

Arctic Warrior Events Center (AWEC) Audio Video (A/V) System Replacement

STATEMENT OF OBJECTIVES (SOO)

I. Purpose:

1. The Government seeks a contractor to design, procure, install, integrate, calibrate, and maintain a professional grade A/V distribution system certified and accredited to operate at SECRET security levels and below within the Arctic Warrior Events Center (9387 Kuter Ave, Anchorage, AK 99506).

II. Scope or Mission:

1. The Government's requirement is to replace the existing audio and video equipment in the Conference Room Control Room and integrate the system with the Conference Room; replace the existing audio and video display equipment in the Susitna Room and Billy Mitchell Room; and install audio and video equipment in the Denali Room.

2. For the Conference Room, Control Room, and Denali Room this includes necessary upgrades and security required to operate SIPR equipment as needed to run SECRET level Video Teleconferences (VTC), teleconference, and briefings. The Billy Mitchell Room will not function as a classified processing area, or as a VTC.

III. Period and Place of Performance:

1. Arctic Warrior Events Center, 9387 Kuter Ave, Anchorage, AK 99506.

2. Solution shall be fully deployable and operational within 120 days after equipment delivery.

IV. Background:

1. Current equipment is past its end of life and causing disruptions.

V. Performance Objectives:

1. For operation of and interface with the A/V equipment in the Conference Room and Conference Center Control Room there will be a touch-screen administrative control panel located at the head of the conference room table, another on the lectern located at the front of the room, as well as another within the control room, that control video/audio projection to screens at the front of the room. All control panel screen size must be at least an 8" diagonally. Each seat at the conference room table should have an audio/video port embedded in the table that supports HDMI, USB, VGA, and USB-C components for projection onto the screens. See **Figure 1 on Page 7** for layout of the rooms.

2. Operation of and interface with the A/V equipment in the Susitna Room should be consistent with what is currently installed in the room. Currently, the Susitna Room is equipped with speakers, wireless microphones, mechanically driven, drop-down projector screens, and projector mounts. All sub-systems are controlled via a control station and touch panel in a "nook" identified in **Figure 2 on Page 7** as the "A/V

Room”, also known as the “A/V control area”. The Contractor shall install one touchscreen control panel in the A/V control area in the Susitna room with a screen size of at least 8” diagonally. This includes the position of the projectors and locations to plug into the system. See **Figure 2 on Page 7**.

3. Operation and interface with the A/V system in the Denali room should be consistent with the use of the conference room in paragraph V.1, with the only exception is the need for only one touchscreen control panel at the head of the conference table with a screen size of at least 8” diagonally. There is no existing A/V infrastructure in the Denali room. The contractor must provide and install speakers, microphones, and a VTC suite capable of providing SECRET VTCs, and unclassified and classified teleconferences. The control system must be capable of shutting down unclassified teleconference capabilities while a classified briefing or meeting is in progress. See **Figure 3 on Page 8**.
4. Operation of and interface with the A/V equipment in the Billy Mitchell Room should be consistent with what is currently installed in the room. Currently, the Billy Mitchell Room is equipped with speakers and a wall-mounted/inset TV. All sub-systems are controlled via a control station and touch panel in a “nook” identified in **Figure 4 on Page 9** as the “A/V Room”, also known as the “A/V control room”. The Contractor shall install one touchscreen control panel mounted onto the side of the A/V control room in the Billy Mitchell room with a screen size of at least 8” diagonally. This includes full control of the TV (channel, volume, mute/unmute, power on/off, input, etc.), the microphone/audio system, and identify/control locations to plug into the system (also known as wall jacks). Each wall jack in the room must have an audio/video port embedded in the table that supports HDMI, USB, VGA, and USB-C components for projection onto the TV screen and project audio through the existing speakers in the room. Audio output will be Bluetooth capable, allowing any Bluetooth device the ability to connect and play audio through the speakers. Connectivity to Bluetooth will be controlled by the control panel on the wall. Additionally, the Contractor will install a wireless microphone and lapel capability with two wired and wireless microphones, and two lapel microphones. The Billy Mitchell Room currently only has a wired microphone capability, which will be maintained and improved (if necessary) to allow a wired microphone option. Additionally, the Contractor will install two (2) cameras that can connect to a Government provided computer through the wall jacks using USB, allowing the computer to utilize the cameras for Webex or Zoom VTCs. Finally, the Contractor will install a conference phone that can integrate into the A/V system’s microphones and speakers to allow room-wide teleconferences. The conference phone and which speakers and microphones will be controlled by the control panel on the wall. See **Figure 4 on Page 9**.
5. The Denali and Conference Rooms should be able to go to SECRET level for teleconference, video-teleconference, and briefings with appropriate supporting hardware. All hardware and cabling to enable these capabilities must be provided by the Contractor. Additionally, it will be the Government’s responsibility to program the Voice over IP (VoIP) and Voice over Secure IP (VoSIP) phones as the Contractor will not have access to the Cisco Unity Call Manager (CUCM). Finally, the Government will be responsible for providing the necessary IP addresses for the teleconferencing and video-teleconferencing devices. The Contractor will be responsible to ensure all devices are integrated into and fully controlled by the

control system, allowing the touch panels to control all integrated capabilities in each room independently.

6. The completed system should include Commercial Wi-Fi capabilities to provide service throughout the building, compatible with all OPSEC requirements for operating SIPR at times (shutting down the Wi-Fi as needed). The Contractor will be responsible for providing the Wi-Fi access points and commercial internet connection. Maintenance and configuration of the Wi-Fi access points will be the responsibility of the Contractor. Expected response time to address connectivity issues or outages to the Contractor provided Wi-Fi must be addressed within 24 hours.
7. The final product must provide operational redundancy and interoperability between the Conference Room and the Denali Room. All rooms should be able to operate independently in case of equipment malfunction or single room failure.
8. The Contractor shall provide and install (2) projectors in the Conference Room capable of throwing images on a screen size of 246 inches wide by 82 inches high (260 inches diagonally) and projecting multiple displays or layouts (i.e. can display a VTC while also displaying the screen from a computer connected to the A/V system). See **Figure 1 on Page 7** for approximate placement.
9. The Contractor shall provide and install two (2) 10 feet wide, by 6 feet high (or greater) throw ceiling mounted (using the existing ceiling mount system) projectors in the Susitna Room. Each projector must be designed for 24/7 operations, 4K visuals, quad-view for simultaneous source viewing, and **may** contain Wi-Fi, Bluetooth, or other wireless connectivity. See **Figure 2 on Page 7** for approximate placement.
10. The Contractor shall provide and install two (2) 98-inch (or greater) wall mounted displays in the Denali Room, not to exceed a total lateral length of 270 inches. Each display must be designed for 24/7 operations, 4K visuals, quad-view for simultaneous source viewing and **must not** contain Wi-Fi, Bluetooth, or other wireless connectivity. See **Figure 3 on Page 8** for approximate placement.
11. The Contractor shall provide and install one (1) 98-inch (or greater) wall mounted displays in the Billy Mitchell Room. The display must be designed for 24/7 operations, 4K visuals, quad-view for simultaneous source viewing and **may** contain Wi-Fi, Bluetooth, or other wireless connectivity. See **Figure 4 on Page 9** for approximate placement.
12. The Contractor will include any necessary accessories to feed and manage all room displays and establish user-configured video layouts.
13. All equipment must follow DoD and AVIXA industry standards in addition to Intelligence Community, and JITC security standards.
14. Administrative system control for the Conference, Denali, and Susitna rooms should be controlled via 8-inch or great touch panel displays (i.e. Crestron).

- Two (2) locations in the Conference Room (podium and head of table) and should be similar too and integrated with Two (1) control panel in the Control Room.
- One (1) in the Denali Room
- One (1) in the Susitna Room
- One (1) in the Billy Mitchell Room

15. All touch panels shall have the following functions at a minimum:

- Change room classification and display room classification on the LCD/LED display signs within the Conference and Denali rooms, as well as displays above the doors entering the Conference and Denali rooms
- Control power and layout of room displays
- View device status and perform diagnostics
- Control lighting within the room allowing up to five different levels of lighting
- Control routing of workstation display to Conference Room VTC suite
- Turn on/off Wi-Fi access points when a classified VTC, teleconference, or meeting has been selected on the touch panel
 - Wi-Fi shall only be turned off in areas that are actively processing classified information

16. Existing video screens and projectors must be removed by the Contractor and turned over to the Government for disposition. Any holes created by removing the screens must be repaired prior to the new screens being installed. The Contractor shall provide or subcontract the labor and materials necessary to frame and finish the framed openings and match the surrounding drywall surface. The Contractor shall provide patchwork and paint for the entire display wall.

17. The Contractor shall design, procure, install, integrate, and configure the latest in technology, digital audio system for the rooms to complement the A/V systems to include podium microphones, table mics, ability to support wired or wireless microphones connection to in-ceiling audio. Existing equipment may be utilized if compatible and not at its end of life.

18. Each product shall include a warranty as specified in FAR 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. Two (2) types of warranty shall be provided:

1. Workmanship Warranty
2. Equipment Warranty

The warranty program shall provide for restoration of the system and repair of equipment in a timeframe to be specified in a contract. The Contractor shall provide means to transport equipment and bear transportation charges and responsibility for

Commented [SDPG1UP6C1]: The is will be in the contract, do not include in SOO/PWS. This entire paragraph is not appropriate for this action. Standard warranty and workmanship for commercial items covers most of this unless extended warranties are needed.

equipment and repair personnel under warranty while in transit both to and from the Government site.

a. Workmanship Warranty: The Contractor shall provide a minimum 1-year workmanship 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.

b. Equipment Warranty: The Contractor shall provide standard, OEM pass through, extended or otherwise warranties for one (1) year for all hardware and software products. Repairs shall be accomplished within 96-clock hours of receipt of the equipment warranty trouble call. 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. 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.

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.

15. Individuals performing work shall comply with applicable program security requirements.

16. The Contractor shall provide eight (8) hours of classroom training for up to thirty (30) personnel on the system. The training shall ensure Arctic Warrior Events Center personnel can operate, administer, maintain, and provision the proposed system(s) as identified in the objectives listed below. The Contractor shall complete classroom training before the start of the installation phase of the project. The Contractor shall provide all materials needed for the training. The Contractor shall submit a training syllabus and lesson plans to the Government for approval prior to training. The classroom training shall cover the following objectives:

- Cleaning
- Repairs
- Maintenance
- Operation of A/V system, and related system components.

VI. Operating Constraints:

1. Contractor solutions shall comply with National Institute for Standards and Technologies (NIST) and Federal Information Processing Standards (FIPS) and applicable IC standards. See Appendix 1 for list of applicable regulations.

FIGURE 1: Conference Room & Control Room

*Control Room labeled here as AV/TVC Room

*Room Numbers are not current

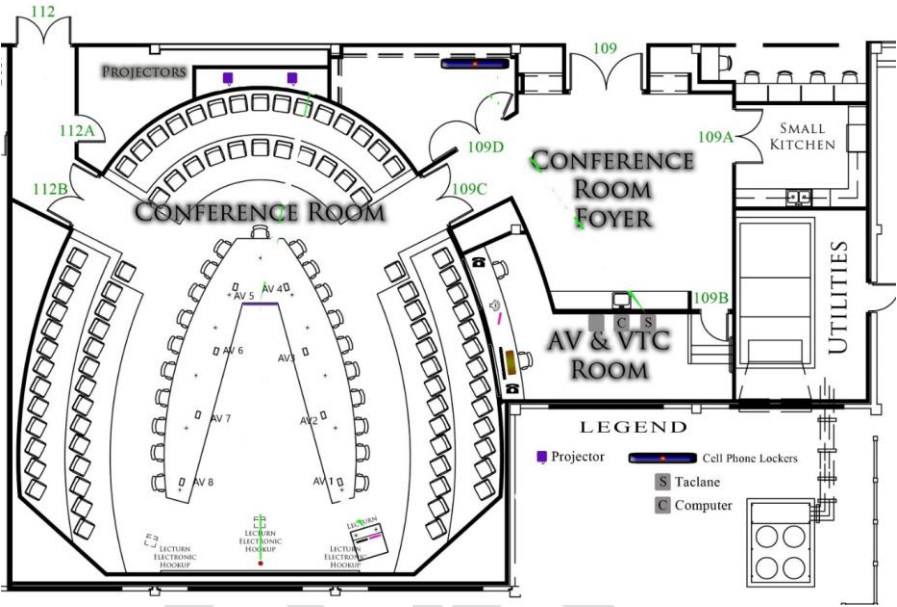


FIGURE 2: Susitna Room

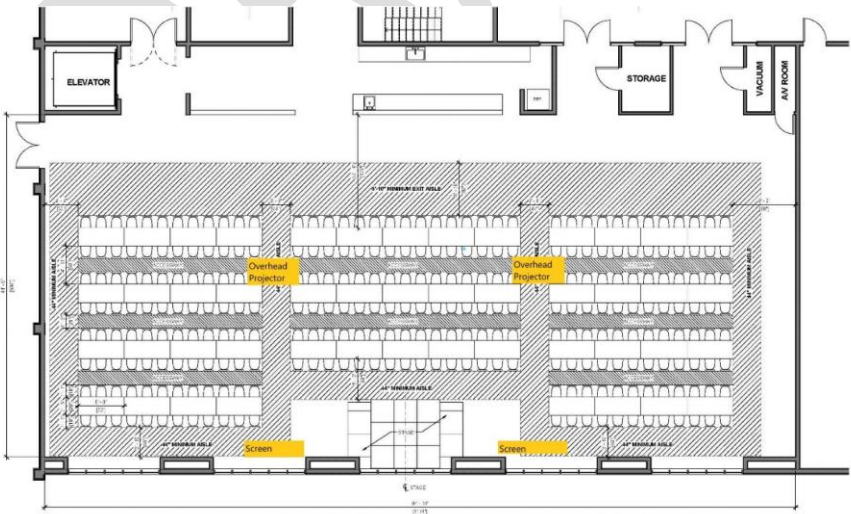


FIGURE 3: Denali Room

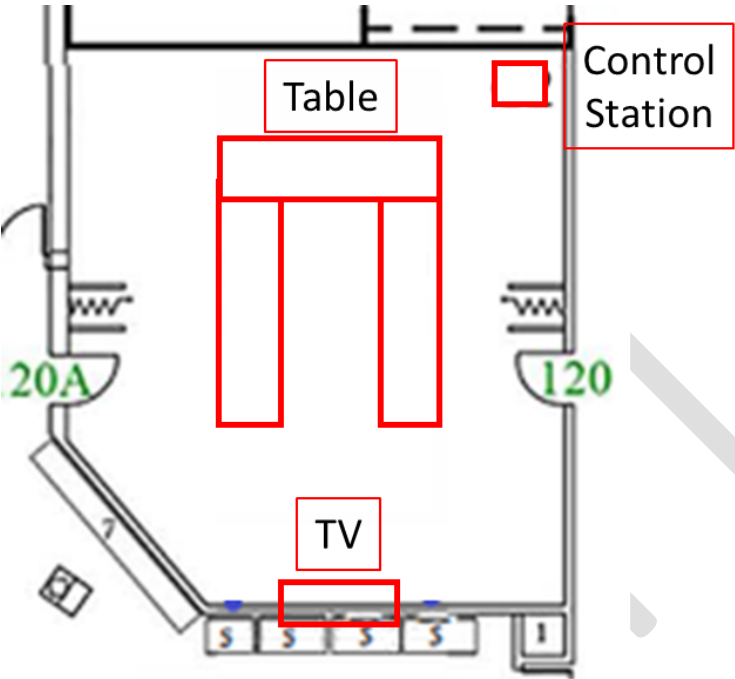
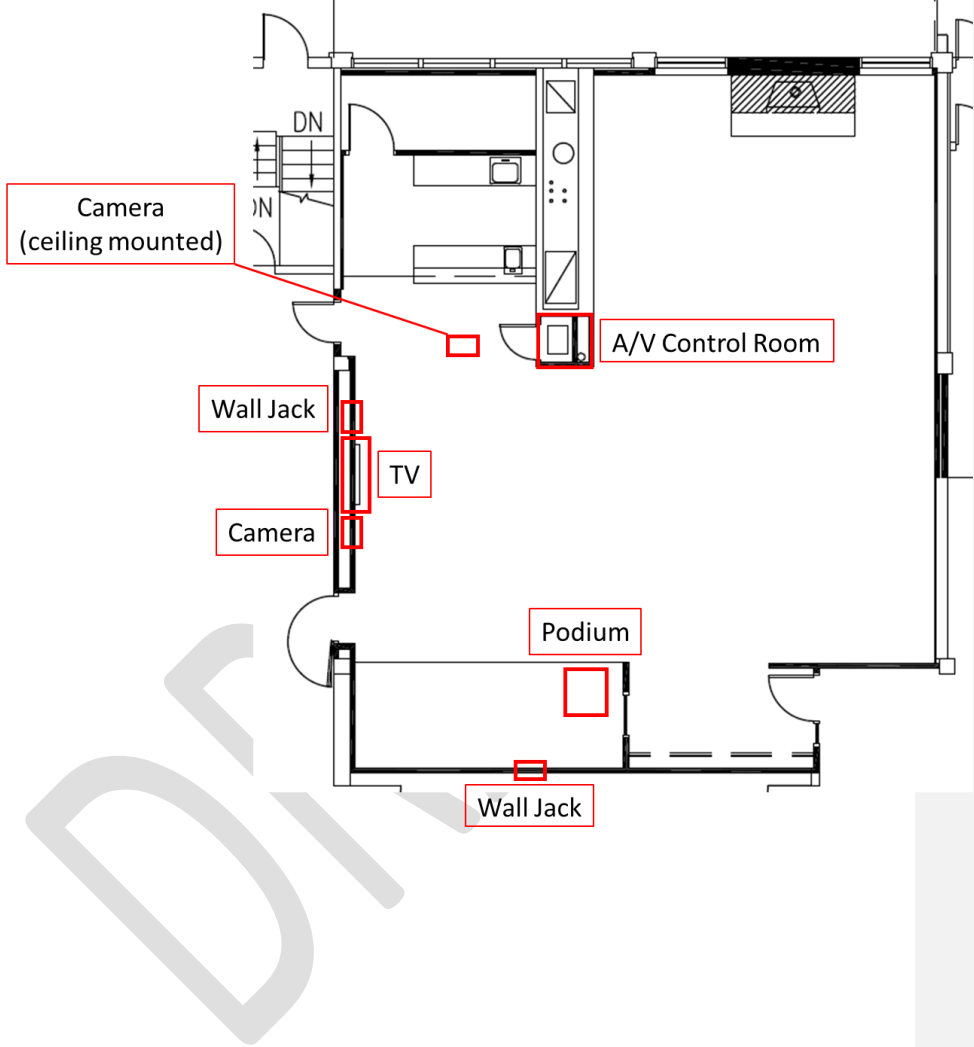


FIGURE 4: Billy Mitchell Room



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 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 10-601 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.
2.	AFI 10-701 Operations Security (OPSEC)	https://static.e-publishing.af.mil/production/1/af_a3/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.

3.	AFI 32-10112 Installation Geospatial Information and Services (Installation GI&S)	https://static.e-publishing.af.mil/production/1/af_a4/publication/afi32-10112/afi32-10112.pdf	<p>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</p>
----	---	---	--

NETWORK OPERATIONS AND INFRASTRUCTURE SOLUTIONS (COMPLIANCE)			
Standard		URL	Description
			specific manufacturer, commercial product, commodity, or service in this publication does not imply endorsement by the Air Force.
4.	AFI 33-332 Air Force Privacy And Civil Liberties Program	https://static.e-publishing.af.mil/production/1/saf_cn/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.
5.	AFI 33-322 Records Management Program	https://static.e-publishing.af.mil/production/1/saf_cn/publication/afi33-322/afi33-322.pdf	Records Management Program
6.	AFI 17-140 Architecting	https://static.e-publishing.af.mil/production/1/saf_cio_a6/publication/afi17-140/afi17-140.pdf	This Air Force Instruction (AFI) implements Air Force Policy Directive (AFPD) 33-4, Enterprise Architecting. This instruction describes the federation of Air Force architectures and its concept for federated architecture development, its associated business rules, governance, and the roles and responsibilities for appropriate Air Force organizations.

NETWORK OPERATIONS AND INFRASTRUCTURE SOLUTIONS (COMPLIANCE)			
Standard		URL	Description
7.	DAFI 17-220 Spectrum Management	https://static.e-publishing.af.mil/production/1/af_a2_6/publication/dafi17-220/dafi17-220.pdf	This instruction establishes guidance and procedures for Air Force-wide management and use of the electromagnetic spectrum and implements Department of Defense Instruction (DoDI) 4650.01, Policy and Procedures for Management and Use of the Electromagnetic Spectrum; DoDI 8320.05, Electromagnetic Spectrum Data Sharing; National Telecommunications and Information Administration (NTIA) Manual of Regulations and Procedures for Federal Radio Frequency Management; Air Force Policy Directive (AFPD) 33-5, Warfighting Integration; and the procedures established by the Joint Staff J65A United States Military Communications-Electronics Board (USMCEB).
8.	AFI 17-210 Radio Management	https://static.e-publishing.af.mil/production/1/af_a2_6/publication/afi17-210/afi17-210.pdf	This standard specifies requirements for types of land mobile radios, frequency ranges and encryption standards. It provides requirements processing, validation, and handling procedures for classified and unclassified Personal Wireless Communication Systems (PWCS), and training. It provides procedures for the management, operation, and procurement of commercial wireless service for all PWCS.

NETWORK OPERATIONS AND INFRASTRUCTURE SOLUTIONS (COMPLIANCE)			
Standard		URL	Description
9.	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
10.	AFMAN 17-1203 Information Technology (IT) Asset Management (ITAM)	https://static.e-publishing.af.mil/production/1/saf_cn/publication/afman17-1203/afman17-1203.pdf	<p>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).</p>

NETWORK OPERATIONS AND INFRASTRUCTURE SOLUTIONS (COMPLIANCE)			
Standard		URL	Description
11.	AFMAN 17-1301 Computer Security (COMPUSEC)	https://static.e-publishing.af.mil/production/1/saf_cn/publication/afman17-1301/afman17-1301.pdf	This AFMAN implements Computer Security in support of AFPD 33-2, Information Assurance Program and AFI 33-200, IA Management Computer Security (COMPUSEC) is defined within the IA Portion of AFI 33-200.
12.	AFPD 33-3 Information Management	https://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.
13.	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.
14.	DoDI 8500.01 – Cyber Security (CS)	http://www.dtic.mil/whs/directives/corres/pdf/850001/2014.pdf	The purpose of the Defense Cybersecurity program is to ensure that IT can be used in a way that allows mission owners and operators to have confidence in the confidentiality, integrity, and availability of IT and DoD information, and to make choices based on that confidence

NETWORK OPERATIONS AND INFRASTRUCTURE SOLUTIONS (COMPLIANCE)			
Standard		URL	Description
15.	DoDI 8551.01 – Ports, Protocols and Services Management	http://www.dtic.mil/whs/directives/corres/pdf/855101p.pdf	
16.	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).
17.	DFARS 252.227-7013 Rights in Technical Data Non- Commercial Items	http://farsite.hill.af.mil/reghtml/regs/far2afmcfars/fardfars/dfars/Dfars252_227.htm#P696_47162	Provides guidelines for rights in technical data on non-commercial items

NETWORK OPERATIONS AND INFRASTRUCTURE SOLUTIONS (COMPLIANCE)			
Standard		URL	Description
18.	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.
19.	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
20.	DFARS 252.227-7015 Technical Data Commercial Items	http://www.acq.osd.mil/dpasp/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.
21.	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.
22.	DoD 5220.22-M, National Industrial Security Program Operating Manual	http://www.dtic.mil/whs/directives/corres/pdf/522022m.pdf	Provides baseline standards for the protection of classified information released or disclosed to industry in connections with classified contracts under the National Industrial Security Program.

NETWORK OPERATIONS AND INFRASTRUCTURE SOLUTIONS (COMPLIANCE)			
Standard		URL	Description
23.	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.
24.	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
25.	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.
26.	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.
27.	DoD CIO Net-Centric Data Strategy	http://dodcio.defense.gov/Portals/0/Documents/Net-Centric-Data-Strategy-2003-05-092.pdf	This Strategy lays the foundation for realizing the benefits of net centricity by identifying data goals and approaches for achieving those goals. To realize the vision for net-centric data, two primary objectives must be emphasized: (1) increasing the data that is available to communities or the Enterprise and (2) ensuring that data is usable by both anticipated and unanticipated users and applications. (Source: Department of Defense Net-Centric Data Strategy, DoD CIO, 9 May 2003)

NETWORK OPERATIONS AND INFRASTRUCTURE SOLUTIONS (COMPLIANCE)			
Standard		URL	Description
28.	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.
29.	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.
30.	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
31.	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.
32.	DoDI 1100.22 Policy and Procedures For Determining Workforce Mix	http://www.dtic.mil/whs/directives/corres/pdf/110022p.pdf	Provides manpower mix criteria and guidance for risk assessments to be used to identify and justify activities that are inherently Governmental (IG); commercial (exempt from private sector performance); and commercial (subject to private sector performance).

NETWORK OPERATIONS AND INFRASTRUCTURE SOLUTIONS (COMPLIANCE)			
Standard		URL	Description
33.	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.
34.	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.
35.	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
36.	AFI 17-130, Air Force Cybersecurity Program Management	https://static.e-publishing.af.mil/production/1/saf_cn/publication/afi17-130/afi17-130.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.
37.	AFI 16-1001, Verification, Validation, and Accreditation (VV&A)	https://static.e-publishing.af.mil/production/1/saf_aq/publication/afi16-1001/afi16-1001.pdf	AF VV&A program guidance

NETWORK OPERATIONS AND INFRASTRUCTURE SOLUTIONS (COMPLIANCE)			
Standard		URL	Description
38.	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)).

NETWORK OPERATIONS AND INFRASTRUCTURE SOLUTIONS (COMPLIANCE)			
Standard		URL	Description
39.	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.

40.	Federal Information Security Management Act (FISMA) 2002	http://www.dhs.gov/federal-information-security-management-act-fisma	<p>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.”</p> <p>FISMA requires Federal agencies to:</p> <ul style="list-style-type: none"> •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. <p>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</p>
-----	--	---	--

NETWORK OPERATIONS AND INFRASTRUCTURE SOLUTIONS (COMPLIANCE)			
Standard		URL	Description
			associated methods and techniques” for information systems used or operated by an agency or Contractor, excluding national security systems.
41.	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
42.	GiG Technical Guidance Federation GIG-F	https://gtg.csd.disa.mil/uam/login.do	<p>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.</p>

NETWORK OPERATIONS AND INFRASTRUCTURE SOLUTIONS (COMPLIANCE)			
Standard		URL	Description
43.	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.
44.	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
45.	IEEE/EIA 12207.0 Standard for Information Technology	http://IEEE.org	IEEE/EIA 12207.0, "Standard for Information Technology – Software Life Cycle Processes", is a standard that establishes a common framework for software life cycle process. This standard officially replaced MIL-STD-498 for the development of DoD software systems in May 1998.[1] Other NATO nations may have adopted the standard informally or in parallel with MIL-STD-498. This standard defines a comprehensive set of processes that cover the entire life-cycle of a software system—from the time a concept is made to the retirement of the software. The standard defines a set of processes, which are in turn defined in terms of activities. The activities are broken down into a set of tasks. The processes are defined in three broad categories: Primary Life Cycle Processes, Supporting Life Cycle Processes, and Organizational Life Cycle Processes.

NETWORK OPERATIONS AND INFRASTRUCTURE SOLUTIONS (COMPLIANCE)			
Standard		URL	Description
46.	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
47.	ITU Recommendation on 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.

48.	CJCSI 6212.01F Interoperability and Supportability of Information Technology and National Security Systems	http://www.dtic.mil/cjcs/directives/cdata/unlimit/621201.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.
49.	DODI 5015.02 DoD Records Management Program	http://www.dtic.mil/whs/directives/corres/pdf/501502p.pdf	Establishes policy and assigns responsibilities for the management of DoD records in all media, including electronic

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

NETWORK OPERATIONS AND INFRASTRUCTURE SOLUTIONS (COMPLIANCE)			
Standard		URL	Description
51.	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.
52.	DODD 8100.1 Department of Defense Information Network (DoDIN) Overarching Policy	http://www.acq.osd.mil/ie/bdi/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
53.	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.
54.	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
55.	Title 44 USC Section 3542	http://us-code.vlex.com/vid/sec-definitions-19256373	<p>(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—</p> <p>(i) the function, operation, or use of which—</p> <p>(I) involves intelligence activities;</p> <p>(II) involves cryptologic activities related to national security;</p> <p>(III) involves command and control of military forces;</p> <p>(IV) involves equipment that is an integral part of a weapon or weapons system; or</p> <p>(V) subject to subparagraph (B), is critical to the direct fulfillment of military or intelligence missions; or</p> <p>(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.</p> <p>(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).</p>

NETWORK OPERATIONS AND INFRASTRUCTURE SOLUTIONS (COMPLIANCE)		
Standard	URL	Description
56. 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.
57. 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.
58. 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.

NETWORK OPERATIONS AND INFRASTRUCTURE SOLUTIONS (COMPLIANCE)		
Standard	URL	Description
59. 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.
60. 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.
61. 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.
62. 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.
63. 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.

NETWORK OPERATIONS AND INFRASTRUCTURE SOLUTIONS (COMPLIANCE)			
Standard		URL	Description
64.	CNSSI 4009: National Information Assurance (IA) Glossary	http://jite.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.
65.	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.
66.	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.
67.	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-commercial-cloud-computing-services.pdf	This Memorandum serves to reinforce existing policy and processes, and is in effect for all DoD networks and systems.
68.	DoD Instructions, 8500 Series	http://www.dtic.mil/whs/directives/corres/ins1.html	DoD Issuances

NETWORK OPERATIONS AND INFRASTRUCTURE SOLUTIONS (COMPLIANCE)			
Standard		URL	Description
69.	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.
70.	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.
71.	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.
72.	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
73.	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.
74.	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.
75.	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.

NETWORK OPERATIONS AND INFRASTRUCTURE SOLUTIONS (COMPLIANCE)			
Standard		URL	Description
76.	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
77. 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.

NETWORK OPERATIONS AND INFRASTRUCTURE SOLUTIONS (COMPLIANCE)			
Standard		URL	Description
78.	Class Deviation - Contracting for Cloud Services (DFARS 239.99/252.23 9-7999)	http://www.acq.osd.mil/dpa/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.
79.	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).
80.	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
81.	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.
82.	NSTISSAM TEMPEST/1-92/TEMPEST Certification	http://www.nsa.gov/applications/ia/tempest/index.cfm	TEMPEST is compromising emanations are defined as unintentional intelligence-bearing signals which, if intercepted and analyzed, may disclose the information transmitted, received, handled, or otherwise processed by any information-processing equipment.

NETWORK OPERATIONS AND INFRASTRUCTURE SOLUTIONS (COMPLIANCE)			
Standard		URL	Description
83.	AFMAN 17-1303 Cybersecurity Workforce Improvement Program	https://static.e-publishing.af.mil/production/1/saf_cn/publication/afman17-1303.pdf	This rewrite identifies cybersecurity baseline certification requirements for the AF cybersecurity workforce; stipulates minimum certification requirements for various cyber roles and risk management positions; sets qualifications criteria; clarifies the cybersecurity-coding position process; and codifies the waiver policy for baseline certification requirements.
84.	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
85.	DoDI 8540.01 Cross Domain (CD) Policy	http://www.dtic.mil/whs/directives/corres/pdf/854001p.pdf	Establishes policy, assigns responsibilities, and identifies procedures for the interconnection of information systems (ISs) of different security domains using CD solutions (CDSs) in accordance with the authority in DoD Directive (DoDD) 5144.02

NETWORK OPERATIONS AND INFRASTRUCTURE SOLUTIONS (COMPLIANCE)			
Standard		URL	Description
86.	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.
87.	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.
88.	DoD IPv6 Memorandum July 3, 2009, and DoD CIO IPV6 Memorandum, September 29, 2003	http://jtc.fhu.disa.mil/apl/ipv6/pdf/distr_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).

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.

Deliverable Item #	Data Item Title
A001	As Built
A002	Work Schedule
A003	Status Report
A004	Meeting Minutes
A005	Test Plan
A006	Test Report

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.