BY ORDER OF THE
SECRETARY OF THE AIR FORCE

AIR FORCE POLICY DIRECTIVE 33-3

28 MARCH 2006

Communications and Information

INFORMATION MANAGEMENT

NOTICE: This publication is available digitally on the AFDPO WWW site at: **http://www.e-publishing.af.mil.**

OPR: SAF/XCISI (Mr. Lawrence Shade)

Certified by: SAF/XC
(Lt Gen Michael W. Peterson)

Supersedes AFPD 37-1 dated 19 November 1993 and Department of Defense Directive (DoDD) 8000.1/AF Supplement dated 30 November 1994

Pages: 11
Distribution: F

This Air Force Policy Directive (AFPD) establishes the framework for how the Air Force creates, uses, and preserves information and data to achieve its strategic priorities, fulfill its missions, support its programs, deliver its capabilities, and meet its accountability obligations prescribed by statute. This directive applies to all military and civilian Air Force personnel, members of the Air Force Reserve and Air National Guard, and other individuals or organizations as required by binding agreement or obligation with the Department of the Air Force. This directive implements Department of Defense (DOD)Directive (DODD) 5015.2, *DOD Records Management Program,* November 21, 2003; DODD 5040.3, *DOD Joint Visual Information Services,* November 21, 2003; DODD 5040.4, *Joint Combat Camera (COMCAM) Program,* November 21, 2003; DODD 5040.5, *Alteration of Official DOD Imagery, November 21, 2003*; DODD 5400.7, *DOD Freedom of Information Act (FOIA) Program,* October 28, 2005*;* DODD 5400.11, *DOD Privacy Program,* November 16, 2004; the information management (IM) elements of DODD 8000.1, *Management of DOD Information Resources and Information Technology,* February 27, 2002; DODD 8320.2, *Data Sharing in a Net-Centric Department of Defense,* December 2, 2004; and DODD 8910.1, *Management and Control of Information Requirements,* November 21, 2003 . Send all recommendations for changes or comments to Secretary of the Air Force (SAF/XCISI), 1800 Air Force Pentagon, Washington DC 20330, through appropriate channels, using AF IMT 847, **Recommendation for Change of Publication**, with a courtesy copy to Headquarters Air Force Communications Agency (HQ AFCA/EASD), 203 W. Losey St, Room 1100, Scott AFB IL 62225-5222. Ensure that all records created as a result of processes prescribed in this publication are maintained in accordance with Air Force Manual (AFMAN) 37-123, *Management of Records* (will become AFMAN 33-363), and disposed of in accordance with the Air Force Records Information Management System (AFRIMS) Records Disposition Schedule (RDS) located at **https://afrims.amc.af.mil/rds_series.cfm**. Several widely accepted terms for information management are used in this directive to communicate net-centric objectives; refer to **Attachment 1** for a glossary of references and supporting information.

SUMMARY OF REVISIONS

This revision updates the entire Policy Directive and changes the implementing publication of this directive from the 37 series to the 33 series.

1. Background. Public Law (PL) 104-13, PL 104-106, *Clinger-Cohen Act of 1996* (CCA), and PL 107-347, *E-Government Act of 2002*, requires each federal agency to designate a Chief Information Officer to ensure compliance with federal information policies and implement IM to improve agency productivity, efficiency, and effectiveness.

1.1. IM is a key focus area of the Air Force. Information within the Air Force must be managed as an asset, supporting the warfighter during mission and support operations, as well as achieving the traditional purposes of IM, such as controlling official records. The word "information" has two meanings within the DOD: the first refers to unprocessed data; the second refers to the meaning a person assigns to that data. An information and data management process involves both meanings. Conceptually, viewing information as an "asset to be managed" incorporates and aligns into one discipline the multiple disciplines traditionally associated with IM (data management, records management [RM], multimedia management, documents management, workflow management, and publications/forms management). IM interacts with Air Force knowledge management programs by providing control over the items employed and produced by knowledge-based management activities.

1.2. This policy ensures the right information exists, is accessible, and is understood and discoverable by all Air Force personnel with on-demand access to appropriate authoritative, relevant, and assured information needed to perform their duties efficiently and effectively. To accomplish this, Air Force personnel must use their knowledge of current and anticipated information needs to develop and operate our information resources so that information is collected and made available when and where it is needed in the Air Force enterprise for use by decision makers. Agility and flexibility are essential for information exchange: to respond to ad hoc user-directed queries in seconds and minutes, not hours and days; and to meet the requirements of newly implemented machine-to-human and machine-to-machine flows instantaneously.

2. Objectives.

2.1. Provide policy and responsibilities for the representation of, access to, and maintenance, management, analysis, and integration of "information assets" (all forms of data and content) across Air Force information sources.

2.2. Establish the framework for the development, implementation, management, and control needed to make "information decisions" visible to any interested and authorized party, and to efficiently include and resolve the needs of all stakeholders, so these decisions are made for the benefit of the entire Air Force enterprise, the DOD, Joint, Coalition, or inter-agency partners.

2.3. Ensure the ability to discover, access, store, protect, share, and exploit mission-critical information regardless of its physical location, media, source, owner, or other defining characteristics.

2.4. Provide a policy that minimizes the effort required by personnel and applications to conduct IM activities and enterprise services, and that supports personnel with on-demand access to assured, rele-

vant, authoritative, and sufficient data, as well as providing a high degree of automation of the IM process.

2.5. Provide an approach that reduces or eliminates the creation of official Air Force information assets in paper form.

2.6. Provide a means to reduce existing repositories of paper records through adaptation of existing and future electronic business processes.

2.7. Ensure and promote an Air Force policy that accommodates DOD policy by providing a service-oriented environment that ensures integration and interoperability of Air Force information assets across all appropriate DOD environments.

2.8. Ensure and promote policy that adheres to all applicable legal and regulatory guidance.

2.9. Advocate and procure Air Force enterprise services, including electronic and information technology (E&IT) (Title 29, United States Code [U.S.C.], Section 794d, *Electronic and information technology*), in the requirements, resourcing, and acquisition processes through planned and existing IM strategies, programs, and initiatives.

3. Policy.

3.1. IM is ultimately everyone's responsibility. Air Force leaders at all levels are responsible for the management and control of all Air Force information resources under their purview. All Air Force personnel must adhere to all applicable policies and procedures as they carry out their responsibilities to manage information, information services, and information systems.

3.2. Information producers ensure that authoritative and relevant assets are made available to appropriate consumers on a timely basis. Producers develop vocabularies describing their assets and ensure linkage of their vocabulary with the Air Force Core Taxonomy.

3.3. The Air Force directs all business and warfighting information management through the establishment, use, and maintenance of shared enterprise services and information to securely interconnect people, information and capabilities, independent of time or location. This substantially improves planning at different echelons, provide widespread access to information and services, and significantly shorten decision-making cycles.

3.4. The Air Force manages all information as assets that must be available to authorized personnel and Joint or Coalition partners (with appropriate permissions and a need-to-know) when requested during mission operations and operational support activities.

3.5. The Air Force applies the same management principles consistently to all information assets regardless of source, owner, classification, media, location, or other defining characteristics.

3.5.1. Information assets shall be made visible, accessible, and understandable as early as possible in the life cycle to support mission objectives.

3.5.2. Information asset management shall be implemented with a high degree of automation consistent with DOD direction for creation of associated metadata "tagging" for each asset.

3.6. The Air Force eliminates the production of paper copies of information assets that require management and control in accordance with federal and DOD policies and guidance. To the maximum

extent permissible, official versions of information assets will be maintained, controlled, and disposed of electronically.

3.7. The Air Force modifies standard operating procedures to reduce and eventually eliminate current repositories of paper assets. The goal is for Air Force personnel to digitize existing paper assets, place those digitized assets under control of the Air Force IM policy, and destroy the paper asset, in accordance with federal and DOD policies and guidance.

3.8. The Air Force establishes a governance structure to manage enterprise services and control the IM process.

3.9. The Air Force ensures adherence to federal and DOD regulatory and legal requirements. The Air Force will:

3.9.1. Publish rules and notices in the Federal Register when they have substantial and direct impact on the public, or as otherwise required by law or regulation.

3.9.2. Manage and safeguard all forms of information against unauthorized access, use, and dissemination.

3.9.2.1. Make records publicly available in accordance with DODD 5400.7 requirements.

3.9.2.2. Collect, manage, and safeguard personal information in accordance with DODD 5400.11.

3.9.3. Ensure that information is managed in compliance with accessibility requirements.

3.9.4. Ensure records required for official business are retained according to applicable laws and federal and DOD guidelines.

3.10. Air Force IM policy applies to all Air Force information assets during all phases of the information life cycle; including creation, storage, protection, discovery, and final disposition.

3.11. Air Force IM policy applies to all information technology (IT) capabilities that the Air Force develops, procures, deploys, and manages; with a net-centric construct and produces supporting strategies, policies, and governance structure.

4. Responsibilities.

4.1. The Secretary of the Air Force Office of Warfighting Integration and Chief Information Officer (SAF/XC) provides IM policy, guidance, and procedures to establish the framework to achieve and maintain decision superiority to include, but not limited to, RM, FOIA, Privacy Act, Federal Register, and Information Collects and Reports Control.

4.2. The Secretary of the Air Force Office of the Administrative Assistant (SAF/AA) provides departmental guidance/procedures for publications, forms, and publishing.

4.3. Headquarters Air Education and Training Command develops and conducts IM training for all Air Force personnel, not just IM personnel.

4.4. Air Force major commands, direct reporting units, and field operating agencies - Directors of Communications and Information specifically, and information managers at all levels generally – ensure compliance with all IM statutory and regulatory requirements and publish instructions to guide subordinate organizations. Communications and Information functional managers at all levels must

work with other functional communities to acquire, train, classify, use, and develop the careers of Air Force IM personnel.

5. Prescribed AF Form. AF Form 4332, **Accountable Communications Receipt Authorization**. Form will be used to designate individuals who are authorized to sign for and accept accountable mail.

MICHAEL W. WYNNE
Secretary of the Air Force

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

Title 29, U.S.C., Section 794d, *Electronic and information technology* (29 U.S.C. 794d) (*Section 508 of the Rehabilitation Act of 1973*)

Title 40, U.S.C., Sections 11101-11704, *Information Technology Management* (40 U.S.C. 11101-11704) (*Clinger-Cohen Act of 1996 (CCA)*)

Title 44, U.S.C., Chapter 29, *Records Management by the Archivist of the United States and by the Administrator of General Services*, Chapter 31, *Records Management by Federal Agencies*, and Chapter 33, *Disposal of Records*

Title 44, U.S.C., Sections 3501-3520, *Coordination of Federal Information Policy* (44 U.S.C. 3501-3520) (*Paperwork Reduction Act of 1995 (PRA)*)

PL 107-347, *E-Government Act of 2002*

DODD 4630.5, *Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS),* May 5, 2004

DODD 5015.2, *DOD Records Management Program*, November 21, 2003

DODD 5330.3/Air Force Supplement, *Document Automation and Production Service (DAPS)*, March 24, 2005

DODD 5040.3, *DOD Joint Visual Information Services*, November 21, 2003

DODD 5040.4, *Joint Combat Camera (COMCAM) Operations*, November 21, 2003

DODD 5040.5, *Alteration of Official DOD Imagery,* November 21, 2003

DODD 5400.7, *DOD Freedom of Information Act (FOIA) Program*, October 28, 2005

DODD 5400.11, *DOD Privacy [Act] Program (PA),* November 16, 2004

DODD 8000.1, *Management of DOD Information Resources and Information Technology,* February 27, 2002

DODD 8320.2, *Data Sharing in a Net-Centric Department of Defense,* December 2, 2004

DODD 8500.1, *Information Assurance (IA),* November 21, 2003

DODD 8910.1, *Management and Control of Information Requirements,* November 21, 2003

DODI 4525.7, *Military Postal Service and Related Services*, April 2, 1981

DODI 4525.8, *DOD Official Mail Management*, December 26, 2001

DODI 4525.8/Air Force Supplement, *DOD Official Mail Management,* December 6, 2005

DODI 5040.02, *Visual Information (VI),* August 30, 2005

DODI 5040.6, *Life-Cycle Management of DO D Visual Information (VI),* October 21, 2002

DODI 5040.07, *Visual Information Production Procedures,* August 30, 2005

DODI 5040.8, *Visual Information (VI) Activity Management*, January 26, 2005

DOD 4525.6-M, *Department of Defense Postal Manual*, August 15, 2002

DOD 4525.6-M/Air Force Supplement, *Military Post Office Operating Procedures*, April 20, 1990

DOD 4525.8-M/Air Force Supplement, *Official Mail Manual*, April 18, 1994

DOD 5015.2-STD, *Design Criteria Standard for Electronic Records Management Software Applications*, June 19, 2002

DODR 5400.7/Air Force Supplement, *DoD Freedom of Information Act (FOIA) Program*, June 24, 2002

AFMAN 37-123, *Management of Records* (will become AFMAN 33-363)

AFRIMS RDS, **https://afrims.amc.af.mil/rds_series.cfm**

Abbreviations and Acronyms

AFMAN—Air Force Manual

AFPD—Air Force Policy Directive

AFRIMS—Air Force Records Information Management System

CCA—Clinger-Cohen Act

DAPS—*Document Automation and Production Service*

DOD—Department of Defense

DODD—Department of Defense Directive

E&IT—electronic and information technology

FOIA—Freedom of Information Act

IM—information management

IMT—information management tool

IA—information assurance

IT—information technology

NSS—National Security System

PA—Privacy Act

PRA—Paper Reduction Act

RDS—Records Disposition Schedule

RM—records management

SAF—Secretary of the Air Force

SOE—service-oriented enterprise

STD—Standard

U.S.C.—United States Code

Terms

—The following terms are specific to Air Force Information and Data Management. Where no citation appears, the term has been derived from several sources or from common usage.

Automated Information System (AIS) Applications—The product or deliverable of an acquisition program. An AIS application performs clearly defined functions for which there are readily identifiable security considerations and needs that are addressed as part of the acquisition. An AIS application may be a single software application (e.g., Integrated Consumable Items Support); multiple software applications that are related to a single mission (e.g., payroll or personnel); or a combination of software and hardware performing a specific support function across a range of missions (e.g., Global Command and Control System, Defense Messaging System). AIS applications are deployed to enclaves for operations, and have their operational security needs assumed by the enclave. An AIS application is analogous to a "major application"; however, this term is not used in order to avoid confusion with the DOD acquisition category of Major Automated Information System. (DODD 8500.1)

Content—Items available to consumers and users, which include data, information, documents, records, applications, and services.

Data—Representation of facts, concepts, or instructions in a formalized manner suitable for communication, interpretation, or processing by humans or by automatic means. Any representations such as characters or analog quantities to which meaning is or might be assigned.

Data Management—The process of planning, coordinating, sharing, and controlling organizations data resources.

Document Management—The process of managing documents through their life cycle: from inception through creation, review, storage, dissemination, and archival or deletion. Document management can also be a database system to organize stored documents, or a search mechanism to quickly find specific documents.

Electronic and Information Technology (E&IT)—Includes IT and any equipment, or interconnected system of equipment used in the creation, conversion, or duplication of data or information. The term E&IT includes, but is not limited to, telecommunications products (such as telephones), information kiosks, and transaction machines. IT does not include any equipment that contains embedded IT used as an integral part of the product, but whose principal function is not the acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information. (29 U.S.C. 794d)

Enclave—A collection of computing environments connected by one or more internal networks under the control of a single authority and security policy, including personnel and physical security. Enclaves always assume the highest mission assurance category and security classification of the AIS applications or outsourced IT-based processes they support, and derive their security needs from those systems. They provide standard information assurance (IA) capabilities such as boundary defense, incident detection and response, and key management, and also deliver common applications such as office automation and electronic mail. Enclaves are analogous to general support systems. Enclaves may be specific to an organization or a mission, and the computing environments may be organized by physical proximity or by function independent of location. Examples of enclaves include local area networks and the applications they host, backbone networks, and data processing centers. (DODD 8500.1)

Information—1. Facts, data, or instructions in any medium or form. 2. The meaning that a human assigns to data by means of the known conventions used in their representation.

Information Asset—Any information that has enterprise value and is created, managed, or accessed during the operation of the organization.

Information Management (IM)—The planning, budgeting, manipulating, and controlling of information throughout its life cycle. (***Note***: The information life cycle is typically characterized as creation or collection, processing, dissemination, use, storage, protection, and disposition.) (DODD 8000.1)

Information System—A discrete set of information resources organized for collection, storage, processing, maintenance, use, sharing, dissemination, disposition, display, or transmission of information. (***Note***: Includes automated information system (AIS) applications, enclaves, outsourced IT-based processes, and platform IT interconnections.) (DODD 8500.1)

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. This includes equipment used by the executive agency directly or used by a contractor under a contract with the executive agency, 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” includes computers, ancillary equipment, software, firmware, and similar procedures, services (including support services), and related resources. Notwithstanding the preceding, the term "IT” does not include any equipment that is required by a federal contractor incident to a federal contract. The term “IT” includes National Security Systems (NSS), and is synonymous with the term "information system" (IS). (DODD 4630.5, *Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)*, May 5, 2004; and 40 U.S.C. 11101(6))

Interoperability—Interoperability is the ability of systems, units or forces to provide data, information, materiel, and services and to accept the same from other systems, units, or forces and to use the data, information, materiel, and services so exchanged to enable them to operate effectively together. IT and NSS 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. (DODD 4630.5)

Knowledge—Information from multiple domains that has been synthesized, through inference or deduction, into meaning or understanding that was not previously known.

Knowledge Management (KM)—The handling, directing, governing, or controlling of natural knowledge processes (acquire/validate, produce, transfer/integrate knowledge) within an organization in order to achieve the goals and objectives of the organization (JP 6-0). KM seeks to make the best use of the knowledge that is available to an organization, creating new knowledge, and increasing awareness and understanding in the process. KM can also be defined as the capturing, organizing, and storing of knowledge and experiences of individual workers and groups within an organization and making this information available to others in the organization.

Metadata—Data that define other data. Metadata are an information product, such as classification, format, size, keywords, etc.

National Security System (NSS)—Any telecommunications or IS operated by the U.S. Government, the function, operation, or use of which: 1) involves intelligence activities; 2) involves cryptologic activities

related to national security; 3) involves command and control of military forces; 4) involves equipment that is an integral part of a weapon or weapons system; or 5) is critical to the direct fulfillment of military or intelligence missions—(this does not include systems that are used for routine administrative and business applications, including payroll, finance, logistics, and personnel management applications). (DODD 8000.1, 40 U.S.C. 11103) (***Note***: For information assurance (IA) purposes only, pursuant to AFPD 33-2, *Information Assurance (IA) Program*, the term NSS also includes any telecommunications or IS that is protected at all times by procedures established for managing classified information.)

Outsourced IT-based Process—A general term used to refer to outsourced business processes supported by private sector information systems, outsourced information technologies, or outsourced information services. An outsourced IT-based process performs clearly defined functions for which there are readily identifiable security considerations and needs that are addressed in both acquisition and operations. (DODD 8500.1)

Platform IT Interconnection—Network access to platform IT. Platform IT interconnection has readily identifiable security considerations and needs that must be addressed in both acquisition, and operations. Platform IT refers to computer resources, both hardware and software, that are physically part of, dedicated to, or essential in real time to the mission performance of special purpose systems such as weapons, training simulators, diagnostic test and maintenance equipment, calibration equipment, equipment used in the research and development of weapons systems, medical technologies, transport vehicles, buildings, and utility distribution systems such as water and electric. Examples of platform IT interconnections that impose security considerations include communications interfaces for data exchanges with enclaves for mission planning or execution, remote administration, and remote upgrade or reconfiguration. (DODD 8500.1)

Record—Information, regardless of medium, detailing business transactions. Records include all books, papers, maps, photographs, machine-readable materials, and other documentary materials, regardless of physical form or characteristics. Records are made or received by an Agency of the United States Government under Federal law or in connection with the transaction of public business. Records are preserved or appropriate for preservation by that Agency or its legitimate successor as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of the Government or because of the value of data in the record. (DOD 5015.2-STD, *Design Criteria Standard for Electronic Records Management Software Applications*, June 19, 2002; and 44 U.S.C. 3301)

Records Management (RM)—The planning, controlling, directing, organizing, training, promoting, and other managerial activities involved in records creation, maintenance and use, and disposition in order to achieve adequate and proper documentation of the policies and transactions of the Federal Government and effective and economical management of agency operations. (44 U.S.C. 2901(2))

Role-based Environment—A method to allow access to information based on the roles associated with a user's authentication credentials. Role-based access to information is vital to ensure that users can only access the information needed to perform their assigned duties.

Service-Oriented Enterprise (SOE)—An enterprise in which technologies, infrastructure, governance, policies, funding, and processes of the organization operate within the context of sharing information and capabilities in the enterprise. It provides a means of achieving IT agility and flexibility to support rapidly evolving mission processes and changing goals and objectives. An SOE includes the Enterprise Architecture and follows a component-based capability development methodology to produce modular, reusable and easily adaptable, loosely coupled, software and services.

Taxonomy—A hierarchical arrangement of subjects to enable discovery and management of information assets. The Air Force Core Taxonomy is a structure providing 3 to 4 levels of hierarchy - and is segregated by organization, mission, and resources. Information producers will provide vocabularies for their specific assets, which will interface with the Air Force Core Taxonomy.