BY ORDER OF THE SECRETARY OF THE AIR FORCE

AIR FORCE INSTRUCTION 17-140

29 JUNE 2018

Cyberspace

ARCHITECTING

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

ACCESSIBILITY: Publications and forms are available for downloading or ordering on the e-Publishing website at **www.e-Publishing.af.mil**

RELEASABILITY: There are no releasability restrictions on this publication

OPR: SAF/CIO A6SA

Certified by: SAF/CIO A6S
(Maj Gen Patrick C. Higby)

Supersedes: AFI33-401, 17 May 2011

Pages: 37

This Air Force Instruction (AFI) implements Air Force Policy Directive (AFPD) 17-1, *Information Dominance Governance and Management*, and Headquarters Air Force Mission Directive (HAF MD) 1-26, *Chief Information Dominance and Chief Information Officer*. It provides guidance for developing, maintaining, and implementing sound integrated and interoperable architectures across the Air Force; making architecture data discoverable, accessible, understandable, linked, and trustworthy; and ensuring interoperability for Information Technology (IT) and National Security System (NSS) systems and services that are Air Force only and not subject to Joint/Department of Defense (DoD) interoperability processes.

This AFI is consistent with DoDI 5000.75, *Business Systems Requirements and Acquisition*; Chairman Joint Chiefs of Staff Instruction (CJCSI) 3170.01I, *Joint Capabilities Integration and Development System (JCIDS)*; *Manual for the Operations of the Joint Capabilities Integration and Development System*; and Air Force Manual (AFMAN) 33-363, *Management of Records*.

This publication applies to individuals at all levels who prepare, manage, review, certify, approve, disseminate and/or use official Air Force architectures and interoperability assessments, including the Air Force Reserve (AFR) and Air National Guard (ANG), except where noted otherwise.

The authorities to waive wing/unit level requirements in this publication are identified with a Tier ("T-0, T-1, T-2, T-3") number following the compliance statement. See AFI 33-360, *Publications and Forms Management*, for a description of the authorities associated with the Tier numbers. Submit requests for waivers through the chain of command to the appropriate Tier waiver approval authority, or alternately, to the requestor’s commander for non-tiered compliance items.

Ensure that all records created as a result of processes prescribed in this publication are maintained in accordance with AFMAN 33-363, *Management of Records*, and disposed of in accordance with Air Force Records Disposition Schedule in the Air Force Records Information Management System (AFRIMS). Refer recommended changes and questions about this publication to the Office of Primary Responsibility (OPR) using the AF Form 847, *Recommendation for Change of Publication*; route AF Forms 847 from the field through the appropriate functional chain of command. This publication may be supplemented at any level, but all Supplements must be routed to the OPR of this publication for coordination prior to certification and approval.

SUMMARY OF CHANGES

This document has been substantially revised and needs to be completely reviewed. This instruction supersedes AFI 33-401, *Air Force Architecting*. This instruction incorporates interoperability guidance contained in expired Air Force Guidance Memorandum (AFGM) 2015-33-03. This publication establishes policy and assigns roles and responsibilities for developing, maintaining, storing, and implementing sound integrated and interoperable architectures across the Air Force for Information Technology (IT) and National Security System (NSS) across the four DoD mission areas to support decision-making processes and ensure the alignment of Air Force’s IT and NSS environment with the critical mission needs of the Air Force. It redefines the Air Force Enterprise Architecture (AFEA) framework and removes architecture approval and certification guidance and removes the Terms of Reference for the Architecture Executive Committee and Architecture Development Working Group.

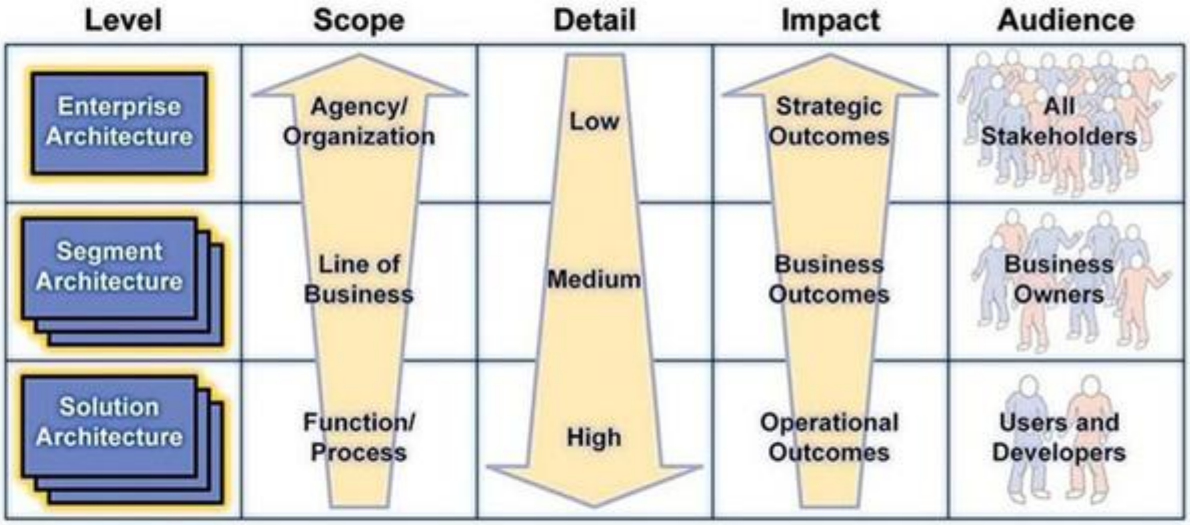
Chapter 1

ENTERPRISE ARCHITECTURE

1.1. Overview. Enterprise Architecture (EA) is a conceptual blueprint that defines the structure and operations of an organization. An organization uses EA to determine how to most effectively achieve its current and future objectives. The Air Force and DoD use EA to support key processes for requirements, acquisition, systems engineering, programming and budgeting of funds, interoperability, and portfolio management. EA includes a baseline (as-is) architecture, a target (to-be) architecture, and a sequencing plan for transitioning between the two.

1.1.1. **Levels of Architectures** . Depending on their purpose, architectures have different perspectives and varying amounts of information. As shown in **Figure 1.1**, enterprise-level, segment-level, and solution-level architectures provide different points of view by varying the level of detail and addressing related but distinct concerns.

Figure 1.1. Levels of Architecture. (Federal Enterprise Architecture Practice Guidance, 2007).



Level	Scope	Detail	Impact	Audience
Enterprise Architecture	Agency/ Organization	Low	Strategic Outcomes	All Stakeholders
Segment Architecture	Line of Business	Medium	Business Outcomes	Business Owners
Solution Architecture	Function/ Process	High	Operational Outcomes	Users and Developers

1.1.1.1. **Enterprise-level architecture** . Driven by an organization's strategy, enterprise-level architecture helps an organization identify whether its resources are properly aligned to its mission, strategic goals, and objectives. Enterprise-level architectures have a baseline (as-is) architecture, a target (to-be) architecture, and a transition strategy for the organization.

1.1.1.2. **Segment-level architecture** . Segment-level architecture describes individual elements of the enterprise, such as core missions, common or shared business services, and enterprise services. Segment-level architecture has a baseline (as-is), as well as a target (to-be) and a transition strategy for a portion of the enterprise. There are multiple segments within an enterprise architecture.

1.1.1.3. **Solution-level architecture** . Solution-level architecture is the most detailed level of architecture and portrays the relationships among elements to answer a problem. Solution architecture is the most common level of architecture developed. Solution-level architecture aligns to segment-level and enterprise-level architectures.

1.1.2. **Inputs to Architecture** . There are inputs to architectures that significantly impact their development and use as well as their ability to integrate with other architectures. These inputs can exist at any level of architecture and serve to guide and constrain architectures.

1.1.2.1. **Reference Architecture** . Reference Architecture is defined as an authoritative source of information about a specific subject area that guides and constrains architectures and solutions by providing common information, guidance, reusable components, and direction about the subject area. Reference architectures use this presentation of common information and components to provide a pattern for solving similar problems across multiple domains, which drives efficiency and interoperability. Reference architectures can exist at any architecture level and come from sources external and internal to the Air Force. For example, the Department of Defense Chief Information Officer (DoD CIO) developed a Cybersecurity Reference Architecture to convey the technical direction to guide and constrain cybersecurity solution architectures to meet DoD Information Enterprise cybersecurity goals. The Air Force has the Base Area Network Functional Specification which provides minimum functional standards to Major Commands (MAJCOM) that are deploying technologies throughout the Air Force.

1.1.2.2. **Mission threads** . Mission threads are a description of the end-to-end set of activities and systems that accomplish the execution of a specific mission and represent a horizontal segment of architecture. The resulting thread has a mission thread owner who works with architects to describe a capability by combining tasks, conditions, standards, and ways and means to create a desired effect. Mission threads draw from doctrine, training, and readiness manuals, and other authoritative capability-related data sources. Mission threads reduce interoperability risk by highlighting critical interfaces seen when solutions are placed into a real world context. This includes the cyber aspect of mission threads as IT evolves.

1.2. Air Force Enterprise Architecture .

1.2.1. **Definition** . The Air Force Enterprise Architecture (AFEA) is the collection of architecture data from strategic guidance and Air Force segment and solution architectures. It describes the people, processes, data, technology, and information used in the current state of Air Force investments and capabilities as well as future state and transition plans.

1.2.2. **Scope** . The AFEA applies to IT and NSS in the warfighting, business, intelligence, and information environment mission areas.

1.2.3. **Purpose** . The purpose of the AFEA is to enhance interoperability, mission effectiveness, security and cybersecurity, and financial efficiencies and to shape future technology transitions through guided investment portfolio strategies and decisions based on joint capability and interoperability requirements and defined standards.

1.2.4. **Objectives** .

1.2.4.1. The AFEA provides information on the Air Force core functions and missions and their interdependencies that supports Senior Leader decision-making to improve interoperability internally and externally to the Air Force.

1.2.4.2. The AFEA provides enterprise-wide visibility of people, processes, data, technology, and information.

1.2.4.3. The Air Force mission areas of the AFEA align to corresponding DoD mission area architectures helping to show the alignment of investments to portfolios.

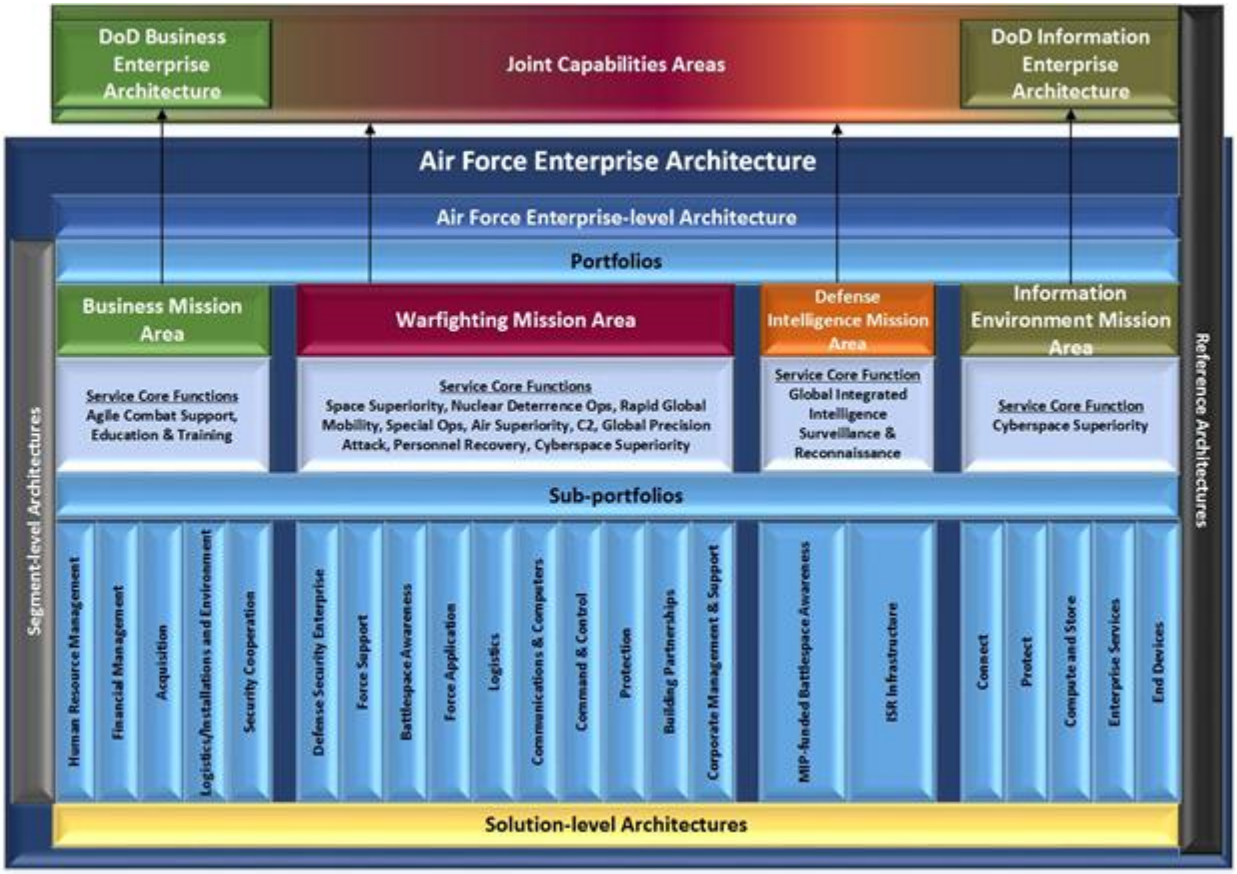
1.2.4.4. The AFEA supports analysis to identify redundancies, dependencies, and gaps in capabilities across the Air Force.

1.2.4.5. The AFEA guides, informs, and constrains segment and solution architectures.

1.2.4.6. The AFEA integrated dictionary provides a standard lexicon for the architecture data.

1.2.5. **Air Force Enterprise Architecture Framework** . **Figure 1.2** is a diagram showing the AFEA framework. Starting at the bottom of **Figure 1.2**, solution-level architectures fit into sub-portfolios which align to mission areas that are supported by the Service Core Functions. Segment-level architectures can exist from the sub-portfolios through the mission areas. The Air Force enterprise-level architecture is based on strategic guidance and the collection of architecture data from the mission area architectures. The mission area architectures align to the AFEA and DoD-level architectures. Reference architectures can exist at any level to guide and constrain enterprise-level, segment-level, and solution-level architectures.

Figure 1.2. Air Force Enterprise Architecture Framework.


DoD Business Enterprise Architecture
Joint Capabilities Areas
DoD Information Enterprise Architecture
Air Force Enterprise Architecture
Air Force Enterprise-level Architecture
Portfolios
Business Mission Area
Warfighting Mission Area
Defense Intelligence Mission Area
Information Environment Mission Area
Service Core Functions
Agile Combat Support, Education & Training
Service Core Functions
Space Superiority, Nuclear Deterrence Ops, Rapid Global Mobility, Special Ops, Air Superiority, C2, Global Precision Attack, Personnel Recovery, Cyberspace Superiority
Service Core Function
Global Integrated Intelligence Surveillance & Reconnaissance
Service Core Function
Cyberspace Superiority
Sub-portfolios
Human Resource Management
Financial Management
Acquisition
Logistics/Installations and Environment
Security Cooperation
Defense Security Enterprise
Force Support
Battlespace Awareness
Force Application
Logistics
Communications & Computers
Command & Control
Protection
Building Partnerships
Corporate Management & Support
MIP-funded Battlespace Awareness
ISR Infrastructure
Connect
Protect
Compute and Store
Enterprise Services
End Devices
Segment-level Architectures
Reference Architectures
Solution-level Architectures

1.2.6. **Architecture Data Integration** . Analysis and reporting is possible through the vertical and horizontal integration of architecture data. Vertical data integration begins by combining detailed solution architectures within a sub-portfolio, then the sub-portfolios are combined within a portfolio, and finally the portfolios are combined to provide the full breadth and depth of information in the AFEA. Horizontal integration is done through the analysis of mission threads (paragraph 1.1.2.2.).

1.2.6.1. **Analysis** . By having business and operational processes and the information assets that support them, it is possible to see how the Air Force is meeting the goals and objectives defined in the Air Force Strategic Master Plan.

1.2.6.2. **Portfolio Assignment** . Upon registration in Information Technology Investment Portfolio Suite (ITIPS), solutions architectures are assigned to a portfolio/sub-portfolio in the AFEA framework.

1.2.6.3. **Architecture Data Repositories** . Architecture data repositories are used to collect and integrate architecture data making analysis across many architectures possible.

Chapter 2

ROLES AND RESPONSIBILITIES

2.1. Secretary of the Air Force, Office of Information Dominance and Chief Information Officer (SAF/CIO A6) . In addition to duties in HAF MD 1-26, the SAF/CIO A6:

2.1.1. Appoints the Air Force Chief Architect.

2.1.2. Directs the Air Force Chief Architect to establish an office to develop the Air Force Enterprise Architecture (AFEA) and Air Force architecting policy.

2.1.3. Maintains a list of all Air Force IT systems in ITIPS.

2.1.4. Oversees the development, use, and maintenance of Air Force architectures (enterprise, segment, solution, and reference).

2.1.5. Advises the Air Force Chief of Staff on options and solutions to identified interoperability issues.

2.1.6. Uses approved architecture data and architecture data analysis to support decision-making and DoD efforts for example but not limited to the Federal Data Center Consolidation Initiative and the Joint Information Environment.

2.1.7. Develops guidance to require and demonstrate that Air Force Information Technology (IT) is interoperable and supportable with other relevant IT, internal and external to the Air Force.

2.1.8. Oversees the implementation of processes for the development, review, and approval of Air Force Information Support Plans.

2.1.9. Oversees the implementation of processes for the development and certification of the Net-Ready Key Performance Parameter for Air Force IT.

2.1.10. Oversees the implementation of processes for the interoperability test, evaluation, and certification of IT before connection to a DoD network.

2.1.11. Participates in other DoD Components' Information Support Plan (ISP) reviews.

2.1.12. Coordinates on Net-Ready Key Performance Parameter (NR KPP) on IT and National Security System (NSS) with joint, multinational, or interagency requirements prior to the Air Force Requirements Oversight Council and, when Air Force is the sponsor, prior to Joint Requirements Oversight Council.

2.1.13. Establishes procedures consistent with DoDI 8330.01 for interoperability certification or recertification for IT that does not have joint, multinational, interagency interoperability requirements.

2.1.14. Designates an Air Force Interoperability Certification Manager as approval authority for all Air Force IT with no joint, multinational, or interagency interoperability requirements and not governed by DoDI 8100.04, *DoD Unified Capabilities*, as described in Enclosure 3 of DoDI 8330.01.

2.1.15. Designates an Air Force representative to take part in and support the DoD Interoperability Steering Group.

2.1.16. Designs, develops, tests, evaluates, and incorporates IT interoperability into all Air Force IT. **(T-0).**

2.1.16.1. Requires that interoperability requirements are coordinated with the Chairman of the Joint Chiefs of Staff and the Combatant Commanders, and that each IT system design identifies all external IT interfaces with required joint, multinational, interagency, and other non-DoD systems. **(T-0).**

2.1.16.2. Recommends tradeoffs among operational effectiveness, operational suitability, cybersecurity (formerly information assurance), survivability, and IT interoperability to the USD (AT&L), the DoD CIO, and the Chairman of the Joint Chiefs of Staff. **(T-0).**

2.1.16.3. Requires IT programs be adequately funded to carry out the interoperability functions specified in DoDI 8330.01 and this guidance. **(T-0).**

2.1.17. Coordinates with Director, National Geospatial-Intelligence Agency on all geospatial intelligence-related requirements, ISPs, test strategies and plans, test and evaluation results, and interoperability certifications.

2.1.18. Coordinates with SAF/AQ to include technology and program protection requirements in architecting policies and processes to minimize the risk that DoD's warfighting mission capability could be impaired due to vulnerabilities in system design and architecture.

2.1.19. Coordinates with Deputy Chief of Staff, Intelligence, Surveillance and Reconnaissance (AF/A2) on all intelligence, surveillance, and reconnaissance and intelligence-related requirements, Program Protections Plans (PPP), ISPs, test and evaluation strategies/plans/results, and interoperability certifications.

2.2. Air Force Chief Data Officer (AF/CO).

2.2.1. Collaborates with the Air Force Chief Architect to define, guide, inform, and constrain the Air Force Data Architecture.

2.2.2. Establishes the scope, standards, and methodology for publication into the Air Force Enterprise Information Model.

2.2.3. Participates in Enterprise Architecture (EA) governance bodies.

2.3. Air Force Chief Architect. There is one Air Force Chief Architect who reports to the SAF/CIO A6.

2.3.1. Responsible for the AFEA.

2.3.2. Provides the status of the AFEA to the SAF/CIO A6.

2.3.3. Reviews the AFEA with the SAF/CIO A6 at least annually.

2.3.4. Participates in Federal, DoD, and Headquarters Air Force architecture governance bodies.

2.3.5. Establishes governance to oversee the development, assessment, alignment, adjudication, approval, compliance, maintenance, configuration management, change management, and application of the AFEA.

2.3.6. Maintains a list of Chief Architects appointed by Mission Area Owners, HAF/SAF Functionals, Air Force Reserve (AFR), Air National Guard (ANG), and Major Commands (MAJCOM).

2.3.7. Sets Air Force EA standards in line with DoD guidance and industry best practices. **(T-0).**

2.3.8. Defines architecture configuration management standards for the AFEA, and uses consensus standards in lieu of government specifications and standards, unless inconsistent with law or otherwise impractical.

2.3.9. Provides policy and guidance for architecture development including defining architecture data requirements and criteria.

2.3.10. Updates architecture development policy and guidance to address topics such as operational technology, agile software development, and rapid prototyping.

2.3.11. Provides oversight, analysis, and policy guidance to ensure compliance with mandated standards for developing, maintaining, and implementing sound integrated and interoperable architectures across the Air Force.

2.3.12. Establishes criteria for architecture compliance with Federal laws, and DoD, Joint Staff and Air Force policies and procedures.

2.3.13. Ensures all architectural views submitted as part of the AFEA or for interoperability assessments comply with the latest version of Department of Defense Architecture Framework (DoDAF). **(T-0).**

2.3.14. Develops and maintains the enterprise-level architecture portion of the AFEA.

2.3.15. Defines, develops, and maintains a common lexicon to assist with standardizing terms.

2.3.16. Provides a library of reference architectures and instructions on how they should be used to the Chief Architects.

2.3.17. Identifies enterprise-wide standards, services, and approaches for use in architecture development.

2.3.18. Captures and maintains strategic alignment of the AFEA to Air Force strategy and higher level (DoD/Joint Staff) requirements, to include goals and objectives defined in the Air Force Strategic Master Plan, Core Support Plans, and Flight Plans.

2.3.19. Ensures the AFEA aligns to DoD Mission Area architectures.

2.3.20. Oversees the maturation of the EA programs across the Air Force based on the General Accountability Office's (GAO) Enterprise Architecture Management Maturity Framework (EAMMF).

2.3.21. Establishes, operates and maintains the AFEA repository.

2.3.22. Organizes and coordinates architecture integration activities both internal and external to the Air Force enterprise.

2.3.23. Defines job skills requirements for Enterprise Architects.

2.3.24. Defines architecture education and training requirements.

2.3.25. Defines standard statement(s) for inclusion in requirements documents related to contracting for architecture services.

2.4. Mission Area Owners, HAF/SAF Functionals, AFR, ANG, MAJCOMs.

2.4.1. Collaborates with the Air Force Chief Architect to establish and maintain architecture policy, representing the needs of decision makers.

2.4.2. Plans architecting and interoperability for their area of responsibility and provides financial, manpower, and other resources to fulfill requirements.

2.4.3. Appoints a Chief Architect in writing and forwards a copy to the Air Force Chief Architect. As needed, appoints a Lead Architect to support the Chief Architect.

2.4.4. Approves architectures under their purview.

2.4.5. Uses approved architecture data and architecture data analysis to support decision-making.

2.4.6. Ensures subordinate organizations and Communities of Interest adhere to architecture standards and processes.

2.4.7. Provides Air Force representation, as required, on DoD IT Standards Registry (DISR) technical working groups for review and disposition of technical standards in support of SAF/CIO A6 and the command assigned the network management role.

2.4.8. Includes the Cyberspace Core Function Lead, in Architecture Review processes as the stakeholder for capacity and supportability on Air Force networks.

2.5. Chief Data Officer for Mission Area, HAF/SAF Functional, AFR, ANG, or MAJCOM.

2.5.1. Collaborates with the peer Chief Architect in the development of the data architecture for segment and solution architectures.

2.5.2. Ensures all information assets follow the Air Force Enterprise Information Model standards.

2.5.3. Facilitates identification of authoritative data for each information asset within their area of responsibility.

2.5.4. Assesses data health of information assets within their area of responsibility.

2.5.5. Mission Area Chief Data Officers collaborate with HAF/SAF Functional, AFR, ANG, and MAJCOM Chief Data Officers to identify data architecture efficiencies across the mission area.

2.5.6. HAF/SAF Functional Chief Data Officers identify and assign data stewards for each information asset within their area of responsibility in collaboration with Process Owners and AFR, ANG, and MAJCOM Chief Data Officers.

2.6. Chief Architect for Mission Area, HAF/SAF Functional, AFR, ANG, or MAJCOM. Each organization appoints a Chief Architect who interacts with the Air Force Chief Architect.

2.6.1. Interacts with the Air Force Chief Architect on matters related to the AFEA.

2.6.2. Manages the segment-level and solution-level architectures under their purview.

2.6.3. Captures and maintains strategic alignment of the segment-level and solution-level architecture to any applicable strategic guidance.

2.6.4. Aligns architectures to the segment-level, enterprise-level, or DoD architecture above them.

2.6.5. Defines architecture requirements and policy specific to their area of responsibility to include an architecture approval process.

2.6.6. Determines which architectures under their purview are required to support DoD and Air Force capabilities and processes and designates them as relevant to the AFEA.

2.6.7. Ensures that AFEA-related architectures conform to DoDAF.

2.6.8. Ensures the vertical and horizontal integration of AFEA-related architectures within their area.

2.6.9. Collaborates with other Chief Architects on the horizontal integration of AFEA-related architectures.

2.6.10. Coordinates and collaborates with other Chief Architects when an AFEA-related architecture spans multiple Service Core Functions (SCF) or portfolios by designating one of the Chief Architects with primary responsibility. If an agreement cannot be reached, the Chief Architects will raise the issue to the first Chief Architect that is in both their chains of command. If the issue cannot be resolved, it will continue up the chain of command ultimately to the Air Force Chief Architect to resolve.

2.6.11. Ensures architectures that are part of the AFEA are complete as a part of the review process.

2.6.12. Reviews and recommends approval of AFEA-related architectures for their respective organization after coordinating with applicable Chief Architects.

2.6.13. Enforces the use of enterprise-wide standards, services, and approaches whenever possible in the architectures.

2.6.14. Publishes approved architectures to an architecture data repository.

2.6.15. Defines architecture training and certification requirements for their architects.

2.6.16. Ensures architects are trained.

2.6.17. Participates in architecture governance bodies.

2.6.18. Applies architecture configuration management standards and processes.

2.6.19. Appropriately marks architectures with Classification and Distribution Statements.

2.6.20. Participates in architecture review processes in which they are a stakeholder (e.g. information exchange, network supportability, compliance issues).

2.7. Solution Architecture Steward. The Solution Architecture Steward represents the needs of a stakeholder community and is the primary source of information needed for solution-level architecture development. A Solution Architecture Steward participates throughout the solution architecture development and validates the architecture at the end of the architecture development process. Program Managers and Requirements Leads are examples of Solution Architecture Stewards. Solution Architecture Steward:

2.7.1. States the requirements for an architecture development effort and provides applicable documentation such as laws, regulations, and policies.

2.7.2. Identifies Subject Matter Experts (SME) and allocates time for identified SMEs to collaborate regarding the creation and validation of the architecture.

2.7.3. Conducts a thorough functional review of the architecture to validate the architecture meets the purpose for which it was built.

2.7.4. Signs a validation letter stating that the solution architecture meets the intended purpose.

2.7.5. Informs their Chief Architect that the architecture has been validated.

2.8. Architect.

2.8.1. Analyzes, defines, builds, maintains, and improves an architecture for a stated purpose.

2.8.2. Supports decision makers with architecture data and analysis.

2.8.3. Assists consumers and other architects with understanding the subject architecture to ensure an accurate reflection of interdependent capabilities and requirements for related architectures.

2.8.4. Uses enterprise-wide standards, services, and approaches whenever possible in the architecture.

2.8.5. Follows a documented change management process.

2.8.6. Stays current in tools, methods, and frameworks and maintains all required certifications (as applicable).

2.8.7. Submits architectures to the appropriate approval authority as required.

2.9. Architecture Consumer. An architecture consumer is a person who uses an architecture or the results of architecture analysis to gain information about the architecture's subject. Within a project team, an architecture consumer may be the project manager or the requirements manager. Portfolio Managers or cybersecurity assessors are also examples of architecture consumers.

2.9.1. Employs architecture and architecture analysis to support decision-making within their area of responsibility.

2.9.2. Uses architecture to reduce the complexity of the problem and understand the relationships identified with the architecture.

2.9.3. Uses architecture to identify gaps.

2.9.4. Uses architecture to find potential redundancies.

2.9.5. Uses architecture to understand resource allocation.

2.10. Air Force Interoperability Certification Manager.

2.10.1. Oversees development, review, and approval of Air Force ISPs which applies to IT that is not joint, multinational, or interagency. **(T-0).**

2.10.2. Reviews and approves requests to waive the requirement for interoperability testing of Air Force-unique systems. **(T-0).** Upon approval, provides the DoD CIO with copies of the waiver request and approval memorandum. If the waiver request is disapproved, the ISP and joint interoperability testing must occur. **(T-0).**

2.11. Air Force Representative to the DoD Interoperability Steering Group.

2.11.1. Serves as the Air Force interface to DoD CIO, Joint Staff, Program Managers, Program Sponsors and the Joint Interoperability Test Command (JITC) on coordination of interoperability issues among the DoD Components, and between DoD and other Federal level agencies/activities, and allied/coalition partners, as required. See DoDI 8330.01 for more information about the DoD Interoperability Steering Group.

2.11.2. Coordinates with JITC for interoperability certification testing. **(T-0).**

2.11.3. Assists Program Managers with preparing an Interim Certificate to Operate (ICTO) request for consideration by the Interoperability Steering Group when all the requisite actions (ISP approval, NR KPP certification, JITC coordination) have not been completed.

2.11.4. Reviews, endorses, and submits ICTO requests to the Interoperability Steering Group. Returns unendorsed ICTO requests to Program Managers for further development.

2.11.5. Tracks IT and NSS. IT or NSS with significant interoperability deficiencies, or not making significant progress toward achieving Joint Interoperability Test Certification, are placed on the Operating at Risk List. **(T-0).** The Operating at Risk List contains all IT systems denied an ICTO and that have not received a waiver. The Operating at Risk List is maintained by the Defense Information Systems Agency (DISA)**.**

2.12. Program Managers.

2.12.1. Incorporate funding requirements, manpower and associated resources into program planning to ensure architecture, interoperability, and supportability requirements are completed and approved in sufficient time to meet milestone dates.

2.12.2. Incorporate funding requirements, manpower and associated resources into program planning to ensure interoperability testing requirements are budgeted and approved in sufficient time to meet milestone dates.

2.12.3. Coordinate with the Air Force Representative to the DoD Interoperability Steering Group and with JITC for interoperability certification tests conducted by the JITC.

2.12.4. Designate a Chief Developmental Tester or Test Manager (for non-oversight programs) to oversee the execution of test requirements, per AFI 63-101/20-101 and AFI 99-103.

2.12.5. Develop an ISP for all IT and NSS for programs governed by DoDI 5000.02 that exchange data, unless waived by the SAF/CIO A6 Interoperability Certification Manager. For programs governed by DoDI 5000.75, provide ISP-type information in the design specification for all IT that exchange data.

2.12.6. Register Air Force IT in ITIPS which will generate an ITIPS number. Registration in ITIPS automatically generates a DoD IT Portfolio Repository (DITPR) number for certain records. Either the ITIPS number or DITPR number must be documented on the ISP.

2.12.7. Ensure that risk-reducing countermeasures for security-related threats are identified and recorded in the program's Program Protection Plan (PPP). Per AFI 63-101/20-101, *Integrated Life Cycle Management*, include the approved PPP as supporting document in the attachment section of the ISP.

2.12.8. Describe IT/NSS dependencies and interface requirements in sufficient detail to enable supportability requirements planning, test planning, and for verification of the NR KPP.

2.12.9. Contact ACC/A5JI for Air Force systems using Tactical Data Links (TDL) to schedule an Air Force System Interoperability Test to obtain their TDL military standard (MIL-STD) compliance certification.

Chapter 3

ENTERPRISE ARCHITECTURE PRACTICE

3.1. Use of Architectures. The information and relationships contained in the Air Force Enterprise Architecture (AFEA) provides visibility that will be used to support the following decision-making processes.

3.1.1. **Transformations.** Whether it is migrating a system to the cloud or revamping an entire capability area, architecture data supports transformation through the use of defined, consistent, related, structured data that is applied to the current state, the future state, and transition plan.

3.1.2. **Business Process Reengineering** . Architectures document processes, which are analyzed by the organization's management office for improvements such as faster delivery and reduced costs.

3.1.3. **Rationalization/Identification of Redundancies** . Through the consistent capture of data, capabilities, systems, and applications, information can be compared allowing for the identification of potential redundancies that can be analyzed for rationalization.

3.1.4. **Capability Requirements** . Architectures are used to support AFI 10-601, *Operational Capability Requirements Development*, and AF/A5R Requirements Development Guidebook, Volumes 1-4, to validate and prioritize all Air Force capability requirements. Architecture is also used for capability risk analysis by identifying capability relationships and program interdependencies that could cause risk to other organizations and programs if unfilled or delayed.

3.1.5. **Portfolio Management and IT Investment Review** . Architecture data supports AFI 17-110, *IT Portfolio Management and Capital Planning and Investment Control*, through the analysis of architecture data by portfolios and showing the relationships between portfolio objectives and DoD/Air Force enterprise vision, mission, goals. Architectures also support portfolio management by showing performance measures and identifying capability gaps, opportunities, and redundancies. Additionally, an investment's solution architecture must be compliant with DoD and Air Force guidance to support operational and technical testing of IT systems. **(T-1).**

3.1.6. **Clinger-Cohen Act (CCA) Compliance** . The Clinger-Cohen Act's purpose is to ensure that an IT investment supports the agency's mission. AFMAN 17-1402, *Air Force Clinger-Cohen Act Compliance Guide*, defines the CCA compliance and reporting process. There are eleven CCA compliance elements, two of which are related to architectures. CCA Compliant Element 8 deals with showing how the investment is consistent with DoD Information Enterprise policies and architecture, to include standards. CCA Compliance Element 9 focuses on ensuring a program has a Cybersecurity Strategy that is consistent with DoD policies, standards, and architectures. Refer to AFMAN 17-1402, Architecture Assessment Checklist for CCA Compliance, for specific architecture requirements.

3.1.7. **Risk Management** . Architecture supports AFI 17-101, *Risk Management Framework (RMF) for Air Force IT*, which outlines the security architecture using technical standards, protocols, technology, and guidance to establish consistent, secure environments needed for IT deployment.

3.1.8. **Acquisition** . Architecture supports DoDI 5000.02, DoDI 5000.75, and AFI 63-101/20-101 by using DoDAF to present architecture data in a consistent manner to support program documentation at decision points within the acquisition process.

3.1.9. **System Engineering** . Architecture supports implementation of AFI 63-101/20-101, Chapter 5, Systems Engineering. Enterprise Architecture (EA), with authoritative data, is essential to make informed systems engineering decisions throughout the Acquisition and Sustainment Life Cycle. EA supports a digital engineering approach, data-driven design reviews, and model-based systems engineering processes and methodologies. These processes and methodologies enable analysis and decision-making to explicitly consider cost and capability tradeoffs not just of the weapon/business system design, but also of the systems of systems (SoS) architecture and potential family of future upgrades and variants. Systems Engineers should consider use of architecture, modeling, and analytical tools for all steps of the Systems Engineering Process.

3.1.10. **Test and Evaluation** . Architecture data includes detailed information about interfaces that are critical to testing and evaluation in support of AFI 99-103, *Capabilities-Based Test and Evaluation.*

3.1.11. **Interoperability** . Air Force IT must be able to exchange and use data and information, to the maximum extent practical, with existing and planned systems and IT services within the Air Force as well as across component, joint, combined, and coalition forces, other US Government departments and agencies, and non-governmental organizations. **(T-0).** Architecture data is used to describe the information exchanges, describe characteristics of the data being exchanged, and the operational processes that the exchanges support.

3.2. Architecture Development.

3.2.1. All architectures that are part of the Air Force Enterprise Architecture (AFEA) will use the latest version of the DoD Architecture Framework. Information about DoDAF can be found at the public website, **http://dodcio.defense.gov/Library/DoD-Architecture-Framework/**. **(T-0).**

3.2.2. For AFEA-related architectures, architecture will be data-driven. **(T-1)**

3.2.3. Architectures will be developed and implemented consistent with the following principles:

3.2.3.1. Air Force systems and services will be conceived, designed, operated and managed to address Air Force capability requirements. **(T-1)**

3.2.3.2. Air Force solutions will use enterprise-wide standards, services, and approaches to deliver seamless capabilities, help IT consolidations through reuse, and simplify the use of end-user functions. **(T-1)**

3.2.3.3. Air Force architecture data will be discoverable, accessible, understandable, linked, and trustworthy to all authorized users, including unanticipated users. **(T-0).**

3.2.3.4. Air Force architecture data will be made understandable and consistent through the use of the AFEA lexicon and the use of authoritative data sources. **(T-1)**

3.2.3.5. Air Force systems and services will be made interoperable through the definition and enforcement of technology standards, interface profiles, and implementation guidance. **(T-0)**

3.2.4. Update architecture in accordance with the current version of DoDAF when there is a reason to change it. **(T-2).** An architecture does not have to be updated solely to conform to the latest version of DoDAF.

3.2.5. Use architecture tools that are DoDAF Metamodel (DM2) compliant and able to exchange architecture data in standard formats, including but not limited to Extensible Markup Language. **(T-2).**

3.2.6. Use appropriate reference architectures to guide and constrain segment and solution architectures. **(T-2).**

3.2.7. Ensure architectures are traceable to higher level architectures; specifically, that solution architectures align to higher level segment and enterprise architectures. **(T-2).**

3.2.8. Ensure architectures can be traced to strategic guidance such as Flight Plans. **(T-2).**

3.2.9. Ensure architectures that are part of the AFEA are complete. **(T-2)** Complete means the required, minimum set of data elements needed for the AFEA to support strategic-level decision-making have been included in the architecture. There will be no waivers issued for architectures that are not complete. For older programs and capabilities that do not have an architecture, it will suffice to provide a Plan of Actions and Milestones which will provide a timeline of when the solution architecture will be developed. **Exception**: Programs that will be retired within the Future Years Defense Program (FYDP) do not need to develop an architecture.

3.2.10. Post approved architectures to the relevant segment or enterprise architecture repository where they will be discoverable, accessible, reusable, shared, secure, interoperable, and understandable. **(T-2).**

3.2.11. Ensure architectures use validated cybersecurity solutions, products, and services when available and cost effective. **(T-1)**

3.2.12. Updates to an existing architecture will maintain the current cybersecurity posture of the system, including all of its program protection requirements. **(T-1)**

3.2.13. Architectures governed by DoDI 5000.02 will be allocated cybersecurity and related system security requirements and will be assessed for vulnerabilities. **(T-0)**

3.2.13.1. The architectures will address, at a minimum, how the solution:

3.2.13.1.1. Is structured to protect and preserve system functions or resources, e.g. through segmentation, separation, isolation, or partitioning. **(T-0)**

3.2.13.1.2. Monitors, detects, and responds to security anomalies. **(T-0)**

3.2.13.1.3. Contributes to the development of Anti-Tamper architectures and technologies in coordination with the DoD Executive Agent for Anti-Tamper, based on the presence of Critical Program Information (CPI) in the solution and the consequence of CPI compromise as well as system exposure, per DoDD 5200.47E. **(T-0)**

3.2.13.2. Ensure architectures apply DoDI 8500.01 and DoDI 8510.01 in accordance with Air Force implementation and governance procedures. **(T-0)**

3.2.14. Ensure architectures use trusted suppliers or appropriate Supply Chain Risk Management (SCRM) countermeasures for system elements that perform mission-critical functions. Cyber protection measures for mission-critical functions (MCF) and critical components (CC) must, at a minimum, include software assurance (SwA), hardware assurance (HwA), procurement strategies, and anti-counterfeit practices in accordance with DoDI 5200.44, *Protection of Mission Critical Functions to Achieve Trusted Systems & Networks (TSN).* **(T-0)**

Chapter 4

INTEROPERABILITY AND SUPPORTABILITY

4.1. Interoperability.

4.1.1. In accordance with DoDI 8330.01, Air Force IT must interoperate, to the maximum extent practicable, with existing and planned systems and IT services within the bounds of the Air Force as well as external organizations without compromising its existing cybersecurity posture and Critical Program Information. (**T-0)** External organizations are component, joint, combined, and coalition forces, other US Government departments and agencies, and non-governmental organizations.

4.1.2. Applicability.

4.1.2.1. Interoperability applies to IT (systems, applications, products, or IT services) that the Air Force acquires, procures, or operates, including IT that:

4.1.2.1.1. Supports all DoD mission areas.

4.1.2.1.2. Provides Air Force enterprise services.

4.1.2.2. Interoperability does not apply to IT that:

4.1.2.2.1. Only performs the functions of simulation or training and only stores, processes, or exchanges simulated data, and has no possibility of exporting data into an operational system.

4.1.2.2.2. Is used exclusively for demonstration or simulation, imports but does not export real-world data, and does not use that data to support any operational process or decision-making.

4.1.3. All Air Force IT and NSS must participate in and comply with interoperability risk assessments set forth in DoD or Air Force policy. **(T-0).** This is true for all mission areas, warfighter, business, intelligence and enterprise information environment.

4.1.4. Program Managers must use the interoperability tab in ITIPS to determine requirements for interoperability assessments, waiver eligibility, and other courses of action. **(T-1).** The tab includes explanatory guidance or policy references for each question. Answering questions in this tab is the first step toward determining interoperability certification actions.

4.1.5. All IT must have a NR KPP as part of its interoperability requirements documentation. **(T-0).**

4.2. Interoperability Assessments.

4.2.1. **Information Support Plans (ISPs).** ISPs apply to programs governed by DoDI 5000.02 and DoDI 8330.01. ISPs enable the Air Force and Joint communities to conduct IT/NSS supportability assessments. The ISP is technical document that provides Program Managers a means to identify and resolve potential information support implementation issues and risks that, if not properly managed, will limit or restrict the ability of a program to be operationally employed to support existing and future mission requirements. It is an authoritative document that directly informs the program's Test and Evaluation Master Plan with threshold and objective operations parameters, and it is a key vehicle that supports validation of a program's eligibility for interoperability certification. The ISP contains or includes a link to the NR KPP along with supporting architectural data.

4.2.1.1. The ISP identifies IT and information (including intelligence) needs, dependencies, and interfaces for programs in all acquisition categories, focusing on interoperability, information and system supportability, and information sufficiency concerns.

4.2.1.2. The ISP assesses the program's path toward becoming Net-centric and describes the program's Cybersecurity compliance, and addresses supportability topics like Intelligence, Bandwidth and Spectrum.

4.2.1.3. The ISP includes an operational employment concept; system interface descriptions; required information exchanges; and IT and NSS information support requirements derived from analysis of applicable Joint Operating Concepts, Joint Functional Concepts, Joint Integrating Concepts, and JCIDS documentation. In addition, it includes the associated integrated architecture(s), potential issues or risks, and proposed solutions or risk mitigation plans.

4.2.1.4. Air Force organizations with equity in programs undergoing review will provide subject-matter expert (SME) support for assessment of ISPs via the Global Information Grid (GIG) Technical Guidance Federation (GTG-F) system. **(T-0)**

4.2.1.5. **Requirements to Develop an ISP.**

4.2.1.5.1. **Acquisition** . An ISP is required for all IT or NSS acquisition category (ACAT) and non-ACAT programs that exchange data of any type to other systems (e.g. not a stand-alone system or application). For systems that will be part of a Family of Systems or System of Systems (FoS/SoS), an ISP is normally required. However, if the Milestone Decision Authority/Cognizant Fielding Authority for the FoS/SoS agree, an annex to the FoS/SoS ISP may be developed to meet the ISP requirement for the new system. If the FoS/SoS program does not have an ISP (i.e., a legacy fielded system not undergoing a major modification), then an ISP must be developed. **(T-0).**

4.2.1.5.2. **Procurement** . An ISP is required for IT/NSS commercial-off-the-shelf or government-off-the-shelf (COTS/GOTS) procurements that exchange information of any type to other systems (e.g. not a stand-alone system or application). This is true even when the system being procured has been certified for use on the Air Force Network, unless a waiver is authorized. The level of detail in the ISP will be consistent with JCIDS requirements at each major milestone or decision point, and the technical and programmatic information available on the system. **(T-0).**

4.2.1.5.3. **Fielded Systems – Major Modification** . Fielded systems that exchange information of any type to other systems (e.g. not a stand-alone system or application) that did not develop an ISP or a Command, Control, Communications, and Computers Intelligence Support Plan (C4ISP) during the acquisition phase are required to develop a system level ISP if they undergo a major modification/change. A major modification/change occurs when any of the following criteria are met (also for modifications that involve a new capability to exchange information):

4.2.1.5.3.1. A NR KPP must be developed or modified as a result of the planned modification, per AFI 10-601, para 6.4. **(T-1).**

4.2.1.5.3.2. JCIDS documents are developed or modified as the result of the planned modification, per DoDI 8330.01. **(T-0).**

4.2.1.5.3.3. The modification exceeds 10% of ACAT II minimum thresholds, per AFI 10-601, Table 6.1. **(T-1).**

4.2.1.5.3.4. Fielded Systems – Interoperability Recertification. For those legacy systems that were not required to develop an ISP and must undergo a J-6 Interoperability Recertification, a system-level ISP must be developed to support the recertification effort. **(T-0).**

4.2.1.6. **ISP Submission Requirements.**

4.2.1.6.1. **Pre-Engineering and Manufacturing Development (Pre-EMD)** . DoDI 5000.02 requires that Program Managers plan for and Milestone Decision Authorities conduct a Pre-Engineering and Manufacturing Development Review before releasing the final Request for Proposal for the EMD Phase. Pre-EMD Review documents, which include the ISP, must be provided in final draft form prior to this review. **(T-0).**

4.2.1.6.2. **Milestone B (MS B)** . MS B will be conducted according to the procedures outlined in DoDI 5000.02. Unless submitted and approved in support of the Pre-EMD Review, all remaining MS B information requirements (including any significant changes to documents following the Pre-EMD Review) will be satisfied prior to the milestone. **(T-0).**

4.2.1.6.3. **Major Milestones and Decision Points (Milestone C, Critical Design Review, etc.)** . Per DoDI 5000.02, ISPs that were developed at MS B must be updated at each major decision point to reflect any changes in the requirements or design of the system since the initial ISP was developed. **(T-0).**

4.2.1.6.4. **Fielded Systems – Major Modification** . When a fielded system undergoes a Major Modification, the existing ISP must be updated (see paragraph **4.2.1.5.3** for what constitutes a major modification). **(T-0).**

4.2.1.6.5. **Fielded Systems – Interoperability Recertification** . When a fielded system undergoes a periodic Joint Staff J6 Interoperability & Supportabilty (I&S) Recertification, the existing ISP must be updated. The ISP must be evaluated for need of an update upon expiration of an existing I&S Certification. **(T-0).**

4.2.1.7. **Additional ISP Guidance** . Air Force Instructions that require the development of ISPs include: AFI 10-601, AFI 63-101/20-101, and AFI 99-103. All Air Force organizations involved in the acquisition of IT or NSS are required to develop ISPs according to the above instructions. Specific guidance and instructions for ISP development, staffing and approval are provided in the Air Force Program Manager's Guide for Developing and Processing Information Support Plans and Associated Interoperability Guidance, available on the restricted access Air Force Interoperability & ISP SharePoint site: **https://cs2.eis.af.mil/sites/13157/default.aspx**.

4.2.1.8. **ISP Exceptions** . Air Force-unique interoperability policy may be waived using the procedures below. The waiver process will identify low risk systems connected to the Air Force's network infrastructure and increase visibility of systems supporting the warfighter. These waivers do not apply to other requirements such as survivability or cybersecurity. Waivers are submitted to the Air Force Interoperability Certification Manager.

4.2.1.8.1. The ISP is not required for programs with functions of simulation or training and only stores, processes, or exchanged simulated data, and has no possibility of exporting data into an operational system. ISPs are also not required for systems used exclusively for demonstration or simulation, imports but does not export real-world data, and does not use that data to support any operational process or decision making.

4.2.1.8.2. The ISP is not required for programs designated as DoD Unified Capabilities and governed by DoDI 8100.04.

4.2.1.8.3. An ISP waiver may be granted on a case-by-case basis for Air Force unique programs with Commercial Off-the-Shelf solutions that have minimal or manual data exchange requirements and for programs with system data that is not exchanged via the DoD Information Network.

4.2.1.9. **Global Information Grid (GIG) Technical Guidance Federation (GTG-F) Tool.**

4.2.1.9.1. The ISP will be developed within the GIG Technical Guidance Federation (GTG-F) using the Enhanced Information Support Plan (EISP) Enterprise Service Version template. **(T-0).** The GTG-F is an integrated ISP development, staffing, analysis, approval and archiving environment used by DoD and Joint commands. The CAC-enabled GTG-F homepage is located at **https://gtg.csd.disa.mil/**. The GTG-F supports unclassified ISPs. The Air Force Program Manager's Guide for Developing and Processing Information Support Plans and Associated Interoperability Guidance describes an alternate process for classified ISPs.

4.2.1.9.2. ISPs are approved after formal assessment through the GTG-F review process. The formal review process must be repeated for each major decision point in the acquisition lifecycle. Additional reviews may be required when programs have unique reporting requirements based on interoperability concerns raised by assessor organizations to the Air Force Interoperability Certification Manager. Specific guidance and instructions for ISP development, staffing and approval are provided in the Air Force Program Manager's Guide for Developing and Processing Information Support Plans and Associated Interoperability Guidance, available on the Air Force restricted access Interoperability & ISP SharePoint site: **https://cs2.eis.af.mil/sites/13157/default.aspx**.

4.2.2. **ISP-type Information Submission Requirements for Programs governed by DoDI 5000.75** . The DoDI 5000.75 removes the requirement to develop an ISP for business systems. ISP-type information will be included in the design specifications. **(T-0).** AFMAN 63-144, Defense Business System Life Cycle Management, provides Air Force specific guidance on implementation and oversight management of defense business systems.

4.2.3. **Net-Ready Key Performance Parameter (NR KPP).**

4.2.3.1. Per DoDI 8330.01, all IT/NSS must have a NR KPP as part of its interoperability requirements documentation. **(T-0).**

4.2.3.2. The NR KPP identifies operational, net-centric requirements in terms of threshold and objective values for Measures of Effectiveness (MOE) and Measures of Performance (MOP). The NR KPP covers all communication, computing, and electromagnetic spectrum requirements involving information elements among producer, sender, receiver, and consumer. Information elements include the information, product, and service exchanges. These exchanges enable successful completion of the warfighter mission or joint business processes.

4.2.3.3. Refer to the "Content Guide for the Net-Ready KPP" found in Appendix E to Enclosure D in the JCIDS Manual for additional information about the NR KPP.

4.2.4. **Air Force Interoperability Certification Requirements.**

4.2.4.1. For programs required to have Interoperability Certification, Interoperability & Supportability is an end-to-end process that concludes with the Interoperability Certification. Interoperability testing must be comprehensive, cost effective, and completed with interoperability certification granted, before fielding of a new IT capability or upgrade. **(T-1).**

4.2.4.2. For programs that require a Test and Evaluation Master Plan (TEMP), an interoperability Development Test Plan must be included in the TEMP and interoperability demonstrated by Milestone C/Acquisition Authority to Proceed to support interoperability certification during Initial Operational Test & Evaluation. **(T-1).**

4.2.4.3. To ensure the entrance criteria is met for the system to get into a Joint Interoperability Test, Program Managers must coordinate closely with the Joint Interoperability Test Command under DISA to review the NR KPPs and ensure test plan adequacy to verify the system meets NR KPP requirements, TEMPs (if applicable), test criteria, and associated developmental and operational test plans for interoperability. **(T-0).**

4.2.4.3.1. For Air Force systems using Tactical Data Links (TDL), Program Managers must contact ACC/A5JI to schedule an Air Force System Interoperability Test to obtain their TDL military standard (MIL-STD) compliance certification. Once obtained, ACC/A5JI will nominate the system for entrance into a Joint Interoperability Test to obtain its joint interoperability certification. **(T-1).**

4.2.4.3.2. AF/A2 must ensure interoperability test, evaluation and certification of Intelligence Surveillance and Reconnaissance (ISR) NSS before connection to an Intelligence Community network. **(T-1).**

4.2.4.3.3. Joint Interoperability Test Command must ensure interoperability test, evaluation, and certification of IT before connection to a DoD network. **(T-0).**

4.3. Supportability.

4.3.1. **Intelligence Supportability** . Intelligence integration in support of Air Force and joint systems development is essential in modernization processes in order to develop systems that work as advertised without scheduling delays, cost over-runs, and problems with supportability and interoperability. Ideally, intelligence integration should occur early in the acquisition process, preferably at the conceptual phase.

4.3.1.1. **Intelligence Sensitivity** . The first step of this process is to determine whether or not the program/initiative is intelligence-sensitive. The customer should engage with their supporting intelligence representative to determine whether or not intelligence support is required. If the program/initiative is determined to be intelligence-sensitive, then an Intelligence Appendix to the ISP must be created. **(T-1).** Refer to the Intelligence Appendix in the Air Force Program Manager's Guide for Developing and Processing Information Support Plans and Associated Interoperability Guidance on the GTG-F site for further instruction.

4.3.1.2. **Other Intelligence Considerations** . If intelligence support is required, follow the procedures in the Intelligence Chapter of the Defense Acquisition Guidebook. Additionally, the Life-Cycle Mission Data Plan should be used to define specific intelligence mission data requirements for a program. Intelligence mission data includes, but is not limited to the following functional areas: characteristics and performance, electronic warfare integrated reprogramming, order of battle, geospatial intelligence and signatures. Also, programs should follow the procedures in accordance with DoDD 5250.01, *Management of Intelligence Mission Data in DoD Acquisition*.

4.3.2. **Spectrum Supportability** .

4.3.2.1. Spectrum Supportability represents a nation's indication of its intent to support, to the extent practical, sufficient electromagnetic spectrum necessary for the operation of a spectrum-dependent equipment or system during its expected life cycle. The equipment or system must be authorized to use spectrum that is, or will be, available from system development, through developmental and operational testing, to actual operation in the electromagnetic environment. The assessment of an equipment or system having "spectrum supportability" requires, at a minimum, receipt of equipment spectrum certification, reasonable assurance of the availability of sufficient frequencies for operation, and consideration of the electromagnetic compatibility. Positive spectrum supportability is not to be construed to be an authorization to transmit or a radio-frequency assignment.

4.3.2.2. In accordance with DoDI 4650.01, *Policy and Procedures for Management and Use of the Electromagnetic Spectrum*, paragraph 4e, all spectrum dependent systems will determine if there will be sufficient spectrum to support operation of the system during its life cycle. **(T-0).**

4.3.2.3. Air Force spectrum dependent system developers/Program Managers will ensure that spectrum supportability requirements are addressed through:

4.3.2.3.1. Proper submission of a DD Form 1494, *Application for Equipment Frequency Allocation*, by the acquiring activity for spectrum certification activities and Host National Coordination. **(T-1).**

4.3.2.3.2. Description of spectrum dependent system use, e.g. high-level operational concept graphic (OV-1), and other artifacts that show how systems or system-of-systems will use the electromagnetic spectrum. Descriptions should also depict as applicable: Air-to-Air, Air-Ground-Air, Air/Space, Ground-to-Ground. **(T-1).**

4.3.2.3.3. On-going reviews and assessments of relevant JCIDS documents and ISPs. **(T-1).**

4.3.2.3.4. Review of relevant NR KPPs ensuring spectrum is appropriately addressed. **(T-1).**

4.3.2.3.5. Initiation of the Spectrum Supportability Risk Assessment process, as required for each acquisition milestone decision action, i.e. Regulatory, Technical, Operational and E3 Risks which adversely impact operations. **(T-1).**

4.3.2.4. For help determining specific spectrum supportability issues, contact the Air Force Spectrum Management Office or MAJCOM spectrum management office. See AFI 17-220, *Spectrum Management*, for spectrum requirements processing. Detailed procedures for processing spectrum supportability requirements in the ISP are available in the Air Force Program Manager’s Guide for Developing and Processing Information Support Plans and Associated Interoperability Guidance.

4.3.3. **Bandwidth Supportability** .

4.3.3.1. The ISP review process assesses bandwidth requirements. These are external dependencies on the DoD communications architecture, to include line-of-sight wireless networks, datalinks, satellite communications, other beyond-line-of-sight communications, and wired/fiber networks. Through the ISP assessment process, the DoD CIO reviews program ISPs for section 1047(d) of the Duncan Hunter National Defense Authorization Act for Fiscal Year 2009 (Public Law 110-417) compliance. Section 1047(d) specifies, as part of the Milestone B approval process, that a review will be performed for major defense acquisition programs and major system acquisition programs to ensure the bandwidth requirements needed to support such programs are or will be met and how. **(T-0).** For defense business systems governed by DoDI 5000.75, the MS-B equivalent is the Acquisition Authority to Proceed (ATP). **(T-0).**

4.3.3.2. The Milestone C ISP submission will address bandwidth requirements in greater detail. **(T-0).** The submission must address the information sharing requirements and its potential impact to the DoD Information Network. In order for DoD Networks/resources to accommodate a program’s future bandwidth, considerations must address areas such as Terrestrial Transport, Satellite Transport, Internet Protocol, Voice, and Video.

4.3.3.3. The DoD CIO provides guidance to programs, directly or through the Air Force Representative to the Interoperability Steering Group. The DoD CIO also assesses bandwidth supportability risks and informs the Defense Acquisition Executive of pertinent elevated risks through periodic summary reviews of acquisition programs.

4.3.3.4. Detailed guidance on the DoD Bandwidth requirements process is available in the Defense Acquisition Guide under Section 7.11.

BRADFORD J. SHWEDO, Lt Gen, USAF
Chief of Information Dominance and
Chief Information Officer

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

AF/A5R Requirements Development Guidebook, Vol 1-4, 20 March 2018

AFI 10-601, *Operational Capability Requirements Development*, 6 November 2013

AFI 17-101, *Risk Management Framework (RMF) for Air Force Information Technology (IT)*, 02 February 2017

AFI 17-110, *Information Technology Portfolio Management and Capital Planning and Investment Control*, 23 May 2018

AFI 17-220, *Spectrum Management*, 16 March 2017

AFI 33-360, *Publications and Forms Management*, 1 December 2015

AFI 63-101/20-101, *Integrated Life Cycle Management*, 9 May 2017

AFI 99-103, *Capabilities-based Test and Evaluation*, 6 April 2017

AFMAN 17-1402, *Air Force Clinger-Cohen Act (CCA) Compliance Guide*, 20 June 2018

AFMAN 33-363, *Management of Records*, 1 March 2008

AFMAN 63-144, *Defense Business System Life Cycle Management*, 31 March 2016

AFPD 17-1, *Information Dominance Governance and Management*, 12 April 2016

Air Force Base Area Network Functional Specification, 2015

Air Force Program Manager's Guide for Developing and Processing Information Support Plans and Associated Interoperability Guidance, Version 3.0, 26 January 2016

CJCSI 3170.01I, *Joint Capabilities Integration and Development System (JCIDS)*, 23 January 2015

Defense Acquisition Guidebook, Defense Acquisition University, **https://www.dau.mil/tools/dag**

DoD Architecture Framework (DoDAF), Version 2.02, **http://dodcio.defense.gov/Library/DoD-Architecture-Framework/**

DoD Cybersecurity Reference Architecture, Version 4.0, 1 Jul 2016, **https://wmaafip.csd.disa.smil.mil**

DoD Information Enterprise Architecture Version 2.0, July 2012

DoD Reference Architecture Description, June 2010

DoDD 5000.01, *The Defense Acquisition System*, 12 May 2003

DoDD 5200.47E, *Anti-Tamper (AT)*, 4 September 2015

DoDD 5250.01, *Management of Intelligence Mission Data in DoD Acquisition*, 22 January 2013

DoDD 8000.01, *Management of the Department of Defense Information Enterprise*, 17 March 2016

DoDD 8115.01, *Information Technology Portfolio Management*, 10 October 2005

DoDI 4650.01, *Policy and Procedures for Management and Use of the Electromagnetic Spectrum*, 9 January 2009

DoDI 5000.02, *Operation of the Defense Acquisition System*, 7 January 2015

DoDI 5000.75, *Business Systems Requirements and Acquisition,* 2 February 2017

DoDI 5200.44, *Protection of Mission Critical Functions to Achieve Trusted Systems & Networks,* 5 November 2012

DoDI 8100.04, *DoD Unified Capabilities*, 9 December 2010

DoDI 8310.01, *Information Technology Standards in the DoD*, 2 February 2015

DoDI 8320.03, *Unique Identification (UID) Standards for Supporting the DoD Information Enterprise*, 4 November 2015

DoDI 8330.01 *Interoperability of Information Technology (IT), Including National Security Systems (NSS)*, 21 May 2014

DoDI 8500.01, *Cybersecurity*, 14 March 2014

DoDI 8510.01, *Risk Management Framework (RMF) for DoD Information Technology (IT)*, 12 March 2014

Federal CIO Council, *A Common Approach to Federal Enterprise Architecture*, May 2012

Federal Enterprise Architecture Program Management Office, *Federal Enterprise Architecture Practice Guidance*, November 2007

Government Accountability Office, *Organizational Transformation: A Framework for Assessing and Improving Enterprise Architecture Management*, August 2010

HAF Mission Directive 1-26, *Chief Information Dominance and Chief Information Officer*, 5 February 2015

Information Dominance Flight Plan, February 2017

Joint Interoperability Test Command Interoperability Process Guide v2.0, 23 March 2015

Manual for the Operations of the Joint Capabilities Integration and Development System, 12 February 2015

United States Air Force Strategic Master Plan, May 2015

Prescribed Forms

None

Adopted Forms

AF Form 847, Recommendation for Change of Publication

DD Form 1494, Application for Equipment Frequency Allocation

Abbreviations and Acronyms

ACAT— Acquisition Category

AF— Air Force

AFEA— Air Force Enterprise Architecture

AFGM— Air Force Guidance Memorandum

AFI— Air Force Instruction

AFMAN— Air Force Manual

AFPD— Air Force Policy Directive

AFR— Air Force Reserve

AFRIMS— Air Force Records Information Management System

ANG— Air National Guard

AT -Anti—Tamper

C4ISP— Command, Control, Communications, and Computers Intelligence Support Plan

CC— Critical Components

CCA –Clinger-Cohen Act

CIO— Chief Information Officer

CJCSI— Chairman of the Joint Chiefs of Staff Instruction

COTS -Commercial Off-the-Shelf

CPI— Critical Program Information

DISA— Defense Information Systems Agency

DISR— DoD IT Standards Registry

DITPR— DoD IT Portfolio Repository

DM2— DoDAF Metamodel

DoD—Department of Defense

DoDAF— DoD Architecture Framework

DoDD— DoD Directive

DoDI— DoD Instruction

EA— Enterprise Architecture

EAMMF— Enterprise Architecture Management Maturity Framework

EISP— Enhanced Information Support Plan

EMD— Engineering and Manufacturing Development

GAO— Government Accountability Office

GOTS -Government Off-the-Shelf

GTG-F -Global Information Grid (GIG) Technical Guidance Federation Tool

HAF— Headquarters United States Air Force

HwA— Hardware Assurance

ICTO— Interim Certificate To Operate

ISP— Information Support Plan

ISR— Intelligence, Surveillance, and Reconnaissance

IT— Information Technology

ITIPS— Information Technology Investment Portfolio Suite

JCIDS— Joint Capabilities Integration and Development System

JITC— Joint Interoperability Test Command

MAJCOM— Major Command

MCF— Mission Critical Functions

MD— Mission Directive

MDA— Milestone Decision Authority

MOE— Measures of Effectiveness

MOP— Measures of Performance

MS— Milestone

NR KPP –Net-Ready Key Performance Parameter

NSS— National Security System

PPP— Program Protection Plan

RDS— Records Disposition Schedule

RMF— Risk Management Framework

SAF— Secretary of the Air Force

SCF— Service Core Function

SCRM— Supply Chain Risk Management

SME— Subject Matter Expert

SMP— Strategic Master Plan

SoS— System of Systems

SwA—Software Assurance

TDL— Tactical Data Link

TEMP— Test and Evaluation Master Plan

TSN—Trusted Systems & Networks

UC—Unified Capabilities

Terms

Accessible — Data and services can be accessed via the Global Information Grid by users and applications in the enterprise. Data and services are made available to any user of applications, except where limited by law, policy, security classification, or operational necessity. (DoD Information Enterprise Architecture Version 2.0)

Air Force Enterprise Architecture (AFEA)— The AFEA is the collection of architecture data from strategic guidance and Air Force segment and solution architectures that describes the people, processes, data, technology, and information used in the current state of Air Force investments and capabilities as well as future state and transition plans.

Air Force Records Disposition Schedule (RDS)— is outlined in AFMAN 33-363, Management of Records.

Air Force Strategic Master Plan (SMP)— Translates the Air Force strategy into guidance, goals, and objectives within a 20-year timeframe. The SMP is the primary source document for the development and alignment of subordinate strategic planning across the entire Air Force. The alignment of Air Force priorities and goals to national guidance informs planning and actions at successively lower level of Air Force organizations and forms the basis for the development of future force options and performance management plans.

Anti-Tamper (AT)— Systems engineering activities intended to prevent or delay exploitation of Critical Program Information in U.S. defense systems in domestic and export configurations to impede countermeasure development, unintended technology transfer, or alteration of a system due to reverse engineering.

Architecture— A systematic approach that organizes and guides design, analysis, planning, and documentation activities. (CIO Council, A Common Approach to Federal Enterprise Architecture)

Architecture Consumer—An architecture consumer is a person who uses an architecture or the results of architecture analysis to gain information about the architecture's subject.

Architecture Data Repository— Stores architecture data which makes the architectures discoverable. When architecture is data-driven, it is possible to conduct real-time analysis on the data contained within the repository.

Authoritative Data Source— A recognized or official data source with a designated mission statement, source, or product to publish reliable and accurate data for subsequent use by customers. An authoritative data source may be the functional combination of multiple separate data sources. (DoDI 8320.03)

Capability— The ability to complete a task or execute a course of action under specified conditions and level of performance. (CJCSI 3170.01I)

Community of Interest— A collaborative group of users who exchange information in pursuit of their shared goals, interests, missions, or business processes, and who therefore must have a shared vocabulary for the information they exchange. (DoD Information Enterprise Architecture Version 2.0)

Consensus Standards— Standards developed through the cooperation of all parties who have an interest in participating in the development and/or use of the standards.

Countermeasures— Actions, devices, procedures, techniques, or other measures that reduce the vulnerability of an information system. Synonymous with security controls and safeguards.

Critical Component (CC)— A component which is or contains ICT, including hardware, software, and firmware, whether custom, commercial, or otherwise developed, and which delivers or protects mission critical functionality of a system or which, because of the system's design, may introduce vulnerability to the mission critical functions of an applicable system. (DoDI 5200.44)

Critical Program Information (CPI)— U.S. capability elements that contribute to the warfighters' technical advantage, which if compromised, undermines U.S. military preeminence. U.S. capability elements may include, but are not limited to, software algorithms and specific hardware residing on the system, its training equipment, or maintenance support equipment.

Cybersecurity— Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation.

Data Architecture— Consists of a Conceptual, Logical, and Physical representation of data. A Data Architecture includes abstraction, conceptual, logical, and physical models; high-level data concepts and their relationships; data requirements; data structures; and metadata models.

Data Element— A unit of data for which the definition, identification, representation, and permissible values are specified by means of a set of attributes and are incorporated in or a part of an authoritative data source.

Data Steward— Subject-matter expert for one or more authoritative data sources.

Defense Acquisition System— The management process by which the Department of Defense provides effective, affordable, and timely systems to the users. (DoDD 5000.01)

DoD IT Standards Registry (DISR)— A registry that provides a set of rules governing the arrangement, interaction, and interdependence of system parts or elements, whose purpose is to direct that a conformant system satisfies a named set of requirements. It defines the service areas, interfaces, standards (registry elements), and standards profiles applicable to all DoD systems. Use of the registry is mandated for the development and acquisition of new or modified fielded IT systems throughout the DoD. The DISR is accessed through the CAC-enabled GTG-F portal at **https://gtg.csd.disa.mil**. (DoDI 8310.01)

DoD Architecture Framework (DoDAF)— 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. (Background page of DoDAF website)

Enterprise— An area of common activity and goals within an organization or between several organizations, where information and other resources are exchanged. (CIO Council, A Common Approach to Federal Enterprise Architecture)

Enterprise Architecture (EA)— Enterprise Architecture (EA) is a conceptual blueprint that defines the structure and operations of an organization. The intent of an enterprise architecture is to determine how an organization can most effectively achieve its current and future objectives. (**http://searchcio.techtarget.com/definition/enterprise-architecture**)

Enterprise Information Model— Provides a high level view of all data available throughout the enterprise. It consists of an enterprise data dictionary containing registered authoritative data sources, an information asset catalog, and a services registry that describes enterprise services that utilize cataloged information assets and display outputs of operationalizing data.

Flight Plan— A document generated to achieve alignment across functional areas, influence resourcing decisions, provide informative inputs to support plans, or direct discrete activities (i.e. non-Core Function-related). Flight Plans must be aligned with Air Force Strategy and the Strategic Master Plan. Flight plans may also be used to develop a Planning Choice Proposal. (USAF Strategic Master Plan)

Hardware Assurance (HwA)— The level of confidence that hardware functions only as intended and is free of vulnerabilities, defects, and weaknesses, either intentionally or unintentionally designed or inserted as part of the hardware throughout the life cycle.

Information Asset— A documented data element, or, an aggregation of data elements, that has meaning based on its collective context; can come from one or more authoritative data sources.

Information Support Plan— The Information Support Plan is a technical document required by DoDI 5000.02 and DoDI 8330.01 that provides Program Managers a means to identify and resolve potential information support implementation issues and risks that, if not properly managed, will limit or restrict the ability of a program to be operationally employed to support existing and future mission requirements.

Information Technology (IT)— Any equipment or interconnected system or subsystem of equipment used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency. This includes if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency that requires the use of that equipment; or of that equipment to a significant extent in the performance of a service or the furnishing of a product. IT includes computers, ancillary equipment, software, firmware, and similar procedures, services (including support services), and related resources, but does not include any equipment acquired by a federal contractor incidental to a federal contract. (DoDD 8000.01)

Interoperability— The ability of systems, units, or forces to provide data, information, materiel, and services to, and accept the same from, other systems, units, or forces, and to use the data, information, materiel, and services exchanged to enable them to operate effectively together. IT interoperability includes both the technical exchange of information and the end-to-end operational effectiveness of that exchange of information as required for mission accomplishment. Interoperability is more than just information exchange. It includes systems, processes, procedures, organizations, and missions over the life cycle and must be balanced with cybersecurity (formerly information assurance). (DoDI 8330.01)

IT Portfolio Management— The management of selected groupings of IT resources using strategic planning, architectures, and outcome-based performance measures to achieve a mission capability. (DoDD 8115.01)

Joint Capabilities Integration and Development System (JCIDS)— A process used by the Joint Requirements Oversight Council to fulfill its statutory responsibilities to the Chairman of the Joint Chiefs of Staff (CJCS), including but not limited to identifying, assessing, validating, and prioritizing joint military capability requirements. (CJCSI 3170.01I)

Mission Areas (MA)— A defined area of responsibility with functions and processes that contribute to mission accomplishment. (Definitions) The DoD Mission Areas are the Warfighting Mission Area (WMA), Business Mission Area (BMA), DoD portion of Intelligence Mission Area (DIMA), and Enterprise Information Environment (EIE) Mission Area (EIEMA). (para. 2.2.) (DoDD 8115.01)

Mission Critical Functions (MCF)— Any function, the compromise of which would degrade the system effectiveness in achieving the core mission for which it was designed. (DoDI 5200.44)

National Security System (NSS)— (2)(A) The term “national security system” means any information system (including any telecommunications system) used or operated by an agency or by a contractor of an agency, or other organization on behalf of an agency(i) the function, operation, or use of which- (I) involves intelligence activities; (II) involves cryptologic activities related to national security; (III) involves command and control of military forces; (IV) involves equipment that is an integral part of a weapon or weapon 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). (44 United States Code 3542(b)).

Net—Ready Key Performance Parameter - The NR KPP identifies operational, net-centric requirements in terms of threshold and objective values for Measures of Effectives (MOE) and Measures of Performance (MOP). The NR KPP covers all communication, computing, and electromagnetic spectrum requirements involving information elements among producer, sender, receiver, and consumer. Information elements include the information, product, and service exchanges. These exchanges enable successful completion of the warfighter mission or joint business processes.

Program — A directed, funded effort that provides a new, improved, or continuing materiel, weapon, or information system, or service capability in response to an approved need. (Defense Acquisition University Glossary)

Program Protection Plan (PPP)— A risk-based, comprehensive, living plan to guide efforts for managing the risks to CPI and mission-critical functions and components.

Program Protection Planning— The integrating process for managing risks to advanced technology and mission-critical system functionality from foreign collection, design vulnerability or supply chain exploit/insertion, and battlefield loss throughout the acquisition lifecycle.

Reference Architecture— An authoritative source of information about a specific subject area that guides and constrains the instantiations of multiple architectures and solutions. (DoD Reference Architecture Description, June 2010)

Risk Management Framework (RMF)— A structured approach used to oversee and manage risk for an enterprise.

Segment Architecture— Describes individual elements of the enterprise, such as core mission areas, common or shared business services, and enterprise services. Segment architecture has a baseline (as-is), as well as a target (to-be) and a transition strategy for a portion or segment of the enterprise. (Federal Enterprise Architecture Practice Guidance, 2007)

Service Core Functions (SCF)— Functional areas that delineate the appropriate and assigned core duties, missions, and tasks of the Air Force as an organization, responsibility for each of which is assigned to a Core Function Lead. SCFs express the ways in which the USAF is particularly and appropriately suited to contribute to national security, although they do not necessarily express every aspect of what the USAF contributes to the nation.

Software Assurance (SwA)—The level of confidence that software functions as intended and is free of vulnerabilities, either intentionally or unintentionally designed or inserted as part of the software throughout the lifecycle. (DoDI 5200.44)

Solution— A materiel or non-materiel opportunity or solution to satisfy one or more capability gaps/reduce or eliminate one or more capability gaps. (JCIDS Manual)

Solution Architecture— Solution Architecture defines the architecture in sufficient level of detail required to implement solutions to meet the business requirements and ensures alignment with the enterprise architecture.

Supply Chain Risk Management (SCRM)— A systematic process for managing supply chain risk by identifying susceptibilities, vulnerabilities and threats throughout DoD's "supply chain" and developing mitigation strategies to combat those threats whether presented by the supplier, the supplied product and its subcomponents, or the supply chain (e.g., initial production, packaging, handling, storage, transport, mission operation, and disposal). (DoDI 5200.44)

Supportability— The ability of the system to identify and/or predict failures down to a certain subsystem level within a given percentage of accuracy. (JCIDS Manual)

Target Architecture— The representation of a desired future state or "to be built" for the enterprise within the context of the strategic direction. (CIO Council, A Common Approach to Federal Enterprise Architecture)

Trusted Systems and Networks (TSN)— A comprehensive systematic approach that analyzes threats, vulnerabilities, and mitigation strategies to preserve mission assurance.

Understandable— Users and applications can comprehend the data, both structurally and semantically, and readily determine how the data may be used for their specific needs. (DoD Information Enterprise Architecture Version 2.0)

Vulnerability— Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source.