BY ORDER OF THE
SECRETARY OF THE AIR FORCE

AIR FORCE POLICY DIRECTIVE 33-1

27 JUNE 2006

Communications and Information

INFORMATION RESOURCES 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/XCXP

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

Supersedes AFPD33-1, 17 September 1993

Pages: 10

This Air Force policy directive (AFPD) establishes AF policy for responsibly acquiring, planning, and managing its information resources. The policy directive details the expanded statutory responsibilities for information resources management (IRM) and information technology (IT) and applies to all AF information resources, information processes, information integration and national security systems (NSS). This publication 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 Directive (DoDD) 8000.1, *Management of DoD Information Resources and Information Technology,* and DoDD 8115.01 *Information Technology Portfolio Management*. Send all recommendations for changes or comments to Air Force Office of Warfighting Integration and Chief Information Officer (SAF/XCXP), 1800 Air Force Pentagon, Washington DC 20330-1800, through appropriate channels, using AF IMT 847, *Recommendation for Change of Publication*, with an information 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 AFMAN 37-123, *Management of Records* (will convert to AFMAN 33-363), and disposed of in accordance with the Air Force Records Information Management (AFRIMS) Records Disposition Schedule (RDS) located at **https://afrims.amc.af.mil.rds_series.cfm**. See **Attachment 1** for a glossary of references and supporting information.

SUMMARY OF CHANGES

This publication is a major revision and assigns overall responsibility for the 33-series publications to the Secretary of the Air Force, Office of Warfighting Integration and Chief Information Officer (SAF/XC). It also changes the title of this directive to Information Resources Management (IRM).

1. Background. The *Paperwork Reduction Act of 1995* (PRA) (Title 44 United States Code Sections 3501-3520) requires each federal agency to designate a Chief Information Officer (CIO) to ensure compliance with federal information policies and implement IRM to improve agency productivity, efficiency, and effectiveness. Subsequent legislation has refined and expanded these information policies and CIO responsibilities, including the management of IT investments and acquisitions in compliance with the *Clinger-Cohen Act of 1996* (CCA) (Title 40 United States Code Sections 11101-11704); ensuring that IT and NSS are interoperable and compliant with federal and DoD standards (Title 10 United States Code Sections 2222 and 2223); and the management and promotion of electronic government services pursuant to the *E-Government Act of 2002* (Title 44 United States Code Section 3501 note, and Sections 3601-3606). Additional requirements and guidance are established by the Office of Management and Budget (OMB), and promulgated through OMB Circular A-130, *Management of Federal Information Resources.* The aforementioned Acts and sections of United States Code are implemented through DoD Directives 8000.1 and 8115.01. The Air Force implements these DoD issuances through this Policy Directive. **Note:** As defined in this AFPD, the term IT includes NSS and is considered synonymous with the term "information system" (IS).

1.1. IRM policies and processes, in order to effectively implement the CCA and other statutory requirements, must ensure IT investments:

1.1.1. Support core mission functions.

1.1.2. Are consistent with the AF enterprise architecture (EA) and integrate work processes and information flows with technology to fulfill the agency's mission and strategic plan.

1.1.3. Are reflected using a portfolio management approach where decisions on whether to invest in IT are based on real and potential return on investment, and decisions to terminate or make additional investments are based on performance--much like an investment broker is measured and rewarded based on managing risk and achieving results.

1.1.4. Are identified through a disciplined approach, including requirements analysis and documentation of formal system development to reduce risk and enhance manageability. Lead an incremental, phased approach using the DoD's evolutionary acquisition process in concert with test and evaluation's seamless verification concept.

1.2. AF direction to transform to an enterprise-wide, net-centric, knowledge-based operational environment requires we identify, fund and manage our information resources in a manner that ensures we reach this vision. Information resources include information, IT, and the associated personnel and funding. The intent of IRM is to provide the policy and processes to analyze, select, control, and evaluate those IT investments we must pursue to support the AF mission. Our IT budget submission must reflect our strategy and investments to leverage IT to support transformation by focusing investments on critical systems essential to our expeditionary forces. Effective IRM provides an avenue to focus our resources in achieving unparallel air, space, and information capabilities.

2. Policy. The AF recognizes that having accurate and current information, with the ability to effectively use it, is essential in maintaining combat superiority and improving support operations. The IRM discipline extends through all echelons of government, all levels of military operations, and across coalition, joint, and service operations. Managing information resources at each level of the military command structure is crucial to ensure information resources are available to support combat and support operations. The AF has established the following IRM policy and will:

2.1. Apply capital planning and investment control through portfolio management to ensure IT investments meet mission goals, improve mission performance, and are integrated with the processes for making budget, financial, and program management decisions within the AF. Additionally, the AF will prepare an annual report as part of the AF IT budget submission to Congress.

2.2. Apply performance-based and results-based management to IT management to establish goals and improve the efficiency and effectiveness of AF activities and delivery of services through the effective use of IT.

2.3. Review AF processes for improvement before making significant IT investments.

2.4. Develop and maintain an IRM strategic plan that identifies and documents the goals, objectives, and IT investments we must pursue to support the AF mission.

2.5. Ensure the effective and efficient design and operation of all major IRM processes to include work processes of the AF.

2.6. Perform IT acquisitions using the DoD's evolutionary acquisition process. Base IT investment decisions on capabilities-based requirements. Remain flexible when considering the time-sensitivity of the capabilities needed, while verifying capabilities against requirements through test and evaluation. In accordance with federal and DoD direction, the AF will monitor and improve project planning and execution by implementing earned value management practices.

2.7. Develop a trained workforce to effectively and efficiently plan, acquire, and manage information resources.

2.8. Develop an enterprise-wide view of information life-cycle activities including people, processes, information, and technology. Leverage the enterprise-wide view with current and emerging technologies to support warfighting, operational support, operational and statutory requirements.

2.9. Institute real-time monitoring, management, and display of performance metrics and standards adherence; and make the information available to decision makers and leaders at all levels.

2.10. Develop and institute a process to ensure information systems meet prescribed standards for security, interoperability, supportability, sustainability, and usability (SISSU) prior to operating on the AF Network.

3. Responsibilities.

3.1. Chief of Warfighting Integration and Chief Information Officer (SAF/XC) will:

3.1.1. As the AF CIO, have clear authority, responsibility, and accountability for the AF's IRM activities. The SAF/XC may delegate specific CIO responsibilities, in writing, to another organization within the AF.

3.1.2. Provide oversight of AF information resources and support the milestone decision authority in the oversight of IT and NSS.

3.1.3. Establish a repeatable AF IT Portfolio Management process consistent with DoD and the federal government direction based on a formal governance structure. Integrate IT capital planning and investment management control/evaluation with the AF planning, programming, budgeting, and execution processes. Ensure all approved IT/NSS investments conform to DoD and AF strategic priorities, as well as established architectures and standards. Ensure procurements are

made based on capability assessments that provide the desired effects to the Joint Warfighter and Combatant Commanders.

3.1.4. Prepare an annual report on the AF IT budget, to include an assessment of AF IT/NSS resource allocation and execution, for submission to the Office of the Secretary of Defense (OSD) and Congress.

3.1.5. Establish goals for improving productivity, efficiency and effectiveness of operations, delivery of services through appropriate and effective use of IT, assessment of IT investments, and progress on key AF IT initiatives against performance goals.

3.1.6. Assess the requirements established for AF personnel regarding the knowledge and skill in IRM and the adequacy of such requirements for facilitating the performance goals established for IRM.

3.1.7. Ensure AF missions are analyzed and, based on the analysis, refine the AF's mission-related and administrative processes as appropriate, before making significant investments in IT to be used in support of the performance of those missions.

3.1.8. Provide implementation guidance for registration of IT, and the CCA and other statutory certification processes (e.g., 10 US.C 2222).

3.1.9. Provide policy, guidance, and standards for IT applications/capabilities development and software lifecycle management.

3.1.10. Participate in AF program reviews (e.g., Program Executive Officer, Capabilities Review and Risk Assessments, etc.) and senior information exchanges (e.g., staff meetings, off-sites, etc.) involving IT acquisitions to confirm the AF is complying with CCA and other applicable mandates and laws.

3.1.11. Establish a governance structure to ensure effective management of information resources.

3.1.12. Develop and maintain an IRM strategic plan that describes how IRM activities help accomplish and support AF missions.

3.2. Assistant Secretary of the Air Force for Financial Management and Comptroller (SAF/FM) and Chief Financial Officer (CFO). SAF/FM, as the CFO, and SAF/XC, in consultation with the Secretary of the Air Force and appropriate AF corporate process elements, will:

3.2.1. Ensure all approved IT investments conform to DoD and AF strategic priorities as well as established architectures and standards.

3.2.2. Ensure the accounting, financial, and asset management systems and other information systems of the AF are designed, developed, maintained, and used effectively to provide financial or program performance data for financial statements of the AF.

3.2.3. Ensure financial and related program performance data are provided on a reliable, consistent, and timely basis to AF financial management systems.

3.2.4. Ensure financial statements support:

3.2.4.1. Assessments and revisions of mission-related processes and administrative processes of the AF.

3.2.4.2. Performance measurement of information systems investments made by the AF.

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

3.3.1. Assist SAF/XC by ensuring that acquisition community structures, policies, and processes are in compliance with legal and policy requirements for acquisition oversight, economic efficiency, innovative contracting methods, earned value management, information assurance, and interoperability and supportability requirements.

3.3.2. Assist SAF/XC staff in clarifying statutory (e.g., CCA) compliance requirements and help ensure timely completion and processing of required actions for certification/confirmation. Initiate statutory compliance and certification, for Major Automated Information System (MAIS) programs, at program initiation or the earliest point possible.

3.3.3. Ensure service-oriented architecture (SOA) policies and standards are adopted and followed in developing and fielding IT capabilities. Also, ensure IT system development adheres to mandated IT standards outlined in the Defense IT Standards Registry, AF Technical Reference Model, and the DoD IT Security Certification and Accreditation Process (DITSCAP).

3.4. Under Secretary of the Air Force (SAF/US). As the Service Acquisition Executive for Space Programs, SAF/US will:

3.4.1. Assist SAF/XC by ensuring that space program structures, policies, and processes are in compliance with legal and policy requirements for space program acquisition oversight, economic efficiency, innovative contracting methods, earned value management, information assurance, and interoperability and supportability requirements.

3.4.2. Assist SAF/XC staff in clarifying statutory (e.g., CCA) compliance requirements and help ensure timely completion and processing of required actions for certification/confirmation. Initiate statutory compliance and certification, for Space Programs that contain IT components, at program initiation or the earliest point possible.

3.4.3. Ensure SOA policies and standards are adopted and followed in developing and fielding Space Program IT capabilities. Also, ensure space program development adheres to mandated IT standards outlined in the Defense IT Standards Registry, AF Technical Reference Model, and the DoD IT Security Certification and Accreditation Process (DITSCAP).

3.5. MAJCOMs, Field Operating Agencies/Direct Reporting Units will:

3.5.1. Establish an IT capital planning and investment control process, subject to the AF enterprise IRM governance structure.

3.5.2. Provide IT acquisition assistance where appropriate.

3.5.3. Establish goals for improving productivity, efficiency and effectiveness of operations, and the delivery of services through appropriate and effective use of IT.

3.5.4. Use AF EA and applicable domain architectures to help make information resources decisions.

3.5.5. Develop and maintain an IRM strategy that supports the AF IRM strategic plan.

3.5.6. Provide oversight of the IT workforce development program.

3.5.7. Develop active partnerships with mission and business owners seeking to transform operations with IT.

3.5.8. Provide advocacy for state-of-the-art technology to give the competitive edge while balancing technological risks, costs, and objectives when fielding new technologies.

3.5.9. Provide advocacy for e-Government initiatives, such as e-Commerce, that leads to effective and efficient mission/business processes.

4. Measuring Compliance with Policy. The measure of effectiveness of this policy is accomplished through the SAF/XC Strategic Plan Metrics Program to measure the AF Information Resources Strategy Goals.

5. Adopted Form: AF IMT 847, *Recommendation for Change of Publication*.

MICHAEL W. WYNNE
Secretary of the Air Force

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

Title 10, United States Code, Sections 2222 and 2223Title 40, United States Code, Sections 11101-11704 (*Clinger-Cohen Act of 1996* (CCA))

Title 44, United States Code, Sections 3501-3520 (*Paperwork Reduction Act of 1995* (PRA))

Title 44, United States Code, Section 3542

Title 44, United States Code, Sections 3601-3606 (*E-Government Act of 2002*)

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

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

DoDD 8000.1, *Management of DoD Information Resources and Information Technology*, February 27, 2002

DoDD 8100.1, *Global Information Grid (GIG) Overarching Policy*, September 19, 2002

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

DoDD 8500.1, *Information Assurance (IA)*, October 24, 2002

AFPD 33-2, *Information Protection*, 1 December 1996 (will become Information Assurance (IA) Program

AFMAN 37-123*, Management of Records*, 31 August 1994 (will convert to AFMAN 33-363)

Abbreviations and Acronyms

AFPD—Air Force Policy Directive

CCA—Clinger-Cohen Act

CFO—Chief Financial Officer

CIO—Chief Information Officer

DoD—Department of Defense

EA—Enterprise Architecture

IRM—Information Resources Management

IA—Information Assurance

IM—Information Management

IS—Information System

IT—Information Technology

ITM—Information Technology Management

IT—Information Technology

NSS—National Security Systems

SISSU—security, interoperability, supportability, sustainability, and usability

SOA—service-oriented architecture

USC—United States Code

Terms

—The following terms are specific to AF IRM. Whenever possible, the source of the term is cited parenthetically at the end of the definition. Where no citation appears, the term has been derived from several sources or from common usage.

Automated Information System (AIS) Application—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. Note that 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 (MAIS). (DoDD 8500.1, *Information Assurance (IA)*)

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 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)

Enterprise Architecture (EA)—The explicit description and documentation of the current and desired relationships among business and management processes and information technology. 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. (DoDD 8100.1, *Global Information Grid Overarching Policy*, and OMB Circular A-130, paragraph 8.b.(2)(a))

Information Resources (IR)—Information and related resources, such as personnel, equipment, funds, and IT. (DoDD 8000.1 and 44 USC 3502(6))

Information Resources Management—(IRM)—The process of managing information resources to accomplish agency missions and to improve agency performance, include through the reduction of information collection burdens on the public. (DoDD 8000.1 and 44 US.C 3502(7))

Information System (IS)—A discrete set of information resources organized for collection, storage, processing, maintenance, use, sharing, dissemination, disposition, display, or transmission of information. Includes automated information system (AIS) applications, enclaves, outsourced IT-based processes, and platform IT interconnections. (DoDD 8500.1 and 44 USC 3502(8))

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 that (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 computer, 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)*; DoDD 8000.1; and 40 USC 11101(6)).

IT Investment—The development and sustainment resources needed in support of IT or IT-related initiatives. These resources include, but are not limited to: research, development, test, and evaluation appropriations; procurement appropriations; military personnel appropriations; operations and maintenance appropriations; and Defense Working Capital Fund. (DoDD 8115.01)

National Security System (NSS)—Any telecommunications or information system (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 a system that is to be used for routine administrative and business applications, including payroll, finance, logistics, and personnel management applications). (DoDD 8000.1and 40 USC 11103) (**Note**: For information assurance (IA) purposes only, pursuant to AFPD 33-2, Information Protection (will become *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. (Title 44 United States Code Section 3542(2)).

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)

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

Warfighting Integration—Closing the seams between find, fix, track, target, engage, and assess in the kill chain by the integration of manned, unmanned, and space systems requiring an enterprise approach of total information cycle activities including people, processes, and technology. (XI PAD HQ USAF 02-02)