Reference	Description	Category	Link to Guidance
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/
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
AFI 33-590, 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.	Radios	http://static.e-publishing.af.mil/production/1/saf_cio_a6/publication/afi33-590/afi33-590.pdf
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
AFMAN 33-282, COMPUTER SECURITY (COMPUSEC)	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.	Security Programs	http://static.e-publishing.af.mil/production/1/saf_cio_a6/publication/afman33-282/afman33-282.pdf

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
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	COPY and PASTE in BROWSER: http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-147.pdf
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	COPY and PASTE in BROWSER: http://www.dtic.mil/cjcs_directives/cdata/unlimit/6211_02a.pdf
CNSS 300-National Policy on Control of Compromising Emanations	Requires commercial telecommunications products that process classified information to be certified by the NSA Certified TEMPEST Products Program. FOUO	TEMPEST	Restricted Use. Please see access instructions at: https://www.cnss.gov/CNSS/issuances/Policies.cfm

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
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
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	COPY and PASTE in BROWSER: http://www.gpo.gov/fdsys/pkg/FR-2015-08-26/pdf/2015-20870.pdf
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	http://jitc.fhu.disa.mil/apl/ipv6/pdf/disr_ipv6_product_profile_v4.pdf and https://acc.dau.mil/adl/en-US/31652/file/5809/IPV6%20Policy%20Memo.pdf

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	COPY and PASTE in BROWSER: http://www.dtic.mil/whs/directives/corres/pdf/810002p.pdf
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)	COPY and PASTE in BROWSER: http://www.dtic.mil/whs/directives/corres/pdf/322203p.pdf
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	COPY and PASTE in BROWSER: http://www.dtic.mil/whs/directives/corres/pdf/465010p.pdf
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	COPY and PASTE in BROWSER: http://www.dtic.mil/whs/directives/corres/pdf/501502p.pdf

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	COPY and PASTE in BROWSER: http://www.dtic.mil/whs/directives/corres/pdf/832002p.pdf
DODI 8320.04 Item Unique Identification (IUID) Standards for Tangible Personal Property	Provides guidance on tracking items that have been acquired through the acquisition system.	Product Standards	COPY and PASTE in BROWSER: http://www.dtic.mil/whs/directives/corres/pdf/832004p.pdf
NIST Special Publication 500-290 - Data Format for the Interchange of Fingerprint, Facial & Other Biometric Information	This standard defines the content, format, and units of measurement for the electronic exchange of fingerprint, palmprint, plantar, facial/mugshot, scar, mark & tattoo (SMT), iris, deoxyribonucleic acid (DNA), and other biometric sample and forensic information that may be used in the identification or verification process of a subject.	Product Standards	COPY and PASTE in BROWSER: http://www.nist.gov/customcf/get_pdf.cfm?pub_id=910136
Energy Star Compliance	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.	Misc (Energy Star, etc)	COPY and PASTE in BROWSER: http://www.dtic.mil/whs/directives/corres/pdf/417011p.pdf For FAR 23.704,COPY and PASTE in BROWSER: https://www.acquisition.gov/far/current/html/Subpart%2023_7.html
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

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/vffara.htm
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 Information Security Management Act (FISMA) 2014	The Federal Information Security Modernization Act (FISMA) of 2014 updates the Federal Government's cybersecurity practices by: •Codifying Department of Homeland Security (DHS) authority to administer the implementation of information security policies for non-national security federal Executive Branch systems, including providing technical assistance and deploying technologies to such systems; •Amending and clarifying the Office of Management and Budget's (OMB) oversight authority over federal agency information security practices; and by •Requiring OMB to amend or revise OMB A-130 to "eliminate inefficient and wasteful reporting."	Security Programs	http://www.dhs.gov/federal-information-security-management-act-fisma

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
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://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf

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/validation.html.	Security Programs	http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.201-2.pdf
FTR 1080B-2002	Federal Telecommunications Recommendation that DoD requires VTC and DISN Video Services equipment must meet	Product Standards	

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
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
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 2.0 or higher. TPMs must be in conformance with Trusted Computing Group standards.	Security Programs	http://www.iso.org/iso/home/store/catalogue_ics/catalogue_detail_ics.htm?csnumber=66510
ISO/IEC 19770-2, Software Tagging	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	http://www.iso.org/iso/home/store/catalogue_ics/catalogue_detail_ics.htm?csnumber=65666

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	http://www.itu.int/rec/T-REC-H.320
MIL-STD-129R, DoD Standard Practice Military Marking for Shipment and Storage	This standard provides the minimum requirements for uniform military marking for shipment and storage. Additional markings may be required by the contract or the cognizant activity.	Supply Chain	http://quicksearch.dla.mil/qsDocDetails.aspx?ident_number=35520
NSTISSAM TEMPEST 2-95	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 ciphertext (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.	TEMPEST	http://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0ahUKEwjPhtPOhvrLAhVhsIMKHXA5Aa4QFggcMAA&url=http%3A%2F%2Fece.wpi.edu%2Fcourses%2Fee579sw%2FECE579S%2FNSTISSAM%2520TEMPEST%25202-95.doc&usg=AFQjCNHP99PgznCUQrRElg5hszF0q1iy_A&sig2=RB76EYyZ
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	Restricted use
Radio Frequency Identification (RFID)	Standards and Specification information regarding passive Radio Frequency Identification (RFID).	Product Standards	http://www.acq.osd.mil/log/sci/ait.html

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
NISTIR 7622 Section 806 Supply Chain Risk Management	Section 806 permits consideration of supply chain risk (SCR) in procurement actions related to an NSS using three approaches: Qualified suppliers: an agency may establish supply chain risk management (SCRM) qualification requirements and restrict the procurement to sources that meet such qualification requirements SCRM evaluation factors: an agency may consider supply chain risk as a factor in the evaluation of proposals for the award of a contract or issuance of a delivery order Limitations on subcontracting: an agency may withhold consent to subcontract with a particular source or direct a contractor to exclude a particular source from consideration for a subcontract.	Product Standards	COPY and PASTE to BROWSER: http://dx.doi.org/10.6028/NIST.IR.7622
Special Asset Tagging, IAW DODI 8320.04	Prescribes procedures and assigns responsibilities for establishing accountability and value over uniquely identified items of tangible personal property through use of transaction-derived data in a net-centric environment.	Product Standards	COPY and PASTE to BROWSER: http://www.dtic.mil/whs/directives/corres/pdf/832004p.pdf

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 personnel management applications).	Security Programs	http://us-code.vlex.com/vid/sec-definitions-19256373
Trade Act Agreement (TAA) FAR 25.103e	FAR 25.103e provides that the provisions of the BAA do not apply to purchases of commercial information technology supplies, both hardware and software for purchases after FY 2004. (page 5 of memo under "exceptions"). This statutory provision greatly simplifies purchases of commercial IT items under NETCENTS because military and civilian agency ordering activities do not need to make determinations of "domestic end product", cost of foreign components and qualifying country source determinations as well as analysis of price differences to assess whether or not the evaluation factor preference must be applied described at FAR 25.1 and DFARS 225.1. This exception avoids many of the problems associated with confusion between BAA and TAA provisions.	FAR	https://www.acquisition.gov/?q=/browse/far/25

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
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	COPY and PASTE to BROWSER: http://www.doncio.navy.mil/Download.aspx?AttachID=5555
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/