BY ORDER OF THE SECRETARY
OF THE AIR FORCE

AIR FORCE POLICY DIRECTIVE 17-1

12 APRIL 2016

Cyberspace

INFORMATION DOMINANCE GOVERNANCE AND MANAGEMENT

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

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

RELEASABILITY: There are no releasability restrictions on this publication

OPR: SAF/CIO A6SS

Certified by: SAF/CIO A6
(Lt Gen William J. Bender)

Supersedes: AFPD 33-2, 3 August 2011;
AFPD 33-4, 17 January 2013;
AFPD 33-5, 11 January 2013

Pages: 15

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. This directive implements: Office of Management and Budget (OMB) Circular A-11, *Preparation, Submission, and Execution of the Budget*; OMB Circular A-130, *Management of Federal Information Resources*; OMB Memorandum M-11-29, *Chief Information Officer Authorities*; Department of Defense (DoD) Directive (DoDD) 3700.01, *DoD Command and Control (C2) Enabling Capabilities*; DoDD 7045.20, *Capability Portfolio Management*; DoDD 8000.01, *Management of the Department of Defense Information Enterprise*. DoDD 8115.01 *Information Technology Portfolio Management*; DoDD 8220.1, *Single Agency Manager (SAM) for Pentagon Information Technology Services (ITS)*; DoDD 8521.01, *Department of Defense Biometrics*; 8140.01, Cyberspace Workforce Management; DoD Instruction (DoDI) O-3780.01, *Senior Leader Secure Communications Modernization (SLSCM)*; DoDI S-4660.04, *Encryption of Imagery Transmitted by Airborne Systems and Unmanned Aircraft Control Communications*; DoDI S-5100.92, *Defense and National Leadership Command Capability (DNLCC) Governance*; DoDI 5205.8, *Access to Classified Cryptographic Information*; DoDI 5205.13, *Defense Industrial Base (DIB) Cyber Security/ Information Assurance (CS/IA) Activities*; DoDI 8115.02 *Information Technology Portfolio Management Implementation*; DoDI 8310.01, *Information Technology Standards in the DoD*; DoDI 8320.05, *Electromagnetic Spectrum Data*

Sharing; DoDI 8330.01, *Interoperability of Information Technology (IT) and National Security Systems (NSS)*; DoDI 8510.01, *Risk Management Framework (RMF) for DoD Information Technology (IT)*.

This directive is consistent with: Subtitle III of Title 40 of the Clinger-Cohen Act (CCA) of 1996, National Defense Authorization Act (NDAA) 2005 § 2222, NDAA 2009 (PL110-417) § 908, NDAA 2010 § 1072, NDAA 2010 § 804, NDAA 2012 § 901 and NDAA 2015; Federal Information Security Management Act (FISMA), 44 USC Chap 35, Subchap II; Title 10, USC, Section 2223(b) Information Technology: *Additional Responsibilities of Chief Information Officers of Military Department, 2007;* DoDD 5000.01, *The Defense Acquisition System*; DoDD 5144.02, *DoD Chief Information Officer (DoD CIO)*; DoDI 5000.02, *Operation of the Defense Acquisition System*; DoDI 5200.44, *Protection of Mission Critical Functions to Achieve Trusted Systems and Networks;* CJCSI 5116.05, *Military Command, Control, Communications, and Computers Executive Board*; and CJCSI 5123.01G, *Charter of the Joint Requirements Oversight Council*.

This directive applies to all military and civilian AF personnel, members of the AF Reserve, Air National Guard, and individuals or organizations authorized by an appropriate government official to manage any portion of the AF Information Network (AFIN). It applies to all information, information systems (IS), and cyberspace and information technology (IT) infrastructure within AF purview. Comments and recommended changes regarding this publication should be sent through appropriate channels using AF Form 847, Recommendation for Change of Publication, to the office of primary responsibility (OPR), SAF/A6SS, **usaf.pentagon.saf-cio-a6.mbx.a6ss-workflow@mail.mil.** Ensure that all records created as a result of processes prescribed in this publication are maintained in accordance with AF Manual (AFMAN) 33-363, Management of Records, and disposed of in accordance with AF Records Disposition Schedule (RDS) located in the AF Records Information Management System (AFRIMS).

SUMMARY OF CHANGES

This AFPD, published along with AFPD 17-2, supersedes AFPD 33-4, AFPD 33-5, and those portions of AFPD 33-2 not superseded by AFPD 17-2. This directive aligns and consolidates policies on cyberspace and IT management with current AF doctrine, statutory, and regulatory guidelines.

1. Overview. This directive establishes the AF policy for information dominance governance and management to provide a process for the SAF/CIO A6 to fulfill the duties of the AF CIO established in federal laws and DoD issuances. This directive provides a means by which the AF will cross-functionally align cyberspace programs and capabilities to effectively and efficiently deliver capabilities to users. Cyberspace is defined as a global domain within the information environment consisting of the interdependent network of IT infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.

2. Policy. The AF will:

2.1. Develop cyberspace capabilities to execute, enhance and support Joint, Coalition, and AF core missions, by rapidly developing and implementing innovative solutions, and when appropriate, leveraging commercial products/services to deliver AF capabilities in a Disconnected, Intermittent, Low-Bandwidth environment.

2.2. Deliver cyberspace capabilities to support the four defined DoD mission areas: Warfighting (WMA), Business (BMA), Information Environment (IEMA), and Defense Intelligence (DIMA).

2.3. Optimize the planning, programming, budgeting, and execution of cyberspace investments consistent with national, DoD, Joint and AF policy.

2.4. Establish and track performance measures for cyberspace investments, programs, and acquisitions to ensure compliance with validated requirements.

2.5. Design, develop, incorporate, test, and evaluate all AF IT, to include Platform IT (PIT), and NSS for interoperability and supportability, and as necessary, determine tradeoffs among mission effectiveness, cybersecurity, efficiency, survivability, resiliency, and IT interoperability.

2.6. Ensure cyberspace capabilities are designed to enhance information sharing, collaboration, and situational awareness, consistent with cybersecurity standards and best practices.

3. Responsibilities. The responsibilities for cyberspace and IT are overseen by SAF/CIO A6 and shared among numerous key stakeholders. CIO responsibilities are codified in Title 10, USC § 2223a and 8014; Title 40, USC, Subtitle III; and, Title 44, USC § 3506. Acquisition authority is codified in Title 10, USC § 1704 and 8014. Chief Financial Officer authority is codified in Title 10, USC § 8022. Chief Management Officer and Deputy Chief Management Officer authorities are in Title 10, USC § 2222, and Public Law 110-417, § 908 (NDAA 2009).

3.1. **Under Secretary of the Air Force.** As Chief Management Officer, provide any determinations required for defense business systems under Title 10, USC § 2222.

3.2. **Chief of Information Dominance and Chief Information Officer (SAF/CIO A6).** SAF/CIO A6 has a wide range of responsibilities which are listed in detail in the SAF/CIO A6 Mission Directive (AFMD 1-26). These responsibilities may be summarized as follows::

3.2.1. Set the strategic direction for fully exploiting cyberspace by leading Air Staff-level executive groups and boards in the development of policies, strategies, roadmaps, and technical baselines.

3.2.1.1. Charter AF cyberspace governance and Warfighting Integration forums and, in coordination with the Core Function Leads (CFLs), appoint representatives to cyberspace governance forums external to the AF.

3.2.2. Execute all responsibilities and functions outlined in statutes, directives, and regulations pertaining to an Agency Chief Information Officer or military department CIO.

3.2.3. Develop and implement a deliberate budget and investment review and approval process, within existing corporate processes, to integrate cyberspace requirements and investments across all mission areas.

3.2.4. Ensure an operationally resilient, reliable, interoperable, and secure AF Information Network to meet the needs of AF core missions and AF responsibilities for Joint and Coalition Operations.

3.2.5. Serve as the Functional Authority for military and civilian IT, cyberspace, and information management career fields for the life cycle program management of IT and cyberspace capabilities.

3.2.6. For all acquisitions subject to DoDI 5000.02, review and approve the Cybersecurity Strategy for acquisitions of systems containing IT prior to milestone decisions or contract award. For ACAT ID, IAM, and IAC programs, forward the Cybersecurity Strategy to the DoD CIO for review and approval. For SAP systems, conduct the review in coordination with SAF/AA. For nuclear systems, conduct the review in coordination with AF/A10.

3.2.7. Oversee, establish, integrate and maintain the target baseline (TB) and implementation baseline (IB) in coordination with appropriate governance forums.

3.3. **Deputy Chief of Staff for Intelligence, Surveillance, and Reconnaissance (AF/A2)** will:

3.3.1. Advocate for a prioritized integration of battlespace awareness warfighting systems and intelligence, surveillance, and reconnaissance (ISR) enterprise interoperability under the Warfighting Integration governance forums and with other appropriate forums as needed.

3.3.2. Participate in cyberspace governance forums.

3.3.3. Coordinate and facilitate the review of DIMA cyberspace capabilities and investment.

3.3.4. Identify opportunities to share capabilities and investment between DIMA and the other mission areas.

3.3.5. Coordinate intelligence activities required to fully characterize the cyber threat.

3.3.5.1. Facilitate the provision of cyber intelligence data for acquisition development programs.

3.3.5.2. Facilitate the provision of cyber intelligence data to support modeling and simulation (M&S) and test and evaluation (T&E) activities.

3.4. **Deputy Chief of Staff for Operations (AF/A3)** will:

3.4.1. Advocate for the integration of cyberspace capabilities into AF operational capabilities-based planning and development processes in coordination with the Cyberspace Superiority Core Function Lead (CFL).

3.4.2. Participate in cyberspace governance forums and identify mission assurance requirements and priorities for all phases of operations.

3.4.3. Coordinate and facilitate the review of cyberspace capabilities through the Warfighting Integration governance forums.

3.5. **The Deputy Chief of Staff for Strategic Plans and Requirements (A5/8)** will:

3.5.1. Be responsible for AF Joint Capabilities Integration and Development System planning and requirements development processes and procedures for cyberspace capabilities.

3.5.2. Collaborate with Cyberspace Superiority CFL, MAJCOMs, other Services, and the defense S&T community to support future AF cyberspace capabilities development through concept development and experimentation.

3.5.3. Ensure program funding is aligned with the validated requirement for each acquisition phase.

3.5.4. Participate in cyberspace governance forums.

3.6. **Air Force, Director of Test and Evaluation (AF/TE) will:**

3.6.1. Participate in cyberspace governance forums and identify T&E requirements.

3.6.2. Develop and implement a comprehensive test strategy that includes cyber testing, and institute T&E policy consistent with AF and DoD policies.

3.6.3. Provide guidance, direction, and oversight of all AF T&E activities, including integration of cyber test, throughout program lifecycle.

3.6.4. Ensure AF T&E infrastructure utilizes latest cyber intelligence data to provide an operationally representative cyber environment for T&E.

3.7. **The Administrative Assistant to the Secretary of the Air Force (SAF/AA) will:**

3.7.1. IAW AFPD 16-14, *Security Enterprise Governance*, provide assistance to SAF/CIO A6 in the presentation and vetting of cyberspace issues and agenda items to the Air Force Security Enterprise Executive Board when appropriate.

3.7.2. On behalf of the security enterprise and special access program (SAP) community, participate in cyberspace governance forums.

3.7.3. As the Senior Security Official and Security Program Executive, ensure Personnel, Information, Industrial, and Insider Threat security programs are aligned with and support cyberspace policy and execution.

3.7.4. Support the SAF/CIO A6 in execution of CIO responsibilities for Special Access Program networks.

3.8. **Assistant Secretary of the Air Force for Acquisition (SAF/AQ)** will:

3.8.1. Participate in cyberspace governance forums.

3.8.2. Work with SAF/CIO A6 to ensure AF cyber acquisition programs are consistent with the Information Dominance Flight Plan and the AF Enterprise Architecture developed by SAF/CIO A6.

3.8.3. Ensure the execution of AF acquisition and sustainment programs appropriately implement cyberspace and warfighting integration requirements, including;

interoperability, reusability of application designs; and promoting the adoption of IT as common services and the AF common computing environment. These requirements will be implemented IAW AFPD 63-1/20-1, *Integrated Life Cycle Management*.

3.8.4. Ensure compliance with Electromagnetic Environmental Effects control and anti-tamper requirements during the acquisition of AF cyber systems.

3.8.5. Ensure the acquisition program office Program Manager is responsible for cybersecurity of the weapon system, to include IT interfaces and embedded computer hardware and software, and has allocated sufficient resources to cybersecurity.

3.8.6. Ensure all acquisition programs plan and conduct robust developmental and operational cyber testing prior to system deployment.

3.8.7. Designate DoD/AF information systems that the AF Service Acquisition Executive has determined are critical to the direct fulfillment of military or intelligence missions as "applicable systems" in accordance with DoDI 5200.44, *Protection of Mission Critical Functions to Achieve Trusted Systems and Networks*.

3.9. **Assistant Secretary of the Air Force, Financial Management and Comptroller (SAF/FM)** will:

3.9.1. Coordinate, as required, on business case analysis and economic analysis supporting cyberspace requirements.

3.9.2. In accordance with 10 USC § 8022, approve and supervise all financial cyberspace programs to ensure compliance with finance and accounting standards.

3.9.3. Participate in cyberspace governance forums.

3.10. **Director of Business Transformation and Deputy Chief Management Officer (SAF/MG)** will:

3.10.1. Coordinate and facilitate the cross-functional review of AF Defense Business Systems (DBS) and support the USecAF as the business systems Pre-Certification Authority through the Enterprise Senior Working Group.

3.10.2. Coordinate the development of business enterprise architecture, including the capture of business processes and supporting AF DBS.

3.10.3. Participate in cyberspace governance forums.

3.10.4. Be responsible for the Service Development and Delivery Process for development of Defense Business System requirements and capabilities.

3.11. **Air Force Space Command (AFSPC)** will:

3.11.1. Serve as lead command for AF cyberspace operations and Cyberspace Superiority CFL.

3.11.2. Develop the Cyberspace Superiority Core Function Support Plan aligned with the AF Information Dominance Flight Plan and IEMA roadmap developed by SAF/CIO A6.

3.11.3. Participate in cyberspace governance forums.

3.11.4. Establish capability needs and requirements for cyberspace infrastructure within the Cyberspace Superiority CFL portfolio.

3.11.5. Develop and maintain the AF Operational Baseline (OB) which is synchronized with the Target Baseline (TB) and Implementation Baseline (IB) developed by SAF/CIO A6.

3.11.6. Deploy AF approved cyber weapon systems.

3.11.7. In conjunction with the National Security Agency, provide oversight and guidance for AF COMSEC, AF Cryptologic Modernization and the development, fielding and sustainment of cryptologic solutions within the AF.

3.11.8. Develop a trained, educated, experienced force to conduct cyberspace operations.

3.12. Air Force Materiel Command will:

3.12.1. Serve as the core functional lead integrator for agile combat support.

3.12.2. Conduct technological research and materiel development activities to acquire, perform developmental testing of, field and sustain current and future cyberspace capabilities.

3.13. **CFLs** will:

3.13.1. Plan and program cyberspace investments for assigned service core functions based on the AF Strategic Master Plan and IDFP, the IEMA Roadmap, and other IDFP-aligned roadmaps.

3.13.2. Coordinate with cyberspace governance forums and to enhance collaborative efforts potentially reducing costs, complexity, and unnecessary duplication of effort.

3.13.3. Establish mission capability needs and requirements for cyberspace infrastructure within the respective CFL portfolio.

3.13.4. Provide investment performance information to SAF/CIO A6.

3.13.5. Serve as the Functional Sponsor for Defense Business System requirements within the Service Development and Delivery Process leading into the Defense Acquisition System.

3.14. **All HAF Functionals, MAJCOMs, DRUs, and FOAs** will:

3.14.1. Participate in the cyberspace governance forums, as required. Identify new cyberspace requirements to responsible CFL.

3.14.2. Ensure all cyberspace investments are identified and registered in the SAF/CIO A6-directed management control system.

3.14.3. Maintain enterprise architectures for their areas of responsibility, to include mission-unique IS solution architectures, and be able to integrate their architectural data using AF-directed repositories.

3.14.4. Develop and exercise contingency plans for mission assurance when operating under conditions of diminished or denied NSS, mission critical IT and data availability.

3.14.5. Identify and advocate for rapid innovation initiatives, both leveraging cyberspace capabilities and operating through cyberspace.

3.14.6. Ensure that subordinate organizations identify the Protection Level of their cyber and computer/communications assets and apply integrated defense measures IAW AFI 31-101, *Integrated Defense*.

3.15. The General Counsel (SAF/GC) and The Judge Advocate General (AF/JA) will advise the AF on legal matters related to information dominance governance and management.

4. Applicability to ISR and Counterintelligence Authorities and Policies. Nothing in this directive shall alter or supersede the existing authorities and policies of the Director of National Intelligence (DNI) regarding the protection of Sensitive Compartmented Information (SCI) or intelligence SAPs. The application of the provisions and procedures of this directive to SCI or other intelligence ISs is encouraged where they may complement or address areas not otherwise specifically addressed. AF ISR and counterintelligence governance, compliance, and reporting is governed by applicable Attorney General, DNI, Under Secretary of Defense (Intelligence), Director of Central Intelligence, and Director, National Security Agency directives and guidelines.

DEBORAH L. JAMES
Secretary of the Air Force

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

Title 10, USC, Section 2223(b), *"Information Technology: Additional Responsibilities of Chief Information Officers of Military Department,* 2007

Title 44, USC, Section 3541, *Federal Information Security Management Act (FISMA)*, 2002

National Defense Authorization Act (NDAA), Published Annually

Clinger-Cohen Act (CCA), 1996

OMB Circular A-11*, Preparation, Submission, and Execution of the Budget,* August 3, 2012

OMB Circular A-130, *Management of Federal Information Resources,* November 28, 2000

OMB Memorandum M-11-29, *Chief Information Officer Authorities,* August 8, 2011

NIST Special Publication 800-59, *Guideline for Identifying an Information System as a National Security System,* August 2003

DoDD 3700.01, *DoD Command and Control (C2) Enabling Capabilities*, October 22, 2014

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

DoDD 5144.02, *DoD Chief Information Officer (DoD CIO)*, November 21, 2014

DoDD 7045.20, *Capability Portfolio Management*, September 25, 2008;

DoDD 8000.01, *Management of the Department of Defense Information Enterprise,* February 10, 2009

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

DoDD 8140.01, Cyberspace Workforce Management, August 11, 2015

DoDD 8521.01E, *Department of Defense Biometrics*, February 21, 2008

DoDI O-3780.01, *Senior Leader Secure Communications Modernization (SLSCM)*, May 22, 2014

DoDI S-4460.01, *Encryption of Imagery Transmitted by Airborne Systems and Unmanned Aircraft Control Communications*, July 27, 2011

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

DoDI S-5100.92, *Defense and National Leadership Command Capability (DNLCC) Governance*, May 11, 2009

DoDI S-5200.16, *Objectives and Minimum Standards for Communications Security (COMSEC) Measures Used in Nuclear Command and Control (NC2) Communications (U)*, November 14, 2007;

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

DoDI 5205.8, *Access to Classified Cryptographic Information*, November 8, 2007;

DoDI 8115.02, *Information Technology Portfolio Management Implementation,* October 30, 2006

DoDD 8220.1, *Single Agency Manager (SAF) for Pentagon Information Technology Services (ITS)*, March 1, 1995;

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

DoDI 8320.05, *Electromagnetic Spectrum Data Sharing*, August 18, 2011

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

DoDI 8500.01, *Cybersecurity*, March 14, 2014

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

CJCSI 5116.05, *Military Command, Control, Communications, and Computers Executive Board*, April 23, 2014

CJCSI 5123.01G Charter of the Joint Requirements Oversight Council, February 12, 2015

JP 3-12, *Cyberspace Operations*, February 5, 2013

AFPD 16-14, *Security Enterprise Governance*, July 24, 2014

AFI 31-101, *Integrated Defense*, October 8, 2009

AFI 38-101, *Air Force Organization*, March 16, 2011

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

AF Information Dominance Flight Plan (IDFP), v2.0, May 1, 2015

Prescribed Forms

None

Adopted Forms

AF Form 847, *Recommendation for Change of Publication*

Abbreviations and Acronyms

AF —Air Force

AFI—Air Force Instruction

AFIN—Air Force Information Network

AFMAN—Air Force Manual

AFPD—Air Force Policy Directive

AFRIMS—Air Force Records Information Management System

AFSPC—Air Force Space Command

BMA —Business Mission Area

C2—Command and Control

CCA—Clinger-Cohen Act

CFL—Core Function Lead

CIO—Chief Information Officer

DBS—Defense Business System

DCMO—Deputy Chief Management Officer

DoD—Department of Defense

DoDD—Department of Defense Directive

DoDI—Department of Defense Instruction

DIMA —Defense Intelligence Mission Area

DRU—Direct Report Units

EA—Enterprise Architecture

FISMA—Federal Information Security Management Act

FOA—Field Operating Agency

HAF—Headquarters Air Force

IB—Implementation Baseline

IDFP —Information Dominance Flight Plan

IEMA —Information Environment Mission Area

IS —Information System

ISR—Intelligence, Surveillance, and Reconnaissance

IT—Information Technology

ITIL—Information Technology Infrastructure Library

MAJCOM—Major Command

NDAA—National Defense Authorization Act

NSS—National Security System

OB—Operational Baseline

OMB—Office of Management and Budget

OPR—Office of Primary Responsibility

PEO—Program Executive Officer

PIT —Platform Information Technology

RDS—Records Disposition Schedule

SCF—Service Core Function

T&E —Test and Evaluation

TB—Target Baseline

USC —United States Code

USecAF —Undersecretary of the Air Force

Terms

AF Information Network (AFIN) — The globally interconnected, end-to-end set of AF information capabilities, and associated processes for collecting, processing, storing, disseminating, and managing information on-demand to AF warfighters, policy makers, and support personnel, including owned and leased communications and computing systems and services, software (including applications), data, security services, other associated services, and national security systems." (Derived from the JP 3-12 definition of DoDIN).

Business Mission Area (BMA)—The BMA ensures that the right capabilities, resources, and materiel are reliably delivered to our warfighters: what they need, where they need it, when they need it, anywhere in the world. In order to cost-effectively meet these requirements, the DoD current business and financial management infrastructure - processes, systems, and data standards - are being transformed to ensure better support to the warfighter and improve accountability to the taxpayer. Integration of business transformation for the DoD business enterprise is led by the Deputy Secretary of Defense in his role as the Chief Operating Officer of the Department. (DoDI 8115.02).

Core Function Lead—SecAF/CSAF-appointed senior leader responsible for specific Core Functions (CF) providing AF-level, long-term views. CFLs integrate Total Force concepts, capabilities, modernization, and resourcing to ensure future assigned core capabilities across the range of military operations as directed by AF Strategy and Strategic Planning Guidance. CFLs are responsible for the Core Function Support Plan and recommendations for the development of the POM for the assigned CF. CFLs have tasking authority regarding CF issues to identify enabling capabilities and integration requirements/opportunities. (AFPD 90-11).

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. (DoDI 8500.01).

Cyberspace—A global domain within the information environment consisting of the interdependent network of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers. (Joint Pub 3-12) NOTE: synonymous with cyber when used as an adjective.

Defense Intelligence Mission Area (DIMA)—The DIMA includes IT investments within the Military Intelligence Program and Defense component programs of the National Intelligence Program. The USD(I) has delegated responsibility for managing the DIMA portfolio to the Director, Defense Intelligence Agency, but USD(I) retains final signature authority. DIMA management will require coordination of issues among portfolios that extend beyond the Department of Defense to the overall Intelligence Community. (DoDI 8115.02).

Enterprise Architecture (EA)—The explicit description and documentation of the current and desired relationships among business and management processes and supporting resources (e.g., IT, personnel). It describes the "current architecture" and "target architecture," to include the rules, standards, and systems life cycle information to optimize and maintain the environment which the agency wishes to create and maintain by managing its IT portfolio. The EA must also provide a strategy that will enable the agency to support its current state and also act as the roadmap for transition to its target environment. These transition processes will include an agency's capital planning and investment control processes, agency EA planning processes, and agency systems life cycle methodologies. The EA will define principles and goals and set direction on such issues as the promotion of interoperability, open systems, public access, compliance with Government Paperwork Elimination Act, end user satisfaction, and IT security. The agency must support the EA with a complete inventory of agency information resources, including personnel, equipment, and funds devoted to information resources management and information technology, at an appropriate level of detail.

Governance—Governance is the framework of rules and practices that ensures continuity, collaboration, and de-confliction of interests across an organization to clearly define policies, processes, and investments. (IDFP V2.0).

Implementation Baseline (IB)—The Implementation Baseline is the baseline of acquisition selected products and their informed/allowed configurations that implement the architecture, standards and protocols, and guidelines specified in the Target Baseline. The Implementation Baseline informs the Operational Baseline of the acquisition selected products and how they are to be configured to support deployment of user applications across the infrastructure topology. The Implementation Baseline governs the implementation of the Development and Integration/Test environments.

Information Dominance —The operational advantage gained from the ability to collect, control, exploit, and defend information to optimize decision making and maximize warfighting effects. (AF Information Dominance Strategy).

Information Environment — The aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information. (JP 3-13).

Information Environment Mission Area (IEMA)—IEMA is the DoD information (IT) portfolio that manages investments in the current and future integrated information sharing, computing and communications environment of the Global Information Grid (GIG). The IE comprises GIG assets that operate as, provide information transport for, perform enterprise management of, and assure various levels and segments of the enterprise network, ranging from local area to wide area networks and from tactical to operational and strategic networks. The domains are Communications, Computing Infrastructure, Core Enterprise Services, and Information Assurance. (DoDI 8115.02).

Information System (IS)—A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. (44 U.S.C. Sec 3502).

Information Technology (IT)—Any equipment, or interconnected system or subsystem of equipment, that is 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 equipment used by a Component directly, or used by a contractor under a contract with the Component, which (i) requires the use of such equipment, or (ii) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. The term “IT” also includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources. Notwithstanding the above, the term “IT” does not include any equipment that is required by a Federal contractor incidental to a Federal contract. Note: The above term is considered synonymous with the term “information system” as defined and used in AF programs. The term “IT” does not include National Security Systems (NSS) according to 44 USC 3502.

IT Portfolio Management (Portfolio management)—The management of selected groupings of IT resources using strategic planning, architectures, and outcome-based performance measures to achieve a mission capability (CJCSI 8410.01, Warfighting Mission Area Information Technology Portfolio Management and Net-Centric Data Sharing). (DoDD 8115.01).

Lead Command —A type of MAJCOM that consolidates responsibilities for a particular function in a single MAJCOM, supporting the entire AF as applicable. (AFI 38-101).

Mission Area Roadmap—A plan which guides the implementation of capabilities across a Mission Area. (DoDD 8115.02).

National Security System (NSS)—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, the function, operation, or use of which involves intelligence activities; involves cryptologic activities related to national security; involves command and control of military forces; involves equipment that is an integral part of a weapon or weapons system; or is critical to the direct fulfillment of military or intelligence missions. (40 USC 11103. See also NIST SP 800-59).

Operational Baseline (OB)—The Operational Baseline is the set of components of the AF IT infrastructure that specifies the exact laydown and configurations of hardware and software within all facilities in the AF infrastructure topology and provide the required warfighter capabilities and performance.

Platform Information Technology (PIT) — A special purpose system which employs computing resources (i.e., hardware, firmware, and optionally software) that are physically embedded in, dedicated to, or essential in real time to the mission performance. It only performs (i.e., is dedicated to) the information processing assigned to it by its hosting special purpose system (this is not for core services). Examples include, but are not limited to: SCADA type systems, training simulators, diagnostic test and maintenance equipment. (AFI 33-210).

Target Baseline (TB)—The Target Baseline specifies the standards, protocols, guidelines and implementation constraints for the future state of the AFIN Infrastructure. It is used to inform the development of the implementation baseline. The Target Baseline is thoroughly documented and continually updated based upon emerging industry standards and the evolving AFEA.

Warfighting Integration—Ensuring information interoperability and compatibility of warfighting capabilities (e.g., people, processes, and technology) across the Air Force service core functions and within joint capability areas.

Warfighting Mission Area (WMA—)—The WMA provides life cycle oversight to applicable DoD Component and Combatant Commander IT investments (programs, systems, and initiatives). WMA IT investments support and enhance the Chairman of the Joint Chiefs of

Staff's joint warfighting priorities while supporting actions to create a net-centric distributed force, capable of full spectrum dominance through decision and information superiority. WMA IT investments ensure Combatant Commands can meet the Chairman of the Joint Chiefs of Staff's strategic challenges to win the war on terrorism, accelerate transformation, and strengthen joint warfighting through organizational agility, action and decision speed, collaboration, outreach, and professional development. (DoDI 8115.02).