NetCentric Products Standards				
Reference	**Description**	**Category**	**Link to Guidance**	**Authority**
Acquisition Streamlining and Standardization Information System (ASSIST)	ASSIST is the official source for specifications and standards used by the Department of Defense and it always has the most current information. Over 111,000 technical documents are indexed in ASSIST, and the ASSIST document database houses over 180,000 PDF files associated with about 82,000 of the indexed documents. There are more than 33,000 active ASSIST user accounts and over 6,000 active Shopping Wizard accounts. Managed by the DoD Single Stock Point (DODSSP) in Philadelphia, the ASSIST-Online web site provides free public access to most technical documents in the ASSIST database. The ASSIST Shopping Wizard provides a way to order documents from the DODSSP that are not available in digital form.	Product Standards	https://assist.dla.mil/online/start/	DoD
AFGM 2015-33-01, End-of-Support Software Risk Management	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.	Security Programs	http://static.e-publishing.af.mil/production/1/saf_cio_a6/publication/afgm2015-33-01/afgm2015-33-01.pdf	DoD
AFI 17-210, Radio Management	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. Previously AFI 33-590 superseded by AFI 17-210	Radios	http://static.e-publishing.af.mil/production/1/saf_cio_a6/publication/afi17-210/afi17-210.pdf	AF
AFI 63-101/20-101, Integrated Life Cycle Management	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.	Life Cycle Mgt	http://static.e-publishing.af.mil/production/1/saf_aq/publication/afi63-101_20-101/afi63-101_20-101.pdf	AF

NetCentric Products Standards				
Reference	Description	Category	Link to Guidance	Authority
AFMAN 17-1202, Collaboration Services and Voice Systems Management	This instruction 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. This manual is for use by individuals responsible for implementation, acquisition, and management of electronic collaboration services, appliance Video-Teleconferencing (VTC) equipment, and telephone services that are converging under UC Real Time Services (RTS) establishing the basic guidance framework for Air Force personnel. The scope for this publication includes information on policy, standards, reporting, requirements, services, engineering, and systems management for use in complying with DoD and Air Force instructions for UC RTS including collaboration, VTC communications connectivity, and telephone services in the secure and non-secure interactive group environments. This manual assists action officers who implement collaboration services (voice, video, and/or data) to satisfy customer	Network	http://static.e-publishing.af.mil/production/1/saf_cio_a6/publication/afman17-1202/afman17-1202.pdf	AF
AFMAN 17-1203 Information Technology (IT) Asset Management (ITAM)	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).	Information Mgt	http://static.e-publishing.af.mil/production/1/saf_cio_a6/publication/afman17-1203/afman17-1203.pdf	AF

NetCentric Products Standards				
Reference	**Description**	**Category**	**Link to Guidance**	**Authority**
AFMAN 17-1301, COMPUTER SECURITY (COMPUSEC)	Computer Security (COMPUSEC) is a cybersecurity discipline identified in AFI 17-130. Compliance ensures appropriate implementation of measures to protect all AF Information System (IS) resources and information. The COMPUSEC objective is to employ countermeasures designed for the protection of confidentiality, integrity, availability, authentication, and non-repudiation of United States (US) government information processed by AF ISs.	Security Programs	http://static.e-publishing.af.mil/production/1/saf_cio_a6/publication/afman17-1301/afman17-1301.pdf	AF
AFMAN 17-1303, CYBERSECURITY WORKFORCE IMPROVEMENT PROGRAM	By Order of the Secretary of the Air Force, this Air Force Guidance Memorandum immediately AFMAN33-285 Cybersecurity Workforce Improvement Program, 20 Mar 2015 Information. Compliance with this Memorandum is mandatory. To the extent its directions are inconsistent with other Air Force publications, the information herein prevails, in accordance with (IAW) AFI 33-360, Publications and Forms Management. Ensure that all records created as a result of processes prescribed in this publication are maintained IAW Air Force Manual (AFMAN) 33-363, Management of Records, and disposed of IAW Air Force Records Information Management System (AFRIMS) Records Disposition Schedule (RDS).	Information Assurance	http://static.e-publishing.af.mil/production/1/saf_cio_a6/publication/afman17-1303/afman17-1303.pdf	AF
Automated Identification Technology (AIT)	As OASD(SCI) continues to modernize the DoD supply chain, it will be actively involved with RFID implementation as well as other components of the suite of technologies knows as AIT. By applying RFID in tandem with other AIT, the DoD will be able to fully realize the capabilities offered by these enabling technologies.	Supply Chain	http://www.acq.osd.mil/log/rfid/index.htm	DoD
CJCSI 6211.02D, Defense Information Systems Network Responsibilities	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).	Network	http://www.jcs.mil/Portals/36/Documents/Library/Instructions/6211_02a.pdf?ver=2016-02-05-175050-653?ver=2016-02-05-175050-653	DoD

NetCentric Products Standards				
Reference	**Description**	**Category**	**Link to Guidance**	**Authority**
CNSSAM TEMPEST/1-13 RED/BLACK Installation Guidance	This document defines the guidance for the design of facilities and the installation of equipment and systems that receive, transmit, route, switch, manipulate, graph, store, archive, calculate, generate, print, scan, or in any other manner process or transfer National Security Information (NSI). This guidance is part of the potential solution for facilities, systems and equipment identified as requiring TEMPEST countermeasures. Additional TEMPEST countermeasures, including facility and/or equipment shielding may also be a part of a potential solution, but is beyond the scope of this document.	TEMPEST	https://www.cnss.gov/CNSS/issuances/Memoranda.cfm	Federal
CNSSP-11 NATIONAL POLICY GOVERNING THE ACQUISITION OF INFORMATION ASSURANCE (IA) AND IA-ENABLED INFORMATION TECHNOLOGY PRODUCTS	This policy establishes processes and procedures for the evaluation and acquisition of COTS and GOTS IA or IA-enabled IT products1 to be used on U.S. NSS. The processes and procedures established in this policy will reduce the risk of compromising the NSS and the information contained therein and will: - Ensure the security-related features of IA and IA-enabled IT products perform as claimed. - Ensure the security evaluations of IA and IA-enabled IT products produce achievable, repeatable, and testable results. - Promote cost effective and timely evaluations of IA and IA-enabled IT products.	Security Programs	https://www.cnss.gov/CNSS/issuances/Policies.cfm	Federal
CNSSP-19 National Policy Governing the Use of High Assurance Internet Protocol Encryptor (HAIPE) Products	For High Assurance Internet Protocol Encryption (HAIPE) devices, CNSSP-19 requires NSA HAIPE certification for these products. A HAIPE is a programmable IP INFOSEC device with traffic protection, networking and management features that provide IA services for IPv4 and IPv6 networks used by aircraft, vehicles and portable models. Vendors will have an NSA issued certificate.	Network	https://www.cnss.gov/CNSS/issuances/Policies.cfm	Federal

NetCentric Products Standards				
Reference	**Description**	**Category**	**Link to Guidance**	**Authority**
DFARS 252.225.7021 Trade Agreements	Identifies situations when a contractor can deliver non-U.S. made, qualifying country, or designated country end products: (c) The Contractor shall deliver under this contract only U.S.-made, qualifying country, or designated country end products unless— (1) In its offer, the Contractor specified delivery of other nondesignated country end products in the Trade Agreements Certificate provision of the solicitation; and (2)(i) Offers of U.S.-made, qualifying country, or designated country end products from responsive, responsible offerors are either not received or are insufficient to fill the Government's requirements; or (ii) A national interest waiver has been granted.	FAR	http://farsite.hill.af.mil/	DoD
DFARS: Network Penetration Reporting and Contracting for Cloud Services	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.	Network	http://www.gpo.gov/fdsys/pkg/FR-2015-08-26/pdf/2015-20870.pdf	Federal
DoD Cloud Computing Security Requirements Guide	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 Cloud Computing Security Requirements Guide (CC SRG). DoD Instruction (DoDI) 8500.01, entitled Cybersecurity, directs Director DISA, under the authority, direction, and control of the DoD CIO to develop and maintain Control Correlation Identifiers (CCIs), Security Requirements Guides (SRGs), Security Technical Implementation Guides (STIGs), and mobile code risk categories and usage guides that implement and are consistent with DoD cybersecurity policies, standards, architectures, security controls, and validation procedures, with the support of the National Security Agency Central Security Service (NSA/CSS), using input from stakeholders, and using automation whenever possible. DoDI	Software	https://iasecontent.disa.mil/cloud/Downloads/Cloud_Computing_SRG_v1r2.pdf	DoD

NetCentric Products Standards				
Reference	**Description**	**Category**	**Link to Guidance**	**Authority**
DoD Commercial Mobile Device Implementation Plan	This memorandum provides a phased Commercial Mobile Device (CMD) Implementation Plan that promotes the development and use of mobile non-tactical applications within the Department of Defense (DoD) enterprise. The Implementation Plan updates the DoD Mobile Device Strategy, Reference (a), to permit secure classified and protected unclassified mobile solutions that leverage commercial off-the-shelf products. The Implementation Plan is contingent on available funding and will be followed by a DoD Instruction with additional guidance on the use of wireless voice, video, and data capabilities.	Radios	http://archive.defense.gov/news/DoDCMDImplementationPlan.pdf	DoD
DoD IPv6 Memorandum, July 3 2009, and DoD CIO IPv6 Memorandum, 29 September 2003	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).	Network	https://www.hpc.mil/images/hpcdocs/ipv6/dod_recommended_ipv6_contractual_language-2010-oct-08v2.0.pdf	DoD
DoDD 8100.02, Use of Commercial Wireless Devices, Services, and Technologies in the DoD Global Information Grid (GIG)	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.	GIG	http://www.esd.whs.mil/Directives/issuances/dodd/	DoD
DoDI 3222.03, DoD Electromagnetic Environmental Effects (E3) Program	Reissue DoD Directive (DoDD) 3222.3 (Reference (a) as a DoD instruction (DoDI) in accordance with the authority in DoDD 5144.02 (Referernce (b)). The mission of the DoD E3 IPT is to promote communication, coordination, commonality, and synergy among the DoD Components for E3-related matters.	Misc (Energy Star, etc)	http://www.esd.whs.mil/Directives/issuances/dodi/	DoD
DoDI 4170.11, Installation Energy Management	See Section 3.b.(2)	Misc (Energy Star, etc)	http://www.esd.whs.mil/Directives/issuances/dodi/	DoD

NetCentric Products Standards				
Reference	**Description**	**Category**	**Link to Guidance**	**Authority**
DoDI 4650.10 Land Mobile Radio (LMR) Interoperability and Standardization	In accordance with the authority in DoDD 5144.02 and guidance in DoDD 3025.18, DoDI 8330.01, and DoDI 5535.10, this instruction establishes policy and assigns responsibility to ensure that LMR systems support interoperable and secure communications with other federal, State, local, and tribal LMR user; and directs the establishment of a list of DoD-required Telecommunications Industry Associate (TIA) Project 25 (P25) interfaces to support LMR interoperability.	Radios	http://www.esd.whs.mil/Directives/issuances/dodi/	DoD
DoDI 5015.02, DoD Records Management Program	Establishes policy and assigns responsibilities for the management of DoD records in all media, including electronic	Records and Document Mgt	http://www.esd.whs.mil/Directives/issuances/dodi/	DoD
DODI 8320.02, Sharing Data, Information, and Information Technology (IT) Services in the Department of Defense	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.	NetCentric Strategy	http://www.esd.whs.mil/Directives/issuances/dodi/	DoD
DODI 8320.04 Item Unique Identification (IUID) Standards for Tangible Personal Property	Reissues DoD Instruction (DoDI) 8320.04 (Reference (b)) to establish policy and assign responsibilities for the process of uniquely identifying tangible personal property and their associated selected attributes. The unique item identifier (UII) will be used globally as the common data key in financial, property accountability, acquisition, and logistics (including supply and maintenance) automated information systems to enable asset accountability, valuation, life-cycle management, and counterfeit materiel risk reduction.	Product Standards	http://www.esd.whs.mil/Directives/issuances/dodi/	DoD
Electronic Biometric Transmission Specification (EBTS)	This website provides a listing of FBI approved biometric products and EBTS standards documents.	Biometrics	https://www.fbibiospecs.cjis.gov/	Federal
Energy Star Approved Products List	The Energy Star Approved Products List provides listings of products that meet ENERGY STAR® guidelines.	Misc (Energy Star, etc)	https://www.energystar.gov/products	Federal

NetCentric Products Standards				
Reference	Description	Category	Link to Guidance	Authority
Factory Mutual (FM) 3610 - Approval Standard for Intrinsically Safe Apparatus and Associated Apparatus for use in Class I, II, and III, Division 1, Hazardous (Classified) Locations	This standard states LMR recertification must occur any time outer case has been breached in a manner, which exposes internal circuits of unit. (This does not include: replacement of antenna; changing/replacing battery pack; software loaded into unit; replacing a control knob; replacing an escutcheon or belt clip). If for any reason a radio needs repair, it then needs to be re-certified as FM Approved. Indicated by a green dot on the radio and battery. Also defines safe operating standards and radio frequency exposure	Radios	http://www.fmglobal.com/page.aspx?id=50030000	Federal
FAR 23.704 - Electronic Product Environmental Assessment Tool (EPEAT®)	Contracting officers, when acquiring an electronic product, except as specified in paragraphs (a)(1)(i), (ii), or (iii) of this section, shall acquire an EPEAT® registered electronic product, unless the agency determines, in accordance with agency procedures, that the EPEAT® registered product will not be cost effective over the life of the product. This subpart applies to acquisitions of electronic products to be used in the United States, unless otherwise provided by agency procedures. When acquiring electronic products to be used outside the United States, agencies must use their best efforts to comply with this section.	Misc (Energy Star, etc)	http://farsite.hill.af.mil	Federal
FAR 52.223-15 – Energy Efficiency in Energy-Consuming Products	This clause requires energy-consuming products are energy efficient products (i.e., ENERGY STAR® products or FEMP-designated products) at the time of contract award unless the energy-consuming product is not listed in the ENERGY STAR® Program or FEMP or otherwise approved in writing by the Contracting Officer.	Misc (Energy Star, etc)	http://farsite.hill.af.mil/	Federal
FAR Subpart 25.1 -- Buy American Act – Supplies	Under the Buy American Act, heads of executive agencies are required to determine, as a condition precedent to the purchase by their agencies of materials of foreign origin for public use within the United States, (1) that the price of like materials of domestic origin is unreasonable, or (2) that the purchase of like materials of domestic origin is inconsistent with the public interest.	Supply Chain	http://farsite.hill.af.mil	Federal

NetCentric Products Standards				
Reference	**Description**	**Category**	**Link to Guidance**	**Authority**
Federal Energy Management Program	Federal agencies are required to meet energy management mandates outlined by the following federal legal authorities: •Executive Order 13693: Planning for Federal Sustainability in the Next Decade •Energy Independence and Security Act of 2007 •Energy Policy Act of 2005 •Executive Order 13221: Energy-Efficient Standby Power Devices •Energy Policy Act of 1992 •National Energy Conservation Policy Act This site provides a listing of covered product categories that meet federal procurement requirements.	Misc (Energy Star, etc)	https://energy.gov/eere/femp/energy-efficient-products-and-energy-saving-technologies	Federal
Federal Information Processing Standards (FIPS)	Overview: Under the Information Technology Management Reform Act (Public Law 104-106), the Secretary of Commerce approves standards and guidelines that are developed by the National Institute of Standards and Technology (NIST) for Federal computer systems. These standards and guidelines are issued by NIST as Federal Information Processing Standards (FIPS) for use government-wide. NIST develops FIPS when there are compelling Federal government requirements such as for security and interoperability and there are no acceptable industry standards or solutions. See background information for more details.	Misc (Energy Star, etc)	http://www.nist.gov/itl/fipscurrent.cfm	Federal
Federal Information Security Modernization Act of 2014	Federal Information Security Modernization Act of 2014 - Amends the Federal Information Security Management Act of 2002. This Executive Order provides for the use of automated tools in agencies' information security programs, including for periodic risk assessments, testing of security procedures, and detecting, reporting, and responding to security incidents.	Security Programs	https://www.dhs.gov/fisma	Federal
FedRAMP Approved Products List	This website provides a listing of FedRAMP approved products for Cloud computing. See the Marketplace tab for a list of products. This APL acts under governance of FedRAMP which is a government-wide program with input from numerous departments, agencies, and government groups. The program’s primary decision-making body is the Joint Authorization Board (JAB), comprised of the CIOs from DOD, DHS, and GSA. In addition to the JAB, OMB, the Federal CIO Council, NIST, DHS, and the FedRAMP Program Management Office (PMO) play keys roles in effectively running FedRAMP.	Software	https://www.fedramp.gov/	Federal

NetCentric Products Standards				
Reference	**Description**	**Category**	**Link to Guidance**	**Authority**
FIPS 140-2	For products that use cryptographic-based security to protect sensitive but unclassified information in computer and telecommunication systems (including voice systems), the use of validated cryptography must be in place per FIPS 140-2. Governed by Federal Information Security Management Act (FISMA) in 2002, there is no longer a statutory provision to allow for agencies to waive FIPS. CMVP) validates cryptographic modules to FIPS 140-2 and provides an APL found at http://csrc.nist.gov/groups/STM/cmvp/validation.html. Vendors will have a FIPS 140-2 certificate.	Product Standards	http://csrc.nist.gov/publications/PubsFIPS.html	Federal
FIPS 200 - Minimum Security Requirements for Federal Information and Information Systems	FIPS 200 is the second standard that was specified by the Federal Information Security Management Act of 2002 (FISMA). It is an integral part of the risk management framework that NIST has developed to assist federal agencies in providing levels of information security based on levels of risk. FIPS 200 specifies minimum security requirements for federal information and information systems and a risk-based process for selecting the security controls necessary to satisfy the minimum requirements	Radios	http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.200.pdf	Federal
FIPS 201-2 Personal Identity Verification (PIV) of Federal Employees and Contractors	The Personal Identity Verification (PIV) standard for Federal Employees and Contractors, Federal Information Processing Standard (FIPS 201), was developed to establish standards for identity credentials. It encompasses NISTSP 800-73, 800-76 and 800-78. It describes technical acquisition and formatting specifications for the biometric credentials of the PIV system, including the PIV Card1 itself. It enumerates procedures and formats for fingerprints and facial images by restricting values and practices included generically in published biometric standards. The primary design objective behind these particular specifications is high performance universal interoperability. NOTE: This is applicable only to fingerprint and facial images used on PIV Smart Cards. It does not apply to other biometric use such as fingerprints for background investigations. The NIST Personal Identity Verification Program (NPIVP) validates PIV components required by FIPS 201 and maintains an APL athttp://fips201ep.cio.gov/index.php. A list of validated middleware can be found athttp://csrc.nist.gov/groups/SNS/piv/npivp/v	Security Programs	http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.201-2.pdf	Federal

NetCentric Products Standards				
Reference	**Description**	**Category**	**Link to Guidance**	**Authority**
GiG Technical Guidance Federation GIG-F	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.	GIG	https://gtg.csd.disa.mil/uam/login.do	DoD
Homeland Security Presidential Directive 12 (HSPD 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.	Product Standards	http://www.dhs.gov/homeland-security-presidential-directive-12	Federal
ISO/IEC 11889-1:2015 through ISO/IEC 11889-4:2015	Trusted Platform Module (TPM) Mandate - In accordance with DODI 8500.01, computer assets (e.g., server, desktop, laptop, thin client, tablet, smartphone, personal digital assistant, mobile phone) will include a Trusted Platform Module (TPM) version 1.2 or higher. TPMs must be in conformance with Trusted Computing Group standards.	Security Programs	http://www.iso.org/iso/search.htm?qt=11889&sort=rel&type=simple&published=on&active_tab=standards	DoD
ISO/IEC 19770-2:2015, Software Identification Tag	ISO/IEC 19770-2:2015 establishes specifications for tagging software to optimize its identification and management. (http://en.wikipedia.org/wiki/ISO/IEC_19770)	Software	https://www.iso.org/standard/65666.html	
ITU Recommendation H.320, Narrow-band Visual Telephone Systems and Terminal Equipment	International Telecommunication Union recommendation that DoD requires for VTC and DISN Video Services equipment must meet. This standard sets BONDING (Bandwith on Demand) algorithms to ensure bandwith in proper increments. This included with FTR 1080B-2002.	Product Standards	https://www.itu.int/rec/T-REC-H.320/en	Federal

NetCentric Products Standards				
Reference	**Description**	**Category**	**Link to Guidance**	**Authority**
MIL-STD-129P, Military Marking for Shipment and Storage	Standards and Specification information regarding passive Radio Frequency Identification (RFID).	Product Standards	http://www.acq.osd.mil/log/sci/.AIT.html/MIL-STD-129PCH4.pdf	DoD
NIST SP 800-147: BIOS Protection Guidelines	This document provides guidelines for preventing the unauthorized modification of Basic Input/Output System (BIOS) firmware on PC client systems. Unauthorized modification of BIOS firmware by malicious software constitutes a significant threat because of the BIOS's unique and privileged position within the PC architecture. A malicious BIOS modification could be part of a sophisticated, targeted attack on an organization —either a permanent denial of service (if the BIOS is corrupted) or a persistent malware presence (if the BIOS is implanted with malware).	Security Programs	http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-147.pdf	Federal
NIST Special Publication 500-290 Data Format for the Interchange of Fingerprint, Facial	This standard defines the content, format, and units of measurement for the electronic DNA and other biometric sample and forensic information that consists of a variety of mandatory and optional items. This information sis primarily intended for interchange among criminal justice administrations or organizations that rely on automated identification systems or use other biometric and image data for id purposes. (It appears the DoD Biometrics has dissolved) REPLACED WITH: NIST Special Publication 500-290 Data Format for the Interchange of Fingerprint, Facial & Other Biometric Information (ANSI/NIST-ITL 1-2011) AND Electronic Biometric Transmission Specification (EBTS)	Biometrics	http://ws680.nist.gov/publication/get_pdf.cfm?pub_id=910136	DoD
NSTISSAM TEMPEST/1-92/TEMPEST Certification	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.	TEMPEST	https://www.iad.gov/iad/search.cfm?criteria=NSTISSAM+TEMPEST%2F1-92%2FTEMPEST+Certification+	Federal

NetCentric Products Standards				
Reference	**Description**	**Category**	**Link to Guidance**	**Authority**
Section 508 of the Rehabilitation Act of 1973	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.	Misc (Energy Star, etc)	http://www.opm.gov/html/508-textOfLaw.asp	Federal
Title 44 USC Section 3542	(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	Security Programs	https://www.gpo.gov/fdsys/granule/USCODE-2011-title44/USCODE-2011-title44-chap35-subchapIII-sec3542	Federal
Unified Capabilities Requirements 2013 (UCR 2013)	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).	Unified Capabilities	http://www.disa.mil/Network-Services/UCCO/Archived-UCR	DoD
Updated Guidance on the Acquisition and Use of Commercial Cloud Computing Services	This memo clarifies and updates DoD guidance when acquiring commercial cloud services.	NetCentric Strategy	http://www.doncio.navy.mil/Download.aspx?AttachID=5555	DoD

NetCentric Products Standards				
Reference	**Description**	**Category**	**Link to Guidance**	**Authority**
US Government Configuration Baseline (USGCB)	The United States Government Configuration Baseline (USGCB) is a Federal government-wide initiative that provides guidance to agencies on what should be done to improve and maintain an effective configuration settings focusing primarily on security. The USGCB baseline evolved from the Federal Desktop Core Configuration mandate. USGCB continues to be one of the most successful government IT programs aimed at helping to increase security, reduce costs, and accelerate the adoption of new government technologies, while creating a more managed desktop environment.	Misc (Energy Star, etc)	http://usgcb.nist.gov/	Federal