAN 33-282 Computer Security (COMPUSEC)	http://static.e-publishing.af.mil/production/1/saf_cio_a6/publication/afman33-282/afman33-282.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.
19.	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.
20.	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.
21.	AFPD 33-4 Information Technology Governance	http://static.e-publishing.af.mil/production/1/saf_cio_a6/publication/afpd33-4/afpd33-4.pdf	This directive establishes the AF policy for IT Governance to fulfill the AF CIO responsibilities established in federal laws and DoD issuances and the AF IT Governance Executive Board, which will oversee existing IT investment councils, boards, and working groups throughout the IT lifecycle to effectively and efficiently deliver capabilities to users. This directive focuses on aligning IT policy, CIO policy, and capabilities management with doctrine, statutory, and regulatory guidelines that govern accountability and oversight over IT requirements to resource allocation, program development, test, and deployment and operations under the direction and authority of the AF IT Governance Executive Board chaired by the AF CIO.

NETWORK OPERATIONS AND INFRASTRUCTURE SOLUTIONS (COMPLIANCE)			
Standard		**URL**	**Description**
22.	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.
23.	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
24.	DoDI 8551.01 – Ports, Protocols and Services Management	http://www.dtic.mil/whs/directives/corres/pdf/855101p.pdf	
25.	CJCSI 6211.02D – Defense Information Systems Network (DISN) Responsibilities	http://www.dtic.mil/cjcs_directives/cdata/unlimit/6211_02.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).
26.	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**
27.	Department of Defense Architecture Framework (DoDAF) Ver2.02 Aug 2010	http://dodcio.defense.gov/dodaf20.aspx	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.
28.	DFARS 252.227-7014 Rights in Non-commercial Computer Software	http://farsite.hill.af.mil/reghtml/regs/far2afmcfars/fardfars/dfars/Dfars252_227.htm#P696_47162	Guidance on rights in technical data and computer software small business innovation research (SBIR) program.
29.	DFARS 252.227-7015 Technical Data Commercial Items	http://www.acq.osd.mil/dpap/dars/dfars/html/current/227_71.htm#227.7102-2	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.
30.	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.
31.	DoD 5220.22-M, National Industrial Security Program Operating Manual	http://www.dtic.mil/whs/directives/corres/pdf/522022m.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.

NETWORK OPERATIONS AND INFRASTRUCTURE SOLUTIONS (COMPLIANCE)			
Standard		**URL**	**Description**
32.	DoD Discovery Metadata Specification (DDMS)	https://metadata.ces.mil/dse/irs/DDMS/	Visibility, accessibility, and understandability are the high priority goals of the DoD Net-Centric Data Strategy. Of these goals, visibility and discovery are intimately linked. Visibility of a resource is, in a practical sense, useless, if the resource is not easily discoverable. With the express purpose of supporting the visibility goal of the DoD Net-Centric Data Strategy, the DDMS specifies a set of information fields that are to be used to describe any data or service asset, i.e., resource, that is to be made discoverable to the Enterprise, and it serves as a reference for developers, architects, and engineers by laying a foundation for Discovery Services.
33.	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).
34.	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.
35.	DoD Mobile Application Strategy	http://www.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.
36.	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**
37.	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.
38.	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.
39.	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
40.	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.
41.	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).
42.	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**
43.	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.
44.	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.
45.	AFI 33-200, Information Assurance	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.
46.	AFI 33-210, AF Certification and Accreditation (C&A) Program (AFCAP)	http://static.e-publishing.af.mil/production/1/saf_cio_a6/publication/afi33-210/afi33-210.pdf	AF C&A program guidance

NETWORK OPERATIONS AND INFRASTRUCTURE SOLUTIONS (COMPLIANCE)			
Standard		**URL**	**Description**
47.	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)).
48.	NetCentric Enterprise Solutions for Interoperability (NESI)	https://nesix.spawar.navy.mil/home.html	NESI is a body of architectural and engineering knowledge that guides the design, implementation, maintenance, evolution, and use of the Information Technology (IT) portion of net-centric solutions for defense application.

NETWORK OPERATIONS AND INFRASTRUCTURE SOLUTIONS (COMPLIANCE)			
Standard		**URL**	**Description**
49.	AFI 33-111 Voice Systems Management	http://static.e-publishing.af.mil/production/1/934aw/publication/afi33-111_934awsup_i/afi33-111_934awsup_i.pdf	This instruction contains guidelines and procedures for managing Air Force voice systems and networks. Ensures installation, removal, modification, and relocation of telephone services are necessary to either sustain billing integrity, or to provide new service to offices/locations without base telephone service already present, or to maintain telephone numbers with primary offices that appear in the base telephone directory. Assure telephone services remain attached to organizations/functions versus individual personnel; do not submit requests to relocate telephone number(s) or telephone instrument(s) when personnel are assigned to a new office unless the reassignment is associated with an organizational restructure and the individual continues to perform the same organizational function. Otherwise, personnel transitioning to a new office will inherit the existing telephone number(s) and instrument(s) at the new location and update the Global Address Listing with their new telephone number(s). If no base telephone service is available at the new location, TCOs will submit a request to obtain service.
50.	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.
51.	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**
52.	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.
53.	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.

NETWORK OPERATIONS AND INFRASTRUCTURE SOLUTIONS (COMPLIANCE)			
Standard		**URL**	**Description**
54.	GiG Technical Guidance Federation GIG-F	https://gtg.csd.disa.mil/uam/login.do	The GIG Technical Guidance Federation (GTG-F) is a suite of software applications on the NIPRNet and SIPRNet (June 2012) that provides technical guidance across the Enterprise to achieve net-ready, interoperable, and supportable GIG systems. The GTG-F assists program managers, portfolio managers, engineers and others in answering two questions critical to any Information Technology (IT) or National Security Systems (NSS): (1) Where does the IT or NSS fit, as both a provider and consumer, into the GIG with regard to End-to-End technical performance, access to data and services, and interoperability; (2) What must an IT or NSS do to ensure technical interoperability with the GIG. The GTG-F content provides the technical information to various users in addressing and resolving technical issues needed to meet functional requirements (i.e., features and capabilities) of the GIG. This GTG-F content consists of and is based on GIG net-centric IT standards, associated profiles, engineering best practices and reference implementation specifications.
55.	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.
56.	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**
57.	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.
58.	AFI 33-115 Air Force Information Technology (IT) Service management	http://static.e-publishing.af.mil/production/1/saf_cio_a6/publication/afi33-115/afi33-115.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 Defense Message System (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.

NETWORK OPERATIONS AND INFRASTRUCTURE SOLUTIONS (COMPLIANCE)			
Standard		**URL**	**Description**
59.	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
60.	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.
61.	CJCSI 6212.01F Interoperability and Supportability of Information Technology and National Security Systems	http://www.dtic.mil/cjcs_directives/cdata/unlimit/6212_01.pdf	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.
62.	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**
63.	Joint Vision 2020	http://www.dtic.mil/futurejointwarfare/	Strategic Guidance: Joint Vision 2020 builds upon and extends the conceptual template established by Joint Vision 2010 to guide the continuing transformation of America's Armed Forces.
64.	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.
65.	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.
66.	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**
67.	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.
68.	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.
69.	Title 44 USC Section 3542	http://us-code.vlex.com/vid/sec-definitions-19256373	(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**
70.	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.
71.	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.
72.	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.
73.	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.
74.	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.
75.	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.
76.	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.
77.	Department of Defense Chief Information Officer Cloud Computing Strategy	http://www.defense.gov/news/DoDCloudComputingStrategy.pdf	This strategy is to enable the Department to increase secure information sharing and collaboration, enhance mission effectiveness, and decrease costs using cloud services.

NETWORK OPERATIONS AND INFRASTRUCTURE SOLUTIONS (COMPLIANCE)			
Standard		**URL**	**Description**
78.	CNSSI 4009: National Information Assurance (IA) Glossary	http://www.ncix.gov/publications/policy/docs/CNSSI_4009.pdf	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.
79.	Executive Order 13526: Classified National Security Information	http://www.whitehouse.gov/the-press-office/executive-order-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.
80.	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.
81.	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.
82.	DoD Instructions, 8500 Series	http://www.dtic.mil/whs/directives/corres/ins1.html	DoD Issuances
83.	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.
84.	NIST SP 800-59: Guideline for Identifying an Information System as a National Security System	http://csrc.nist.gov/publications/nistpubs/800-59/SP800-59.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.
85.	NIST SP 800-66, Revision 1: An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule	http://csrc.nist.gov/publications/nistpubs/800-66-Rev1/SP-800-66-Revision1.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.

NETWORK OPERATIONS AND INFRASTRUCTURE SOLUTIONS (COMPLIANCE)			
Standard		**URL**	**Description**
86.	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.
87.	NIST SP 800-122: Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)	http://csrc.nist.gov/publications/nistpubs/800-122/sp800-122.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.
88.	NIST SP 800-144: Guidelines on Security and Privacy in Public Cloud Computing	http://csrc.nist.gov/publications/nistpubs/800-144/SP800-144.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.
89.	NIST SP 800-37, Revision 1: Guide for Applying the Risk Management Framework to Federal Information Systems	http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.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.
90.	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**
91.	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.
92.	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.
93.	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).
94.	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.

NETWORK OPERATIONS AND INFRASTRUCTURE SOLUTIONS (COMPLIANCE)			
Standard		**URL**	**Description**
95.	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.
96.	NSTISSAM TEMPEST/1-92/TEMPEST Certification	http://www.nsa.gov/applications/ia/tempest/index.cfm	TEMPEST is compromising emanations are defined as unintentional intelligence-bearing signals which, if intercepted and analyzed, may disclose the information transmitted, received, handled, or otherwise processed by any information-processing equipment.
97.	AFMAN 33-285 Cybersecurity Workforce Improvement Program	http://static.e-publishing.af.mil/production/1/saf_cioa6/publication/afman33-285/afman33-285.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.
98.	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.
99.	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