NETCENTS-2 SOLUTIONS
Network Operations and Infrastructure – Small Business (SB) Companion
Technical Operations Network Task Order (TONTO)
Performance Work Statement (PWS)

Name:	Technical Operations Network Task Order (TONTO)
Organization:	Cryptologic and Cyber Systems Division (AFLCMC/HNCYD)
Address:	

Executive Summary

The purpose of this effort is to provide Weapon System (WS) maintenance, operations, and support services inclusive of Tier 0 (Help Desk/Communications Focal Point), Tier 1 (In-person at the customers' desks) and Tier 2 (Remote and on-site network and computer infrastructure administration) support for the Cyber Command & Control Mission System (C3MS) WS. The 624th Operations Center (624 OC) and its supporting augmentation units provide full spectrum cyberspace operations for the 24th Air Force (24 AF) including developing, integrating, and operating advanced cyber capabilities within the C3MS WS. The 624 OC provides the 24 AF/CC with the ways and means to propagate and implement cyber warfare strategies and effects by utilizing the Command and Control Situational Awareness (C2SA) capabilities of the C3MS WS. AFLCMC/HNCY "C3MS Program Office" is responsible for the deployment and sustainment of the C3MS WS.

The C3MS WS enables offensive and defensive cyberspace operations, spanning multiple service component networks to provide continuous real-time situational awareness (SA) including network status, infrastructure vulnerabilities, systems interoperability, asset utilization, activity & event data, and intelligence information. This WS operates on a continuous 24/7 basis and actively monitors networked mission systems and unit activities to generate a common operational picture of AF cyber assets. The system is composed of three logical segments; Hardware, Infrastructure, and Mission Applications.

- Hardware Segment includes client workstations, data walls, servers, and network infrastructure hosted within the across multiple physical locations and includes four security domains.
- Infrastructure segment includes multiple Commercial-Off-The-Shelf (COTS) functions like databases, server and desktop operating systems (OS), 3rd party software applications, virtualization software, security software, and various network functions across the four security domains.
- Mission Application segment is composed of both client-server and web-based applications which provide Cyber C2 functions like Planning, Order Generation and Distribution, Execution Monitoring, and Assessment.

The TONTO will provide overall system maintenance, operation and support services to ensure C3MS meets requirements and matures in an efficient and effective manner.

NETCENTS-2 Network Operations and Infrastructure SB
TONTO PWS

1. Purpose

The purpose of this effort is to provide maintenance, operations and support services in line with standard Air Force (AF) General Cyberspace Support and Management procedures for multiple mission application systems and initiatives for the Cyber Command and Control Mission System (C3MS). During the period of performance (PoP) for the TONTO effort, the number of mission applications, systems and system services will increase, and the configuration of the system will evolve significantly.

The C3MS WS enables the 24 AF, Air Forces Cyber (AFCYBER) and Joint Force Headquarters – Cyber (JFHQ-C) to exercise command authority over assigned and attached forces to carry out AF and joint cyberspace operations to support AF, joint, and national requirements. It supports operational-level C2SA of assigned and attached forces to 24 AF/AFCYBER.

C3MS is operated by the 624 OC, Air National Guard's (ANG) 119th Command and Control Squadron (CACS), and AF Reserve Command's (AFRC) 854th Combat Operations Squadron (COS). C3MS provides operational level C2 and Situational Awareness of the AF Cyberspace Forces, networks and mission systems. The C3MS WS evolved from the legacy AF Network Operations Center (AFNOC) concept, personnel and equipment suite. With the activation of United States Cyber Command and 24 AF, senior leaders recognized the need for an operational-level cyberspace C2 capability and C3MS provides this capability.

The primary location of C3MS is Joint Base San Antonio (JBSA)-Lackland AFB, TX. C3MS maintenance, operations and support must be extensible to all other augmentation, Continuity of Operations Plan Site(s) and Alternate Operating Location(s).

2. Scope

The services required under the C3MS TONTO contract include all engineering, disciplines required to execute maintenance, operations, and support services of systems in accordance with (IAW) the DoD 5000.02 product life cycle. It will be applied to support all systems and initiatives within the C3MS portfolio (AFLCMC/HNCYD) and secondary technologies supporting mission operations.

3. Requirement/Description of Services

The services required under this contract focus on direct mission support. This focus includes the maintenance, operations, and support service functions that will enable optimum C3MS WS operations. Table 3.1 provides an estimated skill mix by labor category for this contracted effort. The Level of Effort is derived from the C3MS Program Office analysis of the work to be performed.

Table 3.1: Estimated Skill Mix/Level of Effort

Labor Category
Database Administrator
Help Desk Technician
Network Administrator
Network Engineer
IT Hardware Technician
Network Intrusion Detection/Protection Analyst
Oracle Database Administrator
SharePoint Administrator
SharePoint Developer
Splunk Administrator
Storage Area Network (SAN) Administrator
Server Administrator
Virtual System and Desktop Infrastructure Engineer
Virtual Desktop Infrastructure Administrator
Website Administrator
Web Developer
Vulnerability Analyst

The majority of the support will be performed within Government facilities at Joint Base San Antonio – Lackland and Port San Antonio.

3.1 Systems Maintenance, Operations and Support Services

The contractor shall provide a wide range of system and network maintenance, operations and support services for successful operation of C3MS WS and AF Information Technology assets within 24 AF and 624 OC in compliance of Department of Defense (DoD) and AF directives. This includes supporting existing legacy infrastructure, networks, systems, and operations, as well as evolving the infrastructure, networks, systems and operations to comply with the DoD and AF enterprise architecture. The Contractor shall schedule release installations during nights and weekends to avoid disrupting operations. Unscheduled breaks/fixes shall occur as soon as possible to restore operations tempo. The Contractor shall ensure an Authorized

Service Interruption (ASI) is granted by 624 OC leadership prior to installations. The Contractor shall supply personnel who have the minimum skills, experience, education and certifications to meet the following minimum requirements:

- Contractor shall be able to communicate effectively (written/verbal), possess strong interpersonal skills, be self-motivated, and be innovative in a fast-paced environment.
- Contractor shall hold and maintain a TS/SCI Clearance.
- Contractor personnel shall have at a minimum 3 years of relevant experience to include relevant education and certifications (i.e. Cisco Certified Network Professional, VMWare Certified Professional) for the work that they shall perform.
- Contractor shall have technical personnel certified at a minimum Information Assurance Technical Level II IAW DoD Directive 8140.01 and DoD Directive 8570.01M.
- Contractor shall have management personnel certified at a minimum Information Assurance Management Level II IAW DoD Directive 8140.01 and DoD Directive 8570.01M.

3.1.1 Maintenance, Operation and Support Services

3.1.1.1 The following identify the general concept of support levels:

- Tier 0 – Help Desk Support via phone, chat, website input or customer walk-up.
- Tier 1 – Technical Support at the customer's desk, conference room, primary duty location, or specified location to perform assessment, installation, replacement, and initial troubleshooting of client system hardware and software to either to resolve or escalate trouble tickets or change requests (CRs) to support mission operations.
- Tier 2 – Advanced System Administration and Network Operations across C3MS WS sites and AF infrastructure to coordinate and perform assessment, installation, replacement (scheduled and unscheduled), and troubleshooting of hardware and software to either to resolve or escalate trouble tickets or CRs to the appropriate office in support of mission operations. Support shall be on-site or utilize remote means when necessary.
- Tier 3 – Hardware and software support from the Program Office or vendors. Tier 3 will be provided by the Mission Applications Support Contract (MASC) Contrctor.

3.1.1.3 Performance required of all Contractor Maintenance, Operations and Support Services

The contractor shall:

- Perform General Cyberspace Support Activities and Management for the successful operation of C3MS WS and AF Information Technology assets within 24 AF and 624 OC IAW Technical Orders, AF and applicable directives.
- Coordinate, support, validate, install (and provide verification testing directly after install), and report status of C3MS WS and AF Information Technology assets (within 24 AF and

624 OC) scheduled and unscheduled maintenance releases, patches, security and hardware/software updates.

- Comply with Time Compliance Technical Orders, Time Compliance Network Orders, Maintenance Tasking Orders, Cyber Control Orders, and Cyber Tasking Orders.
- Coordinate, support, escalate, and track trouble and CR tickets with internal 624 OC offices and outside Air Force and DoD units and organizations IAW applicable directives and publications.
- Control production of C3MS WS and AF Information Technology assets (within 24 AF and 624 OC) in coordination with AF directives and guidance and IAW Technical Order 00-33A-1001 and applicable directives.
- Develop, perform and report inspections of the C3MS WS hardware and software IAW Technical Order 00-33A-1001, AF Instruction 33-200, and applicable directives.
- Maintain corrosion prevention and control program and perform corrosion prevention and control activities on C3MS WS and supporting infrastructure hardware IAW Technical Order 00-33A-1001 and applicable directives.
- Maintain an electric static discharge (ESD) program and ensure personnel are compliant with Technical Order 00-33A-1001, Technical Order 00-25-234 and applicable directives.
- Develop, input, maintain, and make available to government C3MS WS and AF Information Technology assets’ configuration management records, Cyberspace Infrastructure Planning Systems records, and historical records IAW Technical Order 00-33A-1001, Technical Order 00-33D-3003 and applicable directives.
- Perform AF life cycle management in support of C3MS WS and AF Information Technology assets (within 24 AF and 624 OC) IAW AFI 23-111, Technical Order 00-33A-1001 and applicable directives.
- Perform with AF material management procedures IAW AF Manual 23-122, Technical Order 00-33A-1001 and applicable directives.
- Be appointed to and perform AF Information Technology Equipment Custodian duties to maintain accountability and be responsible for all C3MS WS and AF Information Technology assets IAW AF Manual 33-153.
- Develop, maintain, coordinate, and deliver to the government any publications, operating instructions or other materials required for the operation, maintenance and support of the C3MS WS and AF Information Technology assets (within 24 AF and 624 OC) IAW Technical Order 00-33A-1001 and applicable directives. The contractor shall maintain all publications and records IAW AF Instruction 33-322, AF Manual 33-363 and applicable directives.
- Unless specified otherwise in the Task Order, the contractor shall provide all tools required to maintain C3MS and manage tool assets IAW Technical Order 00-33A-1001 and applicable directives.
- Manage the Test Measurement & Diagnostic Equipment program. The contractor shall maintain and operate all test equipment required for maintenance of the C3MS WS and maintain assets IAW Technical Order 00-20-14, Technical Order 00-33A-1001 and applicable directives.

- Resolve all outages and CRs within paragraph 3.1.1.4 Service Level Agreements time frames.
- Accurately capture in the approved AF Automated Information System all actions on systems/equipment to include; unscheduled maintenance, preventative maintenance, routine administration (Remote and on-site), Time Compliance Technical Orders (TCTO), Time Compliance Network Orders (TCNO), Maintenance Tasking Orders (MTO), Cyber Control Orders (CCO) and Cyber Tasking Orders (CTO) IAW Technical Order 00-33A-1001 and applicable directives.
- Enter in the approved AF Automated Information System system(s) and component failure according to Technical Order 00-20-2, Maintenance Documentation; material consumption according to Technical Order 00-20-3, Maintenance Processing of Repairable Property and Repair Cycle Asset Control System; and Time Compliance Technical Order (TCTO) reporting requirements according to Technical Order 00-5-15, AF Time Compliance Technical Order and applicable directives.
- Be appointed as the Primary and Alternate Communications Security (COMSEC) Responsible Officer (CRO)/Secure Voice Responsible Officer (SVRO) and perform all the duties IAW AFMAN 33-283 and applicable directives.
- Operate, process, configure and maintain all data, voice and video encryption equipment and encryption keying material required perform Communications Security (COMSEC) duties IAW AFMAN 33-283 and applicable directives.
- Maintain, operate and support Power Stripes, Universal Power Supplies (UPS) and connections to Power Distribution Unit (PDU) IAW Technical Order 00-33A-1001 and applicable directives.
- Perform backups IAW the C3MS WS Risk Management Framework (RMF) System Backup and Recovery Plan (SBRP) and all maintenance tasks IAW the C3MS maintenance technical order and applicable directives.
- Not change or alter the C3MS WS System configuration without approval.
- Coordinate, implement, maintain and document approved changes to the C3MS WS baseline with the Information Systems Security Manager, Configuration Manager, and WS Manager in writing.
- Report all security incidents in writing and verbally (via approved classified communication platform) to the Information Systems Security Manager, Weapon Defense Flight and Unit Security Manager within 30 minutes of discovery. For after-hours reporting local Operating Instructions shall be followed.
- 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 support all software revisions deployed or resident on the system and sub-systems. The data rights ownership/licensing guidance is specified in DFARS 252.227-7013(b) and (e) and DFARS 252.227-7014(b) and (e) and DFARS 252.227-7017.
- 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 AF

and industry rules and regulations. Any equipment removal and/or disposal shall be coordinated with a designated official at the host base communications squadron.

- 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 24 hours to complete the repair(s) or replace the malfunctioning system(s) or components, unless otherwise stated in the Task Order. The minimum charge per-call shall not exceed 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 Principal Period of Maintenance. 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.
- Restore services in the priority order determined by the Government and applicable directives. The contractor shall work on repair actions until service is restored based on priority. The contractor shall work closely with the Government on all service or system outages, trouble calls/tickets and notify the Contracting Officer Representative and Quality Assurance Evaluator and Communications Focal Point in writing upon restoration of service providing the time service was restored and a description of repair action.
- Coordinate with the Contracting Officer, Quality Assurance Personnel and other government personnel to resolve gaps or deficiencies in required equipment or property to maintain, operate and support C3MS.
- Resolve formal customer complaints and corrective action requests within 14 days of receipt.

3.1.1.4 Outage and CR Resolution Service Level Agreements/Time Frames

Overall Outage Service Level Agreements (Tier 0 to Tier 2)

Percentage of Outages	Resolved within
25%	2 hours
25%	6 hours
25%	24 hours
25%	72 hours

Customer Systems Outage Service Level Agreements (Tier 1)

Percentage of Outages	Resolved within
25%	2 hours
40%	6 hours
25%	24 hours
10%	72 hours

Systems and Network Outage Service Level Agreements (Tier 2)

Percentage of Outages	Resolved within
25%	2 hours
25%	6 hours
25%	24 hours
25%	72 hours

Overall CR Service Level Agreements (Tier 0 to Tier 2)

Percentage of CRs	Resolved within
25%	2 hours
25%	6 hours
25%	24 hours
25%	72 hours

Customer Systems CR Service Level Agreements (Tier 1)

Percentage of CRs	Resolved within
50%	2 hours
25%	6 hours
25%	24 hours
25%	72 hours

Systems and Network CR Service Level Agreements (Tier 2)

Percentage of CRs	Resolved within
25%	2 hours
25%	6 hours
25%	24 hours
25%	72 hours

3.1.1.5 Cyber Security Services

The contractor shall:

- Ensure that all services meet the requirements of the DoD Cyber Security 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.
- Provide applications services that are in compliance with and support Department of Defense, AF, and Intelligence Community Public Key Infrastructure (PKI) policies as applicable.
- Support activities to make applications PK-enabled (PKE) in order to achieve standardized, PKI-supported capabilities for digital signatures, encryption, identification and authentication.
- 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.

- Assist in defining user and registration requirements to Local Registration Authorities (LRAs).
- Provide solutions that meet confidentiality, data integrity, authentication, and non-repudiation requirements in applicable directives.
- Provide solutions shall comply with National Institute for Standards and Technologies (NIST) and Federal Information Processing Standards (FIPS) and applicable IC standards.
- Ensure that all deliverables comply with the Defense Information Systems Agency (DISA) Security Technical Implementation Guides (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.
- 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.
- Provide services and solutions to accomplish lifecycle entity identity management from user creation to user revocation. Entities are defined as both human and non-human users possessing accounts within C3MS and AF Networks.
- Support user creation (identity confirmation, credentialing, and enrollment), user management (provisioning across single or multiple systems and services, automated provisioning workflow and self-service), user access (identification, authentication and authorization) and user revocation (de-provisioning and disablement).
- Enable the de-provisioning process through automated account disablements and token revocation.
- Provide access controls with rights, roles and privileges.
- Provide the capability for all accounts to comply with FIPS 196 and other directives, by using approved methods of authentication such as, but not limited to, the following:
    - PKI based authentication.
    - Username and Password.
    - One-Time Password Tokens.
    - Biometrics with PIN or password.
- Support and implement Disaster Recovery and Continuity of Operations Plans (COOP).
- Ensure all interactions between people, machines and services are verified using security policy.
- Conduct confirmed two-way authentication using DoD-PKI and Federal Bridge credentials or applicable Intelligence Community Public Key Infrastructure and bridge.
- Authorize access to data based on groups and roles as approved in DD Form 2875 and other approved methods.
- Delegate roles and groups based on policy.
- Mediate graduated access to data for various types of users.

- Monitor and log all activities to provide for both real time assessment and historical analysis.
- Scan systems and devices for vulnerabilities.
- Appoint a Cyberspace Defense Analysis Point of Contact to ensure compliance with the applicable requirements of AF Instruction 10-712, Cyberspace Defense Analysis (CDA) Operations and Notice and Consent Process. The contractor shall ensure compliance with notice and consent requirements by annually. The contractor shall compile the summary letter based on the unit annual reports and submit to the 624 OC and Wing Cyber Security office as requested. The contractor shall ensure all systems and devices within 24 OC and 624 OC facilities and control are specified in the summary letter.
- Enable efficient cross-domain information sharing across networks operating at different classification levels (e.g., SIPRNET, NIPRNET and JWICS).
- Operate, maintain and configure point-to-point, VPN and bulk encryption for network and long-haul circuits.

3.1.1.6 Surge Requirements

- Surge requirements include greater than expected requirements/workload for existing services within the scope of Task Order awarded. Normally, surge requirements are of short duration, from 1 to 6 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.

3.1.1.7 Special Asset Tagging

- The Contractor shall comply with DFARS 252.245-7001 regarding Special Asset Tagging requirements.

3.1.1.8 Maintenance, Operations and Support Alternative

- The government may select an 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, operation and support by giving the contractor 30-days' notice and a contract modification. Any change in type of maintenance, operation and support will not be considered a partial termination of the Task Order for the convenience of the government.

3.1.2 Help Desk /Communications Focal Point Maintenance, Operations and Support (Tier 0)

The contractor shall:

- Operate a Help Desk (Tier 0) and Communications Focal Point at a location of the government's choice to support approximately 500 local customers (624 OC and 24 AF) and subordinate units and personnel utilizing the C3MS WS Monday thru Friday (not including Contract holidays) from 0600 to 1800 Central Standard Time IAW but not limited to Technical Order 00-33A-1001 and applicable directives.
- Provide a toll-free telephone number and on-call Help Desk (Tier 0) support any time (after hours) the Help Desk/Communications Focal Point is not manned.

- Schedule Video Teleconferences for customers.
- Verify Video Teleconferences systems and connections to the correct remote system are operational no less than 10 minutes prior to the scheduled conference between Monday thru Friday (not including Contract holidays) from 0600 to 1800 Central Standard Time.
- Accept outage reports and CRs via phone, chat, website input and customer walk-up.
- Submit tickets through the AF Approved Information System to the appropriate office for resolution and implementation.
- Brief and report the status of C3MS and supporting AF infrastructure service interruptions related to the 624 OC and 24 AF operations IAW directives.
- Be appointed the primary and alternate Telephone Control Officer. The contractor shall accept customer telephone/voicemail requests, process, and coordinate with the host base communications squadron for long distance PINs, telephone moves, additions, programming changes, voicemail changes/resets and removal of service. The contractor shall maintain a record of issued and recovered long-distance telephone pin numbers by customer rank, name, issued date and recovered date for five years.
- Maintain and perform Personal Wireless Communications System program and associated functions for 624 OC and 24 AF IAW AF Manual 33-153 and applicable directives.

3.1.3 Customer Systems Maintenance, Operations and Support Services (Tier 1)

The contractor shall:

- Perform assessments, surveys, engineering support, installations, replacements (scheduled and unscheduled), initial troubleshooting, ticket escalation, and outage resolution of all customer devices including but not limited to:
  - Desktop devices (computers, laptops, zero-clients, tablets)
  - Peripherals (monitors, keyboards, mice, token readers, webcams, keyboard-video-mouse (KVM) devices)
  - Secure and non-secure telephones (Voice over IP, vIpers, Defense Red Switch Network (DRSN), and Defense Switched Network (DSN) devices)
  - Data-wall displays
  - Video Teleconferencing (VTC) systems
  - Digital signage
  - Projectors
  - Copiers
  - Printers
  - Digital senders
  - Facsimile machines
  - Clocks
  - Televisions.
- Maintain cabling in a neat and clean manner between customer devices and outlets or connections.
- Perform Periodic Inspections, Preventative Maintenance and Cleaning of customer devices.

- Train customers upon request on customer facing systems’ software and hardware operation and use.

3.1.3 Network Maintenance, Operations and Support Services (Tier 2)

The contractor shall:

- Perform assessments, surveys, engineering support, installations, replacements (scheduled and unscheduled), initial troubleshooting, ticket escalation, outage resolution, maintain, operate and support of all the virtual and physical hardware and software network devices and physical infrastructure (cabling) of the C3MS WS and AF Information Networks assets including but not limited to:
  - Switches
  - Routers
  - VPNs
  - Government and commercial encryption devices
  - Load Balancers
  - Firewalls
  - Proxies
  - Network taps
  - Network Intrusion Devices
  - Intrusion Detection Systems
  - Cross Domain Solution devices
- Maintain and support all physical data, voice, and video cabling and supporting infrastructure to connect the C3MS WS infrastructure and AF Information Technology assets within applicable standards to support the transport of voice, video and data.
- Load encryption keys in all network encryption devices IAW applicable directives.
- Provide on call and after hours support.

3.1.4 Systems Maintenance, Operations and Support Services (Tier 2)

The contractor shall:

- Perform assessments, surveys, engineering support, installations, replacements (scheduled and unscheduled), initial troubleshooting, ticket escalation, outage resolution, maintain, operate and support of all the virtual and physical hardware and software infrastructure of the C3MS WS and AF Information Networks assets including but not limited to:
  - Microsoft Windows and Linux servers
  - Application servers
  - Databases
  - Storage Area Network
  - Virtual Desktop Infrastructure
  - Storage devices
  - Data wall systems and displays
  - Video Teleconferencing (VTC) systems
  - Authentication and authorization systems

    - Domain Name Systems
    - Active Directory
    - Web Servers
    - Host-based Intrusion Detection (HIDS) infrastructure and systems
    - Dynamic Host Configuration Protocol (DHCP) servers
    - Defense Red Switch Network systems
    - Voice Over IP Call Managers
    - Cross Domain Solution devices
- Provide on call and after hours support.

3.1.5 Defensive Cyber Operations

The contractor shall:

- Conduct comprehensive threat analyses for defense of the C3MS WS.
- Use automated tools to analyze and detect anomalous behavior using real time/logged information to preclude and prevent internal attacks on AF information and computing resources.
- Scan systems and devices for vulnerabilities.
- Take actions to prevent and halt the compromise of the C3MS WS.
- Develop instructional material and train government civilian and military personnel in defensive cyber operations not limited to:
    - Analyzing malware or other threats
    - Data loss prevention
    - Incident response tools and techniques
    - Incident handling and forensics fundamentals
    - Intrusion detection and prevention
    - Network device hardening and auditing
    - Network infrastructure security and defense
    - Packet analysis
    - Pen testing methodology and information gathering
    - Penetration testing exploitation and reporting
    - Risk management
    - Tools for identifying malware
- Provide on call and after hours support.

3.1.6 Projects/Planning

The contractor shall:

- Support, coordinate and act as the focal point for C3MS and AFIN services (within 24 AF and 624 OC) planning, engineering, project management and configuration management.
- Document the approved requirements process and provide education and training on the requirements process to AF/DoD customers.

- Evaluate existing projects/requirements and make recommendations to customers as to which should be continued.
- Upon government approval and provision of funding continue processing and implementation of existing projects/requirements.

3.1.6.1 Project Management/Requirements Processing

The contractor shall:

- Process and track customer requirements, engineer solutions and manage project implementation IAW directives.
- Develop/Manage Enterprise Master Integrated Schedule, tracking milestones, major projects, completion dates (i.e., Microsoft Project Management type program (Gantt charts).
- Produce Implementation Plan for approved projects and programs.
- Implement ITIL Process to support organizational increase on high reliable IT services.
    - Reduce costs.
    - Improve IT services through the use of proven best practice processes.
    - Improve customer satisfaction through a more professional approach to service delivery.
    - Improve energy efficiency and reduce greenhouse emissions.
    - Minimize energy consumption to meet percentage reduction requirements set forth in Executive Orders 13423 and 13514.
    - Follow applicable environmental energy efficiency guidelines when purchasing new hardware or electronic equipment.
    - Follow applicable environmental guidelines when disposing of hardware or electronic equipment.
    - Coordinate initial design plans with civil engineers to ensure compliance with environmental and energy guidelines.
- The contractor shall analyze approved requirements generated by AFCYBER unit Requirements Analysis Working Group (RAWG), Configuration Control Boards (CCBs), and process each requirement through a formal development process. The formal development process shall provide 24 AF/AFCYBER customers and leadership with a prioritized estimated delivery schedule, based on a prioritization schema defined by 24 AF/AFCYBER senior leaders.
- The contractor shall analyze approved requirements generated by AFCYBER unit Configuration Control Boards (CCBs), and process each requirement through a formal development process.
- The contractor shall integrate custom applications using current programming languages used by the 624 OC Mission System components to continuously deliver new capabilities and refine existing capabilities to meet current operational requirements.
- The contractor shall integrate third party software solutions, as required, to meet AFCYBER operational needs.
- The contractor shall create software administration guides for applications.

3.1.7 Certification and Accreditation

The Contractor shall provide assistance to the customer as required for:

- Conducting analysis of the certification and accreditation program.
- Development and execution of certification and accreditation through technical research and analysis and development of solutions to ensure security and integration of the enterprise through the Certification & Accreditation process.
- Process improvement recommendations.
- Implementing technical solutions to meet certification and accreditation requirements.

4. Contractual Requirements

4.1 Staffing Plan

The Contractor shall provide a staffing plan as an attachment to its proposal that presents its plan to staff for all positions IAW Table 4. This staffing plan shall identify by individual the skills, experience and certifications that each individual fulfills. All individuals on the Task Order shall obtain a CAC and a Top Secret SCI level clearance (and security badge) IAW Table 4 timelines upon start of Task Order or being hired onto the Task Order. Functional Leads shall possess DoD 8570 Level III certifications in their field (technical or management) when they are assigned to the program and shall be staffed on the first day of Task Order performance.

Table-4: Staffing Requirements Timeline

Required Date	Positions Filled
PoP Start Date	½ Key Personnel
15 Business Days after PoP Start	40%
20 Business Days after PoP Start	60% & All Key Personnel
30 Business Days after PoP Start	100%

4.1.1 Key Personnel

The Government has determined the following positions to be Key Personnel essential to the performance of this contract. The Contractor shall submit these individuals' resumes to the Program Office for approval. All Key Personnel require a Top Secret SCI level clearance upon start of Task Order. If any Key Personnel needs to be replaced during the PoP, the Contractor shall replace with an individual with equal to or greater than experience and receive Program Office approval. Key Personnel include:

- Project Lead
- Lead System Administrator
- Lead Database Administrator
- Network Engineer

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:

- Provide quality products, incidentals and customer support.
- 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.
- Provide satisfactory new products, product repairs or advance replacements, as appropriate.
- Provide timely and accurate reports.
- Respond to the customer’s requirements as identified.
- Meet subcontracting goals if applicable.

4.2 Program Management / Project Management

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

The contractor shall host a program kickoff meeting within fourteen (14) calendar days of Task Order award at a time, date and place coordinated with and approved by the PMO. The contractor shall pre-coordinate by email with the PMO on specific agenda topics and shall be prepared to discuss their program implementation strategy at this meeting. The contractor shall submit the agenda and briefing five (5) days prior to the meeting. The contractor shall identify known program risks and provide detailed strategies to avoid or limit those risks. Following the Program Kickoff Meeting, the contractor shall submit meeting minutes to include, but not be limited to summarizing topics discussed, Action Items, briefing slides and handouts for Program Office approval.

The contractor shall provide monthly status reports (CDRL A001) presenting overall program status, personnel experience/training/certifications on the contract and program risks and risk management strategies for those risks. The monthly status report will include the current contractor personnel roster.

In support of Section 2330a of title 10, United States Code (10 USC 2330a) which requires the Secretary of Defense to submit to Congress an annual inventory of contracts for services performed during the prior fiscal year for or on behalf of the DoD the Contractor shall report ALL contractor labor hours (including subcontractor labor hours) required for performance of services provided under this contract via a secure data collection site. The contractor is required to completely fill in all required data fields using the following web address: http://www.ecmra.mil/ (A038). Reporting inputs will be for the labor executed during the PoP during 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 31 October of each calendar year. Contractors may direct questions to the help desk at http://www.ecmra.mil/.

4.2.1 Services Delivery Summary

The Services Delivery Summary (SDS) will be IAW AFI 63-101, Acquisition and Sustainment Life Cycle Management and FAR Subpart 37.6, Performance-Based Acquisition. SLAs will be defined in each Task Order.

PERFORMANCE OBJECTIVE	PWS	PERFORMANCE MEASURE/THRESHOLD
Customer Satisfaction	3.1	Contractor receives less than 2 formal customer complaints / corrective action requests per quarter. Contractor shall successfully resolve complaints within 14 days of receipt 100% of the time.
Security, Software, Hardware Updates	3.1.1.3	All security updates met 100% of the time against Monthly Security Release Report. Software and Hardware updates and upgrades met 100% of the time against the directive document timeframes.

Trouble Tickets, Change Tickets, Time Compliance Technical Orders, Time Compliance Network Orders, Maintenance Tasking Orders, Cyber Control Orders, Cyber Tasking Orders; Tracking and Control of Production	3.1.1.3;
	3.1.1.4;
	3.1.2
		Random sampling of outages, Trouble Tickets, Change Tickets, Time Compliance Technical Orders, Time Compliance Network Orders, Maintenance Tasking Orders, Cyber Control Orders, Cyber Tasking Orders against directives.

Inspections	3.1.1.3	Random sampling of Acceptance, Transfer, Storage, Functional, Operational, Periodic and Preventative Maintenance Inspections. Government Quality Assurance personnel will perform technical inspections and report findings to the Contracting Officer. The Contractor shall successfully resolve all deficiencies identified within 30 days.
Corrosion Prevention and Control Program	3.1.1.3	Random sampling of program documents and Preventative Maintenance Inspections. Government Quality Assurance personnel will perform technical inspections and report findings to the Contracting Officer. The Contractor shall successfully resolve all deficiencies identified within 30 days.

Electro Static Discharge Program	3.1.1.3	Random sampling of program documents and Government Quality Assurance personnel will monitor Contractor personnel procedures and documentation. Government Quality Assurance personnel will report findings to the Contracting Officer. The Contractor shall successfully resolve all deficiencies identified within 30 days.
Configuration Management and Historical Records	3.1.1.3	Random sampling of program documents, hardware and software. Government Quality Assurance and Cyber Security personnel will compare Contractor documentation, hardware and software against Program Management Office documentation and report findings to the Contracting Officer. The Contractor shall successfully resolve all deficiencies identified within 30 days.
Life Cycle Management	3.1.1.3	Random sampling of program documents and assets. Government Quality Assurance personnel will perform inspections and report findings to the Contracting Officer. The Contractor shall successfully resolve all deficiencies identified within 30 days.
Material Management	3.1.1.3	Random sampling of program documents and assets. Government Quality Assurance personnel will perform inspections and report findings to the Contracting Officer. The Contractor shall successfully resolve all deficiencies identified within 30 days.
Information Technology Asset Management	3.1.1.3	Random sampling of program documents and Government Information Technology Assets. Government Quality Assurance personnel will perform inspections and report findings to the Contracting Officer. The Contractor shall successfully resolve all deficiencies identified within 30 days.
Tool Management Program	3.1.1.3	Random sampling of program documents and tools. Government Quality Assurance personnel will perform inspections and report findings to the Contracting Officer. The Contractor shall successfully resolve all deficiencies identified within 30 days.
Test Measurement and Diagnostic Equipment Program	3.1.1.3	Random sampling of program documents and Test Measurement and Diagnostic Equipment. Government Quality Assurance personnel will perform inspections and report findings to the Contracting Officer. The Contractor shall successfully resolve all deficiencies identified within 30 days.

Communications Security and Secure Voice Responsible Officer Program	3.1.1.3	Random sampling of program documents and Communications Security assets and material. Government Quality Assurance and Cyber Security personnel will perform inspections and report findings to the Contracting Officer. The Contractor shall successfully resolve all deficiencies identified within 30 days.
C3MS Backups	3.1.1.3	All backups met 100% of the time against C3MS WS RMF SBRP. The Contractor shall successfully resolve all deficiencies identified within 30 days.
Security Incidents	3.1.1.3	Random sampling of documents. Government Cyber Security personnel will perform inspections and report findings to the Contracting Officer. The Contractor shall successfully resolve all deficiencies identified within 30 days.
Records Management	3.1.1.3	Random sampling of program documents and records. Government Quality Assurance, Knowledge Management and Base Records Management personnel will perform inspections and report findings to the Contracting Officer. The Contractor shall successfully resolve all deficiencies identified within 30 days.
Outage Resolution Service Level Agreements	3.1.1.4	Monthly review of trouble tickets against monitoring systems reports.
Cyber Security Services	3.1.1.5	Random sampling of documents, hardware and software. Government Cyber Security personnel will perform inspections and report findings to the Contracting Officer. The Contractor shall successfully resolve all deficiencies identified within 30 days.
Help Desk/Communications Focal Point Maintenance, Operations, and Support	3.1.2	Random sampling of documents, hardware and software. Government Quality Assurance and Cyber Security personnel will perform inspections and report findings to the Contracting Officer. The Contractor shall successfully resolve all deficiencies identified within 30 days.
Customer Systems Maintenance, Operations and Support	3.1.3	Random sampling of documents, hardware and software. Government Quality Assurance and Cyber Security personnel will perform inspections and report findings to the Contracting Officer. The Contractor shall successfully resolve all deficiencies identified within 30 days.

Network Maintenance, Operations and Support	3.1.4	Random sampling of documents, hardware and software. Government Quality Assurance and Cyber Security personnel will perform inspections and report findings to the Contracting Officer. The Contractor shall successfully resolve all deficiencies identified within 30 days.
System Maintenance, Operations and Support	3.1.5	Random sampling of documents, hardware and software. Government Quality Assurance and Cyber Security personnel will perform inspections and report findings to the Contracting Officer. The Contractor shall successfully resolve all deficiencies identified within 30 days.
Defensive Cyber Operations	3.1.6	Random sampling of documents, hardware and software. Government Quality Assurance and Cyber Security personnel will perform inspections and report findings to the Contracting Officer. The Contractor shall successfully resolve all deficiencies identified within 30 days.

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 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 NetOps and Infrastructure Solutions contract of which this PWS is a part (including all clauses that are or shall be included or incorporated by reference into that contract).

4.3 Security Management

4.3.1 Safeguarding Classified Information

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

The Contractor will follow local classified process IAW the proscribed Federal guidance of the NISPOM and FAR “Subpart 4.4 along with DD Form 254. When transmitting classified information ensure all classified information is properly sanitized and/or degaussed of all sensitive/classified information IAW AFSSI 5020.

4.3.2 Personnel Security

Individuals performing work under this task order shall comply with applicable program security requirements as stated in the task order. All personnel shall possess Top Secret clearances and be eligible for Sensitive Compartmented Information (SCI) access at the time they report for work on this program.

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. IAW 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).

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

4.3.5 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 IAW 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 IAW 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.

4.4 Place of Performance

The places of performance shall be Primary, Alternate Operating Location(s) and Continuity of Operations Plan (COOP) Site(s):

- Primary: 3515 S. Gen McMullen - Joint Base San Antonio-Lackland (Port San Antonio) Building 171 and Building 1623
- AOL: Classified
- COOP Site: Classified

When this Task Order requires the contractor to work in a Government facility, the Government will furnish or make available working space, network access and equipment to include:

- Windows PC with Microsoft Office Suite (Outlook, Word, Excel, PowerPoint, etc.)
- Telephone (local/long distance calls authorized as dictated by Task Order performance requirements)
- Facsimile
- Copier
- Printer

4.5 Normal Hours of Operation

The average work week is 40 hours. The average workday is 8 hours and the window in which those 8 hours may be scheduled is between 6:00 AM and 6:00 PM, Monday through Friday or as specified in this Task Order, except for days listed in Clause G021, Contract Holidays, in the overarching ID/IQ contract. Billable hours are limited to the performance of services as defined in the Task Order. Government surveillance of contractor performance is required to give reasonable assurance that efficient methods and effective cost controls are being used. Work in excess of the standard 40 hour work week requires prior written approval by the Quality Assurance Personnel (QAP).

4.6 Billable Hours

In order for man-hours to be billed, deliverable services must have been performed in direct support of a requirement in the Task Order PWS. In the course of business, situations may arise where Government facilities may not be available for performance of the Task Order requirements (i.e., base closure due to weather, Force Protection conditions, etc.). When the base is officially closed no contractor services will be provided and no charges will be incurred and/or billed to any Task Order. There may also be occasions when support contractors are invited to participate in morale and recreational activities (i.e., holiday parties, golf outings, sports days and other various social events). Contractor employees shall not be directed to attend such events by the Government. Since a contract employee is not a government employee, the contract employee cannot be granted the same duty time activities as Government employees. Participation in such events is not billable to the Task Order and contractor employee participation should be IAW the employees' company's policies and compensation system.

4.7 Contractor Identification

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

4.8 Training

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

5. 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 3 (or higher) using the SEI SCAMPI, a method by an SEI-authorized lead appraiser, or comparable documented systems engineering processes, for the entire performance period of the contract, inclusive of options. Formal certifications must be held at the prime offeror's organizational level performing the contract. If not ISO certified or SEI appraised, acceptable comparable System Engineering processes shall be maintained for the entire performance period of the contract, inclusive of options. These processes include: requirements management; configuration management; development of specifications; definition and illustration of architectures and interfaces; design; test and evaluation/verification and validation; deployment and maintenance. The government reserves the right to audit and/or request proof of these comparable quality processes for the entire performance period of the contract, inclusive of options.

In addition, small business companion contract awardees that elect to take advantage of provisions outlined in clause H139 must comply with the quality processes requirements. This means that at the time of award and as a minimum, the prime contractor shall be appraised at ISO 9001:2000 or ISO 9001:2008 or ISO/IEC 20000 or CMMI Development Level 3 (or higher) using the Software Engineering Institute's (SEI) SCAMPI A method by an SEI-authorized lead appraiser and must be held at the prime offeror's organizational level performing the contract for the entire performance period of the contract, inclusive of options. Evidence of comparable Systems Engineering (SE) processes will not be accepted.

6. DELIVERABLES

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

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

Sequence Number	Data Item Description	Title
A001	DI-MGMT-80227	Contractor's Progress, Status and Management Report
A002	DI-SESS-80643D	Specification Change Notice (SCN)
A003	DI-ILSS-81495	Failure Mode Effects, and Criticality Analysis Report
A004	DI-MGMT-80501	Contractor's Corrective Action Plan
A005	DI-MGMT-81842	Vulnerability Scan Compliance (VSC) Report
A006	DI-MISC-80841/T	Vulnerability Analysis Report
A007	DI-MISC-81627	System Deficiency Report (SDR) Data
A008	DI-MISC-81807	Software/Firmware CR
A009	DI-QCIC-80736	Quality Deficiency Report
A010	DI-RELI-80255	Failure Summary and Analysis Report
A011	DI-SESS-81343A	Information Security (INFOSEC) Boundary Configuration Management Plan
A012	DI-MGMT-81857	System Security Administrator Operators Documentation (SSAD)
A013	DI-MGMT-82000	DoD Information Assurance Certification and Accreditation Process (DIACAP) and RMF Deliverable Data

6.1 Manpower Reporting

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 PoP 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.

7. APPLICABLE PUBLICATIONS AND REFERENCES

7.1 Publications and References

Applicable publications, directives, handbooks, manuals, and standards provide guidance and direction in performance of the requirements. The contractor shall comply with the most current version of any applicable document. Unless otherwise specified the issue of these documents are those listed in the following indexes:

Organization	Publication Index
AF Publications	http://www.e-publishing.af.mil/
AF Technical Orders	https://www.my.af.mil/etims/ETIMS/index.jsp
Committee on National Security Systems Instructions	https://www.cnss.gov/CNSS/issuances/Instructions.cfm
Defense Federal Acquisition Regulation Supplement and Procedures, Guidance, and Information	http://www.acq.osd.mil/dpap/dars/dfarspgi/current/
DISA Issuances and Policies	http://www.disa.mil/About/DISA-Issuances
DISA Security Technical Implementation and Requirement Guides	http://iase.disa.mil/stigs/Pages/index.aspx
Department of Defense	http://www.dtic.mil/whs/directives/
Department of Homeland Security FISMA	https://www.dhs.gov/fisma
Intelligence Policy and Directives	https://www.dni.gov/index.php/intelligence-community/ic-policies-reports
National Institute of Standards and Technology	https://www.nist.gov/publications
National Security Agency Information Assurance Directorate	https://www.iad.gov/iad/index.cfm

The Contractor shall be responsible for notifying the Contracting Officer in writing within 30 days of publication revisions/changes/supplements if there is any impact on the scope of work to be performed under this contract or order hereto.

7.1.1 Directive Documents. The terms "directive" shall be defined as follows:

7.1.1.1 Directive Publication

Compliance with directive publications by the Contractor is mandatory. If a directive publication requires compliance with one or more publications or parts of other publications, the referenced publication(s) shall be applicable to the Contractor as it applies to the original directive. The following is a listing, not all inclusive, of the majority of applicable directive publications:

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 AF Policy Directive (AFPD) 10-2, Readiness. It applies to all US AF Major Commands (MAJCOM), Air National Guard (ANG), AF 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 AF Operational Reports (AF OPREP-3). It establishes and describes the AF 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 AF 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 AF Instruction (AFI) instead of repeating instructions in separate directives.

NETWORK OPERATIONS AND INFRASTRUCTURE SOLUTIONS (COMPLIANCE)

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

NETWORK OPERATIONS AND INFRASTRUCTURE SOLUTIONS (COMPLIANCE)

Standard		URL	Description
5.	AFI-1604 AF Information Security Program	http://static.e-publishing.af.mil/production/1/saf_aa/publication/afi16-1404/afi16-1404.pdf	This publication implements AF Policy Directive (AFPD) 16-14, Security Enterprise Governance; DoD Directive 5210.50, Management of Serious Security Incidents Involving Classified Information, DoDI 5210.02, Access and Dissemination of RD and FRD, DoDI 5210.83, DoD Unclassified Controlled Nuclear Information (UCNI), DoD Manual 5200.01, DoD Information Security Program, Volume 1, Volume 2, Volume 3, and Volume 4; and DoDM 5200.45, Instructions for Developing Security Classification Guides.
6.	AFI 31-501 Personnel Security Program Management	http://static.e-publishing.af.mil/production/1/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.

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 AF 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 AF military and civilian personnel that perform or utilize GeoBase functions, products or systems, including those in the Air National Guard and U.S. AF 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 IAW AFMAN 37-123, Management of Records and disposed of IAW the AF 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 AF.
8.	AFI 33-332 AF 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

NETWORK OPERATIONS AND INFRASTRUCTURE SOLUTIONS (COMPLIANCE)

Standard		URL	Description
			referred to as a Privacy Act system of records. The AF must publish SORNs in the Federal Register, describing the collection of information for new, changed or deleted systems to inform the public and give them a 30 day opportunity to comment before implementing or changing the system.
9.	AFI 33-364 Records Disposition Procedures and Responsibilities	http://static.e-publishing.af.mil/production/1/saf_cio_a6/publication/afi33-364/afi33-364.pdf	Records Disposition Procedures
10.	AFI 33-401 AF Architecting	http://static.e-publishing.af.mil/production/1/saf_cio_a6/publication/afi33-401/afi33-401.pdf	This AF Instruction (AFI) implements AF Policy Directive (AFPD) 33-4, Enterprise Architecting. This instruction describes the federation of AF architectures and its concept for federated architecture development, its associated business rules, governance, and the roles and responsibilities for appropriate AF 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 AF-wide management and use of the electromagnetic spectrum and implements DoD Instruction 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; AF Policy Directive (AFPD) 33-5, Warfighting Integration; and the procedures established by the Joint Staff J65A United States Military Communications-Electronics Board (USMCEB).

NETWORK OPERATIONS AND INFRASTRUCTURE SOLUTIONS (COMPLIANCE)

Standard		URL	Description
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.
13.	AFI 36-2201 AF Training Program	http://static.e-publishing.af.mil/production/1/af_a1/publication/afi36-2201/afi36-2201.pdf	This AF Instruction (AFI) applies to Total Force – Active Duty, AF Reserve, Air National Guard (ANG), and Department of AF Civilian. Ensure that all records created as a result of processes prescribed in this publication are maintained IAW AFMAN 33-363, Management of Records, and disposed of IAW the AF 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.

NETWORK OPERATIONS AND INFRASTRUCTURE SOLUTIONS (COMPLIANCE)

Standard		URL	Description
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 AF 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 AF 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 AF, 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 AF mission readiness and warfighting capabilities. This manual applies to all AF military, civilians, contractor personnel under contract by the DoD, and other individuals or organizations as required by binding agreement or obligation with the Department of the AF. This manual applies to the Air National Guard (ANG) and the AF Reserve Command (AFRC).

NETWORK OPERATIONS AND INFRASTRUCTURE SOLUTIONS (COMPLIANCE)			
Standard		URL	Description
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 AF Manual (AFMAN) implements Executive Order (E.O.) 13103, Computer Software Piracy and AF 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 AF (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 WS; see AFPD 63-1/20-1, Integrated Life Cycle Management).
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.

NETWORK OPERATIONS AND INFRASTRUCTURE SOLUTIONS (COMPLIANCE)			
Standard		URL	Description
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 DoD Directive 5015.2, DoD Records Management Program, and AF Policy Directive (AFPD) 33-3, Information Management. It establishes the requirement to use the AF 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 AF 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.

NETWORK OPERATIONS AND INFRASTRUCTURE SOLUTIONS (COMPLIANCE)

Standard		URL	Description
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.
22.	DoDI 8510.01 - DoD 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

NETWORK OPERATIONS AND INFRASTRUCTURE SOLUTIONS (COMPLIANCE)			
Standard		URL	Description
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.	DoD Architecture Framework (DoDAF) Ver2.02 Aug 2010	http://dodcio.defense.gov/dodaf20.aspx	The DoDArchitecture Framework (DoDAF), Version 2.0 is the overarching, comprehensive framework and conceptual model enabling the development of architectures to facilitate the ability of 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.

NETWORK OPERATIONS AND INFRASTRUCTURE SOLUTIONS (COMPLIANCE)

Standard		URL	Description
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.

NETWORK OPERATIONS AND INFRASTRUCTURE SOLUTIONS (COMPLIANCE)

Standard		URL	Description
35.	DoD Mobile Application Strategy	http://archive.defense.gov/news/dodmobilitystrategy.pdf	It is intended to align the progress of various mobile device pilots and initiatives across DoD under common objectives, ensuring that the warfighter benefits from such activities and aligns with efforts composing the Joint Information Environment.
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: DoDNet-Centric Data Strategy, DoD CIO, 9 May 2003
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.

NETWORK OPERATIONS AND INFRASTRUCTURE SOLUTIONS (COMPLIANCE)

Standard		URL	Description
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 DoDInformation 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 DoDfor 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).

NETWORK OPERATIONS AND INFRASTRUCTURE SOLUTIONS (COMPLIANCE)

Standard		URL	Description
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 AF 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.
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) IAW 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, AF Cybersecurity Program Management	http://static.e-publishing.af.mil/production/1/saf_cio_a6/publication/afi33-200/afi33-200.pdf	This AFI provides general direction for implementation of IA and management of IA programs according to AFPD 33-2. Compliance ensures appropriate measures are taken to ensure the availability, integrity, and confidentiality of AF 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.

NETWORK OPERATIONS AND INFRASTRUCTURE SOLUTIONS (COMPLIANCE)

Standard		URL	Description
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
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.	AFMAN 33-145 Collaboration Services and Voice Systems Management	http://static.e-publishing.af.mil/production/1/saf_cio_a6/publication/afman33-145/afman33-145.pdf	It establishes procedures and guidance for Collaboration Services including electronic collaboration and management of Video Teleconferencing (VTC) resources to include systems, equipment, personnel, time, and money and provides the directive guidance for AF VTC and voice systems management activities.
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.

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.

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

NETWORK OPERATIONS AND INFRASTRUCTURE SOLUTIONS (COMPLIANCE)

Standard		URL	Description
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.

NETWORK OPERATIONS AND INFRASTRUCTURE SOLUTIONS (COMPLIANCE)

Standard		URL	Description
58.	AFI 33-115 AF Information Technology (IT) Service management	http://static.e-publishing.af.mil/production/1/saf_cio_a6/publication/afi33-115/afi33-115.pdf	This AF instruction (AFI) implements AF 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 AF. It provides the roles, standards, and guidance relating to the messaging classes used by the AF: organizational DMS High Grade Service (HGS), and Simple Mail Transfer Protocol (SMTP) electronic mail (E-mail) messaging. This instruction applies to all AF organizations, personnel, Air National Guard, AF 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.
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

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

NETWORK OPERATIONS AND INFRASTRUCTURE SOLUTIONS (COMPLIANCE)

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

NETWORK OPERATIONS AND INFRASTRUCTURE SOLUTIONS (COMPLIANCE)

Standard		URL	Description
64.	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 DoDfor commercial wireless services, devices, and technological implementations.
65.	DODD 8100.1 DoD 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.
66.	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, IAW DoDChief 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.

NETWORK OPERATIONS AND INFRASTRUCTURE SOLUTIONS (COMPLIANCE)			
Standard		**URL**	**Description**
67.	STIGs	http://iase.disa.mil/stigs/Pages/index.aspx	The 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.
68.	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
69.	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 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 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.
70.	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.
71.	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.
72.	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.
73.	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.

NETWORK OPERATIONS AND INFRASTRUCTURE SOLUTIONS (COMPLIANCE)

Standard		URL	Description
74.	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.
75.	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.
76.	DoD Chief Information Officer Cloud Computing Strategy	http://dodcio.defense.gov/Portals/0/Documents/Cloud/DoD%20Cloud%20Computing%20Strategy%20Final%20with%20Memo%20-%20July%205%202012.pdf	This strategy is to enable the Department to increase secure information sharing and collaboration, enhance mission effectiveness, and decrease costs using cloud services.
77.	CNSSI 4009: National Information Assurance (IA) Glossary	http://jitc.fhu.disa.mil/pki/documents/committee_on_national_security_systems_instructions_4009_june_2006.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.
78.	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.
79.	Designation of the DISA as the DoD 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 DISA as the DoD Enterprise Cloud Service Broker.
80.	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.

NETWORK OPERATIONS AND INFRASTRUCTURE SOLUTIONS (COMPLIANCE)

Standard		URL	Description
81.	DoD Instructions, 8500 Series	http://www.dtic.mil/whs/directives/corres/ins1.html	DoD Issuances
82.	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.
83.	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 IAW law and as directed by the President.
84.	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.
85.	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.

NETWORK OPERATIONS AND INFRASTRUCTURE SOLUTIONS (COMPLIANCE)

Standard		URL	Description
86.	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.
87.	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.
88.	NIST SP 800-37, Revision 1: Guide for Applying the RMF 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 RMF 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.
89.	DISA, the STIG	http://iase.disa.mil/stigs/Pages/index.aspx	The 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
90.	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 IAW 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.
91.	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.
92.	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 DoD networks to provide end-to-end Unified Capabilities (UC).

NETWORK OPERATIONS AND INFRASTRUCTURE SOLUTIONS (COMPLIANCE)

Standard		URL	Description
93.	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.
94.	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.
95.	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.

NETWORK OPERATIONS AND INFRASTRUCTURE SOLUTIONS (COMPLIANCE)

Standard		URL	Description
96.	AFMAN 33-285 Cybersecurity Workforce Improvement Program	http://static.e-publishing.af.mil/production/1/saf_cio_a6/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.
97.	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.
98.	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
99.	DoDI 8540.01 Cross Domain (CD) Policy	http://www.dtic.mil/whs/directives/corres/pdf/854001p.pdf	Establishes policy, assigns responsibilities, and identifies procedures for the interconnection of information systems (ISs) of different security domains using CD solutions (CDSs) IAW the authority in DoD Directive (DoDD) 5144.02

NETWORK OPERATIONS AND INFRASTRUCTURE SOLUTIONS (COMPLIANCE)

Standard		URL	Description
100.	DFARS: Network Penetration Reporting and Contracting for Cloud Services	https://www.federalregister.gov/articles/2015/08/26/2015-20870/defense-federal-acquisition-regulation-supplement-network-penetration-reporting-and-contracting-for	DoD is issuing an interim rule amending the DFARS to implement a section of the National Defense Authorization Act for Fiscal Year 2013 and a section of the National Defense Authorization Act for Fiscal Year 2015, both of which require contractor reporting on network penetrations. Additionally, this rule implements DoD policy on the purchase of cloud computing services.
101.	DoDD 8140.01 Cyberspace Workforce Management	http://www.dtic.mil/whs/directives/corres/pdf/814001_2015_dodd.pdf	Reissue and renumber DoDD 8570.01 to update and expand establish polices and assigned responsibilities for managing the DoD cyberspace workforce.
102.	DoD IPv6 Memorandum July 3, 2009, and DoD CIO IPV6 Memorandum, September 29, 2003	http://jitc.fhu.disa.mil/apl/ipv6/pdf/disr_ipv6_product_profile_v4.pdf and https://acc.dau.mil/adl/en-US/31652/file/5809/IPV6%20Policy%20Memo.pdf	This document provides the engineering-level definition of "Internet Protocol (IP) Version 6 (IPv6) Capable" products necessary for interoperable use throughout the U.S. DoD (DoD).
103.	DODI 4650.10 Land Mobile Radio (LMR) Interoperability and Standardization	http://www.dtic.mil/whs/directives/corres/pdf/814001_2015_dodd.pdf	Reissue and renumber DoDD 8570.01 to update and expand establish polices and assigned responsibilities for managing the DoD cyberspace workforce.

104.	AF Instruction 33-150	http://static.e-publishing.af.mil/production/1/saf_cio_a6/publication/afi33-150/afi33-150.pdf	This AF Instruction (AFI) implements AF Policy Directive AFPD 33-1, Cyberspace Support. It establishes the management of cyberspace resources to include systems, equipment, personnel, time, and money and provides the directive guidance for Air Force cyberspace support activities. This publication applies to all military and civilian Air Force personnel, members of the Air Force Reserve Command (AFRC), Air National Guard (ANG), third-party governmental employee and contractor support personnel in accordance with appropriate provisions contained in memoranda support agreements and Air Force contracts. In this document, the term "cyberspace support activity" is defined as any action taken to restore communications systems/equipment to operational status, to perform preventive maintenance inspections (PMI) on communications systems/equipment and/or components, or to install or remove communications systems/equipment. The term cyberspace infrastructure refers to equipment and network infrastructure to provide the internet, network operations and command and control, and embedded processors and controllers. The term "Communications systems/equipment" is defined as: transmission, switching, processing, systems-control, and network management systems, as well as equipment, software, and facilities, fixed and deployable, that supports a mission area. The intent of this instruction is to

NETWORK OPERATIONS AND INFRASTRUCTURE SOLUTIONS (COMPLIANCE)

Standard		URL	Description
			ensure only qualified personnel perform cyberspace support activities and prevent damage to communications hardware, software, stored information, and current mission operations.
105.	Technical Order 00-33A-1001	https://www.my.af.mil/TOV3/USAF_TECHPUBS/ETOS/00-33A-1001-WA-1/00-33A-1001.PDF	This manual is to establish procedures for the management of communications/cyber equipment/systems.

Attachment 1 – Deliverables and Standards

Deliverables

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

Applicable Documents and Standards

[Refer to Appendix 1, "Network Operations and Infrastructure Solutions Standards and Documentation" for the applicable certifications, specifications, standards, policies and procedures, represent documents and standards that may be placed on individual contract TOs. Individual TOs may impose additional standards to those required at the contract level. The list in Appendix 1 is not all-inclusive and the most current version of the document in the AF Standard Center of Excellence Repository (SCOER) at the time of task order issuance will take precedence. Other documents required for execution of tasks issued under NETCENTS-2 will be cited in the relevant TO, such as specific FIPS, NIST, or MIL-Standards. Web links are provided wherever possible.