NETCENTS-2 Standards and Policies

November 2018

Reference	Authority	Description	Applicable IDIQ	Category	Sub-Category	Link to Guidance
Acquisition Streamlining and Standardization Information System (ASSIST)	Other Guidance	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.	App Svs, NetOps	Operational Mgt	Informational	https://assist.dla.mil/online/start/
AF Instruction 10-208, Air Force Continuity of Operations (COOP) Program	AFI/AFMAN	This instruction provides guidance for ensuring the continuity of essential operations of the Air Force across a wide range of potential emergencies. Continuity requirements must be incorporated into the daily operations of organizations to ensure seamless and immediate continuation of essential functions during and after a wide range of emergencies, including local or regional natural disasters, health-related emergencies, man-made disasters, accidents, technological limitations or attack-related emergencies.	App Svs, NetOps	Operational Mgt	Lifecycle Management	https://static.e-publishing.af.mil/production/1/af_a3/publication/afi10-208/afi10-208.pdf
AF Instruction 10-601, Operational Capability Requirements Development	AFI/AFMAN	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.	App Svs, NetOps	Operational Mgt	Lifecycle Management	https://static.e-publishing.af.mil/production/1/af_a3_5/publication/afi10-601/afi10-601.pdf
AF Instruction 10-701, Operations Security (OPSEC) (Note mandatory AFGM2018-01 prepended to AFI 10-701)	AFI/AFMAN	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.	App Svs, NetOps	Operational Mgt	Data Security	http://static.e-publishing.af.mil/production/1/af_a3/publication/afi10-701/afi10-701.pdf
AF Instruction 16-1404, Air Force Information Security Program	AFI/AFMAN	This instruction implements DoDD 5210.50 and outlines procedures for Information Protection which is a subset of the Air Force Security Enterprise. Information Protection consists of a set of three core security disciplines: Personnel, Industrial, and Information Security and is used to: -Determine military, civilian, and contractor personnel's eligibility to access classified information or occupy a sensitive position (Personnel Security).-Ensure the protection of classified information and controlled unclassified information (CUI) released or disclosed to industry in connection with classified contracts (Industrial Security).-Protect classified information and CUI that, if subject to unauthorized disclosure, could reasonably be expected to cause damage to national security (Information Security).	App Svs, NetOps	Operational Mgt	Data Security	http://static.e-publishing.af.mil/production/1/saf_aa/publication/afi16-1404/afi16-1404.pdf
AF Instruction 17-101, Risk Management Framework (RMF) for Air Force Information Technology (IT) (Note mandatory AFGM2018-01 prepended to AFI 17-101)	AFI/AFMAN	This AFI provides implementation instructions for the Risk Management Framework (RMF) methodology for Air Force (AF) Information Technology (IT) according to AFPD 17-1, Information Dominance Governance and Management, and AFI 17-130, Air Force Cybersecurity Program Management, which is only one component of cybersecurity.	App Svs, NetOps	Cybersecurity	Risk Management Framework	http://static.e-publishing.af.mil/production/1/saf_cio_a6/publication/afi17-101/afi17-101.pdf
AF Instruction 17-130, Air Force Cybersecurity Program Management (Note mandatory AFGM2018-01 prepended to AFI 17-130)	AFI/AFMAN	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.	App Svs, NetOps	Cybersecurity	Overarching Guidance	http://static.e-publishing.af.mil/production/1/saf_cio_a6/publication/afi17-130/afi17-130.pdf
AF Instruction 17-140, Air Force Architecting	AFI/AFMAN	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.	App Svs, NetOps	Cybersecurity	Architecture	http://static.e-publishing.af.mil/production/1/saf_cio_a6/publication/afi17-140/afi17-140.pdf
AF Instruction 17-210, Radio Management (Note mandatory AFGM2018-01 prepended to AFI 17-210)	AFI/AFMAN	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. Previous AFI 33 590 superseded by AFI 17-210.	App Svs, NetOps, Products	Products Standards	UC Compliance	http://static.e-publishing.af.mil/production/1/saf_cio_a6/publication/afi17-210/afi17-210.pdf
AF Instruction 17-220, Spectrum Management (Note mandatory AFGM2018-01 prepended to AFI 17-220)	AFI/AFMAN	This instruction establishes guidance and procedures for Air Force-wide management and use of the electromagnetic spectrum. It identifies various levels of responsibilities for supporting specturm dependent equipment in support of AF activities.	App Svs, NetOps	Cybersecurity	Spectrum Management	http://static.e-publishing.af.mil/production/1/saf_cio_a6/publication/afi17-220/afi17-220.pdf

NOTE: Depending on your computing environment, some URL's may not execute properly. In this case, copy/paste the entire URL into the address bar of a browser.

AF Instruction 32-10112, Installation IGI&S (GeoBase)	AFI/AFMAN	This instruction conveys 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. This instruction is not intended to overlap or supersede GI&S guidance found in AFI 14-205, Geospatial Information and Services, 4 May 2004.	App Svs, NetOps	Operational Mgt	Geospatial	https://static.e-publishing.af.mil/production/1/af_a4/publication/afi32-10112/afi32-10112.pdf
AF Instruction 33-115, Air Force Information Technology (IT) Service management (AFI's 33-115 and 17-100 have both been superseded by AFGM2018-17-02)	AFI/AFMAN	This instruction defines AF IT Service Management and assigns responsibilities for the configuration, provisioning, maintenance, and management of AFIN using an IT Service Management (ITSM) framework to further integrate capabilities and maintain configuration control of AF networks and data servers. This instruction serves as the single reference for AF IT Service Management policy and applies to all personnel who manage, configure, operate, maintain, defend, or extend any portion of the AFIN or provide support within the AF for the DoDIN and the Joint Information Environment (JIE).	App Svs, NetOps	Cybersecurity	IT Management	https://static.e-publishing.af.mil/production/1/saf_cio_a6/publication/afgm2018-17-02/afgm2018-17-02.pdf
AF Instruction 33-332, Air Force Privacy and Civil Liberties Program	AFI/AFMAN	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.	App Svs, NetOps	Operational Mgt	Data Security	http://static.e-publishing.af.mil/production/1/saf_cio_a6/publication/afi33-332/afi33-332.pdf
AF Instruction 33-364, Records Disposition - Procedures and Responsibilities (Note mandatory AFGM2018-01 prepended to AFI 33-364)	AFI/AFMAN	In the Air Force, economical and efficient records management involves scheduling all records for retention or periodic destruction, preserving records that reflect the organization, functions, policies, decisions, procedures, and essential transactions of the Air Force, preserving records that protect the legal and financial rights of the Government and of individuals that Air Force actions directly affect, offering records of enduring value for permanent preservation in the National Archives, promptly and systematically disposing of records of temporary value, and setting up safeguards against illegal removal, loss, or destruction of records.	App Svs, NetOps	Operational Mgt	Data Security	http://static.e-publishing.af.mil/production/1/saf_cio_a6/publication/afi33-364/afi33-364.pdf
AF Instruction 36-2201, Air Force Training Program	AFI/AFMAN	This instruction implements policies, procedures and standards for delivering training programs and course content.	App Svs, NetOps	Operational Mgt	Application Development	http://static.e-publishing.af.mil/production/1/af_a1/publication/afi36-2201/afi36-2201.pdf
AF Instruction 61-201, Scientific, Research and Development Management of Scentific and Technical Information (STINFO)	AFI/AFMAN	This instruction establishes guidance and procedures to manage STINFO throughout the acquisition life cycle. The purpose of this instruction is to maximize the availability, interchange, and collaboration of STINFO to policy makers, the acquisition community, and public while safeguarding it within the bounds of law, regulation, other directives and executive requirements. It incorporates updated Department of Defense (DoD) policy and consolidates numerous Air Force instructions (AFI61-201, 61-202, 61-203, 61-204, and 61-205) to provide greater clarity concerning the processes and responsibilities of managing Air Force scientific and technical information.	App Svs, NetOps	Operational Mgt	Data Security	http://static.e-publishing.af.mil/production/1/saf_aq/publication/afi61-201/afi61-201.pdf
AF Instruction 63-101/20-101, Integrated Life Cycle Management	AFI/AFMAN	This instruction applies to the management of all acquisition programs (e.g., weapons systems, national security systems and defense business systems) as denoted on the Acquisition Master List, all investment-funded activities (product groups, systems, activities, services, and projects) in any phase of the lifecycle, and Legacy programs in the O&S Phase not previously on the AML.	App Svs, NetOps, Products	Operational Mgt	Lifecycle Management	http://static.e-publishing.af.mil/production/1/saf_aq/publication/afi63-101_20-101/afi63-101_20-101.pdf
AF Instruction 99-103, Capabilities-Based Test and Evaluation	AFI/AFMAN	It describes the planning, conduct, and reporting of cost effective test and evaluation (T&E) programs as an efficient continuum of integrated testing known as seamless verification. The overarching functions of T&E are to mature sys-tem designs, manage risks, identify and help resolve deficiencies as early as possible, and ensure systems are operationally mission capable (i.e., effective and suitable). The Air Force T&E community plans for and conducts integrated testing as an efficient continuum known as seamless verification in collaboration with the requirements and acquisition communities.	App Svs, NetOps	Operational Mgt	Lifecycle Management	http://static.e-publishing.af.mil/production/1/af_te/publication/afi99-103/afi99-103.pdf
AF Manual 10-206, Operational Reporting	AFI/AFMAN	The Air Force requires a single Emergency Mass Notification System (EMNS)to alert and warn 100% of assigned forces quickly and effectively of an emergent event. The EMNS is used for command and control (C2) of an installation's forces and assets, with primary resources used during: Increased Force Protection Measures (FPCONs), Information Protection Implementation, Wing Recall, Force Generation, Crisis Action Team (CAT) Recall/Relocation, Personnel Accountability and Emergency Mass Notification (i.e. Active Shooters, Chemical, Biological, Radiological and Nuclear (CBRN) incidents, Natural disasters, etc). This applies to Network Alerting Systems, Telephone Alerting Systems, Giant Voice, Smart Device Applications, Cloud Solutions and Turnkey systems.	App Svs, NetOps	Operational Mgt	Mass Notification	http://static.e-publishing.af.mil/production/1/af_a3/publication/afman10-206/afman10-206.pdf
AF Manual 16-1405/DoD Manual 5200.02, Air Force Personnel Security Program	AFI/AFMAN	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.	App Svs, NetOps	Operational Mgt	Workforce Management	http://static.e-publishing.af.mil/production/1/saf_aa/publication/dodman5200.02_afman16-1405/dodm5200.02_afman16-1405.pdf

AF Manual 17-1203, Information Technology (IT) Asset Management (ITAM)	AFI/AFMAN	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).	App Svs, NetOps, Products	Cybersecurity	Asset Management	http://static.e-publishing.af.mil/production/1/saf_cio_a6/publication/afman17-1203/afman17-1203.pdf
AF Manual 17-1301, Computer Security (COMPUSEC)	AFI/AFMAN	Computer Security (COMPUSEC) is a cybersecurity discipline identified in AFI 17-130. Compliance ensures appropriate implementation of measures to protect all AF Information System (IS) resources and information. The COMPUSEC objective is to employ countermeasures designed for the protection of confidentiality, integrity, availability, authentication, and non-repudiation of United States (US) government information processed by AF ISs. This publication applies to all AF ISs and devices used to process, store, display, transmit, or protect AF information, regardless of classification or sensitivity, unless exempted.	App Svs, NetOps, Products	Cybersecurity	Information System Security	http://static.e-publishing.af.mil/production/1/saf_cio_a6/publication/afman17-1301/afman17-1301.pdf
AF Manual 17-1303, Cybersecurity Workforce Improvement Program (previously AFMAN 33-285)	AFI/AFMAN	The primary objective of the Air Force (AF) Cybersecurity Workforce Improvement Program (WIP) is to train, educate, certify, and qualify personnel commensurate with their responsibilities to develop, use, operate, administer, maintain, defend, and dispose/retire DoD Systems. All authorized users of DoD information systems (ISs)/Platform Information Technology (PIT) systems must receive initial cybersecurity user awareness training as a condition of access to an IS IAW DoD 8570.01-M, Paragraph C6.2.2.; thereafter, all users will complete annual cybersecurity awareness refresher training. This manual also identifies AF cybersecurity workforce positions, certification and qualifications requirements, and provides policy on cybersecurity workforce reporting, metrics and validation Unless noted, the cybersecurity position requirements (e.g. certification, training, etc.) specified in this manual are the minimum required.	App Svs, NetOps, Products	Cybersecurity	Workforce Management	http://static.e-publishing.af.mil/production/1/saf_cio_a6/publication/afman17-1303/afman17-1303.pdf
AF Manual 33-363, Management of Records (Note mandatory AFGM2018-01 prepended to AFI 33-363)	AFI/AFMAN	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.	App Svs, NetOps	Operational Mgt	Data Security	http://static.e-publishing.af.mil/production/1/saf_cio_a6/publication/afman33-363/afman33-363.pdf
AF Pamphlet 63-128, Integrated Life Cycle Management	AFI/AFMAN	This guidance expands upon the directive requirements in AFI 63-101/20-101; it is not meant to be used as directive guidance but instead conveys expectations, best practices, lessons learned and other descriptive information to help a program manager (PM) initiate and expedite the development and delivery of systems in accordance with Integrated Lifecycle Management. This guidance also addresses Item Unique Identification (IUID) implementation plans.	Products	Operational Mgt	Lifecycle Management	http://static.e-publishing.af.mil/production/1/saf_aq/publication/afpam63-128/afpam63-128.pdf
AF Policy Directive 16-14, Security Enterprise Governance	AFI/AFMAN	This directive establishes Air Force policy and responsibilities for the oversight, management and execution of the Air Force Security Enterprise. This directive provides laws and overarching guidance that governs information and personnel security programs.	App Svs, NetOps	Operational Mgt	Overarching Guidance	http://static.e-publishing.af.mil/production/1/saf_aa/publication/afpd16-14/afpd16-14.pdf
AF Policy Directive 17-1, Information Dominance Governance and Management	AFI/AFMAN	This directive 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.	App Svs, NetOps	Cybersecurity	IT Management	http://static.e-publishing.af.mil/production/1/saf_cio_a6/publication/afpd17-1/afpd_17-1.pdf
AF Policy Directive 33-3, Information Management	AFI/AFMAN	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.	App Svs, NetOps	Cybersecurity	Data Security	http://static.e-publishing.af.mil/production/1/saf_cio_a6/publication/afpd33-3/afpd33-3.pdf
ANSI/TIA/EIA-568.n (n=0,1,2,3,4) - Commercial Building Telecommunications Cabling Standards	Other Guidance	Provides best practices for fiber and cable solutions. Must Be Purchased.	NetOps	Operational Mgt	Guidance	https://www.tiaonline.org/what-we-do/standards/buy-standards/
Automated Identification Technology (AIT)	Other Guidance	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.	Products	Products Standards	Supply Chain Management	https://www.acq.osd.mil/log/sci/ait.html
Business and Enterprise Systems (BES) Process Directory	Other Guidance	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.	App Svs, NetOps	Operational Mgt	Lifecycle Management	https://www.dau.mil/cop/bes/Pages/Default.aspx
CJCSI 6211.02D, Defense Information Systems Network Responsibilities	CJCSI	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).	App Svs, NetOps, Products	Cybersecurity	UC Compliance	http://www.jcs.mil/Portals/36/Documents/Library/Instructions/6211_02a.pdf?ver=2016-02-05-175050-653?ver=2016-02-05-175050-653

CJCSI 6510.01F, Information Assurance (IA) and Support To Computer Network Defense (CND)	CJCSI	This instruction provides guidance on foreign national access to information systems, portable electronic devices, internet access, commercial e-mail, sanitization and declassification of information system storage media. This instruction outlines encryption requirements governed by FIPS 140-2.	NetOps	Operational Mgt	Information System Security	http://www.jcs.mil/Library/CJCS-Instructions/
Cloud Computing, Best Practices for Acquiring IT as a Service	Other Guidance	This guide enables Federal agencies to make smarter, more informed cloud purchasing decisions by utilizing lessons learned and best practices of early adopters to move to a more efficient and more effective government.	NetOps	Cloud Computing	Guidance	https://s3.amazonaws.com/sitesusa/wp-content/uploads/sites/1151/2016/10/cloudbestpractices.pdf
CNSSAM TEMPEST/1-13 RED/BLACK Installation Guidance (Requires CAC/PIV certificate)	CNSSI/CNSSP	This document defines the guidance for the design of facilities and the installation of equipment andsystems that receive, transmit, route, switch, manipulate, graph, store, archive, calculate, generate, print,scan, or in any other manner process or transfer National Security Information (NSI). This guidance ispart of the potential solution for facilities, systems and equipment identified as requiring TEMPESTcountermeasures. Additional TEMPEST countermeasures, including facility and/or equipment shieldingmay also be a part of a potential solution, but is beyond the scope of this document.	NetOps, Products	Products Standards	TEMPEST	https://www.cnss.gov/CNSS/issuances/Memoranda.cfm
CNSSI 1253, Security Categorization and Control Selection for National Security Systems	CNSSI/CNSSP	This instruction serves as a companion document to NIST SP 800-53 for organizations that employ NSS. It provides guidelines for selecting and specifying security controls for information systems supporting the federal government to meet the requirements of FIPS 200.	NetOps	Operational Mgt	Information System Security	http://www.dss.mil/documents/CNSSI_No1253.pdf
Committee on National Security Systems (CNSS) Instruction 4009, Committee on National Security Systems (CNSS) Glossary	CNSSI/CNSSP	Resolves differences between the definitions of terms used by the Department of Defense (DoD), Intelligence Community (IC), and Civil Agencies (e.g. National Institute of Standards and Technology (NIST)); enabling all three to use the same glossary. This will allow for use of consistent terminology in documentation, policy, and process across these communities.	NetOps	Cybersecurity	Guidance	https://www.cnss.gov/CNSS/issuances/Instructions.cfm
Committee on National Security Systems (CNSS) Policy 11, National Policy Governing the Acquisition of Information Assurance (IA) and IA-Enabled Information Technology Products	CNSSI/CNSSP	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.	Products	Products Standards	Security	https://www.cnss.gov/CNSS/issuances/Policies.cfm
Committee on National Security Systems (CNSS) Policy 19, National Policy Governing the Use of High Assurance Internet Protocol Encryptor (HAIPE) Products	CNSSI/CNSSP	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.	Products	Products Standards	Encryption	https://www.cnss.gov/CNSS/issuances/Policies.cfm
Department of Defense (DoD) Information Technology (IT) Enterprise Strategy and Roadmap	Other Guidance	In August 2010, the SecDef announced a 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.	App Svs, NetOps	Operational Mgt	NetCentric Strategy	http://dodcio.defense.gov/Portals/0/Documents/Announcement/Signed_ITESR_6SEP11.pdf
Department of Defense Architecture Framework (DoDAF) Ver2.02 Aug 2010	Other Guidance	This standard is the overarching, comprehensive framework and conceptual model enabling the development of architectures to facilitate the ability of DoD managers at all levels to make key decisions more effectively through organized information sharing. DoD Components are expected to conform to DoDAF to the maximum extent possible in development of architectures within the Department. Conformance ensures that reuse of information, architecture artifacts, models, and viewpoints can be shared with common understanding. Conformance is expected in both the classified and unclassified communities, and further guidance will be forthcoming on specific processes and procedures for the classified architecture development efforts in the Department.	App Svs, NetOps	Operational Mgt	Architecture	http://dodcio.defense.gov/Library/DoD-Architecture-Framework/
Department of Homeland Security, National Cybersecurity and Communications Integration Center (NCCIC), Industrial Control Systems	Other Guidance	NCCIC ICS works to reduce risks within and across all critical infrastructure sectors by partnering with law enforcement agencies and the intelligence community and coordinating efforts among Federal, state, local, and tribal governments and control systems owners, operators, and vendors. Additionally, NCCIC collaborates with international and private sector Computer Emergency Response Teams (CERTs) to share control systems-related security incidents and mitigation measures.	App Svs, NetOps	Cybersecurity	Security	https://ics-cert.us-cert.gov/
DFARS 239.99/252.239-7999 - Class Deviation - Contracting for Cloud Services	FAR/DFARS	New requirements for contracting officers to follow in contracts, task orders, and delivery orders in acquisitions for, or that may involve cloud computing services.	NetOps	Cloud Computing	Acquisition	http://www.acq.osd.mil/dpap/policy/policyvault/USA001321-15-DPAP.pdf
DFARS 252.225.7021 Trade Agreements	FAR/DFARS	Identifies situations when a contractor can deliver non-U.S. made, qualifying country, or designated country end products: (c) The Contractor shall deliver under this contract only U.S.-made, qualifying country, or designated country end products unless—(1) In its offer, the Contractor specified delivery of other nondesignated country end products in the Trade Agreements Certificate provision of the solicitation; and(2)(i) Offers of U.S.-made, qualifying country, or designated country end products from responsive, responsible offerors are either not received or are insufficient to fill the Government's requirements; or (ii) A national interest waiver has been granted.	Products	Products Standards	Acquisition	http://farsite.hill.af.mil/vmdfara.htm
DFARS 252.227-7013 Rights in Technical Data---Non-commercial Items	FAR/DFARS	Provides guidelines for rights in technical data on non-commercial items.	App Svs, NetOps	Operational Mgt	Data Rights	http://farsite.hill.af.mil/reghtml/regs/far2afmcfars/fardfars/dfars/dfars252_227.htm

DFARS 252.227-7014 Rights in Noncommercial Computer Software	FAR/DFARS	Guidance on rights in technical data and computer software small business innovation research (SBIR) program.	App Svs, NetOps	Operational Mgt	Data Rights	http://farsite.hill.af.mil/reghtml/regs/far2afmcfars/fardfars/dfars/dfars252_227.htm
DFARS 252.227-7015 Technical Data Commercial Items	FAR/DFARS	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.	App Svs, NetOps	Operational Mgt	Data Rights	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	FAR/DFARS	Provides requirements for the identification and assertion of technical data.	App Svs, NetOps	Operational Mgt	Data Rights	http://farsite.hill.af.mil/reghtml/regs/far2afmcfars/fardfars/dfars/dfars252_227.htm
DFARS 252.239-7017 Notice of Supply Chain Risk (DEVIATION 2018-O0020)	FAR/DFARS	Provides definitions and terms for Supply Chain Risk Management. Provides updates to paragraphs (a), (b) and (c) of the previous 252.239-7017.	NetOps, Products	Supply Chain Risk Management	Supply Chain Management	http://farsite.hill.af.mil/reghtml/regs/far2afmcfars/fardfars/dfars/dfars252_237.htm#P896_62838
DFARS 252.239-7018 Supply Chain Risk (DEVIATION 2018-O0020)	FAR/DFARS	Provides definitions and terms for Supply Chain Risk Management. Provides updates to paragraphs (a), (b), (c) and (d) of the previous 252.239-7018.	NetOps, Products	Supply Chain Risk Management	Supply Chain Management	http://farsite.hill.af.mil/reghtml/regs/far2afmcfars/fardfars/dfars/dfars252_237.htm#P896_62838
DFARS, Network Penetration Reporting and Contracting for Cloud Services	FAR/DFARS	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.	App Svs, NetOps, Products	Cloud Computing	Security	http://www.gpo.gov/fdsys/pkg/FR-2015-08-26/pdf/2015-20870.pdf
DHS - Federal Information Security Modernization Act of 2014	Law/Executive Document	Federal Information Security Modernization Act of 2014 - Amends the Federal Information Security Management Act of 2002. This Executive Order provides for the use of automated tools in agencies' information security programs, including for periodic risk assessments, testing of security procedures, and detecting, reporting, and responding to security incidents. Covered under Public Law 113-282.	App Svs, NetOps, Products	Laws and Executive Documents	Information System Security	https://www.dhs.gov/fisma
DHS Presidential Directive 12 (HSPD 12), Policy for a Common Identification Standard for Federal Employees and Contractors	Law/Executive Document	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.	NetOps, Products	Laws and Executive Documents	Identity Management	http://www.dhs.gov/homeland-security-presidential-directive-12
DoD 5220.22-M, National Industrial Security Program Operating Manual	DoD	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.	App Svs, NetOps	Operational Mgt	Data Security	http://www.dss.mil/documents/odaa/nispom2006-5220.pdf
DoD CIO, Commercial Mobile Device Implementation Plan	Other Guidance	This memorandum provides a phased Commercial Mobile Device (CMD) Implementation Plan that promotes the development and use of mobile non-tactical applications within the Department of Defense (DoD) enterprise. The Implementation Plan updates the DoD Mobile Device Strategy, Reference (a), to permit secure classified and protected unclassified mobile solutions that leverage commercial off-the-shelf products. The Implementation Plan is contingent on available funding and will be followed by a DoD Instruction with additional guidance on the use of wireless voice, video, and data capabilities.	NetOps, Products	Operational Mgt	UC Compliance	http://archive.defense.gov/news/DoDCMDImplementationPlan.pdf
DoD CIO, Mobile Device Strategy	Other Guidance	This 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.	App Svs, NetOps	Operational Mgt	Mobile Applications	http://archive.defense.gov/news/dodmobilitystrategy.pdf
DoD CIO, Net-Centric Data Strategy	Other Guidance	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.	App Svs, NetOps	Operational Mgt	NetCentric Strategy	http://dodcio.defense.gov/Portals/0/Documents/Net-Centric-Data-Strategy-2003-05-092.pdf
DoD CIO, Net-Centric Services Strategy	Other Guidance	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.	App Svs, NetOps	Operational Mgt	NetCentric Strategy	http://dodcio.defense.gov/Portals/0/documents/DoD_NetCentricServicesStrategy.pdf
DoD CIO, Open Technology Development (OTD) Lessons Learned and Best Practices for Military Software	Other Guidance	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.	App Svs	Operational Mgt	Strategy	http://dodcio.defense.gov/Portals/0/Documents/FOSS/OTD-lessons-learned-military-signed.pdf

DoD Cloud Computing Security Requirements Guide	Other Guidance	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 FedRAMP and this Cloud Computing Security Requirements Guide. DoD Instruction (DoDI) 8500.01, entitled Cybersecurity, directs DISA, under the authority, direction, and control of the DoD CIO to develop and maintain Control Correlation Identifiers, Security Requirements Guides (SRGs), Security Technical Implementation Guides (STIGs), and mobile code risk categories and usage guides that implement and are consistent with DoD cybersecurity policies, standards, architectures, security controls, and validation procedures, with the support of the National Security Agency Central Security Service, using input from stakeholders, and using automation whenever possible.	App Svs, NetOps, Products	Cloud Computing	Information System Security	https://iasecontent.disa.mil/cloud/Downloads/Cloud_Computing_SRG_v1r2.pdf
DoD Cloud Computing Security Requirements Guide (SRG), Version 1	Other Guidance	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.	NetOps	Cloud Computing	Strategy	http://iase.disa.mil/cloud_security/Documents/u-cloud_computing_srg_v1r1_final.pdf
DoD Directive 5205.02E, Operations Security (OPSEC) Program	DoD	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.	App Svs, NetOps	Operational Mgt	Data Security	http://www.esd.whs.mil/Directives/issuances/dodd/
DoD Directive 8000.01, Management of the Department of Defense Information Enterprise	DoD	This directive 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.	App Svs, NetOps	Operational Mgt	Overarching Guidance	http://www.esd.whs.mil/Directives/issuances/dodd/
DoD Directive 8100.02, Use of Commercial Wireless Devices, Services, and Technologies in the DoD Global Information Grid (GIG)	DoD	Applies to all commercial wireless devices, services, and technologies, including voiceand data capabilities, that operate either as part of the DoD GIG, or as part of DoD non-GIGInformation Technology (IT) (stand-alone) systems. This includes, but is not limitedto: commercial wireless networks and Portable Electronic Devices (PED) such as laptopcomputers with wireless capability, cellular/Personal Communications System (PCS) devices, audio/video recording devices, scanning devices, remote sensors, messaging devices, Personal Digital Assistants (PDA), and any other commercial wireless devices capable of storing, processing, or transmitting information.	NetOps, Products	Products Standards	Wireless Devices	http://www.esd.whs.mil/Directives/issuances/dodd/
DoD Directive 8140.01, Cyberspace Workforce Management	DoD	This publication unifies the overall cyberspace workforce and establishes specific workforce elements (cyberspace effects, cybersecurity, and cyberspace information technology (IT)) to align, manage and standardize cyberspace work roles, baseline qualifications, and training requirements. This directive does not address operational employment of the work roles. Operational employment of the cyberspace workforce will be determined by the Joint Staff, Combatant Commands, and other DoD Components to address mission requirements.	App Svs, NetOps	Cybersecurity	Workforce Management	http://www.esd.whs.mil/Directives/issuances/dodd/
DoD Discovery Metadata Specification (DDMS) 5.0	Other Guidance	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.	App Svs, NetOps	Operational Mgt	NetCentric Strategy	https://www.dni.gov/index.php/who-we-are/organizations/enterprise-capacity/ic-cio/ic-cio-related-menus/ic-cio-related-links/ic-technical-specifications/dod-discovery-metadata
DoD Instruction 1100.22, Policy and Procedures for Determining Workforce Mix	DoD	Provides manpower mix criteria and guidance for risk assessments to be used to identify and justify activities that are inherently governmental, commercial (exempt from private sector performance); and commercial (subject to private sector performance).	App Svs, NetOps	Operational Mgt	Workforce Management	http://www.esd.whs.mil/Directives/issuances/dodi/
DoD Instruction 3222.03, DoD Electromagnetic Environmental Effects (E3) Program	DoD	Establishes policy, assigns responsibilities, and provides instructions for the management and implementation of the DoD E3 Program to ensure mutual electromagnetic compatibility and effective E3 control among ground-, air-, maritime, and space-based platforms, electronic and electrical systems, subsystems, and equipment, and with the existing natural and man-made electromagnetic environment (EME).	NetOps, Products	Operational Mgt	Spectrum Management	http://www.esd.whs.mil/Directives/issuances/dodi/
DoD Instruction 4170.11, Installation Energy Management	DoD	This instruction specifies how: DoD utility infrastructure be secure, safe, reliable, and efficient. Utility commodities are procured effectively and efficiently. The Department of Defense maximize energy and water conservation efforts. The Department of Defense invest in cost effective renewable energy sources and energy efficient facility designs and regionally consolidate Defense requirements to aggregate bargaining power to achieve better energy pricing.	NetOps, Products	Operational Mgt	Environmental	http://www.esd.whs.mil/Directives/issuances/dodi/
DoD Instruction 4650.10, Land Mobile Radio (LMR) Interoperability and Standardization	DoD	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.	NetOps, Products	Products Standards	UC Compliance	http://www.esd.whs.mil/Directives/issuances/dodi/
DoD Instruction 5015.02, DoD Records Management Program	DoD	Establishes policy and assigns responsibilities for the management of DoD records in all media, including electronic.	App Svs, NetOps	Operational Mgt	Data Security	http://www.esd.whs.mil/Directives/issuances/dodi/

DoD Instruction 5230.24, Distribution Statements on Technical Documents	DoD	This instruction establishes DoD policies, assigns responsibilities, and prescribes procedures for marking and managing technical documents, including research, development, engineering, test, sustainment, and logistics information, to denote the extent to which they are available for secondary distribution, release, and dissemination without additional approvals or authorizations. It establishes a standard framework and markings for managing, sharing, safeguarding, and disseminating technical documents in accordance with policy and law.	App Svs, NetOps	Operational Mgt	Data Security	http://www.esd.whs.mil/Directives/issuances/dodi
DOD Instruction 8320.02, Sharing Data, Information, and Information Technology (IT) Services in the Department of Defense	DoD	Establishes policies, assigns responsibilities, and prescribes procedures for securely sharing electronic data, information, and IT services and securely enabling the discovery of shared data throughout the DoD.	App Svs, NetOps, Products	Operational Mgt	NetCentric Strategy	http://www.esd.whs.mil/Directives/issuances/dodi/
DOD Instruction 8320.04, Item Unique Identification (IUID) Standards for Tangible Personal Property	DoD	This instruction establishes policy and assigns 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.	Products	Products Standards	Asset Management	http://www.esd.whs.mil/Directives/issuances/dodi/
DoD Instruction 8330.01, Interoperability of Information Technology (IT), Including National Security Systems (NSS)	DoD	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)).	App Svs, NetOps	Cybersecurity	Architecture	http://www.esd.whs.mil/Directives/issuances/dodi/
DoD Instruction 8500.01, Cybersecurity	DoD	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.	App Svs, NetOps	Cybersecurity	Overarching Guidance	http://www.esd.whs.mil/Directives/issuances/dodi/
DoD Instruction 8520.02, Public Key Infrastructure (PKI) and Public Key (PK) Enabling	DoD	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.	App Svs, NetOps	Cybersecurity	Information System Security	http://www.esd.whs.mil/Directives/issuances/dodi/
DoD Instruction 8530.01, Cybersecurity Activities Support to DoD Information Network Operations	DoD	This instruction supports the Joint Information Environment (JIE) concepts as outlined in JIE Operations Concept of Operations (CONOPS) (Reference (d)).It also supports the formation of Cyber Mission Forces (CMF), development of the Cyber Force Concept of Operations and Employment, evolution of cyber command and control, cyberspace operations doctrine in Joint Publication 3-12 (Reference (e)), and evolving cyber threats and supports the Risk Management Framework (RMF) requirements to monitor security controls continuously, determine the security impact of changes to the DODIN and operational environment, and conduct remediation actions as described in DoDI 8510.01 (Reference (f)).	NetOps	Cybersecurity	Information System Security	http://www.esd.whs.mil/Directives/issuances/dodi/
DoD Instruction 8540.01, Cross Domain (CD) Policy	DoD	A DoD CD capability requirement must be met by a Cross Domain Solution (CDS) listed on the Unified Cross Domain Services Management Office (UCDSMO)-managed CDS baseline list. When a CDS baseline list CDS cannot meet the CD capability requirements for the mission, a modified CDS baseline list CDS or new technology will be used in accordance with the selection decision based on analysis of CD alternatives in the procedures of this instruction.	App Svs, NetOps	Cybersecurity	Network Standards	http://www.esd.whs.mil/Directives/issuances/dodi/
DoD Instruction 8551.01, Ports, Protocols, and Services Management (PPSM)	DoD	Updates policy and standardizes procedures to catalog, regulate, and control the use and management of protocols in the Internet protocol suite, and associated ports (also known as "protocols, data services, and associated ports" or "ports, protocols, and services"); referred to in this instruction as PPS on DoD information networks (DODIN) including the connected information systems, platform information technology (IT) systems, platform IT (PIT), and products based on the potential that unregulated PPSM can damage DoD operations and interests.	NetOps	Cybersecurity	Network Standards	http://www.esd.whs.mil/Directives/issuances/dodi/
DoD Instructions, 8500 Series	DoD	The DoDI 8500 series cover cybersecurity risk management processes, PKI enabling, identity authentication for systems, COMSEC, cross domain policy, internet services, ports, protocols and services management, information assurance and security of unclassified systems.	NetOps	Cybersecurity	IT Management	http://www.esd.whs.mil/Directives/issuances/dodi/
DoD IPv6 Memorandum, 08 October, 2010 - Includes DISA Waiver Form DISA-GE323	Other Guidance	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).	NetOps, Products	Cybersecurity	UC Compliance	https://www.hpc.mil/images/hpcdocs/ipv6/dod_recommended_ipv6_contractual_language-2010-oct-08v2.0.pdf
DoD Manual 4140.01, DoD Supply Chain Materiel Management Procedures	DoD	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.	Products	Products Standards	Supply Chain Management	http://www.esd.whs.mil/Directives/issuances/dodm/
DoD Manual 5200.01, DoD Information Security Program: Overview, Classification, and Declassification, Volumes 1 - 4	DoD	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).	App Svs, NetOps	Operational Mgt	Data Security	http://www.esd.whs.mil/Directives/issuances/dodm/
DoD Manual 5200.02/AF Manual 16-1405, Air Force Personnel Security Program	DoDM/AFMAN	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.	App Svs, NetOps	Operational Mgt	Workforce Management	http://static.e-publishing.af.mil/production/1/saf_aa/publication/dodman5200.02_afman16-1405/dodm5200.02_afman16-1405.pdf

DoD Program Manager's Guidebook for Integrating the Cybersecurity Risk Management Framework (RMF) into the System Acquisition Lifecycle	Other Guidance	This guidebook emphasizes integrating cybersecurity activities into existing processes including requirements, SSE, program protection planning, trusted systems and networks analysis, developmental and operational test and evaluation, financial management and cost estimating, and sustainment and disposal.	App Svs, NetOps	Operational Mgt	Risk Management Framework	https://www.dau.mil/tools/t/DoD-Program-Manager-Guidebook-for-Integrating-the-Cybersecurity-Risk-Management-Framework-(RMF)-into-the-System-Acquisition-Lifecycle
DoE - Federal Energy Management Program	Law/Executive Document	Federal agencies are required to meet energy management mandates outlined by the following federal legal authorities: 1) Executive Order 13693: Planning for Federal Sustainability in the Next Decade, 2) Energy Independence and Security Act of 2007, 3) Energy Policy Act of 2005, 4) Executive Order 13221: Energy-Efficient Standby Power Devices, 5) Energy Policy Act of 1992, and 6) National Energy Conservation Policy Act. This site provides a listing of covered product categories that meet federal procurement requirements.	Products	Operational Mgt	Environmental	https://energy.gov/eere/femp/energy-efficient-products-and-energy-saving-technologies
Energy Star Approved Products List	APL	The Energy Star Approved Products List provides listings of products that meet ENERGY STAR® guidelines.	Products	Products Standards	Environmental	https://www.energystar.gov/products
Executive Order 13526, Classified National Security Information	Law/Executive Document	This order prescribes a uniform system for classifying, safeguarding, and declassifying national security information, including information relating to defense against transnational terrorism.	NetOps	Cybersecurity	Data Security	https://www.dni.gov/index.php/ic-legal-reference-book/executive-order-13526
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 (requires site registration)	Other Guidance	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.	Products	Products Standards	UC Compliance	https://www.fmglobal.com/
FAR 23.704 - Electronic Product Environmental Assessment Tool (EPEAT®)	FAR/DFARS	Contracting officers, when acquiring an electronic product, except as specified in paragraphs (a)(1)(i), (ii), or (iii) of this section, shall acquire an EPEAT® registered electronic product, unless the agency determines, in accordance with agency procedures, that the EPEAT® registered product will not be cost effective over the life of the product. This subpart applies to acquisitions of electronic products to be used in the United States, unless otherwise provided by agency procedures. When acquiring electronic products to be used outside the United States, agencies must use their best efforts to comply with this section.	NetOps, Products	Products Standards	Environmental	http://farsite.hill.af.mil/zoomcgi/search.cgi
FAR 52.223-15 – Energy Efficiency in Energy-Consuming Products	FAR/DFARS	This clause requires energy-consuming products are energy efficient products (i.e., ENERGY STAR® products or FEMP-designated products) at the time of contract award unless the energy-consuming product is not listed in the ENERGY STAR® Program or FEMP or otherwise approved in writing by the Contracting Officer.	Products	Products Standards	Environmental	http://farsite.hill.af.mil/zoomcgi/search.cgi
FAR Subpart 25.1 -- Buy American Act – Supplies	FAR/DFARS	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.	Products	Products Standards	Supply Chain Management	http://farsite.hill.af.mil/zoomcgi/search.cgi
FBI Electronic Biometric Transmission Specification (EBTS)	Other Guidance	This website provides a listing of FBI approved biometric products and EBTS standards documents.	Products	Products Standards	Approved Products List	https://www.fbibiospecs.cjis.gov/
Federal Information Processing Standards (FIPS) Publication 140-2, Security Requirements for Cryptographic Modules	FIPS	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.	Products	Products Standards	Encryption	https://csrc.nist.gov/publications/fips
Federal Information Processing Standards (FIPS) Publication 199, Standards for Security Categorization of Federal Information and Information Systems	FIPS	This publication addresses standards for categorizing information and information systems. Security categorization standards for information and information systems provide a common framework and understanding for expressing security that, for the federal government, promotes: effective management and oversight of information security programs, including the coordination of information security efforts throughout the civilian, national security, emergency preparedness, homeland security, and law enforcement communities; and consistent reporting to the Office of Management and Budget and Congress on the adequacy and effectiveness of information security policies, procedures, and practices.	NetOps	Cybersecurity	Information System Security	https://csrc.nist.gov/publications/fips
Federal Information Processing Standards (FIPS) Publication 200, Minimum Security Requirements for Federal Information and Information Systems	FIPS	FIPS 200 is the second standard that was specified by the FISMA 2002 (now FISMA 2014). 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.	Products	Products Standards	Risk Management Framework	https://csrc.nist.gov/publications/fips
Federal Information Processing Standards (FIPS) Publication 201-2, Personal Identity Verification (PIV) of Federal Employees and Contractors	FIPS	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 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 at http://fips201ep.cio.gov/index.php. A list of validated middleware can be found at http://csrc.nist.gov/groups/SNS/piv/npivp/validation.html.	Products	Products Standards	Identity Management	https://csrc.nist.gov/publications/fips

GiG Technical Guidance Federation GIG-F (requires CAC and site registration)	Other Guidance	This guidance is a suite of software applications on the NIPRNet and SIPRNet that provides technical guidance across the Enterprise to achieve net-ready, interoperable, and supportable GIG systems. This GTG-F content consists of and is based on GIG net-centric IT standards, associated profiles, engineering best practices and reference implementation specifications.	App Svs, NetOps, Products	Operational Mgt	NetCentric Strategy	https://gtg.csd.disa.mil/uam/login.do
GSA - FedRAMP Approved Products List	APL	This website provides a listing of FedRAMP approved products for Cloud computing. See the Marketplace tab for a list of products. This APL acts under governance of FedRAMP which is a government-wide program with input from numerous departments, agencies, and government groups. The program's primary decision-making body is the Joint Authorization Board (JAB), comprised of the CIOs from DOD, DHS, and GSA. In addition to the JAB, OMB, the Federal CIO Council, NIST, DHS, and the FedRAMP Program Management Office (PMO) play keys roles in effectively running FedRAMP.	App Svs, NetOps, Products	Cloud Computing	Approved Products List	https://www.fedramp.gov/
GSA - FedRAMP Security Controls for Cloud Service Providers	Other Guidance	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.	NetOps	Cloud Computing	Security	https://www.fedramp.gov/cloud-service-providers/
IEEE 12207-2017 - ISO/IEC/IEEE International Standard - Systems and Software Engineering - Software Lifecycle Processes (Pay-wall)	IEEE	This International Standard establishes a common framework for software life cycle processes, with well defined terminology, that can be referenced by the software industry. It contains processes, activities, and tasks that are to be applied during the acquisition of a software system, product or service and during the supply, development, operation, maintenance and disposal of software products. This is accomplished through the involvement of stakeholders, with the ultimate goal of achieving customer satisfaction.	App Svs, NetOps	Operational Mgt	Lifecycle Management	https://standards.ieee.org/standard/12207-2017.html
Industry Best Practices in Achieving Service Oriented Architecture (SOA)	Other Guidance	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).	App Svs	Operational Mgt	Architecture	https://resources.sei.cmu.edu/asset_files/WhitePaper/2005_019_001_29406.pdf
ISO/IEC 11889-1:2015 through ISO/IEC 11889-4:2015	ISO/IEC	Defines the architectural elements of the Trusted Platform Module, a device which enables trust in computing platforms in general.	Products	Products Standards	Information System Security	https://standards.iso.org/ittf/PubliclyAvailableStandards/index.html
ISO/IEC 19770-2:2015, Software Identification Tag (Pay-wall)	ISO/IEC	This standard establishes specifications for tagging software to optimize its identification and management. It applies to: tag producers, platform providers, software providers, tag consumers, software consumers, IT discovery and processing tool providers. This standard does not prescribe Information Technology Asset Management (ITAM) or other IT-related processes required for reconciliation of software entitlements with software identification tags or other IT requirements and is not intended to conflict either with any organization's policies, procedures or standards or with any national or international laws and regulations.	App Svs, Products	Operational Mgt	Software	https://www.iso.org/standard/65666.html
ISO/IEC 20000-1, Information Technology and Service Management - Part 1: Service Management System Requirements	ISO/IEC	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.	App Svs, NetOps	Operational Mgt	IT Management	https://www.iso.org/standard/51986.html
ITU Recommendation H.320, Narrow-band Visual Telephone Systems and Terminal Equipment	Other Guidance	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.	NetOps, Products	Products Standards	UC Compliance	https://www.itu.int/rec/T-REC-H.320/en
MIL-STD-129P, Military Marking for Shipment and Storage	MIL-STD	Standards and Specification information regarding passive Radio Frequency Identification (RFID).	Products	Products Standards	Asset Management	http://www.acq.osd.mil/log/sci/.AIT.html/MIL-STD-129PCH4.pdf
NIST - Federal Information Processing Standards (FIPS)	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. Note: some specific FIPS standards are singled out in this list.	App Svs, Products	Operational Mgt	Overarching Guidance	https://www.nist.gov/itl/current-fips
NIST SP 500-290, Data Format for the Interchange of Fingerprint, Facial & Other Biometric Information	NIST	This standard defines the content, format, and units of measurement for the electronic DNA and other biometric sample and forensic information that consists of a variety of mandatory and optional items. This information sis primarily intended for interchange among criminal justice administrations or organizations that rely on automated identification systems or use other biometric and image data for id purposes. (It appears the DoD Biometrics has dissolved) REPLACED WITH: NIST Special Publication 500-290 Data Format for the Interchange of Fingerprint, Facial & Other Biometric Information (ANSI/NIST-ITL 1-2011) AND the Electronic Biometric Transmission Specification (EBTS).	Products	Products Standards	Application Development	https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication500-290.pdf
NIST SP 500-292, Cloud Computing Reference Architecture	NIST	Overview of the five major roles & responsibilities using the Cloud Computing Taxonomy. The five major participating actors are the Cloud Consumer, Cloud Provider, Cloud Broker, Cloud Auditor and Cloud Carrier.	NetOps	Cloud Computing	Guidance	https://www.nist.gov/publications/nist-cloud-computing-reference-architecture?pub_id=909505
NIST SP 800-122, Guide to Protecting the Confidentiality of Personality Identifiable Information (PII)	NIST	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.	NetOps	Cybersecurity	Information System Security	https://doi.org/10.6028/NIST.SP.800-122
NIST SP 800-144, Guidelines on Security and Privacy in Public Cloud Computing	NIST	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.	NetOps	Cloud Computing	Information System Security	http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-144.pdf

NIST SP 800-145, Definition of Cloud Computing	NIST	The NIST definition characterizes important aspects of cloud computing and is intended to serve as a means for broad comparisons of cloud services and deployment strategies, and to provide a baseline for discussion from what is cloud computing to how to best use cloud computing. The service and deployment models defined form a simple taxonomy that is not intended to prescribe or constrain any particular method of deployment, service delivery, or business operation.	NetOps	Cloud Computing	Guidance	http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf
NIST SP 800-146, Cloud Computing Synopsis & Recommendations	NIST	This document reprises the NIST-established definition of cloud computing, describes cloud computing benefits and open issues, presents an overview of major classes of cloud technology, and provides guidelines and recommendations on how organizations should consider the relative opportunities and risks of cloud computing.	NetOps	Cloud Computing	Guidance	http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-146.pdf
NIST SP 800-147, BIOS Protection Guidelines	NIST	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).	Products	Products Standards	Information System Security	http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-147.pdf
NIST SP 800-37R1, Guide for Applying the Risk Management Framework to Federal Information Systems	NIST	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.	NetOps	Cybersecurity	Risk Management Framework	http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r1.pdf
NIST SP 800-53R4, Security and Privacy Controls for Federal Information Systems and Organizations	NIST	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.	NetOps	Operational Mgt	Information System Security	http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf
NIST SP 800-59, Guideline for Identifying an Information System as a National Security System	NIST	The guideline is to assist agencies in determining which, if any, of their systems are national security systems as defined by FISMA and are to be governed by applicable requirements for such systems, issued in accordance with law and as directed by the President.	NetOps	Cybersecurity	Information System Security	https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-59.pdf
NIST SP 800-66R1, An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule	NIST	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.	NetOps	Cybersecurity	Data Security	https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-66r1.pdf
NIST SP 800-88R1, Guidelines for Media Sanitization	NIST	This guide will assist organizations and system owners in making practical sanitization decisions based on the categorization of confidentiality of their information.	App Svs, NetOps	Operational Mgt	Data Security	http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf
NSA/CSS TEMPEST Certification Program	Other Guidance	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.	App Svs, NetOps, Products	Products Standards	TEMPEST	https://apps.nsa.gov/iaarchive/programs/iad-initiatives/tempest.cfm
NSTI - ICD 503 Risk Management Framework Course (RMF)	Other Guidance	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.	App Svs, NetOps	Cybersecurity	Risk Management Framework	https://www.nstii.com/courses/systems-security-practitioners-course-sspc/
Section 508 of the Rehabilitation Act of 1973	Law/Executive Document	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.	App Svs, NetOps, Products	Laws and Executive Documents	Application Development	https://www.section508.gov/manage/laws-and-policies
Security Technical Implementation Guides (STIGs)	Other Guidance	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.	App Svs, NetOps	Cybersecurity	Information System Security	http://iase.disa.mil/stigs/Pages/index.aspx
Supplier Performance Risk System (SPRS)	NAVSEA	A web-enabled enterprise application that gathers, processes, and displays data about the performance of suppliers. SPRS is the Department of Defense's single, authorized application to retrieve suppliers' performance information. The Defense Federal Acquisition Regulation Supplement (DFARS) Subpart 213.1 requires contracting officers to consider this data for supply contracts valued at less than or equal to $1 million. SPRS enables procurement specialists to avoid overpaying for supplies and notifies procurement specialists of Federal Supply Class (FSC) specific risks and risk mitigations. SPRS's Supplier Risk Score provides procurement specialists with a composite score that considers each supplier's past performance in the areas of product delivery and quality.	NetOps, Products	Products Standards	Supply Chain Management	https://www.sprs.csd.disa.mil/default.htm

Title 44 USC Section 3542 - Public notice and comment regarding demonstration programs not expressly authorized in law	Law/Executive Document	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) 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.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).	App Svs, NetOps, Products	Laws and Executive Documents	Information System Security	https://www.govinfo.gov/app/details/USCODE-2017-title42/USCODE-2017-title42-chap44-sec3542
U.S. Chief Information Officer, Federal Cloud Computing Strategy	Other Guidance	This strategy is to enable the Department to increase secure information sharing and collaboration, enhance mission effectivness, and decrease costs using cloud services.	NetOps	Cloud Computing	Strategy	https://dodcio.defense.gov/Portals/0/Documents/Mobility/Federal%20Cloud%20Computing%20Strategy%20Feb%208,%202011.pdf
Unified Capabilities Requirements (UCR 2013, Change 1)	Other Guidance	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).	NetOps, Products	Products Standards	UC Compliance	http://www.disa.mil/Network-Services/UCCO/Archived-UCR
Updated Guidance on the Acquisition and Use of Commercial Cloud Computing Services	Other Guidance	This memo clarifies and updates DoD guidance when acquiring commercial cloud services.	App Svs, NetOps, Products	Cloud Computing	Guidance	http://www.doncio.navy.mil/ContentView.aspx?id=7864
US Government Configuration Baseline (USGCB)	Law/Executive Document	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.	App Svs, Products	Cybersecurity	Information System Security	https://csrc.nist.gov/Projects/United-States-Government-Configuration-Baseline