Application Services Standards

Reference	Description	Category	Link to Guidance	Authority
Acquisition Streamlining and Standardization Information System (ASSIST)	ASSIST is the official source for specifications and standards used by the Department of Defense and it always has the most current information. Over 111,000 technical documents are indexed in ASSIST, and the ASSIST document database houses over 180,000 PDF files associated with about 82,000 of the indexed documents. There are more than 33,000 active ASSIST user accounts and over 6,000 active Shopping Wizard accounts. Managed by the DoD Single Stock Point (DODSSP) in Philadelphia, the ASSIST-Online web site provides free public access to most technical documents in the ASSIST database. The ASSIST Shopping Wizard provides a way to order documents from the DODSSP that are not available in digital form.	Product Standards	https://assist.dla.mil/online/start/	DoD
AFGM 2015-33-01, End-of-Support Software Risk Management	This Guidance Memorandum supersedes AFGM 2014-33-03, Microsoft Windows XP End-of-Life, and highlights current policies and SAF/CIO A6 authorities to mitigate cybersecurity vulnerabilities introduced by unsupported software. Compliance with this Memorandum is mandatory.	Security Programs	http://static.e-publishing.af.mil/production/1/saf_cio_a6/publication/afgm2015-33-01/afgm2015-33-01.pdf	DoD
AFI 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/af_a3/publication/afi10-206/afi10-206.pdf	DoD
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	AF
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	AF

Application Services Standards

Reference	Description	Category	Link to Guidance	Authority
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/publication/afi10-701/afi10-701.pdf	AF
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	DoD
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/afi17-100/afi17-100.pdf	AF
AFI 17-101 RISK MANAGEMENT FRAMEWORK (RMF) FOR AIR FORCE INFORMATION TECHNOLOGY (IT)	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.	Certification & Accreditation	http://static.e-publishing.af.mil/production/1/saf_cio_a6/publication/afi17-101/afi17-101.pdf	AF
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/afi17-130/afi33-200.pdf	AF

Application Services Standards

Reference	Description	Category	Link to Guidance	Authority
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	AF
AFI 17-210, Radio Management	This standard specifies requirements for types of land mobile radios, frequency ranges and encryption standards. It provides requirements processing, validation, and handling procedures for classified and unclassified Personal Wireless Communication Systems (PWCS), and training. It provides procedures for the management, operation, and procurement of commercial wireless service for all PWCS. Previously AFI 33-590 superseded by AFI 17-210	Radios	http://static.e-publishing.af.mil/production/1/saf_cio_a6/publication/afi17-210/afi17-210.pdf	AF
AFI 17-220, 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/afi17-220/afi17-220.pdf	AF
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	AF
AFI 32-10112 Installation GI&S (GeoBase)	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. 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.	Misc (Energy Star, etc)	http://static.e-publishing.af.mil/production/1/af_a47/publication/afi32-10112/afi32-10112.pdf	AF

Application Services Standards

Reference	Description	Category	Link to Guidance	Authority
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	AF
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	AF
AFI 36-2201, Air Force Training Program	This instruction implements DoDD 1322.18, Military Training, 3 September 2004, DoDI 1322.20, Development and Management of Interactive Courseware (ICW) for Military Training, 14 March 1991, with change 1, 16 November 1994, DoDI 1322.26, Development, Management, and Delivery of Distributed Learning, 16 June 2006, and AFPD 36-22, 22 March 2004, Military Training, for developing, managing, and conducting Air Force (AF) technical, ancillary, and recruit training. Force management policies, responsibilities, and procedures specific to AF-level quantitative recruit and technical training requirements are implemented in AFI 36-2616, Trained Personnel Requirements.	Information Mgt	http://static.e-publishing.af.mil/production/1/af_a1/publication/afi36-2201/afi36-2201.pdf	
AFI 61-201, SCIENTIFIC, RESEARCH AND DEVELOPMENT MANAGEMENT OF SCIENTIFIC AND TECHNICAL INFORMATION (STINFO)	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.	Records and Document Mgt	http://static.e-publishing.af.mil/production/1/saf_aq/publication/afi61-201/afi61-201.pdf	AF
AFI 63-101/20-101, Integrated Life Cycle Management	It identifies elements of Air Force systems engineering (SE) practice and management required to provide and sustain, in a timely manner, cost-effective products and systems that are operationally safe, suitable, and effective.	Life Cycle Mgt	http://static.e-publishing.af.mil/production/1/saf_aq/publication/afi63-101_20-101/afi63-101_20-101.pdf	AF

Application Services Standards

Reference	Description	Category	Link to Guidance	Authority
AFI 99-103, Capabilities-Based Test and Evaluation	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.	Misc (Energy Star, etc)	http://static.e-publishing.af.mil/production/1/af_te/publication/afi99-103/afi99-103.pdf	AF
AFMAN 17-1201, 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/saf_cio_a6/publication/afman33-152/afman33-152.pdf	AF
AFMAN 17-1202, Collaboration Services and Voice Systems Management	for Collaboration Services including electronic collaboration and management of Video Teleconferencing (VTC) resources to include systems, equipment, personnel, time, and money and provides the directive guidance for Air Force VTC and voice systems management activities. This manual is for use by individuals responsible for implementation, acquisition, and management of electronic collaboration services, appliance Video-Teleconferencing (VTC) equipment, and telephone services that are converging under UC Real Time Services (RTS) establishing the basic guidance framework for Air Force personnel. The scope for this publication includes information on policy, standards, reporting, requirements, services, engineering, and systems management for use in complying with DoD and Air Force instructions for UC RTS including collaboration, VTC communications connectivity, and telephone services in the secure and non-secure interactive group environments. This manual assists action officers who implement collaboration services (voice, video, and/or data) to satisfy customer requirements and support the diverse major command missions.	Network	http://static.e-publishing.af.mil/production/1/saf_cio_a6/publication/afman17-1202/afman17-1202.pdf	AF

Application Services Standards

Reference	Description	Category	Link to Guidance	Authority
AFMAN 17-1203 Information Technology (IT) Asset Management (ITAM)	This Air Force Manual (AFMAN) implements Executive Order (E.O.) 13103, Computer Software Piracy and Air Force Policy Directives (AFPD) 33-1, Cyberspace Support and supports AFPD 33-2, Information Assurance (IA) Program; AFPD 63-1/20-1, Integrated Life Cycle Management; and AFPD 10-6, Capabilities-Based Planning & Requirements Development. This AFMAN provides the overarching guidance and direction for managing IT hardware and software. The hardware management guidance identifies responsibilities for supporting Air Force (AF) IT hardware (IT assets) and maintaining accountability of Personal Wireless Communications Systems (PWCS) including cellular telephones and pagers. The software management guidance identifies responsibilities for management of commercial off-the-shelf (COTS) and AF-unique software acquired/developed by the AF (other than software internal to a weapon system; see AFPD 63-1/20-1, Integrated Life Cycle Management).	Information Mgt	http://static.e-publishing.af.mil/production/1/saf_cio_a6/publication/afman17-1203/afman17-1203.pdf	AF
AFMAN 17-1301, COMPUTER SECURITY (COMPUSEC)	Computer Security (COMPUSEC) is a cybersecurity discipline identified in AFI 17-130. Compliance ensures appropriate implementation of measures to protect all AF Information System (IS) resources and information. The COMPUSEC objective is to employ countermeasures designed for the protection of confidentiality, integrity, availability, authentication, and non-repudiation of United States (US) government information processed by AF ISs.	Security Programs	http://static.e-publishing.af.mil/production/1/saf_cio_a6/publication/afman17-1301/afman17-1301.pdf	AF
AFMAN 17-1303, CYBERSECURITY WORKFORCE IMPROVEMENT PROGRAM	By Order of the Secretary of the Air Force, this Air Force Guidance Memorandum immediately AFMAN33-285 Cybersecurity Workforce Improvement Program, 20 Mar 2015 Information. Compliance with this Memorandum is mandatory. To the extent its directions are inconsistent with other Air Force publications, the information herein prevails, in accordance with (IAW) AFI 33-360, Publications and Forms Management. Ensure that all records created as a result of processes prescribed in this publication are maintained IAW Air Force Manual (AFMAN) 33-363, Management of Records, and disposed of IAW Air Force Records Information Management System (AFRIMS) Records Disposition Schedule (RDS).	Information Assurance	http://static.e-publishing.af.mil/production/1/saf_cio_a6/publication/afman17-1303/afman17-1303.pdf	AF
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	AF

Application Services Standards

Reference	Description	Category	Link to Guidance	Authority
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	AF
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	AF
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	AF
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	AF
CJCSI 6211.02D, Defense Information Systems Network Responsibilities	This instruction establishes policy and responsibilities for the connection of information systems (ISs) (e.g., applications, enclaves, or outsourced processes) and unified capabilities (UC) products to the DISN provided transport (including data, voice, and video) and access to information services transmitted over the DISN (including data, voice, video, and cross-domain).	Network	http://www.jcs.mil/Portals/36/Documents/Library/Instructions/6211_02a.pdf?ver=2016-02-05-175050-653?ver=2016-02-05-175050-653	DoD
CJCSI 6212.01F,NET READY KEY PERFORMANCE PARAMETER (NR KPP)	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.	Certification & Accreditation	http://jitc.fhu.disa.mil/jitc_dri/pdfs/cjcsi_6212_01f.pdf	DoD

Application Services Standards

Reference	Description	Category	Link to Guidance	Authority
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	DoD
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/	DoD
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	Federal
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	DoD
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	Federal
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	DoD

Application Services Standards

Reference	Description	Category	Link to Guidance	Authority
DFARS: Network Penetration Reporting and Contracting for Cloud Services	DoD is issuing an interim rule amending the DFARS to implement a section of the National Defense Authorization Act for Fiscal Year 2013 and a section of the National Defense Authorization Act for Fiscal Year 2015, both of which require contractor reporting on network penetrations. Additionally, this rule implements DoD policy on the purchase of cloud computing services.	Network	http://www.gpo.gov/fdsys/pkg/FR-2015-08-26/pdf/2015-20870.pdf	Federal
DoD 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
DoD Cloud Computing Security Requirements Guide	The 15 December 2014 DoD CIO memo regarding Updated Guidance on the Acquisition and Use of Commercial Cloud Computing Services defines DoD Component responsibilities when acquiring commercial cloud services. The memo allows components to responsibly acquire cloud services minimally in accordance with the security requirements outlined in Federal Risk and Authorization Management Program (FedRAMP) and this Cloud Computing Security Requirements Guide (CC SRG). DoD Instruction (DoDI) 8500.01, entitled Cybersecurity, directs Director DISA, under the authority, direction, and control of the DoD CIO to develop and maintain Control Correlation Identifiers (CCIs), Security Requirements Guides (SRGs), Security Technical Implementation Guides (STIGs), and mobile code risk categories and usage guides that implement and are consistent with DoD cybersecurity policies, standards, architectures, security controls, and validation procedures, with the support of the National Security Agency Central Security Service (NSA/CSS), using input from stakeholders, and using automation whenever possible. DoDI 8510.01, para 2a states: “This instruction applies to: (2) All DoD IT that receive, process, store, display, or transmit DoD information.	Software	https://iasecontent.disa.mil/cloud/Downloads/Cloud_Computing_SRG_v1r2.pdf	DoD
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://www.ise.gov/sites/default/files/Track1-PeteAttas-WIS3-DDMSOverview.pdf	DoD
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

Application Services Standards

Reference	Description	Category	Link to Guidance	Authority
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
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
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	http://dodcio.defense.gov/Portals/0/Documents/FOSS/OTD-lessons-learned-military-signed.pdf	DoD
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.esd.whs.mil/Directives/issuances/dodd/	DoD
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.esd.whs.mil/Directives/issuances/dodd/	
DoDD 8140.01, Cyberspace Workforce Management	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.	Information Assurance	http://www.esd.whs.mil/Directives/issuances/dodd/	DoD

Application Services Standards

Reference	Description	Category	Link to Guidance	Authority
DoDD 8320.1 Data 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://dap.dau.mil/policy/Documents/Policy/8320-1.pdf	DoD
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.esd.whs.mil/Directives/issuances/dodi/	DoD
DoDI 5015.02, DoD Records Management Program	Establishes policy and assigns responsibilities for the management of DoD records in all media, including electronic	Records and Document Mgt	http://www.esd.whs.mil/Directives/issuances/dodi/	DoD
DoDI 5230.24, Distribution Statements on Technical Documents	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.	Records and Document Mgt	http://www.esd.whs.mil/Directives/issuances/dodi	DoD
DODI 8320.02, Sharing Data, Information, and Information Technology (IT) Services in the Department of Defense	Establishes policies and responsibilities to implement data sharing, in accordance with Department of Defense Chief Information Officer Memorandum, “DoD Net-Centric Data Strategy,” May 9, 2003, throughout the Department of Defense. Directs the use of resources to implement data sharing among information capabilities, services, processes, and personnel interconnected within the Global Information Grid (GIG), as defined in DoD Directive 8100.1, “Global Information Grid (GIG) Overarching Policy,” September 19, 2002.	NetCentric Strategy	http://www.esd.whs.mil/Directives/issuances/dodi/	DoD

Application Services Standards

Reference	Description	Category	Link to Guidance	Authority
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.esd.whs.mil/Directives/issuances/dodi/	DoD
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.esd.whs.mil/Directives/issuances/dodi/	DoD
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.esd.whs.mil/Directives/issuances/dodi/	DoD
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.esd.whs.mil/Directives/issuances/dodi/	DoD
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

Application Services Standards

Reference	Description	Category	Link to Guidance	Authority
Federal Information Security Modernization Act of 2014	Federal Information Security Modernization Act of 2014 - Amends the Federal Information Security Management Act of 2002. This Executive Order provides for the use of automated tools in agencies' information security programs, including for periodic risk assessments, testing of security procedures, and detecting, reporting, and responding to security incidents.	Security Programs	https://www.dhs.gov/fisma	Federal
FedRAMP Approved Products List	This website provides a listing of FedRAMP approved products for Cloud computing. See the Marketplace tab for a list of products. This APL acts under governance of FedRAMP which is a government-wide program with input from numerous departments, agencies, and government groups. The program's primary decision-making body is the Joint Authorization Board (JAB), comprised of the CIOs from DOD, DHS, and GSA. In addition to the JAB, OMB, the Federal CIO Council, NIST, DHS, and the FedRAMP Program Management Office (PMO) play keys roles in effectively running FedRAMP.	Software	https://www.fedramp.gov/	Federal
GiG Technical Guidance Federation GIG-F	The GIG Technical Guidance Federation (GTG-F) is a suite of software applications on the NIPRNet and SIPRNet (June 2012) that provides technical guidance across the Enterprise to achieve net-ready, interoperable, and supportable GIG systems. The GTG-F assists program managers, portfolio managers, engineers and others in answering two questions critical to any Information Technology (IT) or National Security Systems (NSS): (1) Where does the IT or NSS fit, as both a provider and consumer, into the GIG with regard to End-to-End technical performance, access to data and services, and interoperability; (2) What must an IT or NSS do to ensure technical interoperability with the GIG. The GTG-F content provides the technical information to various users in addressing and resolving technical issues needed to meet functional requirements (i.e., features and capabilities) of the GIG. This GTG-F content consists of and is based on GIG net-centric IT standards, associated profiles, engineering best practices and reference implementation specifications.	GIG	https://gtg.csd.disa.mil/uam/login.do	DoD
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.dni.gov/files/documents/ICD/ICD_503.pdf	DoD

Application Services Standards

Reference	Description	Category	Link to Guidance	Authority
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	Commercial
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	Commercial
ISO/IEC 19770-2:2015, Software Identification Tag	ISO/IEC 19770-2:2015 establishes specifications for tagging software to optimize its identification and management. (http://en.wikipedia.org/wiki/ISO/IEC_19770)	Software	https://www.iso.org/standard/65666.html	
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)	https://www.iso.org/standard/51986.html	Commercial
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	Commercial
NSTISSAM TEMPEST/1-92/TEMPEST Certification	TEMPEST is compromising emanations are defined as unintentional intelligence-bearing signals which, if intercepted and analyzed, may disclose the information transmitted, received, handled, or otherwise processed by any information-processing equipment.	TEMPEST	https://www.iad.gov/iad/search.cfm?criteria=NSTISSAM+TEMPEST%2F1-92%2FTEMPEST+Certification+	Federal

Application Services Standards

Reference	Description	Category	Link to Guidance	Authority
Section 508 of the Rehabilitation Act of 1973	On August 7, 1998, President Clinton signed into law the Rehabilitation Act Amendments of 1998 which covers access to federally funded programs and services. The law strengthens section 508 of the Rehabilitation Act and requires access to electronic and information technology provided by the Federal government. The law applies to all Federal agencies when they develop, procure, maintain, or use electronic and information technology. Federal agencies must ensure that this technology is accessible to employees and members of the public with disabilities to the extent it does not pose an "undue burden." Section 508 speaks to various means for disseminating information, including computers, software, and electronic office equipment. It applies to, but is not solely focused on, Federal pages on the Internet or the World Wide Web.	Misc (Energy Star, etc)	http://www.opm.gov/html/508-textOfLaw.asp	Federal
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	DoD
Title 44 USC Section 3542	any information system (including any telecommunications system) used or operated by an agency or by a contractor of an agency, or other organization on behalf of an agency— (i) the function, operation, or use of which— (I) involves intelligence activities; (II) involves cryptologic activities related to national security; (III) involves command and control of military forces; (IV) involves equipment that is an integral part of a weapon or weapons system; or (V) subject to subparagraph (B), is critical to the direct fulfillment of military or intelligence missions; or (ii) is protected at all times by procedures established for information that have been specifically authorized under criteria established by an Executive order or an Act of Congress to be kept classified in the interest of national defense or foreign policy. (B) Subparagraph (A)(i)(V) does not include a system that is to be used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications).	Security Programs	https://www.gpo.gov/fdsys/granule/USCODE-2011-title44/USCODE-2011-title44-chap35-subchapIII-sec3542	Federal
Updated Guidance on the Acquisition and Use of Commercial Cloud Computing Services	This memo clarifies and updates DoD guidance when acquiring commercial cloud services.	NetCentric Strategy	http://www.doncio.navy.mil/Download.aspx?AttachID=5555	DoD

Application Services Standards

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