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

AFI 10-208, Air Force Continuity of Operations (COOP) Program	This Instruction implements Air Force Policy Directive (AFPD) 10-2, Readiness, and is consistent with AFPD 10-8, Homeland Security. It describes policy and requirements for implementing DODI 3020.42, Defense Continuity Plan Development, and DODI O-3020.43, Emergency Management and Incident Command of the Pentagon Facilities; DODI O-3000.08 Balanced Survivability Assessments (BSAs);and O-DODI 5110.11, Raven Rock Mountain Complex (RRMC).	Life Cycle Mgt	http://static.e-publishing.af.mil/production/1/af_a3_5/publication/afi10-208/afi10-208.pdf
AFI 10-601, Operational Capability Requirements Development	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.	Life Cycle Mgt	http://static.e-publishing.af.mil/production/1/af_a3_5/publication/afi10-601/afi10-601.pdf
AFI 10-701, Operations Security (OPSEC)	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.	Security Programs	http://static.e-publishing.af.mil/production/1/af_a3_5/publication/afi10-701/afi10-701.pdf

AFI 16-1404, Air Force Information Security Program	This publication implements Air Force Policy Directive (AFPD) 16-14, Security Enterprise Governance; Department of Defense (DoD) Directive 5210.50, Management of Serious Security Incidents Involving Classfied Information, DoD Instruction (DoDI) 5210.02, Access and Dissemination of RD and FRD, DoDI 5210.83, DoD Unclassified Controlled Nuclear Information (UCNI), DoD Manual (DoDM) 5200.01, DoD Information Security Program, Volume 1, Volume 2, Volume 3, and Volume 4; and DoDm 5200.45, Instructions for Developing Security Classification Guides.	Security Programs	http://static.e-publishing.af.mil/production/1/saf_aa/publication/afi16-1404/afi16-1404.pdf

AFI 17-100 Air Force Information Technology (IT) Service management	By Order of the Secretary of the Air Force, this Air Force Guidance Memorandum immediately changes Air Force Instruction 33-115, Air Force Information Technology (IT) Service Management, 16 September 2014. 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 Mgt	http://static.e-publishing.af.mil/production/1/saf_cio_a6/publication/afi33-115/afi17-100.pdf
AFI 17-101 Certification and Accreditation (C&A) Program (AFCAP)	AF C&A program guidance	Certification & Accreditation	http://static.e-publishing.af.mil/production/1/saf_cio_a6/publication/afi17-101/afi17-101.pdf
AFI 17-130, Air Force Cybersecurity Program Management	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.	Information Assurance	http://static.e-publishing.af.mil/production/1/saf_cio_a6/publication/afi33-200/afi33-200.pdf

AFI 17-140, Air Force Architecting	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.	Enterprise Architecture	http://static.e-publishing.af.mil/production/1/saf_cio_a6/publication/afi17-140/afi17-140.pdf
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
AFI 31-501, Personnel Security Program Management	Use this instruction with the DOD Regulation 5200.2-R and AFPD 31-5 to implement the personnel security program. This instruction requires collecting and maintaining information protected by the Privacy Act of 1974 authorized by Executive Orders 9397, 9838, 10450, 11652, and 12968; and 5 United States Code (U.S.C.) 7513, 7532, 7533; 10 U.S.C. 8013.	Security Programs	http://static.e-publishing.af.mil/production/1/saf_aa/publication/afi31-501/afi31-501.pdf

AFI 32-10112 Installation GI&S (GeoBase)	This instructions convey guidance and procedures allowing commanders and Air Force professionals to maintain a flow of timely geospatial information with due regard for national security, accuracy, and privacy. Describe Geospatial Information and Services (GI&S) support for the installation and facilities mission, hereafter referred to as the GeoBase Program or GeoBase. Explain the organization and execution of the GeoBase Program for all levels of command. GI&S is the key platform for cross functional integration, and to that end this AFI provides guidance for those organizations seeking to integrate with the Geo-Base Service. Provide guidance and procedures for all Air Force military and civilian personnel that perform or utilize GeoBase functions, products or systems, including those in the Air National Guard and U.S. Air Force Reserve. This instruction is not intended to overlap or supersede GI&S guidance found in AFI 14-205, Geospatial Information and Services, 4 May 2004. Ensure that all records created as a result of processes prescribed in this publication are maintained in accordance with AFMAN 37-123, Management of Records and disposed of in accordance with the Air Force Records Disposition Schedule (RDS) located at https://afrims.amc.af.mil/. The use of the name or mark of any specific manufacturer, commercial product, commodity, or service in this publication	Misc (Energy Star, etc)	http://static.e-publishing.af.mil/production/1/af_a4_7/publication/afi32-10112/afi32-10112.pdf

AFI 33-332, Air Force Privacy and Civil Liberties Program	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.	Records and Document Mgt	http://static.e-publishing.af.mil/production/1/saf_cio_a6/publication/afi33-332/afi33-332.pdf
AFI 33-364, Records Disposition Procedures and Responsibilities	Records Dispostion Procedures	Records and Document Mgt	http://static.e-publishing.af.mil/production/1/saf_cio_a6/publication/afi33-364/afi33-364.pdf
AFI 33-580, Spectrum Management	This instruction establishes guidance and procedures for Air Force-wide management and use of the electromagnetic spectrum and implements Department of Defense Instruction (DoDI) 4650.01, Policy and Procedures for Management and Use of the Electromagnetic Spectrum; DoDI 8320.05, Electromagnetic Spectrum Data Sharing; National Telecommunications and Information Administration (NTIA) Manual of Regulations and Procedures for Federal Radio Frequency Management; Air Force Policy Directive (AFPD) 33-5, Warfighting Integration; and the procedures established by the Joint Staff J65A United States Military Communications-Electronics Board (USMCEB).	Network	http://static.e-publishing.af.mil/production/1/saf_cio_a6/publication/afi33-580/afi33-580.pdf

AFI 36-2201, Air Force Training Program	. This Air Force Instruction (AFI) applies to Total Force – Active Duty, Air Force Reserve, Air National Guard (ANG), and Department of Air Force Civilian. Ensure that all records created as a result of processes prescribed in this publication are maintained in accordance with AFMAN 33-363, Management of Records, and disposed of in accordance with the Air Force Records Disposition Schedule (RDS) located athttps://www.my.af.mil/afrims/afrims/afrims/rims.cfm. Refer recommended changes and questions about this publication to the Office of Primary Responsibility (OPR) using the AF IMT 847, Recommendation for Change of Publication; route AF IMT 847s from the field through Major Commands (MAJCOMS) publications/forms managers.	Information Mgt	http://static.e-publishing.af.mil/production/1/af_a1/publication/afi36-2201/afi36-2201.pdf
AFI 61-204, Disseminating Scientific and Technical Information	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	Records and Document Mgt	http://www.dtic.mil/dtic/pdf/stinfodocs/afi_61204.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 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/afman33-153.pdf
AFMAN 17-1301, 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/afman17-1301/afman17-1301.pdf

AFMAN 17-1303	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
AFMAN 33-145, Collaboration Services and Voice Systems Management	It establishes procedures and guidance for Collaboration Services including electronic collaboration and management of Video Teleconferencing (VTC) resources to include systems, equipment, personnel, time, and money and provides the directive guidance for Air Force VTC and voice systems management activities.	Network	http://static.e-publishing.af.mil/production/1/saf_cio_a6/publication/afman33-145/afman33-145.pdf

AFMAN 33-152 User Responsibilities and Guidance for Information Systems	This instruction implements Air Force Policy Directive (AFPD) 33-1, Information Resources Management, AFPD 33-2, Information Assurance (IA) Program, and identifies policies and procedures for the use of cyberspace support systems/services and compliance requirements of Secretary of the Air Force, Chief of Warfighting Integration and Chief Information Officer (SAF/CIO A6) managed programs. These programs ensure availability, interoperability, and maintainability of cyberspace support systems/services in support of Air Force mission readiness and warfighting capabilities. This manual applies to all Air Force military, civilians, contractor personnel under contract by the Department of Defense (DOD), and other individuals or organizations as required by binding agreement or obligation with the Department of the Air Force. This manual applies to the Air National Guard (ANG) and the Air Force Reserve Command (AFRC).	Network	http://static.e-publishing.af.mil/production/1/afmc/publication/afman33-152_afmcsup_i/afman33-152_afmcsup_i.pdf

AFMAN 33-363, Management of Records	This manual implements Department of Defense (DoD) Directive (DoDD) 5015.2, DoD Records Management Program, and Air Force Policy Directive (AFPD) 33-3, Information Management. It establishes the requirement to use the Air Force Records Information Management System (AFRIMS); establishes guidelines for managing all records (regardless of media); and defines methods and the format for record storage, file procedures, converting paper records to other media or vice versa, and outlines the minimum to comply with records management legal and policy requirements.	Records and Document Mgt	http://static.e-publishing.af.mil/production/1/saf_cio_a6/publication/afman33-363/afman33-363.pdf

AFMAN 33-402 - Service Development and Delivery Process (SDDP)	This Air Force Manual (AFMAN) provides guidance for the definition, design, acquisition, implementation and delivery of Business Mission Area (BMA) capabilities using the Service Development and Delivery Process (SDDP). The SDDP is end user-centric to better align the assistance required by an end user to address a process-based problem across a holistic set of Doctrine, Organization, Training, Materiel, Leadership and Education, Personnel, Facilities, and Policy (DOTMLPF-P) solutions. The SDDP details the processes and procedures by which Information Technology (IT) capabilities supporting Air Force (AF) processes are identified, defined, developed and delivered in a way that ensures IT capabilities are necessary, and maximize the potential for successful implementation of IT investments. The SDDP is applicable to large and small scale problems and can be used to implement IT capabilities of all sizes and types.	Life Cycle Mgt	http://static.e-publishing.af.mil/production/1/saf_mg/publication/afman33-402/afman33-402.pdf

AFPD 17-1 Information Dominance Governance and Management	This Air Force (AF) Policy Directive (PD) establishes AF policy for the governance and management of activities to achieve Information Dominance under the direction of the Chief of Information Dominance and Chief Information Officer (SAF/CIO A6). Information Dominance is defined as the operational advantage gained from the ability to collect, control, exploit, and defend information to optimize decision making and maximize warfighting effects	Information Mgt	http://static.e-publishing.af.mil/production/1/saf_cio_a6/publication/afpd17-1/afpd_17-1.pdf
AFPD 33-3, Information Management	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.	Information Mgt	http://static.e-publishing.af.mil/production/1/saf_cio_a6/publication/afpd33-3/afpd33-3.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
Best Practices for Acquiring IT as a Service	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.	Security Programs	http://disa.mil/Services/DoD-Cloud-Broker/~/media/Files/DISA/Services/Cloud-Broker/Creating-Effective-Cloud-Computing-Contracts-for-the-Federal-Government.pdf

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
Business and Enterprise Systems (BES) Process Directory	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	Life Cycle Mgt	https://acc.dau.mil/bes
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.dtic.mil/cjcs_directives/cdata/unlimit/6211_02a.pdf

CJCSI 6212.01F, Interoperability and Supportability of Information Technology and National Security Systems	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.	Certification & Accreditation	http://jitc.fhu.disa.mil/jitc_dri/pdfs/cjcsi_6212_01f.pdf
Class Deviation - Contracting for Cloud Services (DFARS 239.99/252.239-7999)	New requirements for contracting officers to follow in contracts, task orders, and delivery orders in acquisitions for, or that may involve cloud computing services.	NetCentric Strategy	http://www.acq.osd.mil/dpap/policy/policyvault/USA001321-15-DPAP.pdf

Cloud Computing Security Requirements Guide (SRG), Version 1	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.	NetCentric Strategy	http://iase.disa.mil/cloud_security/Documents/u-cloud_computing_srg_v1r1_final.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	

CNSSI 1253: Security Categorization and Controls Selection for National	Instruction serves as a companion document to NIST SP 800-53 for organizations that employ NSS.	Security Programs	http://disa.mil/Services/DoD-Cloud-Broker/~/media/Files/DISA/Services/Cloud-Broker/cnssi-security-categorization.pdf
CNSSI 4009: National Information Assurance (IA) Glossary	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.	Information Assurance	https://www.cnss.gov/CNSS/issuances/Instructions.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
Department of Defense (DoD) Information Technology (IT) Enterprise Strategy and Roadmap	In August 2010, the Secretary of Defense (SecDef) announced a Department of Defense (DoD)–wide Efficiencies Initiative to move America's defense institutions toward a —more efficient, effective, and cost-conscious way of doing business. 1 DoD Components were directed to conduct a —zero-based review of how they carry out their missions and of their priorities, and to rebalance resources to better align with DoD's most critical challenges and priorities. As part of the announcement, the SecDef directed consolidation of information technology (IT) infrastructure assets to achieve savings in acquisition, sustainment, and manpower costs and to improve DoD's ability to execute its missions while defending its networks against growing cyber threats.	NetCentric Strategy	http://dodcio.defense.gov/Portals/0/Documents/Announcement/Signed_ITESR_6SEP11.pdf

Department of Defense Architecture Framework (DoDAF) Ver2.02 Aug 2010	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.	Enterprise Architecture	http://dodcio.defense.gov/Library/DoD-Architecture-Framework/
DFARS 252.227-7013 Rights in Technical Data---Non-commercial Items	Provides guidelines for rights in technical data on non-commercial items	FAR	http://farsite.hill.af.mil/reghtml/regs/far2afmcfars/fardfars/dfars/dfars252_227.htm
DFARS 252.227-7014 Rights in Noncommercial Computer Software	Guidance on rights in technical data and computer software small business innovation research (SBIR) program.	FAR	http://farsite.hill.af.mil/reghtml/regs/far2afmcfars/fardfars/dfars/dfars252_227.htm

DFARS 252.227-7015 Technical Data Commercial Items	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.	FAR	http://farsite.hill.af.mil/reghtml/regs/far2afmcfars/fardfars/dfars/dfars252_227.htm
DFARS 252.227-7017 Identification and Assertion of Use, Release, or Disclosure Restrictions	Provides requirements for the identification and assertion of technical data.	FAR	http://farsite.hill.af.mil/reghtml/regs/far2afmcfars/fardfars/dfars/dfars252_227.htm
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

DoD 4140.1-R, DoD Supply Chain Materiel Management Regulation	This Regulation implements DoD Directive 4140.1 and establishes requirements and procedures for DoD materiel managers and others who need to work within or with the DoD supply system. This Regulation presents DoD logistics personnel with a process-based view of materiel management policy within a supply chain framework.	Supply Chain	http://www.acq.osd.mil/log/sci/exec_info/drid/p41401r.pdf
DoD 5220.22-M, National Industrial Security Program Operating Manual	Provides baseline standards for the protection of classified information released or disclosed to industry in connections with classified contracts under the National Idustrial Security Program.	Security Programs	http://www.dss.mil/documents/odaa/nispom2006-5220.pdf
DoD 8570.01-M, Information Assurance Workforce Improvement Program	Provides guidance for the identification and categorization of positions and certification of personnel conducting Information Assurance (IA) functions within the DoD workforce supporting the DoD Global Information Grid (GIG) per DoD Instruction 8500.2. The DoD IA Workforce includes, but is not limited to, all individuals performing any of the IA functions described in this Manual. Additional chapters focusing on personnel performing specialized IA functions including certification and accreditation (C&A) and vulnerability assessment will be published as changes to this Manual.	Information Assurance	http://www.dtic.mil/whs/directives/corres/pdf/857001m.pdf
DoD Chief Information Officer Cloud Computing Strategy	This strategy is to enable the Department to increase secure information sharing and collaboration, enhance mission effectivness, and decrease costs using cloud services.	NetCentric Strategy	http://dodcio.defense.gov/Portals/0/Documents/Cloud/DoD%20Cloud%20Computing%20Strategy%20Final%20with%20Memo%20-%20July%205%202012.pdf

DoD Discovery Metadata Specification (DDMS) 5.0	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.	Metadata	https://metadata.ces.mil/dse/irs/DDMS/
DoD Global Information Grid Architectural Vision	The security challenges of the 21st century are characterized by change and uncertainty. Operations vary widely and partners cannot be anticipated. However, we are confronting that uncertainty by becoming more agile. Greater levels of agility rest upon leveraging the power of information, the centerpiece of today's Defense transformation to net-centric operations (NCO). Our forces must have access to timely and trusted information. And, we must be able to quickly and seamlessly share information with our partners, both known and unanticipated. The GIG Architectural Vision is key to creating the information sharing environment and will be critical to transformation to NCO.	GIG	http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA484389&Location=U2&doc=GetTRDoc
DoD Instructions, 8500 Series	DoD Issuances	Information Mgt	http://www.dtic.mil/whs/directives/corres/ins1.html

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 Manual 5200.01, DoD Information Security Program: Overview, Classification, and Declassification, V1-V4	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).	Security Programs	http://www.dtic.mil/whs/directives/corres/pdf/520001_vol1.pdf
DoD Mobile Application Strategy	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.	Misc (Energy Star, etc)	http://archive.defense.gov/news/dodmobilitystrategy.pdf
DoD Net-Centric Data Strategy	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	NetCentric Strategy	http://dodcio.defense.gov/Portals/0/Documents/Net-Centric-Data-Strategy-2003-05-092.pdf

DoD Net-Centric Services Strategy	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.	NetCentric Strategy	http://dodcio.defense.gov/Portals/0/documents/DoD_NetCentricServicesStrategy.pdf
DoD Open Technology Development (OTD) Guide	This roadmap outlines a plan to implement OTD practices, policies and procedures within the DoD. It's a handbook for using and making open source in the DOD and the US Government, sponsored by the Secretary of Defense. It provides practical advice on policy, procurement, and good community governance, all under a Creative Commons license.	NetCentric Strategy	
DoDD 5205.02E, Operations Security (OPSEC) Program	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.	Security Programs	http://www.dtic.mil/whs/directives/corres/pdf/520502e.pdf
DoDD 8000.01 Management of the Department of Defense Information Enterprise	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	Information Mgt	http://www.dtic.mil/whs/directives/corres/pdf/800001p.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	http://www.dtic.mil/whs/directives/corres/pdf/810002p.pdf
DoDD 8140.01, Cyberspace Workforce Management	Reissue and renumber DoDD 8570.01 to update and expand establish polices and assigned responsibilities for managing the DoD cyberspace workforce.	Information Assurance	http://www.dtic.mil/whs/directives/corres/pdf/814001_2015_dodd.pdf
DoDD 8320.1Data Administration	This Instruction applies to the administration and standardization of DoD standard data elements generated within the functional areas of audit and criminal investigations for DoD. It also applies to the administration of DoD standard and non-standard data elements generated, stored, or used by the DoD. Data elements will be administered in ways that provide accurate, reliable, and easily accessible data throughout the DoD, while minimizing cost and redundancy. Data elements will be standardized to meet the requirements for data sharing and interoperability throughout the DoD. Data administration will be encouraged and promoted within the DoD.	Data	https://acc.dau.mil/adl/en-US/33650/file/6823/DoDD83201%20Data%20Admin.pdf

DoDI 1100.22 Policy and Procedures for Determining Workforce Mix	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).	Misc (Energy Star, etc)	http://www.dtic.mil/whs/directives/corres/pdf/110022p.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)	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	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	http://www.dtic.mil/whs/directives/corres/pdf/501502p.pdf
DoDI 5230.24, Distribution Statements on Technical Documents	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.	Records and Document Mgt	http://www.dtic.mil/whs/directives/corres/pdf/523024p.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	http://www.dtic.mil/whs/directives/corres/pdf/832002p.pdf
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.dtic.mil/whs/directives/corres/pdf/832004p.pdf

DoDI 8330.01 Interoperability of Information Technology (IT), Including National Security Systems (NSS)	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)).	Enterprise Architecture	http://www.dtic.mil/whs/directives/corres/pdf/833001p.pdf
DoDI 8500.01 Cybersecurity	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	Information Assurance	http://www.dtic.mil/whs/directives/corres/pdf/850001_2014.pdf

DoDI 8510.01,Risk Management Framework (RMF) for DoD Information Technology (IT)	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.	Information Assurance	http://www.dtic.mil/whs/directives/corres/pdf/851001_2014.pdf
DoDI 8520.02 Public Key Infrastructure (PKI) and Public Key (PK) Enabling	This instruction establishes and implements policy, assign responsibilities, and prescribe procedures for developing and implementing a DoD-wide PKI and enhancing the security of DoD information systems by enabling these systems to use PKI for authentication, digital signatures, and encryption.	Encryption	http://www.dtic.mil/whs/directives/corres/pdf/852002p.pdf
DoDI 8530.01, Cybersecurity Activities Support to DoD Information Network Operations	Reissues DoDD O-8530.1 (Reference (b)) as a DoD Instruction (DoDI) and incorporates and cancels DoDI O-8530.2)Reference to establish policy and assign responsibilities to protect the Department of Defense information network (DoDIN) against unauthorized activity, vulnerabilities, or threats.	Security Programs	http://www.dtic.mil/whs/directives/corres/pdf/853001p.pdf
DoDI 8540.01, Cross Domain (CD) Policy	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	http://www.dtic.mil/whs/directives/corres/pdf/854001p.pdf

DoDI 8551.01, Ports, Protocols, and Services Management (PPSM)	This instruction reissues DoDI 8551.1	Network	http://www.dtic.mil/whs/directives/corres/pdf/855101p.pdf
Electronic Biometric Transmission Specifications Version 3.0	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.	Product Standards	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)	http://www.dtic.mil/whs/directives/corres/pdf/417011p.pdf For FAR 23.704: https://www.acquisition.gov/far/current/html/Subpart%2023_7.html
Executive Order 13526: 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.	Security Programs	http://www.whitehouse.gov/the-press-office/executive-order-classified-national-security-information

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) 2002	FISMA was enacted as part of the E-Government Act of 2002 to "provide a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support Federal operations and assets," and also to "provide for development and maintenance of minimum controls required to protect Federal information and information systems." FISMA requires Federal agencies to: •designate a Chief Information Officer (CIO), •delegate to the CIO authority to ensure compliance with the requirements imposed by FISMA, •implement an information security program, •report on the adequacy and effectiveness of its information security policies, procedures, and practices, •participate in annual independent evaluations of the information security program and practices, and •develop and maintain an inventory of the agency's major information systems.	Security Programs	http://www.dhs.gov/federal-information-security-management-act-fisma

FedRAMP Security Controls for Cloud Service Providers	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 Prodivders. 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	http://www.fedramp.gov/resources/documents-2016/
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 199: Standards for Security Categorization of Federal Information and Information Systems	This publications is to develop standards for categorizing information and information systems.	Security Programs	http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf

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
ICD 503 Intelligence Community Information Technology Systems Security Risk Management, Certification and Accreditation	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.	Certification & Accreditation	https://www.nstii.com/courses/systems-security-practitioners-course-sspc/

IEEE/EIA 12207.0, "Standard for Information Technology	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.	Life Cycle Mgt	http://IEEE.org
Industry Best Practices in Achieving Service Oriented Architecture (SOA)	This document was developed under the NetCentric Operations Industry Forum's charter to provide industry advisory services to the DoD, CIO. It presents a list of industry best practices in achieving Service Oriented Architecture (SOA).	NetCentric Strategy	http://www.sei.cmu.edu/library/assets/soabest.pdf

Interim Guidance Memorandum on Use of Commercial Cloud Computing Services	This Memorandum serves to reinforce existing policy and processes, and is in effect for all DoD networks and systems.	NetCentric Strategy	http://www.disa.mil/Services/DoD-Cloud-Broker/~/media/Files/DISA/Services/Cloud-Broker/Interim-Guidance-Memo-on-Use-of-Commerical-Cloud-Computing-Services.pdf
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
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	http://www.iso.org/iso/home/store/catalogue_ics/catalogue_detail_ics.htm?csnumber=65666
ISO/IEC 20000	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 seperate documents, ISO/IEC 20000-1 through 20000-5	Misc (Energy Star, etc)	http://www.iso.org/iso/home.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
Military Standards, Specifications, and Regulations (MIL-STDs, DoD-STDs).	The Acquisition Streamlining and Standardization Information System (ASSIST) is a database system for DOD-wide standardization document information management. The ASSIST database resides at the Department of Defense Single Stock Point for Military Specifications and Standards (DODSSP), located at DAPS, Philadelphia. The ASSIST-Online is a robust, comprehensive web site providing access to current information associated with military and federal specifications and standards in the management of the Defense Standardization Program (DSP), managed by the DoD Single Single Stock Point (DODSSP), Philadelphia, ASSIST-Online provides public access to standardization documents over the Internet. ASSIST-Online includes many powerful reporting features and an exhaustive collection of both digital and warehouse documents.	Product Standards	https://assist.dla.mil/online/start/
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

Netcentric Enterprise Solutions for Interoperability (NESI)	NESI is a body of architectural and engineering knowledge that guides the design, implementation, maintenance, evolution, and use of the Information Technology (IT) portion of net-centric solutions for defense application.	NetCentric Strategy	https://nesix.spawar.navy.mil/home.html
NIST SP 500-292: Cloud Computing Reference Architecture	Overview of the five major roles & responsibilities using the Cloud Computing Taxonomy.	Security Programs	http://disa.mil/Services/DoD-Cloud-Broker/~/media/Files/DISA/Services/Cloud-Broker/nist-cloud-ref-architecture.pdf
NIST SP 800-122:Guide to Protecting the Confidentiality of Personality Identifiable Information (PII)	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.	Security Programs	https://doi.org/10.6028/NIST.SP.800-122
NIST SP 800-144:Guidelines on Security and Privacy in Public Cloud Computing	The primary purpose of this report is 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 arrangment, service agreement, service provider, or deployment model.	NetCentric Strategy	http://csrc.nist.gov/publications/nistpubs/800-144/SP800-144.pdf

NIST SP 800-145: Definition of Cloud Computing	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.	Security Programs	http://disa.mil/Services/DoD-Cloud-Broker/~/media/Files/DISA/Services/Cloud-Broker/NIST-SP800145-DefinitionofCloudComputing.pdf
NIST SP 800-146: Cloud Computing Synopsis & Recommendations	NIST explains the cloud computing technology and provides recommendations for information technology decision makers.	Security Programs	http://disa.mil/Services/DoD-Cloud-Broker/~/media/Files/DISA/Services/Cloud-Broker/nist-cloud-synopsis.pdf
NIST SP 800-37:Guidelines for Applying the Risk Management Framework to Federal Information Systems	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.	Security Programs	http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf
NIST SP 800-53: Security and Privacy Controls for Federal Information Systems and Organizations	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.	Security Programs	http://disa.mil/Services/DoD-Cloud-Broker/~/media/Files/DISA/Services/Cloud-Broker/NIST-SP80053-SecurityandPrivacyControls.pdf
NIST SP 800-59:Guideline for Identifying an Information System as a National Security System	The purpose of these guidelines is to assist agencies in determining whicy, 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.	Security Programs	http://dx.doi.org/10.6028/NIST.SP.800-59

NIST SP 800-66:An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rulie	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.	Security Programs	http://dx.doi.org/10.6028/NIST.SP.800-66r1
NIST SP 800-88 Revision 1:Guidelines for Media Sanitization	This guide will assist organizations and system owners in making practical sanitization decisions based on the categorization of confidentiality of their information.	Records and Document Mgt	http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf

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	https://sgftrlek.files.wordpress.com/2015/07/nstissam-tempest-1-92-pdf.pdf
Radio Frequency Identification (RFID)	Standards and Specification information regarding passive Radio Frequency Identification (RFID).	Product Standards	DoD Standard Practice Military Marking for Shipping and Storage

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
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	http://dx.doi.org/10.6028/NIST.IR.7622

Security Technical Implementation Guides (STIGs)	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.	Security Programs	http://iase.disa.mil/stigs/Pages/index.aspx
Security Technical Implementation Guides (STIGs) CJCSI 6510.01F Information Assurance (IA) AND Support To Computer Network DEFENSE (CND)	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.	Security Programs	http://www.dtic.mil/cjcs_directives/cdata/unlimit/6510_01.pdf
TIA/EIA-TSB-72, Centralized Optical Fiber Cabling Guidelines	Must Be Purchased	Network	http://www.tiaonline.org/

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

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	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/