NETCENTS-2 SOLUTIONS
NetOps and Infrastructure Solutions – Full & Open (F&O)/Small Business (SB) Companion

Civil Engineering (CE) Control System (CS) Cybersecurity Initiative

Task Order Performance Work Statement

Name:	
Organization:	
Address:	

Contents

Executive Summary

This document specifies services required for interconnectivity, interoperability, cyber security, and program management of technical projects and network operations for CE Industrial Control Systems worldwide. The systems described here are under the purview of the Air Force Civil Engineer (AF/A4C) and provide technical and operational support to the active duty Air Force infrastructure base. Systems also include automated control, building automation, utility monitoring/control, and facility/utilities automation for infrastructure identified in the DoD/USAF Critical Infrastructure Program (CIP).

The sponsor for this effort is the Air Force Civil Engineer Center Operations Directorate (AFCEC/CO).

NETCENTS-2 NetOps and Infrastructure F&O
TO PWS
Civil Engineering CS Cybersecurity Initiative

1. Purpose

This contract shall support the AFCEC Operations Directorate (AFCEC/CO) and the Air Force Civil Engineer Authorizing Official (AO) efforts in managing risk, identifying, mitigating, monitoring, and predicting cyber vulnerabilities related to CE Control Systems (CS) worldwide. This contract shall also provide the capability to research and develop new CS lifecycle strategies and methods for less vulnerable and more cost effective CE CS deployments worldwide.

2. Scope

The contractor shall provide a full range of services and deliverables in support of the AFCEC missions. Services and deliverables shall be professional, of high quality, delivered on time, and may be performed in any active duty location worldwide where AF CE does business. Personnel provided under this TO will actively support engineering design, development, and fielding of developed solutions as directed by AFCEC/CO, AFCEC/COM, and AFCEC/COMI. Services and deliverables shall include:

2.0.1. Management and Professional Services. The contractor shall perform management and professional services by providing and coordinating resources, financial management, monitoring performance, and contract actions in preparing and providing deliverables. The contractor shall use the RMF methodology to successfully implement a process to effectively provide training to military, civilians, and contractors concerning the processes for assessment and authorization of CE CS. The contractor shall interact with various Base Civil Engineer organizations to plan and implement cybersecurity solutions throughout the enterprise. The contractor shall utilize effective communication skills to interact and push implementation of Risk Management Framework (RMF) for CE CS.

2.0.2. Studies, Analyses, and Evaluations. The contractor shall provide studies, analyses, and evaluations by providing expertise and services to include planning, coordination execution, reporting and evaluation as they relate to information system security and risk management activities to more effectively manage industrial control system related cybersecurity risks. The contractor shall review and complete the Assessments and Authorization (A&A) documentation required to complete in Enterprise Mission Assurance Support Service (eMASS) for obtaining AO decision to provide an Authorization to Operate (ATO). The contractor shall provide guidance and ensure compliance with DoD cybersecurity policies and regulations in support of RMF workforce roles.

2.0.3. Engineering and Technical Expertise. The contractor shall provide engineering and technical expertise in system risk management framework assessment and authorization processes, analysis and reporting requirements in the area of cybersecurity, computer network defense (CND), and inventory management for CE CS.

3. Requirement/Description of Services

The Contractor shall provide the necessary services to support interconnectivity, interoperability and cybersecurity to AFCEC/CO, the Civil Engineer Maintenance, Inspection and Repair Team (CEMIRT) Division (AFCEC/COM), and Base Civil Engineers (BCEs) for control systems under the purview of AF/A4C that are part of the active duty Air Force. The contractor shall perform all work in accordance with all applicable laws (as identified in Section 7), policy, guidance, instructions, and best commercial practices. The desired end state is cyber-resilient CE infrastructure that is part of a homogenous enterprise information system which meets or exceeds DoD/USAF cybersecurity standards and criteria.

a). In support of AFCEC/CO, the Contractor shall provide services to incorporate cybersecurity into CE CS acquisition (i.e. concept, design, deployment, and sustainment), operations (i.e. interconnectivity and interoperability), and life cycle management (i.e. testing, fielding, commissioning and decommissioning, and supply chain management).

b). In support of the CEMIRT Division and its Mission Areas (MAs), the Contractor shall provide services to develop and deploy an affordable, secured, and centrally managed enterprise network solution for the CE control systems defined in Air Force Guidance Memorandum 2017-32-01, Civil Engineer Control Systems Cybersecurity. The scope shall incorporate all control systems under the purview of AF/A4C and those that have a current memorandum of agreement or understanding (MOA/MOU) between the AF/A4C and supported organizations. The six (6) CEMIRT CS MAs are shown below and outlined in detail in Appendix 4:

a. MA-1: Cyber Threat and Situational Awareness (SA)
b. MA-2: Assessment & Authorization (A&A)
c. MA-3: Hardware/Software (HW/SW) Management
d. MA-4: Network Defense (NetD)
e. MA-5: Incident Management
f. MA-6: Risk Management Framework Workforce

c). The Contractor shall provide the requisite personnel with expertise in Information Technology (IT) cybersecurity, Enterprise IT and Operational Technology Control System network design, systems analyses, project implementation, and life cycle sustainment. Expertise shall include demonstrable performance of tasks that are needed to deliver an affordable, efficient and effective acquisition, operations, and sustainment management concept and structure that foster timely deployment, optimal operation, and effective sustainment of the CE CS Cybersecurity enterprise. The PWS herein describes both the general and mission area-specific requirements for the required contractor necessary to support the CEMIRT ICS Branch and BCE's management and use of the enterprise CE CS Cybersecurity network. The Government work load estimates identified in this Performance Work Statement establish requirements for this task order. Any significant change (increase or decrease) to the work load estimates provided will need to be reviewed; if a cost impact (up or down) is substantiated, may require a formal task order modification of the requirement.

d). The contractor shall provide the required services at Tyndall AFB, FL, multiple AF installations world-wide, facilities and any temporary duties (TDYs) associated with such work.

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

3.1.1 Enclaves

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

3.1.2 Enterprise Level Security (ELS)

3.1.2.1 Cyber Security Architecture

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

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

The contractor shall provide infrastructure capabilities that enable SOA solutions to implement IA in accordance with WS assurance standards. WS standards will be defined at the task order level, but the expected ones are:

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

The contractor shall provide Cyber Security architecture, services, and solutions as stipulated by IC standards or other US, Allied, and Parner standards as specified in TO.

3.1.2.1.1 Confidentiality

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

3.1.2.1.2 Integrity

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

3.1.2.1.3 Availability

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

3.1.2.1.4 Authenticity

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

3.1.2.1.5 Non-Repudiation

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

3.1.2.2 3.1.2.2 Cyber Security Services

a). The Contractor shall provide the requisite services and solutions to support and conduct cybersecurity operations and management including but not limited to, planning and programming support of CE CS, compliance, threat analyses, risk assessment, validation, mitigation, certification, and accreditation.

b). The Contractor shall provide documentation supporting the identification and qualifications for a professional cybersecurity workforces with certification status of personnel performing cybersecurity functions. Certified contractor personnel performing cybersecurity functions whose certification lapses shall be denied access to DoD information systems, or have their access downgraded to a level appropriate for a lower certification status.

c). The Contractor shall ensure that all application deliverables meet the requirements of DoD Instruction 8500.01, Cybersecurity, and DoD Instruction 8581.01, Information Assurance Policy for Space Systems Used by DoD, which supplements IA policy and requirements in the two aforementioned documents. Application deliverables should also meet Certification and Accreditation (C&A) requirements set forth in Intelligence Community Directive (ICD) 503, Intelligence Community Information Technology Systems Security Risk Management, Certification and Accreditation, DoD Instruction 8510.01, Risk Management Framework (RMF) for DoD Information Technology (IT), DoDD 8115.01, Information

Technology Portfolio Management Implementation, and any other current standards and guidance that are applicable.

d). Contractor solutions shall comply with the Federal Information Security Management Act (FISMA) and standards and guidelines set forth by the National Institute for Standards and Technologies (NIST) including Federal Information Processing Standards (FIPS) 199, Standards for Security Categorization of Federal Information and Information Systems, FIPS 200, Minimum Security Requirements for Federal Information and Information Systems, and its mandated reference SP 800-53, Security and Privacy Controls for Federal Information Systems and Organizations, in addition to applicable Intelligence Community (IC) standards.

e). The Contractor shall support activities and meet the requirements of DoD Instruction 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. These activities include defining user and registration requirements to Local Registration Authorities (LRAs).

f). For solutions to Infrastructure as a Service (IaaS), Platform as a Service (PaaS) or similar environments, and thus inheriting existing network security controls, information security assurance is required at the Network layer of the TCP/IP DoD Model. The contractor shall ensure that all infrastructure deliverables comply with the Defense Information Systems Agency (DISA) Security Technical Implementation Guide (STIG) and Computer Network Defense (CND), which includes the need for source code scanning, the DISA Database STIG, and a Web Penetration Test to mitigate vulnerabilities associated with SQL injections, cross-site scripting, and buffer overflows.

g). Personnel performing cybersecurity activities are required to obtain and maintain technical or management certifications to ensure compliance with DoD 8570.01-M, Information Assurance Workforce Improvement Program, 19 December 2005 (with all current changes), DoD Directive 8570.01, Information Assurance Workforce Training, Certification and Workforce Management. The responsibilities may include, but are not limited to, physical and environmental protection, personnel security, incident handling, and security training and awareness.

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

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

The contractor shall ensure that all infrastructure deliverables comply with the Defense Information Systems Agency (DISA) Security Technical Implementation Guide (STIG) and Computer Network Defense (CND)., which includes the need for source code scanning, the DISA Database STIG, and a Web Penetration Test to mitigate vulnerabilities associated with SQL injections, cross-site scripting, and buffer overflows. The contractor shall also support activities and meet the requirements of DoDI 8520.02, Public Key Infrastructure (PKI) and Public Key (PK) Enabling, in order to achieve standardized, PKI-supported capabilities for biometrics, digital signatures, encryption, identification and authentication.

3.1.2.2.2 Threat Analysis

Administer and engineer current and future CND in support of CE CS network defense. Monitor and protect the security of the CE CS from internal and external network defense threats. Support and report events to the appropriate program manager and assist in preparing briefings as required to update the Government on the status of actions and coordinate with all other members involved as directed by the Government

3.1.2.2.3 Certification and Accreditation

a). The Contractor shall provide services and solutions to address the risks associated with CE CS and accomplish the assessment and authorization following the DoDI 8510.01, Risk Management Framework (RMF) for DOD Information Technology, and other prescribed directives to accomplish the A&A inside and outside the continental United States (CONUS and OCONUS).

b). The Contractor shall provide services and solutions to address the implementation of RMF for CE CS while the CE CS community transitions to the risk management framework ensuring implementation of security controls based on appropriate categorization in accordance with CNSSI 1253, Security Categorization and Control Selection for National Security Systems, to accomplish the assess and authorize RMF process for each system. Assessments shall include the review and validation of the A&A packages, advise the Information System Owner (ISO) or representatives concerning confidentiality, integrity, and availability for each system, evaluate threats and vulnerabilities to ascertain the need for additional safeguards.

c). The Contractor shall assemble and submit appropriate documentation are initiated for each system based on findings and recommendations from the security assessment report (SAR) and conduct necessary remediation actions. Ensure security control assessments are completed for each CE CS are working as intended to protect the confidentiality, integrity, and availability at the appropriate levels.

d). The Contractor shall participate in meetings and design reviews to support the implementation of new and upgraded CE CS. The contractor shall work with the respective bases to provide portfolio management to ensure information is complete, accurate, and in accordance with current AF portfolio management directions. The contractor shall assist in registering systems in the Enterprise Information Technology Data Repository (EITDR) or Information Technology Investment Portfolio Suite (ITIPS) making updates as necessary or as prescribed by the CE CS ISO or designee. Complete the Security, Interoperability, Supportability, Sustainability and Usability (SISSU) checklist, as described in the IT LEAN Reengineering and SISSU Guidebook, v6.0, 24 Oct 2008 to ensure needs are communicated early for requirements generation and forward. The contract shall enter and update entries in eMASS for new and updated CE CS.

3.2.2.2.2.1 Systems Engineering

The Contractor shall provide systems engineering solutions for the analysis, design, integration, installation, testing, and life-cycle support of new and upgraded systems associated with delivery of infrastructure capabilities as defined by the AF enterprise architecture. The Contractor shall employ disciplined systems engineering processes in accomplishing contract tasking, using commercial best practices in accordance with AFI 63-1201, LifeCycle Systems Engineering, for systems engineering processes in planning, architecting, requirements development and management, design, technical management and control, technical reviews, technical measurements, integrated risk management, configuration management, data management, interface management, decision analysis, systems management, inspections and maintenance, sources of supply maintenance and repair, and test and evaluation, verification and validation.

These systems engineering solutions shall follow industry standard engineering processes and may include but not be limited to: technical assessments of all user requirements, integration of all GFE and Contractor Furnished Equipment (CFE) as proposed, hardware and software information, network applications, system design, training (COTS or customized)(initial and recurring), maintenance and support, system interface studies and control documents, network integration and test plans, cost analysis/trade-off studies, engineering change proposals, Voice Switching System (VSS) facility and systems/applications studies, VSS call detail recording and traffic measurement data analysis, engineering support (digital transmission/switching equipment) to government engineers. The contractor shall provide reengineering capabilities to examine structures, systems and roles for the purpose of executing a ground-up redesign for achieving long-term, full-scale integration required for the DoDIN.

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

3.2.2.2.2.2 System Upgrade/Update Support

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

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

3.2.2.2.3 Design/Integration Reviews

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

The Contractor shall provide a single source of integration management for worldwide support, planning and sustainment of dissimilar manufacturer's switching systems, applications and peripheral equipment related to the VSS. The Contractor shall identify cross functional applications and technical issues from selected symbiotic functional areas and document the opportunities for resolving the issues. The Contractor shall report impacts on the issues such as costs, return on investment, schedule dependencies and recommend functional and technical solutions. The Contractor shall identify integration issues and problems such as requirements definition, architecture and policy/standards compliance and engineering guidelines compliance. The Contractor shall enable convergence with data systems and/or collaborative tools as specified and required in the TO.

3.2.2.2.3.1 Prototypes

The Contractor shall develop schedules and implementation plans with definable deliverables, including parallel operations where required, identification of technical approaches and a description of anticipated prototype results associated with delivery of infrastructure capabilities as defined by the AF DoD or applicable IC enterprise architecture. The Contractor shall operate and maintain prototype applications, infrastructures, models and databases to determine optimal solutions for integration concepts and problems integral to the integration process.

3.2.2.2.3.2 Preliminary Design/Integration Review (PDR)

During the PDR, the Contractor shall present initial draft system design associated with delivery of infrastructure capabilities as defined by the enterprise architecture for government review.

The draft documents to be reviewed shall include those specified in the TO. Examples may include the system requirements, the final Site Survey Report, System Design, Installation Specification (IS), Engineering Drawings and Installation Plan. This review shall include a list of recommended long-lead time items that the government must order and have available at the time of system installation. This review shall be in sufficient detail to ensure technical understanding of the following: mission and requirements analysis, identification of all equipment and software to be integrated and to be used in the development of the design and the scope and schedule of the work to be performed.

3.2.2.2.3.3 Final Design/Integration Review (FDR)

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

3.2.2.2.4 Site Preparation

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

3.2.2.2.4.1 Pre-Installation Briefing

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

3.2.2.2.4.2 Government Support

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

3.2.2.2.4.3 Installation

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

3.3 Dynamic Test Environment

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

3.3.1 Design

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

3.3.2 Implementation

The Contractor shall provide tools and services to implement the dynamic test environment. This will include but not limited to, configuring the products and technologies required by the design of the test environment; installing those products and technologies in location designated by the design; developing capabilities necessary to fully integrate the products and technologies with each other and with existing infrastructure capabilities; integrating the products, technologies and developed capabilities with existing infrastructure capabilities to configure the test environment and developing and executing test procedures to ensure the proper functioning of the test environment.

3.3.3 Operation

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

3.5 General Requirements.

The Contractor shall support the Government to:

a). Operate Automated Data Processing (ADP) Systems.

1. Possess the expertise and capability to use the ADP systems utilized by AFCEC and its customers in support of the requirements of this PWS.

2. Assist in the dissemination of information gained on a project or program specific basis to all Air Force programs. (CDRL A001)

b). Properly and accurately comprehend, interpret, articulate, understand, and apply information technology (IT) and automation/control system network topology diagrams, engineering drawings and data, repair manuals, technical bulletins, security technical information guides and manufacturer’s catalogs, and the applicable standards for each area.

c). Provide technical guidance on IT or industrial automation network architectures linking to or used in automation/control systems (e.g. Computer-based Supervisory Control and Data Acquisition (SCADA), Enterprise Building Integrator (EBI), etc.).

d). Provide categorization guidance and support for platform IT determination as described in the Air Force Platform IT (AF PIT) Guidebook v1.4 or later and all UFC/UFGS specifically referencing control systems as defined NIST Special Publication (SP) 800-53 (latest edition).

e). Review any CS component software or hardware for compliance with applicable NIST, IEEE and DoD standards and policies.

f). Have working knowledge and skills on control system networks based on any of the Open Platform Communications (OPC) standards, e.g. Building Automation Control Network (BACNet), LONWORKS, MODBUS, etc., as prescribed by the OPC Foundation under their Unified Architecture (UA).

g). Conduct CE CS Cyber Security Data Repository. Plan, direct, or coordinate activities for electronic data processing, information management, and document control. Perform activities that include analyzing the organizations computer needs and recommend possible solutions to develop computer or information system that will track, maintain and report on all data collection efforts as directed by AFCEC/COMI.

h). Conduct CE CS Cybersecurity Data Collection. Perform RMF team member activities to coordinate operational activities with external stakeholders as directed by the AFCEC/CO, AFCEC/COM, or AFCEC/COMI. Perform Enterprise Mission Assurance Support Service (eMASS) activity of CE CS for the management of all cybersecurity compliance activities from system registration to system decommissioning, risk analysis assessments of CE CS, and field support to USAF installations worldwide.

i. Design and Produce Visual Media Products. Support the design and production of visual media products, as required, in support of the AFCEC mission. (CDRL TBD)

j). Develop technical work products (e.g. engineering drawings, network topology diagrams, implementation schedules, electronic briefings, training plans, etc.) utilizing only MS Office products (i.e. MS Visio Professional 2010 or later, MS Project 2010 or later, MS Office Professional 2007 or later, including MS Access, and MS SharePoint 2010 or later).

k). Perform CE CS Information System Security Manager (ISSM), Information System Security Officer (ISSO), and User Representative (UR) / System Administration functions as defined by AFI 17-101 for all CE CS at all active duty AF Bases. List of bases is provided in **Appendix 4 - Mission Area Performance Requirements,** MA-6**.**

l). The Contractor-provided expertise shall meet these additional specific MA tasks as outlined in **Appendix 4 - Mission Area Performance Requirements.**

3.5.1 Contractors Use of NETCENTS-2 Products Contract

The Contractor shall obtain all products and associated peripheral equipment required by each individual TO from the NETCENTS-2 Products contract.

3.5.2 Enterprise Software Initiative

See DFARS 208.7402 regarding use of the DoD's Enterprise Software Initiative (ESI) Blanket Purchase Agreements (BPAs) for software license purchases.

3.5.3 Software License Management

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

3.5.4 Hardware

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

3.5.5 Software Support

Unless specified otherwise in the TO, 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.

3.5.6 Government Furnished Equipment (GFE)

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

3.5.7 Host Nation Installations

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

3.5.8 Tools and Test Equipment

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

3.5.9 Warranty

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

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

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

3.5.9.1 System Warranty

Unless specified otherwise in the TO, the Contractor shall provide a minimum 1-year system warranty (some customers may require 2 or more years of warranty) to include coverage of all equipment supplied, installed and integrated by the contractor associated with delivery of infrastructure capabilities as defined by the AF EA. The system warranty shall ensure the full operational use of the system (CFE and GFE). The contractor shall provide to the government a 24-hour a day, 7-day a week point of contact for the system warranty. The system warranty shall begin at the time the final system DD Form 250 is signed by an authorized government representative. The system warranty shall provide fault diagnosis, hardware and software repair, replacement or redesign. The contractor shall be responsible for diagnosing any problems, identifying malfunctioning equipment and removing the equipment for repair. Prior approval shall be obtained from the authorized government site representative before any GFE is removed from the system. Actual repair of malfunctioning GFE will be the responsibility of the government, unless stated otherwise in the TO. The system warranty shall include transportation for both contractor personnel and equipment to and from the specific site. The system warranty shall provide for a return to service any malfunctioning CFE component or applications within 48 clock hours CONUS, 96 clock hours OCONUS, after notification by the authorized government site representative unless stated otherwise by the TO. Costs for system warranty will be included within each TO proposal provided by the contractor as required by the TO.

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

3.5.9.2 Workmanship Warranty

Unless specified otherwise in the TO, the contractor shall provide a minimum 1-year workmanship warranty (some customers may require 2 or more years of warranty) on all work provided or integrated under this contract. The warranty shall ensure the full operational use of the system (CFE and GFE). The contractor shall provide to the government a 24-hour a day, 7-day a week point of contact for the workmanship warranty. The workmanship warranty shall begin at the time the final system DD Form 250 is signed by an authorized government representative. The workmanship warranty shall provide fault diagnosis, hardware and software repair, replacement or redesign. The contractor shall be responsible for diagnosing and fault isolation of any problems, identifying the poor workmanship causing the problem and affecting an acceptable industry standard repair. Prior approval shall be obtained from the authorized government site representative before any GFE is removed from the system. Actual repair of malfunctioning GFE will be the responsibility of the government. The workmanship system warranty shall include transportation for both contractor personnel and bits, pieces and parts to and from the specific site and the actual repair. The workmanship warranty shall provide for a return to service any malfunctioning CFE component or applications within 48 clock hours CONUS, 96 clock hours OCONUS, after notification by the authorized Government site representative unless stated otherwise by the TO.

3.5.9.4 Equipment Warranty

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

The contractor shall provide a worldwide warranty repair solution capability for systems with qualified maintenance repair personnel and leverage existing OEM support infrastructures to the greatest extent possible. Repairs shall be performed at a time required by the Task/Delivery Order/Delivery Order or as coordinated by the government COR. The contractor shall provide a 24-hour, 7-day a week warranty repair point of contact to receive calls from the government. The contractor shall provide the capability for toll-free telephone access for obtaining technical warranty repair support assistance from worldwide locations. The contractor shall provide the tools, equipment and consumables required for personnel to complete their duties. The contractor shall not invalidate the warranty provided on components purchased under this contract when the government elects to perform user self-maintenance and/or self-installation during the warranty period. Note: The government will perform routine user-maintenance for all equipment both during and after the warranty period using separately orderable spare parts and/or repaired parts from this contract. The government will only be liable for any damage to the equipment that results from government Maintenance or additions to equipment that did not adhere to stand commercial practice. At no additional charge to the government, the contractor shall furnish, for hardware purchased under this contract, all repairs (labor and parts) for the duration of the warranty period. At a minimum, repair during the warranty period shall be equivalent to standard per-call maintenance during the Principal Period of Maintenance (PPM) as specified in this PWS. The government, at its option, may order additional repair coverage during the warranty period. The governments purchase of additional repair coverage will be specified in details by the TO.

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

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

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

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

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

3.6 Maintenance

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

3.9 Special Asset Tagging

See DFARS 252.245-7001 regarding Special Asset Tagging requirements.

4. Contractual Requirements

4.1 Performance Reporting

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

1. Provide quality products, incidentals and customer support.

2. Meet customer’s agreed-upon timelines for scheduled delivery of items, warranty, and/or incidental services: Emergency/critical, Maintenance/Warranty – 24 x 7 x 365, and remote OCONUS, OCONUS vs. CONUS response times.

3. Provide satisfactory product repairs or advance replacement, as appropriate.

4. Provide timely and accurate reports.

5. Respond to the customer’s requests for proposals and configuration assistance as identified in each delivery order.

6. Meet subcontracting goals.

4.2 Program Management

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

4.2.1 Services Delivery Summary

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

PWS PARA	PERFORMANCE OBJECTIVE	PERFORMANCE THRESHOLD	SURVEILLANCE METHOD

PWS Appendix 4 PROVIDE TECHNICAL REPORTS AND PUBLICATIONS	PO-1 Completed on time or ahead of schedule. Documentation requirements include Monthly Status Reports, Trip Reports, Briefings/ Presentations, Publications, Meeting Reports, Initial Security Assessments, risk assessment report, and (CS Cyber Security A&A eMASS Package).	E: 100% first pass yield (FPY), delivered on schedule. VG: 98% FPY, delivered on schedule. Necessary rework accomplished within three (3) work days. S: 90% FPY, delivered on schedule. Necessary rework accomplished within five (5) work days. M: 80-89% FPY, delivered on schedule. Necessary rework accomplished within 10 work days. U: <80% FPY, delivered on schedule. Necessary rework requires more than 10 work days.	- 100% Inspection - Customer feedback
PWS Appendix 4 TIMELINESS	PO-2 Provide the applicable technical reports by the due date and time specified in PWS Appendix 4. Documentation requirements for plans, reports, and analyses are delivered no later than the "as required" date and time as deemed necessary by the Government.	E: 100% first pass yield (FPY), delivered on schedule. VG: 98% FPY, delivered on schedule. Necessary rework accomplished within three (3) work days. S: 90% FPY, delivered on schedule. Necessary rework accomplished within five (5) work days. M: 80-89% FPY, delivered on schedule. Necessary rework accomplished within 10 work days. U: <80% FPY, delivered on schedule. Necessary rework requires more than 10 work days.	- 100% Inspection - Customer feedback

PWS Appendix 4 CS CYBERSECURITY SYSTEM INTEGRATION AND MIGRATION	PO-3 Task orders are completed on time or ahead of schedule. Ensure Enterprise Integration and Service Management provided by the contractor are fulfilled within the timeframe identified by the task order.	E: 100% first pass yield (FPY), delivered on schedule. VG: 98% FPY, delivered on schedule. Necessary rework accomplished within three (3) work days. S: 90% FPY, delivered on schedule. Necessary rework accomplished within five (5) work days. M: 80-89% FPY, delivered on schedule. Necessary rework accomplished within 10 work days. U: <80% FPY, delivered on schedule. Necessary rework requires more than 10 work days.	- 100% Inspection - Customer feedback

4.2.2 TO Management

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

4.2.3 Configuration and Data Management

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

4.2.5 Contract Deliverables

The Contractor shall submit *all* deliverables via e-mail to the AFCEC/COMI Branch Chief and to the Contracting Officer Representative (COR). The Government has ten (10) business days to approve or reject deliverables identified in Table 2 below. No Government response within ten (10) business days signifies Government acceptance of Contractor deliverable

4.2.6 CDRL Types

a). A001: Government required services may take the form of information, advice, opinions, alternatives, studies, presentations, analyses, evaluations, schedules, recommendations, training, and technical support.

b). A002: Status of this project shall be included in the monthly Program Management Reviews (PMR) presented to the Government. The PMR shall generally summarize the status and progress of all activities performed by the contractor under this PWS. Additional topics shall be addressed as requested by the COR. PMRs shall be held as directed by the COR.

Table 2. DELIVERABLES MATRIX

Deliverable Title	*CDRL Type*	*Due Date*
Initial Security Assessment Report; or, *Table-top Security Review* (e.g., ITCR/ITIR)	*A001*	*Within* ***5 business days*** *of,* *Receipt of security review request*
Trip Report		*Within* ***5 business days*** *of return*
Briefing/Presentation		*Within* ***5 business (working) days*** *of notification*
CE CS Cybersecurity A&A/Assess Only packages (eMASS entry)		*Within 10 business days of submittal of notification*
Technical Reports (e.g. Enterprise Network Health Report, COOP/DRP, etc.)		*Within* ***10 business days*** *of notification*
Meeting Minutes/Reports		*As required and within* ***1 business day*** *of meeting*
Publication		*As required and within* ***90 calendar days*** *of notification*
CS PMR Data	*A002*	*Monthly on the* ***3rd business day***
Monthly Status Report (MSR)		*Monthly on the* ***10th business day***

4.3 Security Management

4.3.1 Safeguarding Classified Information

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

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

For assistance and guidance on submitting Classified TO, the NETCENTS-2 Customer Service can be reached at COMM 334-416-5070 / DSN 312-596-5070 Option 1.

4.3.2 Personnel Security

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

Certain TOs may require personnel security clearances up to and including Top Secret and certain TOs may require all employees to be United States citizens. The security clearance requirements will depend on the security level required by the proposed TO. The TOs may also require access to Sensitive Compartmented Information (SCI) for which SCI eligibility will be required. Contractors shall be able to obtain adequate security clearances prior to performing services under the TO. The Contract Security Classification Specification (DD Form 254) will be at the basic contract and TO level and will encompass all security requirements. All contractors located on military installations shall also comply with Operations Security (OPSEC) requirements as set forth in DoD Directive 5205.02, Operations Security Program and AFI 10-701, Operations Security. In accordance with DoD 5200.2-R, Personnel Security Program (Jan 87), DoD military, civilian, consultants and contractor personnel using unclassified automated information systems, including e-mail, shall have, at a minimum, a completed favorable National Agency Check plus Written Inquiries (NACI).

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

4.3.3 Protection of System Data

Unless otherwise stated in the TO, the contractor shall protect system design-related documents and operational data whether in written form or in electronic form via a network in accordance with all applicable policies and procedures for such data, including DOD Regulations 5400.7-R and DoDM 5200.01 to include latest changes and applicable service/agency/combatant command policies and procedures. The contractor shall protect system design related documents and operational data at least to the level provided by Secure Sockets Layer (SSL)/Transport 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.

4.3.4 On-Site Task Approval Process

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

4.3.5 Travel Requirements

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

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

4.3.6 Other Direct Cost (ODC)

The Contractor shall identify ODC and miscellaneous items as specified in each TO. No profit or fee will be added; however, DCAA approved burdened rates are authorized.

5. Quality Processes

As a minimum, the prime contractor shall be appraised at Level 2 or higher for CMMI Development by a Software Engineering Institute (SEI) or ISO 9001:2000 or ISO 9001:2008 or ISO/IEC 20000 for the entire performance period of the contract, inclusive of options. This certification must be held at the prime offeror's organizational level performing the contract.

6. Program Management

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

6.1 Key Personnel

The Contractor agrees to assign under the contract those personnel whose credentials, experience, and expertise meet the qualification requirements identified in the PWS to fulfill the requirements of the contract.

The Contractor agrees that a partial basis of award of this contract will be the key personnel proposed, including those employed by subcontractors, if applicable. Accordingly, the contractor agrees to assign under the contract those key personnel whose credentials, experience and expertise were provided with the proposal and which meet the qualification requirements of the contract.

The CO and COR shall be notified of any proposed changes at least 30 calendar days in advance. The CO reserves the right to reject proposed changes in key personnel. Such notification shall include:

a) An explanation of the circumstances necessitating the substitution
b) A complete resume of the proposed substitute
c) Any other information needed by the CO and COR to enable them to judge that the contractor is maintaining the same quality of personnel as those included at the time of award.

6.2 Key Personnel Labor Categories

The following labor categories are defined in appendix 2 and designated as key personnel:

a) Info Security Analyst (15-1122) (Senior IA Security Analyst)
b) Info Security Analyst (15-1122) (IA Security Analyst)
c) Computer & Info Systems Managers (11-3021) (ISSM/ISSO/AOR support/SCAR/Information Management)
d) Software Developers, System SW (15-1133) (Senior Security Engineer)
e) Software Developers, System SW (15-1133) (Security Engineer)
f) Computer Network Architects (15-1143) (Senior Network Engineer)
g) Computer Network Support Specialists (15-1152) (IT Security Analyst)
h) Computer Systems Analyst (IT Security Analyst)
i) Network & Computer System Admin (System Administrator)

6.3 Contract Holidays

The following days are contract holidays:

New Year's Day	01 January
Martin Luther King, Jr. Day	Third Monday of January
President's Day	Third Monday of February
Memorial Day	Last Monday in May
Independence Day	04 July

Labor Day	First Monday in Sept
Columbus Day	Second Monday in October
Veteran's Day	11 November
Thanksgiving Day	Fourth Thursday in November
Christmas Day	25 December

6.3 Government Down-Time

a) Base closures due to Emergencies. From time to time, the Base Commander may decide to close all or part of the base in response to an unforeseen emergency or similar occurrence. Sample emergencies include, but are not limited to, adverse weather such as snow or flood, an act of God such as a tornado or earthquake, acts of war terrorism, computer failures, or a base disaster such as a natural gas leak or fire. Contractor personnel are "non-essential" for purposes of any instructions regarding the emergency.

(1) Contractor shall be officially dismissed upon notification of a base closure in accordance with paragraph b. Contractor shall promptly secure all Government furnished property appropriately and evacuate in an expedient but safe manner.

(2) With regard to work under the contract, the Government shall retain the following options:

(i). Government may grant a time extension in each task order delayed by the closure, subject to the availability of funds.

(ii). Government may forego the work. The Contractor will not be paid for work not performed.

(iii). Government may reschedule the work on any day satisfactory to both parties.

(iv). The Government may, in its discretion, permit the Contractor to perform at an off-site location during the period of base closure if meaningful work can be accomplished. Contractor shall certify to the Government by letter within five (5) business days of returning to work the nature and scope of the work completed off-site. Contractor shall be permitted to bill the Government at the labor rates identified in the contract.

(b) Base Closure Notification Procedures:

(1) After an official decision to close a base has been made by the Base Commander, local television and radio stations will be notified of the closure.

(2) The Contractor is directed to listen or watch one of the local radio or television stations for notification of a base closure. Contractor should follow instructions intended for non-essential personnel.

(3) The Contractor will not receive any other form of notification of a base closure from the Government. The Contractor is responsible for notification of his employees.

(4) If the decision to close all or part of the base is made during the duty day, and the Base Commander's decision is transmitted through official notification channels, the Contractor shall follow the instructions as given.

(c) Base Closure Due to Non-Emergencies. The Center or Base Commander may elect to close all or part of the base for non-emergency reasons such as time-off award, base open house, etc. In the event of a non-emergency base closure, the COR and the Contractor shall jointly choose a course of action within the following options:

(1) If there is a need for the service during the base closure and a Government employee will be present, Contractor may continue on-site work. Contractor shall bill the Government in accordance with the contract.

(2) If there is a need for work during the base closure but either a Government employee will not be present or access will not be available, the Contractor may work off-site provided meaningful work may be accomplished. Contractor shall certify to the Government by letter within five (5) business days or returning on-site the nature and scope of the work completed off-site. Contractor shall bill the Government at the labor rates specified in the contract.

(3) If there is no need for the service during the scheduled base closure, Contractor shall not work on or off-site. Government may grant a time extension in each task order delayed by the closure or equal to the amount of time of the closure, subject to the availability of funds. The Government will not be liable for time not worked.

(d) CONTINUATION OF ESSENTIAL DEPARTMENT OF DEFENSE (DoD) CONTRACTOR SERVICES DURING CRISIS. The performance of these services are not mission essential during time of crisis. Should a crisis be declared, the CO or his/her representative will verbally advise the Contractor of the revised requirements, followed by written direction.

6.4 Place of Performance

The individuals working in support of this TO shall be located at both OCONUS and CONUS Air Force active duty installations. All contractor personnel on this TO shall be subject to TDY as requested by the Government at both CONUS and OCONUS locations.

6.5 Hours of Work

Working hours are typically 7:00 AM to 4:00 PM, Monday through Friday when at AFCEC; however, the workday window is from 6:00 AM to 6:00 PM. Working hours will be as required while traveling or working at off-site locations (possibly seven days a week).

6.6 Task Management

AFCEC/CO will identify a COR and an Alternate COR. The COR will participate in project meetings and receive task order deliverables. The COR will provide technical assistance and clarification required for the performance of this task order.

6.6 Multi- Functional Team

6.7 Travel Requirements

Travel to both CONUS and OCONUS locations may be required in support of the requirements identified in this PWS. Travel is to be reimbursed only in accordance with the Federal Travel Regulations. All travel must be approved by the COR and /or CO in advance. Travel will be based on the current Federal Travel Regulations and/or Joint Travel Regulations (FTR/JTR). It is the responsibility of the Contractor to have the necessary credentials prior to traveling. The contractor shall produce a trip report using the formats and standards provided by the COR. The trip report shall include meeting minutes, open action items, summary of trip accomplishments and action items taken. Travel will be reimbursed on a NTE reimbursable CLIN; no profit or fee will be paid. *Travel for this task is extensive, requiring an average of 50% travel for select personnel.* The contractor shall coordinate specific travel arrangements with the individual COR to obtain advance, written approval for the travel about to be conducted. The contractor's request for travel shall be in writing and contain the dates, locations, and estimated costs of the travel.

***Travel Note: Contractor travel shall include travel to Air Force Bases (AFBs) and other locations, worldwide, but not to locations designated as unduly hazardous for travel by the Department of State.**

6.8 Host Nation Installations

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

6.8 Government Furnished Equipment and Property (GFE/GFP)

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, Visio, Microsoft Project, etc.)
- Telephone (local and long distance calls authorized as dictated by contract performance requirements)
- Facsimile
- Copier
- Printer
- Portable hard drive if necessary

Appendix 1: NetOps and Infrastructure Solutions Standards & References

Purpose:

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

NETWORK OPERATIONS AND INFRASTRUCTURE SOLUTIONS (COMPLIANCE)			
Standard		URL	Description
1.	AFI 10-206 Operational Reporting	http://static.e-publishing.af.mil/production/1/af_a3_5/publication/afi10-206/afi10-206.pdf	This instruction implements Air Force Policy Directive (AFPD) 10-2, Readiness. It applies to all US Air Force Major Commands (MAJCOM), Air National Guard (ANG), Air Force Reserve Command (AFRC), Field Operating Agencies (FOA), and Direct Reporting Units (DRU). Prior to mobilization/activation AF, ANG, and AFRC units will address the HQ AF Service Watch Cell (AFSWC) on all applicable record copy Air Force Operational Reports (AF OPREP-3). It establishes and describes the Air Force Operational Reporting System. It explains the purpose and gives instructions for preparing and submitting these reports. Refer recommended changes and questions about this publication to AF/A3O, 1480 Air Force Pentagon, Washington, D.C. 20330-1480, Office of Primary Responsibility (OPR) using the AF Form 847, Recommendation for Change of Publication. MAJCOMs are authorized to supplement this Air Force Instruction (AFI) instead of repeating instructions in separate directives.

NETWORK OPERATIONS AND INFRASTRUCTURE SOLUTIONS (COMPLIANCE)			
Standard		**URL**	**Description**
2.	AFI 10-208 Air Force Continuity of Operations (COOP) Program.	http://static.e-publishing.af.mil/production/1/af_a3_5/publication/afi10-208/afi10-208.pdf	This Instruction implements Air Force Policy Directive (AFPD) 10-2, Readiness, and is consistent with AFPD 10-8, Homeland Security. It describes policy and requirements for implementing DODI 3020.42, Defense Continuity Plan Development, and DODI O-3020.43, Emergency Management and Incident Command of the Pentagon Facilities; DODI O-3000.08 Balanced Survivability Assessments (BSAs);and O-DODI 5110.11, Raven Rock Mountain Complex (RRMC).
3.	AFI 10-601 Operational Capability Requirements Development	http://static.e-publishing.af.mil/production/1/af_a3_5/publication/afi10-601/afi10-601.pdf	The primary intent of this instruction is to facilitate timely development and fielding of affordable and sustainable operational systems needed by the combatant commander. The primary goal is to fulfill stated defense strategy needs with effects based, capabilities-focused materiel and non-materiel solutions. These solutions must be well integrated to provide suitable, safe, and interoperable increments of capability that are affordable throughout the life cycle.
4.	AFI 10-701 Operations Security (OPSEC)	http://static.e-publishing.af.mil/production/1/af_a3_5/publication/afi10-701/afi10-701.pdf	This publication provides guidance for all Air Force personnel (military and civilian) and supporting contractors in implementing, maintaining and executing OPSEC programs. It describes the OPSEC process and discusses integration of OPSEC into Air Force plans, operations and support activities.
5.	AFI-1604 Air Force Information Security Program	http://static.e-publishing.af.mil/production/1/saf_aa/publication/afi16-1404/afi16-1404.pdf	This publication implements Air Force Policy Directive (AFPD) 16-14, Security Enterprise Governance; Department of Defense (DoD) Directive 5210.50, Management of Serious Security Incidents Involving Classfied Information, DoD Instruction (DoDI) 5210.02, Access and Dissemination of RD and FRD, DoDI 5210.83, DoD Unclassified Controlled Nuclear Information (UCNI), DoD Manual (DoDM) 5200.01, DoD Information Security Program, Volume 1, Volume 2, Volume 3, and Volume 4; and DoDm 5200.45, Instructions for Developing Security Classification Guides.

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

NETWORK OPERATIONS AND INFRASTRUCTURE SOLUTIONS (COMPLIANCE)			
Standard		**URL**	**Description**
8.	AFI 33-332 Air Force Privacy And Civil Liberties Program	http://static.e-publishing.af.mil/production/1/saf_cio_a6/publication/afi33-332/afi33-332.pdf	Records that are retrieved by name or other personal identifier of a U.S. citizen or alien lawfully admitted for permanent residence are subject to Privacy Act requirements and are referred to as a Privacy Act system of records. The Air Force must publish SORNs in the Federal Register, describing the collection of information for new, changed or deleted systems to inform the public and give them a 30 day opportunity to comment before implementing or changing the system.
9.	AFI 33-364 Records Disposition Procedures and Responsibilities	http://static.e-publishing.af.mil/production/1/saf_cio_a6/publication/afi33-364/afi33-364.pdf	Records Disposition Procedures
10.	AFI 33-401 Air Force Architecting	http://static.e-publishing.af.mil/production/1/saf_cio_a6/publication/afi33-401/afi33-401.pdf	This Air Force Instruction (AFI) implements Air Force Policy Directive (AFPD) 33-4, Enterprise Architecting. This instruction describes the federation of Air Force architectures and its concept for federated architecture development, its associated business rules, governance, and the roles and responsibilities for appropriate Air Force organizations.
11.	AFI 33-580 Spectrum Management	http://static.e-publishing.af.mil/production/1/saf_cio_a6/publication/afi33-580/afi33-580.pdf	This instruction establishes guidance and procedures for Air Force-wide management and use of the electromagnetic spectrum and implements Department of Defense Instruction (DoDI) 4650.01, Policy and Procedures for Management and Use of the Electromagnetic Spectrum; DoDI 8320.05, Electromagnetic Spectrum Data Sharing; National Telecommunications and Information Administration (NTIA) Manual of Regulations and Procedures for Federal Radio Frequency Management; Air Force Policy Directive (AFPD) 33-5, Warfighting Integration; and the procedures established by the Joint Staff J65A United States Military Communications-Electronics Board (USMCEB).

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 Air Force Training Program	http://static.e-publishing.af.mil/production/1/af_a1/publication/afi36-2201/afi36-2201.pdf	This Air Force Instruction (AFI) applies to Total Force – Active Duty, Air Force Reserve, Air National Guard (ANG), and Department of Air Force Civilian. Ensure that all records created as a result of processes prescribed in this publication are maintained in accordance with AFMAN 33-363, Management of Records, and disposed of in accordance with the Air Force Records Disposition Schedule (RDS) located at https://www.my.af.mil/afrims/afrims/afrims/rims.cfm. Refer recommended changes and questions about this publication to the Office of Primary Responsibility (OPR) using the AF IMT 847, Recommendation for Change of Publication; route AF IMT 847s from the field through Major Commands (MAJCOMS) publications/forms managers.
14.	AFI 61-204 Disseminating Scientific And Technical Information	http://static.e-publishing.af.mil/production/1/saf_aq/publication/afi61-204/afi61-204.pdf	This instruction updates the procedures for identifying export-controlled technical data and releasing export-controlled technical data to certified recipients and clarifies the use of the Militarily Critical Technologies List. It establishes procedures for the disposal of technical documents.

NETWORK OPERATIONS AND INFRASTRUCTURE SOLUTIONS (COMPLIANCE)

Standard		URL	Description
15.	AFI 99-103 Capabilities-Based Test And Evaluation	http://static.e-publishing.af.mil/production/1/af_te/publication/afi99-103/afi99-103.pdf	It describes the planning, conduct, and reporting of cost effective test and evaluation (T&E) programs as an efficient continuum of integrated testing known as seamless verification. The overarching functions of T&E are to mature sys-tem designs, manage risks, identify and help resolve deficiencies as early as possible, and ensure systems are operationally mission capable (i.e., effective and suitable). The Air Force T&E community plans for and conducts integrated testing as an efficient continuum known as seamless verification in collaboration with the requirements and acquisition communities.
16.	AFMAN 33-152 User Responsibilities and Guidance for information Systems	http://static.e-publishing.af.mil/production/1/saf_cio_a6/publication/afman33-152/afman33-152.pdf	This instruction implements Air Force Policy Directive (AFPD) 33-1, Information Resources Management, AFPD 33-2, Information Assurance (IA) Program, and identifies policies and procedures for the use of cyberspace support systems/services and compliance requirements of Secretary of the Air Force, Chief of Warfighting Integration and Chief Information Officer (SAF/CIO A6) managed programs. These programs ensure availability, interoperability, and maintainability of cyberspace support systems/services in support of Air Force mission readiness and warfighting capabilities. This manual applies to all Air Force military, civilians, contractor personnel under contract by the Department of Defense (DOD), and other individuals or organizations as required by binding agreement or obligation with the Department of the Air Force. This manual applies to the Air National Guard (ANG) and the Air Force Reserve Command (AFRC).

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 Air Force Manual (AFMAN) implements Executive Order (E.O.) 13103, Computer Software Piracy and Air Force Policy Directives (AFPD) 33-1, Cyberspace Support and supports AFPD 33-2, Information Assurance (IA) Program; AFPD 63-1/20-1, Integrated Life Cycle Management; and AFPD 10-6, Capabilities-Based Planning & Requirements Development. This AFMAN provides the overarching guidance and direction for managing IT hardware and software. The hardware management guidance identifies responsibilities for supporting Air Force (AF) IT hardware (IT assets) and maintaining accountability of Personal Wireless Communications Systems (PWCS) including cellular telephones and pagers. The software management guidance identifies responsibilities for management of commercial off-the-shelf (COTS) and AF-unique software acquired/developed by the AF (other than software internal to a weapon system; see AFPD 63-1/20-1, Integrated Life Cycle Management).
18.	AFMAN 33-282 Computer Security (COMPUSEC)	http://static.e-publishing.af.mil/production/1/saf_cio_a6/publication/afman33-282/afman33-282.pdf	This AFMAN implements Computer Security in support of AFPD 33-2, Information Assurance Program and AFI 33-200, IA Management Computer Security (COMPUSEC) is defined within the IA Portion of AFI 33-200.
19.	AFMAN 33-363 Management of Records	http://static.e-publishing.af.mil/production/1/saf_cio_a6/publication/afman33-363/afman33-363.pdf	This manual implements Department of Defense (DoD) Directive (DoDD) 5015.2, DoD Records Management Program, and Air Force Policy Directive (AFPD) 33-3, Information Management. It establishes the requirement to use the Air Force Records Information Management System (AFRIMS); establishes guidelines for managing all records (regardless of media); and defines methods and the format for record storage, file procedures, converting paper records to other media or vice versa, and outlines the minimum to comply with records management legal and policy requirements.

NETWORK OPERATIONS AND INFRASTRUCTURE SOLUTIONS (COMPLIANCE)

Standard		URL	Description
20.	AFPD 33-3 Information Management	http://static.e-publishing.af.mil/production/1/saf_cio_a6/publication/afpd33-3/afpd33-3.pdf	This policy directive establishes Air Force policy for the management of information assets (all forms of data and content), across all AF information sources, as both a strategic resource and corporate asset supporting the warfighter during mission and support operations.
21.	AFPD 33-4 Information Technology Governance	http://static.e-publishing.af.mil/production/1/saf_cio_a6/publication/afpd33-4/afpd33-4.pdf	This directive establishes the AF policy for IT Governance to fulfill the AF CIO responsibilities established in federal laws and DoD issuances and the AF IT Governance Executive Board, which will oversee existing IT investment councils, boards, and working groups throughout the IT lifecycle to effectively and efficiently deliver capabilities to users. This directive focuses on aligning IT policy, CIO policy, and capabilities management with doctrine, statutory, and regulatory guidelines that govern accountability and oversight over IT requirements to resource allocation, program development, test, and deployment and operations under the direction and authority of the AF IT Governance Executive Board chaired by the AF CIO.
22.	DoDI 8510.01 - DoD Risk Management Framework (RMF) for DoD Information Technology	http://www.dtic.mil/whs/directives/corres/pdf/851001_2014.pdf	Provides procedural guidance for the reciprocal acceptance of authorization decisions and artifacts within DoD, and between DoD and other federal agencies, for the authorization and connection of information systems (ISs). Revised from 2007 version on 12 March 2014.
23.	DoDI 8500.01 – Cyber Security (CS)	http://www.dtic.mil/whs/directives/corres/pdf/850001_2014.pdf	The purpose of the Defense Cybersecurity program is to ensure that IT can be used in a way that allows mission owners and operators to have confidence in the confidentiality, integrity, and availability of IT and DoD information, and to make choices based on that confidence
24.	DoDI 8551.01 – Ports, Protocols and Services Management	http://www.dtic.mil/whs/directives/corres/pdf/855101p.pdf	Provides guidance on ports, protocols, and service management

NETWORK OPERATIONS AND INFRASTRUCTURE SOLUTIONS (COMPLIANCE)			
Standard		**URL**	**Description**
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
27.	Department of Defense Architecture Framework (DoDAF) Ver2.02 Aug 2010	http://dodcio.defense.gov/dodaf20.aspx	The Department of Defense Architecture Framework (DoDAF), Version 2.0 is the overarching, comprehensive framework and conceptual model enabling the development of architectures to facilitate the ability of Department of Defense (DoD) managers at all levels to make key decisions more effectively through organized information sharing across the Department, Joint Capability Areas (JCAs), Mission, Component, and Program boundaries. The DoDAF serves as one of the principal pillars supporting the DoD Chief Information Officer (CIO) in his responsibilities for development and maintenance of architectures required under the Clinger-Cohen Act. DoDAF is prescribed for the use and development of Architectural Descriptions in the Department. It also provides extensive guidance on the development of architectures supporting the adoption and execution of Net-centric services within the Department.
28.	DFARS 252.227-7014 Rights in Non-commercial Computer Software	http://farsite.hill.af.mil/reghtml/regs/far2afmcfars/fardfars/dfars/Dfars252_227.htm#P696_47162	Guidance on rights in technical data and computer software small business innovation research (SBIR) program.

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.
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).

NETWORK OPERATIONS AND INFRASTRUCTURE SOLUTIONS (COMPLIANCE)

Standard		URL	Description
34.	TIA/EIA-TSB-72, Centralized Optical Fiber Cabling Guidelines	http://www.tiaonline.org/	Must be purchased. ANSI/TIA/EIA-568-B series standard incorporates and refines the technical content of TSB67, TSB72, TSB75, TSB95 and TIA/EIA-568-A-1, A-2, A-3, A-4 and A-5.
35.	DoD Mobile Application Strategy	http://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: Department of Defense Net-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.
38.	DoDD 5205.02E, Operations Security (OPSEC) Program	http://www.dtic.mil/whs/directives/corres/pdf/520502e.pdf	Underscores the importance of OPSEC and how it is integrated as a core military capability within Information Operations (IO) that must be followed in daily application of military operations.
39.	DoDD 8000.01 Management of the Department of Defense Information Enterprise	http://www.dtic.mil/whs/directives/corres/pdf/800001p.pdf	Provides direction on creating an information advantage for DoD personnel and mission partners, and establishing and defining roles for CIOs at various levels within the Department of Defense

NETWORK OPERATIONS AND INFRASTRUCTURE SOLUTIONS (COMPLIANCE)			
Standard		**URL**	**Description**
40.	DoDD 8100.02, Use of Commercial Wireless Devices, Services, and Technologies in the DoD Global Information Grid (GIG)	http://www.dtic.mil/whs/directives/corres/pdf/810002p.pdf	Establishes policy and assigns responsibilities for the use of commercial wireless devices, services, and technologies in the DoD Global Information Grid (GIG) (DoD Directive 8100.1, "Global Information Grid (GIG) Overarching Policy," September 19, 2002). Directs the development and use of a Knowledge Management (KM) process to promote the sharing of wireless technology capabilities, vulnerabilities, and vulnerability mitigation strategies throughout the Department of Defense. Promotes joint interoperability using open standards throughout the Department of Defense for commercial wireless services, devices, and technological implementations.
41.	DoDI 1100.22 Policy and Procedures For Determining Workforce Mix	http://www.dtic.mil/whs/directives/corres/pdf/110022p.pdf	Provides manpower mix criteria and guidance for risk assessments to be used to identify and justify activities that are inherently governmental (IG); commercial (exempt from private sector performance); and commercial (subject to private sector performance).
42.	AFI 63-101/20-101, Integrated Life Cycle Management	http://static.e-publishing.af.mil/production/1/saf_aq/publication/afi63-101_20-101/afi63-101_20-101.pdf	It identifies elements of Air Force systems engineering (SE) practice and management required to provide and sustain, in a timely manner, cost-effective products and systems that are operationally safe, suitable, and effective.
43.	DoDI 3222.03, DoD Electromagnetic Environmental Effects (E3) Program	http://www.dtic.mil/whs/directives/corres/pdf/322203p.pdf	Reissue DoD Directive (DoDD) 3222.3 (Reference (a) as a DoD instruction (DoDI) in accordance with the authority in DoDD 5144.02 (Reference (b)). The mission of the DoD E3 IPT is to promote communication, coordination, commonality, and synergy among the DoD Components for E3-related matters.
44.	DoDD 5230.24, Distribution Statements on Technical Documents	http://www.dtic.mil/whs/directives/corres/pdf/523024p.pdf	This instruction updates policies and procedures for marking technical documents, including production, engineering, and logistics information, to denote the extent to which they are available for distribution, release, and dissemination without additional approvals or authorizations.

NETWORK OPERATIONS AND INFRASTRUCTURE SOLUTIONS (COMPLIANCE)			
Standard		**URL**	**Description**
45.	AFI 33-200, Air Force Cybersecurity Program Management	http://static.e-publishing.af.mil/production/1/saf_cio_a6/publication/afi33-200/afi33-200.pdf	This AFI provides general direction for implementation of IA and management of IA programs according to AFPD 33-2. Compliance ensures appropriate measures are taken to ensure the availability, integrity, and confidentiality of Air Force ISs and the information they process. Using appropriate levels of protection against threats and vulnerabilities help prevent denial of service, corruption, compromise, fraud, waste, and abuse.
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 Air Force 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.

NETWORK OPERATIONS AND INFRASTRUCTURE SOLUTIONS (COMPLIANCE)			
Standard		URL	Description
52.	Federal Information Security Management Act (FISMA) 2002	http://www.dhs.gov/federal-information-security-management-act-fisma	FISMA was enacted as part of the E-Government Act of 2002 to “provide a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support Federal operations and assets,” and also to “provide for development and maintenance of minimum controls required to protect Federal information and information systems.” FISMA requires Federal agencies to: •designate a Chief Information Officer (CIO), •delegate to the CIO authority to ensure compliance with the requirements imposed by FISMA, •implement an information security program, •report on the adequacy and effectiveness of its information security policies, procedures, and practices, •participate in annual independent evaluations of the information security program and practices, and •develop and maintain an inventory of the agency’s major information systems. FISMA requires the Director of the Office of Management and Budget (OMB) to ensure the operation of a central Federal information security incident center. FISMA makes the National Institute of Standards and Technology (NIST) responsible for “developing standards, guidelines, and associated methods and techniques” for information systems used or operated by an agency or contractor, excluding national security systems.
53.	FedRAMP Security Controls for Cloud Service Providers	http://cloud.cio.gov/document/fedramp-security-controls	The attachment at the link contains a listing for the FedRAMP low and moderate baseline security controls, along with additional guidance and requirements for Cloud Service Providers. Those controls, guidance, and requirements are key standards for NetOps vendors to meet for any Cloud-related task orders that might have issues on NetOps.

NETWORK OPERATIONS AND INFRASTRUCTURE SOLUTIONS (COMPLIANCE)			
Standard		**URL**	**Description**
54.	GiG Technical Guidance Federation GIG-F	https://gtg.csd.disa.mil/uam/login.do	The GIG Technical Guidance Federation (GTG-F) is a suite of software applications on the NIPRNet and SIPRNet (June 2012) that provides technical guidance across the Enterprise to achieve net-ready, interoperable, and supportable GIG systems. The GTG-F assists program managers, portfolio managers, engineers and others in answering two questions critical to any Information Technology (IT) or National Security Systems (NSS): (1) Where does the IT or NSS fit, as both a provider and consumer, into the GIG with regard to End-to-End technical performance, access to data and services, and interoperability; (2) What must an IT or NSS do to ensure technical interoperability with the GIG. The GTG-F content provides the technical information to various users in addressing and resolving technical issues needed to meet functional requirements (i.e., features and capabilities) of the GIG. This GTG-F content consists of and is based on GIG net-centric IT standards, associated profiles, engineering best practices and reference implementation specifications.
55.	Homeland Security Presidential Directive 12 (HSPD 12)	http://www.dhs.gov/homeland-security-presidential-directive-12	Federal law signed by George Bush that directed promulgation of a Federal standard for secure and reliable forms of identification for Federal employees and contractors. Part two provides detailed specifications that will support technical interoperability among PIV systems of Federal departments and agencies. NIST has been designated as the approval and testing authority to certify products. FIPS 201 implements this policy.
56.	ICD 503, IT Systems Security, Risk Management, Certification and Accreditation	http://www.dni.gov/files/documents/ICD/ICD_503.pdf	This Intelligence Community Directive (ICD) establishes Intelligence Community (IC) policy for information technology systems security risk management, certification and accreditation. This ICD focuses on a more holistic and strategic process for the risk management of information technology systems, and on processes and procedures designed to develop trust across the intelligence community information technology enterprise through the use of common standards and reciprocally accepted certification and accreditation decisions.

NETWORK OPERATIONS AND INFRASTRUCTURE SOLUTIONS (COMPLIANCE)			
Standard		**URL**	**Description**
57.	IEEE/EIA 12207.0 Standard for Information Technology	http://IEEE.org	IEEE/EIA 12207.0, "Standard for Information Technology – Software Life Cycle Processes", is a standard that establishes a common framework for software life cycle process. This standard officially replaced MIL-STD-498 for the development of DoD software systems in May 1998.[1] Other NATO nations may have adopted the standard informally or in parallel with MIL-STD-498.This standard defines a comprehensive set of processes that cover the entire life-cycle of a software system—from the time a concept is made to the retirement of the software. The standard defines a set of processes, which are in turn defined in terms of activities. The activities are broken down into a set of tasks. The processes are defined in three broad categories: Primary Life Cycle Processes, Supporting Life Cycle Processes, and Organizational Life Cycle Processes.
58.	AFI 33-115 Air Force Information Technology (IT) Service management	http://static.e-publishing.af.mil/production/1/saf_cio_a6/publication/afi33-115/afi33-115.pdf	This Air Force instruction (AFI) implements Air Force Policy Directive (AFPD) 33-1, Information Resources Management. It sets forth policies regarding the official or authorized use of government-provided electronic messaging systems on both Non-secure Internet Protocol Router Network (NIPRNet) and SECRET Internet Protocol Router Network (SIPRNet). It identifies the Defense Message System (DMS) as the core-messaging system of record for the Air Force. It provides the roles, standards, and guidance relating to the messaging classes used by the Air Force: organizational DMS High Grade Service (HGS), and Simple Mail Transfer Protocol (SMTP) electronic mail (E-mail) messaging. This instruction applies to all Air Force organizations, personnel, Air National Guard, Air Force Reserve Command, and contractors regardless of the information classification transmitted or received. This instruction provides guidance to differentiate between record and non-record E-mail.

NETWORK OPERATIONS AND INFRASTRUCTURE SOLUTIONS (COMPLIANCE)

Standard		URL	Description
59.	ISO/IEC 20000	http://www.iso.org/iso/home.html	ISO/IEC 20000 is an international standard for IT Service Management (ITSM). It allows IT organizations to ensure the alignment between ITSM processes and their overall organization strategy. It requires the service provider to plan, establish, implement, operate, monitor, review, maintain and improve a service management system (SMS). ISO/IEC 20000 consist of 5 separate documents, ISO/IEC 20000-1 through 20000-5
60.	ITU Recommendation H.320, Narrow-band Visual Telephone Systems and Terminal Equipment	http://www.itu.int/rec/T-REC-H.320	International Telecommunication Union recommendation that DoD requires for VTC and DISN Video Services equipment must meet. This standard sets BONDING (Bandwidth on Demand) algorithms to ensure bandwidth in proper increments. This included with FTR 1080B-2002.
61.	CJCSI 6212.01F Interoperability and Supportability of Information Technology and National Security Systems	http://www.dtic.mil/cjcs_directives/cdata/unlimit/6212_01.pdf	Establishes policies and procedures for developing, coordinating, reviewing, and approving Information Technology (IT) and National Security System (NSS) Interoperability and Supportability (I&S) needs. Establishes procedures to perform I&S Certification of Joint Capabilities Integration and Development System (JCIDS) Acquisition Category (ACAT) programs/systems. Establishes procedures to perform I&S Certification of Information Support Plans (ISPs) and Tailored ISPs (TISPs) for all ACAT, non-ACAT and fielded programs/systems. Defines the five elements of the Net-Ready Key Performance Parameter (NR-KPP). Provides guidance for NR-KPP development and assessment. Establishes procedures for the Joint Interoperability Test Command (JITC) Joint Interoperability Test Certification. Adds the requirement from Joint Requirements Oversight Council Memorandum (JROCM) 010-08, 14 January 2008, “Approval to Incorporate Data and Service Exposure Criteria into the Interoperability and Supportability Certification Process” for reporting of data and service exposure information as part of I&S submissions.

DRAFT COPY

NETWORK OPERATIONS AND INFRASTRUCTURE SOLUTIONS (COMPLIANCE)			
Standard		URL	Description
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
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.
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 Department of Defense for commercial wireless services, devices, and technological implementations.
65.	DODD 8100.1 Department of Defense Information Network (DoDIN) Overarching Policy	http://www.acq.osd.mil/ie/bei/pm/ref-library/dodd/d81001p.pdf	Establishes policy and assigns responsibilities for GIG configuration management, architecture, and the relationships with the Intelligence Community (IC) and defense intelligence components.

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

NETWORK OPERATIONS AND INFRASTRUCTURE SOLUTIONS (COMPLIANCE)

Standard		URL	Description
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).
69.	Security Technical Implementation Guides (STIGs) CJCSI 6510.01F Information Assurance (IA) AND Support To Computer Network DEFENSE (CND)	http://www.dtic.mil/cjcs_directives/cdata/unlimit/6510_01.pdf	The Security Technical Implementation Guides (STIGs) and the NSA Guides are the configuration standards for DOD IA and IA-enabled devices/systems. Since 1998, DISA Field Security Operations (FSO) has played a critical role enhancing the security posture of DoD's security systems by providing the Security Technical Implementation Guides (STIGs). The STIGs contain technical guidance to "lock down" information systems/software that might otherwise be vulnerable to a malicious computer attack. DISA FSO is in the process of moving the STIGs towards the use of the NIST Security Content Automation Protocol (S-CAP) in order to be able to “automate” compliance reporting of the STIGs.

NETWORK OPERATIONS AND INFRASTRUCTURE SOLUTIONS (COMPLIANCE)

Standard		URL	Description
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.
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.	Department of Defense Chief Information Officer Cloud Computing Strategy	http://dodcio.defense.gov/Portals/0/Documents/Cloud/DoD%20Cloud%20Computing%20Strategy%20Final%20with%20Memo%20-%20July%205%202012.pdf	This strategy is to enable the Department to increase secure information sharing and collaboration, enhance mission effectiveness, and decrease costs using cloud services.
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.

NETWORK OPERATIONS AND INFRASTRUCTURE SOLUTIONS (COMPLIANCE)

Standard		URL	Description
79.	Designation of the Defense Information Systems Agency as the Department of Defense Enterprise Cloud Service Broker	http://www.disa.mil/Services/DoD-Cloud-Broker/~/media/Files/DISA/Services/Cloud-Broker/disa-designation-memo.pdf	This memorandum establishes Defense Information Systems Agency (DISA) as the DoD Enterprise Cloud Service Broker.
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.
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 in accordance with 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 Risk Management Framework to Federal Information Systems	http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf	The purpose of this publication is to provide guidelines for applying the Risk Management Framework to federal information systems to include conducting the activities of security categorization, security control selection and implementation, security control assessment, information system authorization, and security control monitoring.
89.	Defense Information Systems Agency, the Security Technical Implementation Guide (STIG)	http://iase.disa.mil/stigs/Pages/index.aspx	The Security Technical Implementation Guides (STIGs) are the configuration standards for DoD IA and IA-enabled devices/systems. The STIGs contain technical guidance to 'lock down' information systems/software that might otherwise be vulnerable to a malicious computer attack.

NETWORK OPERATIONS AND INFRASTRUCTURE SOLUTIONS (COMPLIANCE)			
Standard		**URL**	**Description**
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 in accordance with the security requirements outlined in Federal Risk and Authorization Management Program (FedRAMP) and this Security Requirement Guide (SRG). DISA previously published the concepts for operating in the commercial cloud under the Cloud Security Model. Version 1 defined the overall framework and provided initial guidance for public data. Version 2.1 added information for Controlled Unclassified Information. This document, the Cloud Computing Security Requirements Guide, SRG, documents cloud security requirements in a construct similar to other SRGs published by DISA for the DoD. This SRG incorporates, supersedes, and rescinds the previously published Security Model.
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 Department of Defense networks to provide end-to-end Unified Capabilities (UC).
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.

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

NETWORK OPERATIONS AND INFRASTRUCTURE SOLUTIONS (COMPLIANCE)

Standard		URL	Description
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) in accordance with the authority in DoD Directive (DoDD) 5144.02
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. Department of Defense (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.	AFGM2017-32-01	http://static.e-publishing.af.mil/production/1/af_a4/publication/afgm2017-32-01/afgm2017-32-01.pdf	Guidance memorandum to establish cyber security policy for civil engineer (CE) owned or operated control systems (CS).

NETWORK OPERATIONS AND INFRASTRUCTURE SOLUTIONS (COMPLIANCE)			
Standard		URL	Description
105.	AFI 17-101	http://static.e-publishing.af.mil/production/1/saf_cio_a6/publication/afi17-101/afi17-101.pdf	Risk Management Framework (RMF) For Air Force Information Technology (IT)

Appendix 2: CONTRACTOR QUALIFICATIONS & EXPERIENCE

A. Requirements for Info Security Analyst (15-1122) (Senior IA Security Analyst)

Educational Level: Master's Degree or higher in Electrical and/or Computer Engineering, Computer Science, Information Assurance, Cyber Security, or Management of Information Systems/Technology

Years of Experience: 10 years minimum

Knowledge, Skills, and Abilities (KSAs):

Strong background with both process and network equipment used throughout Industrial Control System (CS) applications and installation techniques

Understanding of IP networking, networking protocols, and security-related technologies with respect to information assurance

Extensive knowledge of network security concepts and best practices, operating system hardening, network device hardening, and experience with network security assessments with respect to common vulnerabilities associated with CS

Participation in the DoD Information Assurance Certification and Accreditation Process (DIACAP) to include artifact generation, requirement analysis, security test and evaluation (ST&E) planning and execution, risk assessment and analysis, and development of Plans of Action and Milestones (POA&M), systems analysis and hardening strategies, incident response and policy analysis, trusted product evaluation, and IA assessments

Detailed understanding of FISMA, NIST 800 series, DoD Federal RMF and ability to articulate such guidelines, policy and processes

Authoring and maintaining security documentation such as System Security Plans, Risk Assessment, ST&E Plans, Incident Reports, Security Assessment Plan, POA&Ms, etc.

Strong background with penetration testing techniques and web application scanners and firewalls technologies

Strong knowledge of data network protocols, design and operations, TCP/IP, Ethernets, etc.

Excellent verbal and written communication skills, ability to work well in a collaborative environment, ability to apply general rules to specific problems to develop and evaluate options to implement solutions.

Certifications: IAM Level III (CISSP or equivalent or higher)

Security Requirement:

1) US Citizenship required
2) DoD government security clearance SECRET or higher

B. Requirements for Info Security Analyst (15-1122) (IA Security Analyst)

Educational Level: Bachelor's Degree or higher in Electrical and/or Computer Engineering, or Computer Science, Information Assurance, Cyber Security, or Management of Information Systems/Technology

Years of Experience: 5 years minimum

Knowledge, Skills, and Abilities (KSAs):

Familiar with both process and network equipment used throughout CS applications and installation techniques

Understanding of IP networking, networking protocols, and security-related technologies with respect to information assurance

Extensive knowledge of network security concepts and best practices, operating system hardening, network device hardening, and experience with network security assessments with respect to common vulnerabilities associated with CS

Participation in the DoD Information Assurance Certification and Accreditation Process (DIACAP) to include artifact generation, requirement analysis, security test and evaluation (ST&E) planning and execution, risk assessment and analysis, and development of Plans of Action and Milestones (POA&M), systems analysis and hardening strategies, incident response and policy analysis, trusted product evaluation, and IA assessments

Detailed understanding of FISMA, NIST 800 series, Federal RMF and ability to articulate such guidelines, policy and processes to diverse audiences

Authoring and maintaining security documentation such as System Security Plans, Risk Assessment, ST&E Plans, Incident Reports, Security Assessment Plan, POA&Ms, etc.

Familiar with penetration testing techniques and web application scanners and firewalls technologies

Strong knowledge of data network protocols, design and operations, TCP/IP, Ethernets, etc.

Excellent verbal and written communication skills, ability to work well in a collaborative environment, ability to apply general rules to specific problems to develop and evaluate options to implement solutions.

Certifications:

IAM Level III (CISSP or equivalent or higher) or IAT Level II in accordance with DoD 8570.M Table 3 is required

Security Requirement:

1). US Citizenship required
2). DoD government security clearance SECRET

C. Requirements for Computer & Info Systems Managers (11-3021) (ISSM/ISSO/AOR support/SCAR/Information Management)

Educational Level: Bachelor's Degree required as minimum, Master's Degree or higher desired in Electrical and/or Computer Engineering, Computer Science, Information Assurance, Cyber Security, or Management of Information Systems/Technology

Years of Experience: 10 years minimum

Knowledge, Skills, and Abilities (KSAs):

Strong background with both process and network equipment used throughout CS applications and installation techniques

Understanding of IP networking, networking protocols, and security-related technologies with respect to information assurance

Working knowledge of network security concepts and best practices, operating system hardening, network device hardening, and experience with network security assessments with respect to common vulnerabilities associated with CS.

Familiar with or participation in the DoD Information Assurance Certification and Accreditation Process (DIACAP) to include artifact generation, requirement analysis, security test and evaluation (ST&E) planning and execution, risk assessment and analysis, and development of Plans of Action and Milestones (POA&M), systems analysis and hardening strategies, incident response and policy analysis, trusted product evaluation, and IA assessments

Familiar with FISMA, NIST 800 series, DoD Federal RMF and ability to articulate such guidelines, policy and processes

Authoring and maintaining security documentation such as System Security Plans, Risk Assessment, ST&E Plans, Incident Reports, Security Assessment Plan, POA&Ms, etc.

Strong background with CS processes, installation, components, configuration, and acquisitions.

Knowledge of data network protocols, design and operations, TCP/IP, Ethernets, etc.

Excellent verbal and written communication skills, ability to work well in a collaborative environment, ability to apply general rules to specific problems to develop and evaluate options to implement solutions.

Certifications:

ISSM IAM Level II (CISSP within 6 months);
ISSO/Information Management IAT Level II (CompTIA Security+ within 6 months);
AOR support/SCAR IAM Level III (CISSP within 6 months) in accordance with DoD 8570.M Table 3 is required

Security Requirement:

1). US Citizenship required
2). DoD government security clearance SECRET or higher

D. Requirements for Software Developers, System SW (15-1133) (Senior Security Engineer)

Educational Level: Bachelor’s degree required as minimum, Master’s Degree or higher desired in Electrical and/or Computer Engineering, Computer Science, Information Assurance, Cyber Security, or Management of Information Systems/Technology

Years of Experience: 10 years minimum

Knowledge, Skills, and Abilities (KSAs):

Strong background with both process and network equipment used throughout CS applications and installation techniques

Understanding of IP networking, networking protocols, and security-related technologies with respect to information assurance

Working knowledge of network security concepts and best practices, operating system hardening, network device hardening, and experience with network security assessments with respect to common vulnerabilities associated with CS.

Performed comprehensive design review for new and or updated CS with regards to information assurance and cyber security requirements

Familiar with or participation in the DoD Information Assurance Certification and Accreditation Process (DIACAP) to include artifact generation, requirement analysis, security test and evaluation (ST&E) planning and execution, risk assessment and analysis, and development of Plans of Action and Milestones (POA&M), systems analysis and hardening strategies, incident response and policy analysis, trusted product evaluation, and IA assessments

Familiar with FISMA, NIST 800 series, Federal RMF and ability to articulate such guidelines, policy and processes

Authoring and maintaining security documentation such as System Security Plans, Risk Assessment, ST&E Plans, Incident Reports, Security Assessment Plan, POA&Ms, etc.

Strong background with CS processes, installation, components, configuration, and acquisitions.

Knowledge of data network protocols, design and operations, TCP/IP, Ethernets, etc.

Excellent verbal and written communication skills, ability to work well in a collaborative environment, ability to apply general rules to specific problems to develop and evaluate options to implement solutions.

Certifications: Meet requirements for IAT Level III (CISSP within 6 months) or IAM Level III in accordance with DoD 8570.M Table 3 is required

Security Requirement:

1). US Citizenship required
2) DoD government security clearance SECRET

E. Requirements for Software Developers, System SW (15-1133) (Security Engineer)

Educational Level: Associate’s Degree or higher in Electrical and/or Computer Engineering, Computer Science, Information Assurance, Cyber Security, or Management of Information Systems/Technology

Years of Experience: 5 years minimum

Knowledge, Skills, and Abilities (KSAs):

Familiar with both process and network equipment used throughout CS applications and installation techniques

Understanding of IP networking, networking protocols, and security-related technologies with respect to information assurance

Working knowledge of network security concepts and best practices, operating system hardening, network device hardening, and experience with network security assessments with respect to common vulnerabilities associated with CS. Performed comprehensive design review for new and or updated CS with regards to information assurance and cyber security requirements

Familiar with or participation in the DoD Information Assurance Certification and Accreditation Process (DIACAP) to include artifact generation, requirement analysis, security test and evaluation (ST&E) planning and execution, risk assessment and analysis, and development of Plans of Action and Milestones (POA&M), systems analysis and hardening strategies, incident response and policy analysis, trusted product evaluation, and IA assessments

Familiar with FISMA, NIST 800 series, DoD Federal RMF and ability to articulate such guidelines, policy and processes

Authoring and maintaining security documentation such as System Security Plans, Risk Assessment, ST&E Plans, Incident Reports, Security Assessment Plan, POA&Ms, etc.

Familiar with CS processes, installation, components, configuration, and acquisitions.

Knowledge of data network protocols, design and operations, TCP/IP, Ethernets, etc.

Excellent verbal and written communication skills, ability to work well in a collaborative environment, ability to apply general rules to specific problems to develop and evaluate options to implement solutions.

Certifications: Meet requirements for IAT Level II (CompTIA Security + or higher within 6 months) or IAM Level II in accordance with DoD 8570.M Table 3 is required

Security Requirement:

1) US Citizenship required
2) DoD government security clearance SECRET

F. Requirements for Computer Network Architects (15-1143) (Senior Network Engineer)

Educational Level: Bachelor's degree required as minimum, Master's Degree or higher desired in Electrical and/or Computer Engineering, Computer Science, Information Assurance, Cyber Security, or Management of Information Systems/Technology

Years of Experience: 10 years minimum

Knowledge, Skills, and Abilities (KSAs):

Strong background with both process and network equipment used throughout CS applications and installation techniques

Understanding of IP networking, networking protocols, and security-related technologies with respect to information assurance

Working knowledge of network security concepts and best practices, operating system hardening, network device hardening, and experience with network security assessments with respect to common vulnerabilities associated with CS

Familiar with or participation in the DoD Information Assurance Certification and Accreditation Process (DIACAP) to include artifact generation, requirement analysis, security test and evaluation (ST&E) planning and execution, risk assessment and analysis, and development of Plans of Action and Milestones (POA&M), systems analysis and hardening strategies, incident response and policy analysis, trusted product evaluation, and IA assessments

Familiar with FISMA, NIST 800 series, DoD Federal RMF and ability to articulate such guidelines, policy and processes

Authoring and maintaining security documentation such as System Security Plans, Risk Assessment, ST&E Plans, Incident Reports, Security Assessment Plan, POA&Ms, etc.

Familiar with CS processes, installation, components, configuration, and acquisitions.

Knowledge of data network protocols, design and operations, TCP/IP, Ethernets, etc.

Excellent verbal and written communication skills, ability to work well in a collaborative environment, ability to apply general rules to specific problems to develop and evaluate options to implement solutions.

Certifications: Meet requirements for IAT Level II (CompTIA Security + or higher within 6 months) or IAM Level I in accordance with DoD 8570.M Table 3 is required

Security Requirement:

1) US Citizenship required
2) DoD government security clearance SECRET

G. Requirements for Computer Network Support Specialists (15-1152) (IT Security Analyst)

Educational Level: Associate’s degree or higher desired in Electrical and/or Computer Engineering, Computer Science, Information Assurance, Cyber Security, or Management of Information Systems/Technology

Years of Experience: 5 years minimum

Knowledge, Skills, and Abilities (KSAs):

Familiar with both process and network equipment used throughout CS applications and installation techniques

Understanding of IP networking, networking protocols, and security-related technologies with respect to information assurance

Working knowledge of network security concepts and best practices, operating system hardening, network device hardening, and experience with network security assessments with respect to common vulnerabilities associated with CS. Performed comprehensive design review for new and or updated CS with regards to information assurance and cyber security requirements

Familiar with or participation in the DoD Information Assurance Certification and Accreditation Process (DIACAP) to include artifact generation, requirement analysis, security test and evaluation (ST&E) planning and execution, risk assessment and analysis, and development of Plans of Action and Milestones (POA&M), systems analysis and hardening strategies, incident response and policy analysis, trusted product evaluation, and IA assessments

Familiar with FISMA, NIST 800 series, DoD Federal RMF and ability to articulate such guidelines, policy and processes

Authoring and maintaining security documentation such as System Security Plans, Risk Assessment, ST&E Plans, Incident Reports, Security Assessment Plan, POA&Ms, etc.

Familiar with CS processes, installation, components, configuration, and acquisitions.

Knowledge of data network protocols, design and operations, TCP/IP, Ethernets, etc.

Excellent verbal and written communication skills, ability to work well in a collaborative environment, ability to apply general rules to specific problems to develop and evaluate options to implement solutions.

Certifications:

Meet requirements for IAT Level II (CompTIA Security + or higher within 6 months) or IAM Level I in accordance with DoD 8570.M Table 3 is required

Security Requirement:

1) US Citizenship required
2) DoD government security clearance SECRET

H. Requirements for Computer Systems Analyst (IT Security Analyst)

Educational Level: Bachelor’s degree or higher desired in Electrical and/or Computer Engineering, Computer Science, Information Assurance, Cyber Security, or Management of Information Systems/Technology

Years of Experience: 5 years minimum

Knowledge, Skills, and Abilities (KSAs):

Familiar with both process and network equipment used throughout CS applications and installation techniques

Understanding of IP networking, networking protocols, and security-related technologies with respect to information assurance

Working knowledge of network security concepts and best practices, operating system hardening, network device hardening, and experience with network security assessments with respect to common vulnerabilities associated with CS. Performed comprehensive design review for new and or updated CS with regards to information assurance and cyber security requirements.

Familiar with or participation in the DoD Information Assurance Certification and Accreditation Process (DIACAP) to include artifact generation, requirement analysis, security test and evaluation (ST&E) planning and execution, risk assessment and analysis, and development of Plans of Action and Milestones (POA&M), systems analysis and hardening strategies, incident response and policy analysis, trusted product evaluation, and IA assessments

Familiar with FISMA, NIST 800 series, DoD Federal RMF and ability to articulate such guidelines, policy and processes

Authoring and maintaining security documentation such as System Security Plans, Risk Assessment, ST&E Plans, Incident Reports, Security Assessment Plan, POA&Ms, etc.

Familiar with CS processes, installation, components, configuration, and acquisitions.

Knowledge of data network protocols, design and operations, TCP/IP, Ethernets, etc.

Excellent verbal and written communication skills, ability to work well in a collaborative environment, ability to apply general rules to specific problems to develop and evaluate options to implement solutions.

Certifications:

Meet requirements for IAT Level II (CompTIA Security + or higher within 6 months) or IAM Level I in accordance with DoD 8570.M Table 3 is required

Security Requirement:

1) US Citizenship required
2) DoD government security clearance SECRET

I. Requirements for Network & Computer System Admin (System Administrator)

Educational Level: Bachelor's degree or higher desired in Electrical and/or Computer Engineering, Computer Science, Information Assurance, Cyber Security, or Management of Information Systems/Technology

Years of Experience: 5 years minimum

Knowledge, Skills, and Abilities (KSAs):

Familiar with both process and network equipment used throughout CS applications and installation techniques

Understanding of IP networking, networking protocols, and security-related technologies with respect to information assurance

Working knowledge of network security concepts and best practices, operating system hardening, network device hardening, and experience with network security assessments with respect to common vulnerabilities associated with CS, plan, coordinate, and implement security measure to protect data, software, and hardware

Familiar with or participation in the DoD Information Assurance Certification and Accreditation Process (DIACAP) to include artifact generation, requirement analysis, security test and evaluation (ST&E) planning and execution, risk assessment and analysis, and development of Plans of Action and Milestones (POA&M), systems analysis and hardening strategies, incident response and policy analysis, trusted product evaluation, and IA assessments

Familiar with FISMA, NIST 800 series, DoD Federal RMF and ability to articulate such guidelines, policy and processes

Authoring and maintaining security documentation such as System Security Plans, Risk Assessment, ST&E Plans, Incident Reports, Security Assessment Plan, POA&Ms, etc.

Familiar with CS processes, installation, components, configuration, and acquisitions.

Knowledge of data network protocols, design and operations, TCP/IP, Ethernets, etc., electronic equipment, computer hardware and software, including applications and programming.

Excellent verbal and written communication skills, ability to work well in a collaborative environment, ability to apply general rules to specific problems to develop and evaluate options to implement solutions.

Certifications: Meet requirements for IAT Level II (CompTIA Security + or higher within 6 months) or IAM Level I in accordance with DoD 8570.M Table 3 is required

Security Requirement:

1) US Citizenship required
2) DoD government security clearance SECRET

Appendix 3: Historical Data

	Off - Site Position	**Description**	**DoD 8570 Level**
PM	VP of Engineering	OFFSITE PROJECT MANAGER	N/A
	Mission Area 2 Position Title	**Mission Area 2 Task**	**8570 Compliance**
1	Sr Security Engineer / Site Lead	VALIDATION	CISSP
2	Sr Security Engineer	VALIDATION	Sec+
3	Sr Security Engineer	MITIGATION TEAM	CASP
4	Sr Security Engineer	RISK ASSESSMENT	Sec+
5	Sr IA Security Analyst	VALIDATION	CISA
6	Security Engineer	VALIDATION	Sec+
7	Security Engineer	RISK ASSESSMENT	Sec+
8	Security Engineer	ISSO	Sec+
9	IA Analyst	RISK ASSESSMENT	Sec+
10	IA Analyst	RISK ASSESSMENT	Sec+
11	IA Analyst	VALIDATION	Sec+
12	Sr IA Security Analyst	VALIDATION	Sec+
13	Security Engineer	RISK ASSESSMENT	Sec+
14	Sr Security Engineer	VALIDATION	Sec+
15	IT Systems Engineer	MITIGATION TEAM	Sec+
16	IT Systems Engineer	MITIGATION TEAM	Sec+
17	IT Systems Engineer	MITIGATION TEAM	Sec+
	Mission Areas 1,3,4,5 Position Title	**Mission Area 1,3,4,5: Task**	**8570 Compliance**
18	Sr. Technical Communicator	Briefings, ETLs, UFCs, JWGs, etc.	Sec+
19	IT Specialist	HELP DESK / SYSTEMS INTEGRATION	Sec+
20	IT Specialist	HELP DESK / SYSTEMS INTEGRATION	GSEC
21	IT Specialist	HELP DESK / SYSTEMS INTEGRATION	CISSP
22	IT Specialist	HELP DESK / SYSTEMS INTEGRATION	Sec+
23	IAM/ISSM	ISSM	CISSP

24	IT Specialist	HELP DESK / SYSTEMS INTEGRATION	Sec+
25	IT Specialist	HELP DESK / SYSTEMS INTEGRATION	Sec+
26	IT Specialist	HELP DESK / SYSTEMS INTEGRATION	Sec+
27	IT Specialist	HELP DESK / SYSTEMS INTEGRATION	Sec+
28	IT Specialist	HELP DESK / SYSTEMS INTEGRATION	Sec+
29	IT Specialist	HELP DESK / SYSTEMS INTEGRATION	CISSP
30	Network Engineer	HELP DESK / SYSTEMS INTEGRATION	Sec+
31	Network Engineer	HELP DESK / SYSTEMS INTEGRATION	Sec+

	Mission Area 6 Position Title	**Mission Area Task**	**8570 Compliance**
Mission Area 6 is a new requirement. No historical data.			

Appendix 4: Mission Area Performance Requirements (Workload Estimates)

Appendix 4

Mission Area Performance Requirements (Workload Estimates)

Mission Area 1 : CYBER THREAT & SITUATIONAL AWARENESS

PERFORMANCE REQUIRMENTS (Workload Estimates)

Program	Task	Description	Workload Estimate
MA-1.1	Analyze Cyber Threats	Analyze CS cyber threats using available Department of Homeland Security (DHS) tools and information portals (e.g. Cyber Security Evaluation Tool (CSET), CS Computer Emergency Response Team (CERT) advisories, etc.), Common Criteria (ISO/IEC 15408), NIST SP 800-53 Rev 4, NIST SP 800-82, and CNSS 1253 CS Overlay Document. Provide reports detailing possible impacts to Civil Engineering (CE) control systems (CS) (CDRL A001).	Anticipated workload is up to 60 CS CERTs monthly.

MA-1.2	Cyber Threat Briefings	Participate in up to five (5) routine military cyber threat briefings up to SECRET level and up to five (5) commercial ethical hacker conventions or similar IT/automation conferences by IT or CS/SCADA vendors as designated or recommended and approved by the government; and, convey such information to AFCEC personnel with appropriate security clearance for consideration and incorporation into legacy CS/SCADA systems and CS Cyber Security enterprise network security.	Anticipated workload is attendance at up to 5 routine military cyber threat briefings and 5 conventions or conferences annually.
MA-1.3	Training Presentations	Develop briefings explaining the RMF security control decision process to the CE Security Controls Assessor and Authorizing Official	Anticipated workload is 2 briefings annually.
Mission Area 2 : ASSESSMENT & AUTHORIZATION (A&A)			
PERFORMANCE REQUIRMENTS (Workload Estimates)			
Program	**Task**	**Description**	**Workload Estimate**
MA-2.1	Risk Assessment Report Review	Conduct up to 10 CS Cyber Security Risk Assessments Reports (RAR) (aka Security Assessment Reports) per year	Up to 10 CS Cyber Security Risk Assessments Reports (RAR) (aka Security Assessment Reports) per year

MA-2.2	Risk Assessment Report Review	Provide assessment of IA scan findings and test results for each CS self-assessment completed	Review and assess 20 self-assessments per month
MA-2.3	CS Design Review	Provide technical support for all aspects of secure design of CS for new or updated CS projects including CS Cyber Security design reviews. See Appendix 4 Note (a)	Up to 4 design reviews per month
MA-2.4	A&A Workflow and Approval Notification	Complete and monitor each CS A&A Package (CDRL A001) received from base ISSO/ISSM throughout approval process;	Up to 30 package validation per month
MA-2.5	A&A Workflow and Approval Notification	Maintain monthly AFCEC/COMI Program Management Review (PMR) data submission elements (CDRL A002)	1 monthly PMR submission
MA-2.6	Information Assurance Management	Perform Authorizing Official Designated Representative (AODR) functions in support of the CE Authorizing Official.	Anticipate 1980 man hours annually
MA-2.7	Information Assurance Management	Perform Security Controls Assessor Representative (SCAR) functions in support of the CE Security Controls Assessor	Anticipate 1980 man hours annually

Mission Area 3 : HARDWARE AND SOFTWARE MANAGEMENT

PERFORMANCE REQUIRMENTS (Workload Estimates)

Program	Task	Description	Workload Estimate
MA-3.1	System Integration	Perform software programming for up to 50 legacy or new CS/SCADA integration into the enterprise CS Cyber Security network enclave annually	Up to 50 integrations or deployments of the AFCEC type accredited enterprise systems
MA-3.2	ITIR/ITCR Process	Review up to 25 Platform IT Information Technology Investment Requests (ITIRs) or Information Technology Capability Requests (ITCRs) per year and make recommendations	Up to 25 ITIRs or ITCRs
MA-3.3	Research, Design, Test and Evaluation (RDT&E) Lab Support	Operate and sustain, at Tyndall AFB under the direction of AFCEC/COMI, the accredited CS Integration Network; to include specifying all required IT equipment and network support for establishing a CE VLAN (or later version) developmental/ operational test (DT/OT) environment in coordination local 325 Communications Squadron	Up to 160 man hours annually

MA-3.4	Help Desk Support	Provide IT and IA help desk support of deployed systems.	Up to 40 support requests of varying complexity per month
MA-3.5	Standards and Criteria Publications	Support CS Subject Matter Expert (SME) with standards and criteria development of CS Cyber Security enterprise deployment and sustainment, commissioning/de-commissioning, and configuration management to facilitate type-accreditation and enterprise operations of USAF CS.	Anticipated publication of at least 3 comprehensive technical documents annually.
MA-3.6	Standards and Criteria Publications	Support AFCEC with standards and criteria development of CS Cyber Security IA Control Overlays in accordance with DoD CNSS 1253 CS Overlay Document.	Anticipate up to 160 man hours annually
MA-3.7	Information Assurance Management	Perform DIACAP Information Assurance Manager (IAM) and RMF Information System Security Manager (ISSM) functions for 4 type accredited AFCEC programs (AMRS, ICEE, CE VLAN, and CE COINE) and for the AFCEC Integration Network.	Anticipate 3960 man hours annually

MA-3.8	POA&M Finding Mitigations	Assist bases with POA&M finding mitigations by interfacing with CS vendors, base personnel and others as necessary. Develop plan and acquire funding estimates to mitigate all POA&M entries and present to Government	Anticipate working with 10 bases simultaneously; 10,000 man hours annually
MA-3.9	CE Enclave Design and Implementation	Revise design of the CE network enclave to accommodate critical infrastructure and meet current type accreditation specs. See Appendix 4 Note (b)	Anticipate 3960 man hours annually

Mission Area 4 : NETWORK DEFENSE

PERFORMANCE REQUIRMENTS (Workload Estimates)

Program	Task	Description	Workload Estimate
MA-4.1	Enterprise Network Health Reporting	Analyze, compile and report monthly on the CS Cyber Security enterprise network performance and susceptibility indicators (i.e. potential cyber threats) using government and/or industry best practices (e.g. Verizon Data Breech Report, etc.) or as directed by AFCEC, in conjunction with AFCYBER	One report monthly

MA-4.2	Continuous Network Monitoring	Perform continuous monitoring of the enterprise CS Cyber Security network enclave (CE VLAN v1.0 or later) to the greatest extent possible and develop network mitigation strategies (i.e. fixes or workarounds) for the CS Cyber Security network performance and susceptibility deficiencies in conjunction with AFCYBER and AFCEC	Anticipate up to 1000 man hours annually
MA-4.3	Network Intrusion Detection	Identify network intrusions and quarantine such intrusions	Anticipate up to 800 man hours annually

Mission Area 5 : INCIDENT MANAGEMENT

PERFORMANCE REQUIRMENTS (Workload Estimates)

Program	**Task**	**Description**	**Workload Estimate**
MA-5.1	Forensic Analysis	Provide as needed remote or on-site, as directed by AFCEC, forensic analysis and incident report of CS Cyber Security incidents (e.g. network intrusion or breech, data compromise/loss, etc.) in accordance with DOD/AF policy and guidance	Anticipate up to 400 man hours annually

MA-5.2	Forensic Analysis	Develop forensic criteria and incident handling and reporting procedures between the AFCEC and AFCYBER, specifically 33 Network Warfare Squadron (AFCERT)	Anticipate up to 200 man hours annually
MA-5.3	Continuity of Operations Plan (COOP)/Disaster Recovery Plan (DRP)	Develop a single comprehensive standardized template for BCE CS Cyber Security COOP/DRP	Anticipate up to 80 man hours annually
Mission Area 6 : RISK MANAGEMENT FRAMEWORK (RMF) WORKFORCE			
PERFORMANCE REQUIRMENTS (Workload Estimates)			
Program	**Task**	**Description**	**Workload Estimate**
MA-6	Information Systems Security Operations	Perform RMF Information System Security Manager (ISSM) and continuous monitoring functions at the following installations (see Appendix 4 Note (c):	
MA-6.1	1	Altus Air Force Base	Anticipate 1980 man hours annually
MA-6.2	2	Arnold Air Force Base	Anticipate 1980 man hours annually
MA-6.3	3	Aviano Air Base	Anticipate 1980 man hours annually
MA-6.4	4	Avon Park Range	Anticipate 1980 man hours annually
MA-6.5	5	Barksdale Air Force Base	Anticipate 1980 man hours annually
MA-6.6	6	Beale Air Force Base	Anticipate 1980 man hours annually
MA-6.7	7	Buckley Air Force Base	Anticipate 1980 man hours annually

MA-6.8	8	Cannon Air Force Base	Anticipate 1980 man hours annually
MA-6.9	9	Cape Canaveral AFS	Anticipate 1980 man hours annually
MA-6.10	10	Cape Cod AFS	Anticipate 1980 man hours annually
MA-6.11	11	Cavalier Air Force Station	Anticipate 1980 man hours annually
MA-6.12	12	Cheyenne Air Force Station	Anticipate 1980 man hours annually
MA-6.13	13	Clear Air Force Station	Anticipate 1980 man hours annually
MA-6.14	14	Columbus Air Force Base	Anticipate 1980 man hours annually
MA-6.15	15	Creech Air Force Base	Anticipate 1980 man hours annually
MA-6.16	16	Davis–Monthan Air Force Base	Anticipate 1980 man hours annually
MA-6.17	17	Dover Air Force Base	Anticipate 1980 man hours annually
MA-6.18	18	Duke Field	Anticipate 1980 man hours annually
MA-6.19	19	Dyess Air Force Base	Anticipate 1980 man hours annually
MA-6.20	20	Eareckson Air Station	Anticipate 1980 man hours annually
MA-6.21	21	Edwards Air Force Base	Anticipate 1980 man hours annually
MA-6.22	22	Eglin Air Force Base	Anticipate 1980 man hours annually
MA-6.23	23	Eielson Air Force Base	Anticipate 1980 man hours annually
MA-6.24	24	Ellsworth Air Force Base	Anticipate 1980 man hours annually
MA-6.25	25	Fairchild Air Force Base	Anticipate 1980 man hours annually
MA-6.26	26	Francis E. Warren Air Force Base	Anticipate 1980 man hours annually
MA-6.27	27	Goodfellow Air Force Base	Anticipate 1980 man hours annually
MA-6.28	28	Grand Forks Air Force Base	Anticipate 1980 man hours annually
MA-6.29	29	Hanscom Air Force Base	Anticipate 1980 man hours annually

MA-6.30	30	Hill Air Force Base	Anticipate 1980 man hours annually
MA-6.31	31	Holloman Air Force Base	Anticipate 1980 man hours annually
MA-6.32	32	Hurlburt Field	Anticipate 1980 man hours annually
MA-6.33	33	Incirlik AB	Anticipate 1980 man hours annually
MA-6.34	34	JB Cape Cod	Anticipate 1980 man hours annually
MA-6.35	35	Joint Base Andrews	Anticipate 1980 man hours annually
MA-6.36	36	Joint Base Charleston	Anticipate 1980 man hours annually
MA-6.37	37	Joint Base Elmendorf-Richardson	Anticipate 1980 man hours annually
MA-6.38	38	Joint Base Fort Dix	Anticipate 1980 man hours annually
MA-6.39	39	Joint Base Lackland Air Force Base	Anticipate 1980 man hours annually
MA-6.40	40	Joint Base Langley–Eustis	Anticipate 1980 man hours annually
MA-6.41	41	Joint Base Lewis-McChord	Anticipate 1980 man hours annually
MA-6.42	42	Joint Base McGuire Air Force Base	Anticipate 1980 man hours annually
MA-6.43	43	Joint Base Pearl Harbor-Hickam	Anticipate 1980 man hours annually
MA-6.44	44	Joint BaseRandolph Air Force Base	Anticipate 1980 man hours annually
MA-6.45	45	Kadena Air Base	Anticipate 1980 man hours annually
MA-6.46	46	Keesler Air Force Base	Anticipate 1980 man hours annually
MA-6.47	47	Kirtland Air Force Base	Anticipate 1980 man hours annually
MA-6.48	48	Kunsan Air Base	Anticipate 1980 man hours annually
MA-6.49	49	Laughlin Air Force Base	Anticipate 1980 man hours annually
MA-6.50	50	Little Rock Air Force Base	Anticipate 1980 man hours annually
MA-6.51	51	Los Angeles Air Force Base	Anticipate 1980 man hours annually

MA-6.52	52	Luke Air Force Base	Anticipate 1980 man hours annually
MA-6.53	53	MacDill Air Force Base	Anticipate 1980 man hours annually
MA-6.54	54	Malmstrom Air Force Base	Anticipate 1980 man hours annually
MA-6.55	55	Maui AFRL	Anticipate 1980 man hours annually
MA-6.56	56	Maxwell Air Force Base	Anticipate 1980 man hours annually
MA-6.57	57	McConnell Air Force Base	Anticipate 1980 man hours annually
MA-6.58	58	Minot Air Force Base	Anticipate 1980 man hours annually
MA-6.59	59	Misawa Air Base	Anticipate 1980 man hours annually
MA-6.60	60	Moody Air Force Base	Anticipate 1980 man hours annually
MA-6.61	61	Morón Air Base	Anticipate 1980 man hours annually
MA-6.62	62	Mountain Home Air Force Base	Anticipate 1980 man hours annually
MA-6.63	63	Nellis Air Force Base	Anticipate 1980 man hours annually
MA-6.64	64	New Boston AFS	Anticipate 1980 man hours annually
MA-6.65	65	Offutt Air Force Base	Anticipate 1980 man hours annually
MA-6.66	66	Osan Air Base	Anticipate 1980 man hours annually
MA-6.67	67	Patrick Air Force Base	Anticipate 1980 man hours annually
MA-6.68	68	Peterson Air Force Base	Anticipate 1980 man hours annually
MA-6.69	69	RAF Lakenheath	Anticipate 1980 man hours annually
MA-6.70	70	RAF Mildenhall	Anticipate 1980 man hours annually
MA-6.71	71	Ramstein Air Base	Anticipate 1980 man hours annually
MA-6.72	72	Robins Air Force Base	Anticipate 1980 man hours annually
MA-6.73	73	Schriever Air Force Base	Anticipate 1980 man hours annually

MA-6.74	74	Scott Air Force Base	Anticipate 1980 man hours annually
MA-6.75	75	Seymour Johnson Air Force Base	Anticipate 1980 man hours annually
MA-6.76	76	Shaw Air Force Base	Anticipate 1980 man hours annually
MA-6.77	77	Sheppard Air Force Base	Anticipate 1980 man hours annually
MA-6.78	78	Spangdahlem Air Base	Anticipate 1980 man hours annually
MA-6.79	79	Thule Air Base	Anticipate 1980 man hours annually
MA-6.80	80	Tinker Air Force Base	Anticipate 1980 man hours annually
MA-6.81	81	Travis Air Force Base	Anticipate 1980 man hours annually
MA-6.82	82	Tyndall Air Force Base	Anticipate 1980 man hours annually
MA-6.83	83	United States Air Force Academy	Anticipate 1980 man hours annually
MA-6.84	84	Vance Air Force Base	Anticipate 1980 man hours annually
MA-6.85	85	Vandenberg Air Force Base	Anticipate 1980 man hours annually
MA-6.86	86	Whiteman Air Force Base	Anticipate 1980 man hours annually
MA-6.87	87	Wright-Patterson Air Force Base	Anticipate 1980 man hours annually
MA-6.88	88	Yokota Air Base	Anticipate 1980 man hours annually
MA-6	Information Systems Security Operations	Perform RMF Information System Security Officer (ISSO) and continuous monitoring functions at the following installations (see Appendix 4 Note (c):	
MA-6.101	1	Altus Air Force Base	Anticipate up to 1980 man hours annually
MA-6.102	2	Arnold Air Force Base	Anticipate up to 1980 man hours annually

MA-6.103	3	Aviano Air Base	Anticipate up to 1980 man hours annually
MA-6.104	4	Avon Park Range	Anticipate up to 1980 man hours annually
MA-6.105	5	Barksdale Air Force Base	Anticipate up to 1980 man hours annually
MA-6.106	6	Beale Air Force Base	Anticipate up to 1980 man hours annually
MA-6.107	7	Buckley Air Force Base	Anticipate up to 1980 man hours annually
MA-6.108	8	Cannon Air Force Base	Anticipate up to 1980 man hours annually
MA-6.109	9	Cape Canaveral AFS	Anticipate up to 1980 man hours annually
MA-6.110	10	Cape Cod AFS	Anticipate up to 1980 man hours annually
MA-6.111	11	Cavalier Air Force Station	Anticipate up to 1980 man hours annually
MA-6.112	12	Cheyenne Air Force Station	Anticipate up to 1980 man hours annually
MA-6.113	13	Clear Air Force Station	Anticipate up to 1980 man hours annually
MA-6.114	14	Columbus Air Force Base	Anticipate up to 1980 man hours annually
MA-6.115	15	Creech Air Force Base	Anticipate up to 1980 man hours annually
MA-6.116	16	Davis–Monthan Air Force Base	Anticipate up to 1980 man hours annually
MA-6.117	17	Dover Air Force Base	Anticipate up to 1980 man hours annually
MA-6.118	18	Duke Field	Anticipate up to 1980 man hours annually
MA-6.119	19	Dyess Air Force Base	Anticipate up to 1980 man hours annually
MA-6.120	20	Eareckson Air Station	Anticipate up to 1980 man hours annually
MA-6.121	21	Edwards Air Force Base	Anticipate up to 1980 man hours annually
MA-6.122	22	Eglin Air Force Base	Anticipate up to 1980 man hours annually
MA-6.123	23	Eielson Air Force Base	Anticipate up to 1980 man hours annually
MA-6.124	24	Ellsworth Air Force Base	Anticipate up to 1980 man hours annually

MA-6.125	25	Fairchild Air Force Base	Anticipate up to 1980 man hours annually
MA-6.126	26	Francis E. Warren Air Force Base	Anticipate up to 1980 man hours annually
MA-6.127	27	Goodfellow Air Force Base	Anticipate up to 1980 man hours annually
MA-6.128	28	Grand Forks Air Force Base	Anticipate up to 1980 man hours annually
MA-6.129	29	Hanscom Air Force Base	Anticipate up to 1980 man hours annually
MA-6.130	30	Hill Air Force Base	Anticipate up to 1980 man hours annually
MA-6.131	31	Holloman Air Force Base	Anticipate up to 1980 man hours annually
MA-6.132	32	Hurlburt Field	Anticipate up to 1980 man hours annually
MA-6.133	33	Incirlik AB	Anticipate up to 1980 man hours annually
MA-6.134	34	Joint Base Cape Cod	Anticipate up to 1980 man hours annually
MA-6.135	35	Joint Base Andrews	Anticipate up to 1980 man hours annually
MA-6.136	36	Joint Base Charleston	Anticipate up to 1980 man hours annually
MA-6.137	37	Joint Base Elmendorf-Richardson	Anticipate up to 1980 man hours annually
MA-6.138	38	Joint Base Fort Dix	Anticipate up to 1980 man hours annually
MA-6.139	39	Joint Base Lackland Air Force Base	Anticipate up to 1980 man hours annually
MA-6.140	40	Joint Base Langley–Eustis	Anticipate up to 1980 man hours annually
MA-6.141	41	Joint Base Lewis-McChord	Anticipate up to 1980 man hours annually
MA-6.142	42	Joint Base McGuire Air Force Base	Anticipate up to 1980 man hours annually
MA-6.143	43	Joint Base Pearl Harbor-Hickam	Anticipate up to 1980 man hours annually
MA-6.144	44	Joint BaseRandolph Air Force Base	Anticipate up to 1980 man hours annually
MA-6.145	45	Kadena Air Base	Anticipate up to 1980 man hours annually
MA-6.146	46	Keesler Air Force Base	Anticipate up to 1980 man hours annually

MA-6.147	47	Kirtland Air Force Base	Anticipate up to 1980 man hours annually
MA-6.148	48	Kunsan Air Base	Anticipate up to 1980 man hours annually
MA-6.149	49	Laughlin Air Force Base	Anticipate up to 1980 man hours annually
MA-6.150	50	Little Rock Air Force Base	Anticipate up to 1980 man hours annually
MA-6.151	51	Los Angeles Air Force Base	Anticipate up to 1980 man hours annually
MA-6.152	52	Luke Air Force Base	Anticipate up to 1980 man hours annually
MA-6.153	53	MacDill Air Force Base	Anticipate up to 1980 man hours annually
MA-6.154	54	Malmstrom Air Force Base	Anticipate up to 1980 man hours annually
MA-6.155	55	Maui AFRL	Anticipate up to 1980 man hours annually
MA-6.156	56	Maxwell Air Force Base	Anticipate up to 1980 man hours annually
MA-6.157	57	McConnell Air Force Base	Anticipate up to 1980 man hours annually
MA-6.158	58	Minot Air Force Base	Anticipate up to 1980 man hours annually
MA-6.159	59	Misawa Air Base	Anticipate up to 1980 man hours annually
MA-6.160	60	Moody Air Force Base	Anticipate up to 1980 man hours annually
MA-6.161	61	Morón Air Base	Anticipate up to 1980 man hours annually
MA-6.162	62	Mountain Home Air Force Base	Anticipate up to 1980 man hours annually
MA-6.163	63	Nellis Air Force Base	Anticipate up to 1980 man hours annually
MA-6.164	64	New Boston AFS	Anticipate up to 1980 man hours annually
MA-6.165	65	Offutt Air Force Base	Anticipate up to 1980 man hours annually
MA-6.166	66	Osan Air Base	Anticipate up to 1980 man hours annually
MA-6.167	67	Patrick Air Force Base	Anticipate up to 1980 man hours annually
MA-6.168	68	Peterson Air Force Base	Anticipate up to 1980 man hours annually

MA-6.169	69	RAF Lakenheath	Anticipate up to 1980 man hours annually
MA-6.170	70	RAF Mildenhall	Anticipate up to 1980 man hours annually
MA-6.171	71	Ramstein Air Base	Anticipate up to 1980 man hours annually
MA-6.172	72	Robins Air Force Base	Anticipate up to 1980 man hours annually
MA-6.173	73	Schriever Air Force Base	Anticipate up to 1980 man hours annually
MA-6.174	74	Scott Air Force Base	Anticipate up to 1980 man hours annually
MA-6.175	75	Seymour Johnson Air Force Base	Anticipate up to 1980 man hours annually
MA-6.176	76	Shaw Air Force Base	Anticipate up to 1980 man hours annually
MA-6.177	77	Sheppard Air Force Base	Anticipate up to 1980 man hours annually
MA-6.178	78	Spangdahlem Air Base	Anticipate up to 1980 man hours annually
MA-6.179	79	Thule Air Base	Anticipate up to 1980 man hours annually
MA-6.180	80	Tinker Air Force Base	Anticipate up to 1980 man hours annually
MA-6.181	81	Travis Air Force Base	Anticipate up to 1980 man hours annually
MA-6.182	82	Tyndall Air Force Base	Anticipate up to 1980 man hours annually
MA-6.183	83	United States Air Force Academy	Anticipate up to 1980 man hours annually
MA-6.184	84	Vance Air Force Base	Anticipate up to 1980 man hours annually
MA-6.185	85	Vandenberg Air Force Base	Anticipate up to 1980 man hours annually
MA-6.186	86	Whiteman Air Force Base	Anticipate up to 1980 man hours annually
MA-6.187	87	Wright-Patterson Air Force Base	Anticipate up to 1980 man hours annually
MA-6.188	88	Yokota Air Base	Anticipate up to 1980 man hours annually

MA-6	Information Systems Security Operations	Perform RMF User Representative (UR) / Systems Administration and continuous monitoring functions at the following installations (see Appendix 4 Note (c):	
MA-6.201	1	Altus Air Force Base	Anticipate up to 1980 man hours annually
MA-6.202	2	Arnold Air Force Base	Anticipate up to 1980 man hours annually
MA-6.203	3	Aviano Air Base	Anticipate up to 1980 man hours annually
MA-6.204	4	Avon Park Range	Anticipate up to 1980 man hours annually
MA-6.205	5	Barksdale Air Force Base	Anticipate up to 1980 man hours annually
MA-6.206	6	Beale Air Force Base	Anticipate up to 1980 man hours annually
MA-6.207	7	Buckley Air Force Base	Anticipate up to 1980 man hours annually
MA-6.208	8	Cannon Air Force Base	Anticipate up to 1980 man hours annually
MA-6.209	9	Cape Canaveral AFS	Anticipate up to 1980 man hours annually
MA-6.210	10	Cape Cod AFS	Anticipate up to 1980 man hours annually
MA-6.211	11	Cavalier Air Force Station	Anticipate up to 1980 man hours annually
MA-6.212	12	Cheyenne Air Force Station	Anticipate up to 1980 man hours annually
MA-6.213	13	Clear Air Force Station	Anticipate up to 1980 man hours annually
MA-6.214	14	Columbus Air Force Base	Anticipate up to 1980 man hours annually
MA-6.215	15	Creech Air Force Base	Anticipate up to 1980 man hours annually
MA-6.216	16	Davis–Monthan Air Force Base	Anticipate up to 1980 man hours annually
MA-6.217	17	Dover Air Force Base	Anticipate up to 1980 man hours annually

MA-6.218	18	Duke Field	Anticipate up to 1980 man hours annually
MA-6.219	19	Dyess Air Force Base	Anticipate up to 1980 man hours annually
MA-6.220	20	Eareckson Air Station	Anticipate up to 1980 man hours annually
MA-6.221	21	Edwards Air Force Base	Anticipate up to 1980 man hours annually
MA-6.222	22	Eglin Air Force Base	Anticipate up to 1980 man hours annually
MA-6.223	23	Eielson Air Force Base	Anticipate up to 1980 man hours annually
MA-6.224	24	Ellsworth Air Force Base	Anticipate up to 1980 man hours annually
MA-6.225	25	Fairchild Air Force Base	Anticipate up to 1980 man hours annually
MA-6.226	26	Francis E. Warren Air Force Base	Anticipate up to 1980 man hours annually
MA-6.227	27	Goodfellow Air Force Base	Anticipate up to 1980 man hours annually
MA-6.228	28	Grand Forks Air Force Base	Anticipate up to 1980 man hours annually
MA-6.229	29	Hanscom Air Force Base	Anticipate up to 1980 man hours annually
MA-6.230	30	Hill Air Force Base	Anticipate up to 1980 man hours annually
MA-6.231	31	Holloman Air Force Base	Anticipate up to 1980 man hours annually
MA-6.232	32	Hurlburt Field	Anticipate up to 1980 man hours annually
MA-6.233	33	Incirlik AB	Anticipate up to 1980 man hours annually
MA-6.234	34	Joint Base Cape Cod	Anticipate up to 1980 man hours annually
MA-6.235	35	Joint Base Andrews	Anticipate up to 1980 man hours annually
MA-6.236	36	Joint Base Charleston	Anticipate up to 1980 man hours annually
MA-6.237	37	Joint Base Elmendorf-Richardson	Anticipate up to 1980 man hours annually
MA-6.238	38	Joint Base Fort Dix	Anticipate up to 1980 man hours annually
MA-6.239	39	Joint Base Lackland Air Force Base	Anticipate up to 1980 man hours annually

MA-6.240	40	Joint Base Langley–Eustis	Anticipate up to 1980 man hours annually
MA-6.241	41	Joint Base Lewis-McChord	Anticipate up to 1980 man hours annually
MA-6.242	42	Joint Base McGuire Air Force Base	Anticipate up to 1980 man hours annually
MA-6.243	43	Joint Base Pearl Harbor-Hickam	Anticipate up to 1980 man hours annually
MA-6.244	44	Joint BaseRandolph Air Force Base	Anticipate up to 1980 man hours annually
MA-6.245	45	Kadena Air Base	Anticipate up to 1980 man hours annually
MA-6.246	46	Keesler Air Force Base	Anticipate up to 1980 man hours annually
MA-6.247	47	Kirtland Air Force Base	Anticipate up to 1980 man hours annually
MA-6.248	48	Kunsan Air Base	Anticipate up to 1980 man hours annually
MA-6.249	49	Laughlin Air Force Base	Anticipate up to 1980 man hours annually
MA-6.250	50	Little Rock Air Force Base	Anticipate up to 1980 man hours annually
MA-6.251	51	Los Angeles Air Force Base	Anticipate up to 1980 man hours annually
MA-6.252	52	Luke Air Force Base	Anticipate up to 1980 man hours annually
MA-6.253	53	MacDill Air Force Base	Anticipate up to 1980 man hours annually
MA-6.254	54	Malmstrom Air Force Base	Anticipate up to 1980 man hours annually
MA-6.255	55	Maui AFRL	Anticipate up to 1980 man hours annually
MA-6.256	56	Maxwell Air Force Base	Anticipate up to 1980 man hours annually
MA-6.257	57	McConnell Air Force Base	Anticipate up to 1980 man hours annually
MA-6.258	58	Minot Air Force Base	Anticipate up to 1980 man hours annually
MA-6.259	59	Misawa Air Base	Anticipate up to 1980 man hours annually
MA-6.260	60	Moody Air Force Base	Anticipate up to 1980 man hours annually
MA-6.261	61	Morón Air Base	Anticipate up to 1980 man hours annually

MA-6.262	62	Mountain Home Air Force Base	Anticipate up to 1980 man hours annually
MA-6.263	63	Nellis Air Force Base	Anticipate up to 1980 man hours annually
MA-6.264	64	New Boston AFS	Anticipate up to 1980 man hours annually
MA-6.265	65	Offutt Air Force Base	Anticipate up to 1980 man hours annually
MA-6.266	66	Osan Air Base	Anticipate up to 1980 man hours annually
MA-6.267	67	Patrick Air Force Base	Anticipate up to 1980 man hours annually
MA-6.268	68	Peterson Air Force Base	Anticipate up to 1980 man hours annually
MA-6.269	69	RAF Lakenheath	Anticipate up to 1980 man hours annually
MA-6.270	70	RAF Mildenhall	Anticipate up to 1980 man hours annually
MA-6.271	71	Ramstein Air Base	Anticipate up to 1980 man hours annually
MA-6.272	72	Robins Air Force Base	Anticipate up to 1980 man hours annually
MA-6.273	73	Schriever Air Force Base	Anticipate up to 1980 man hours annually
MA-6.274	74	Scott Air Force Base	Anticipate up to 1980 man hours annually
MA-6.275	75	Seymour Johnson Air Force Base	Anticipate up to 1980 man hours annually
MA-6.276	76	Shaw Air Force Base	Anticipate up to 1980 man hours annually
MA-6.277	77	Sheppard Air Force Base	Anticipate up to 1980 man hours annually
MA-6.278	78	Spangdahlem Air Base	Anticipate up to 1980 man hours annually
MA-6.279	79	Thule Air Base	Anticipate up to 1980 man hours annually
MA-6.280	80	Tinker Air Force Base	Anticipate up to 1980 man hours annually
MA-6.281	81	Travis Air Force Base	Anticipate up to 1980 man hours annually
MA-6.282	82	Tyndall Air Force Base	Anticipate up to 1980 man hours annually
MA-6.283	83	United States Air Force Academy	Anticipate up to 1980 man hours annually

MA-6.284	84	Vance Air Force Base	Anticipate up to 1980 man hours annually
MA-6.285	85	Vandenberg Air Force Base	Anticipate up to 1980 man hours annually
MA-6.286	86	Whiteman Air Force Base	Anticipate up to 1980 man hours annually
MA-6.287	87	Wright-Patterson Air Force Base	Anticipate up to 1980 man hours annually
MA-6.288	88	Yokota Air Base	Anticipate up to 1980 man hours annually

Appendix 4 Notes:

a) Participates in design reviews for new or upgraded CE CS from base supported projects from various contract types such as: Energy Savings Performance Contract (ESPC), Military Construction (MILCON), Energy Conservation Investment Program (ECIP), or any other projects requiring Information Assurance compliance of the CE CS, Design review capability to be conducted at Tyndall AFB.

b) Develop a CE VLAN design improvement as a requirement for the creators of the VLAN space (A6) to be used by a non-A6 CNDSP in operating and defending the CS inside the CE VLANs. Provide the resources necessary to work with base communication squadrons to design and implement a protected CE VLAN solution.

c) Mission area for base support capability will consist of Information Systems security operations that oversee IA program of a CS in or outside the network environment and may include duties of Information Systems Security Manager (ISSM), Information Systems Security Officer (ISSO) and User Representative (UR) / Systems Administrator as defined in AFI 17-101. Include overseeing, evaluating, and supporting the documentation, validation, and accreditation processes necessary to assure new CS systems meet the organizations IA and cybersecurity requirements.

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.