

AD-A256 988



27 OCTOBER 1992 final

Department of Defense Directive (DODD) 8000.1
Defense Information Management (IM) Program

OASD(C3I), Office of the Director of Defense Information
1225 Jefferson Davis Hwy -- Suite 910
Arlington, VA 22202-4301

Attn: Linda Bagby

same as above

92-29500



Distribution Statement A: Approved for Public Release;
Distribution is Unlimited

DoDD 8000.1 implements the information management program for the Department of Defense, in according with responsibilities assigned the [redacted] Directive for the Assistant Secretary of Defense for Command, Control, Communications and Intelligence. DoDD 8000.1 incorporates policies & responsibilities from SECDEF memorandums & the Corporate Information Management Implementation Plan.

DTIC
LECTE
NOV 13 1992
S B D

Corporate Information Management
Information Management

10

UNCLASSIFIED

REPRODUCED BY
U.S. DEPARTMENT OF COMMERCE
NATIONAL TECHNICAL
INFORMATION SERVICE
SPRINGFIELD, VA 22161

92 11 13





Department of Defense DIRECTIVE

October 27, 1992
NUMBER 8000.1

ASD(C3I)

SUBJECT: Defense Information Management (IM) Program

- References:**
- (a) DoD Directive 5137.1, "Assistant Secretary of Defense for Command, Control, Communications, and Intelligence (ASD(C3I))," February 12, 1992
 - (b) DoD Directive 5122.5, "Assistant Secretary of Defense (Public Affairs)," August 4, 1988
 - (c) Public Law 96-511, "The Paperwork Reduction Act of 1980," December 11, 1980 (44 U.S.C. 350 *et seq.*), as amended
 - (d) Office of Management and Budget Circular A-130, "Management of Information Resources," December 12, 1985
 - (e) through (p), see enclosure 1

A. PURPOSE

This Directive:

1. Establishes policy and assigns responsibilities under reference (a) for implementation, execution, and oversight for the Defense IM Program.
2. Governs the continual evolution and improvement of the essential elements of IM, which include the functional process improvement program, information resources management, and supporting information technology and services throughout the Department of Defense.

B. APPLICABILITY AND SCOPE

This Directive:

1. Applies to the Office of the Secretary of Defense (OSD), the Military Departments (including their National Guard and Reserve components), the Chairman of the Joint Chiefs of Staff and the Joint Staff, the Unified and Specified Combatant Commands, the Inspector General of the Department of Defense (IG, DoD), the Defense Agencies, and the DoD Field Activities (hereafter referred to collectively as "the DoD Components").
2. Applies to all activities relating to the collection, creation, use, dissemination and disposition of all data and information, regardless of medium or intended use. Management of the Freedom of Information Act Program, newspapers, periodicals, publications, the Armed Forces Radio and Television Service, visual information, and audiovisual activities shall be as specified in reference (b).
3. Does not apply to automated information system (AIS), Federal information processing (FIP), or automated data processing equipment (ADPE) resources and services that are an integral part of a weapon or weapon system, test support for a weapon or weapon system, or basic DoD research and development activities.

4. Applies to the IM resources and services used for routine administrative and business applications in conjunction with the preceding activities and to command, control, communications, and intelligence (C3I) unless specifically exempted by the ASD(C3I).

C. DEFINITIONS

Terms used in this Directive are defined in enclosure 2.

D. POLICY

It is DoD policy that:

1. Accurate and consistent information shall be made available to decision-makers expeditiously to effectively execute the DoD missions, as follows:

a. The need for the creation and availability of information shall be determined by the function or activity supported.

b. Data and information shall be corporate assets structured to enable full interoperability and integration across DoD activities.

c. A disciplined life-cycle approach shall be used to manage information systems (ISs) from inception through discontinuance.

d. Security, integrity, and survivability of information are basic to the DoD mission and shall be an integral part of all functional processes.

e. Changes to the functional processes and information of the Department of Defense shall be based on sound business principles and supported by DoD-approved analyses. Where functional economic analyses are warranted, those analyses shall include total costs and investment benefits of all activities in a functional area, including the associated ISs.

f. The identification and validation of process improvements shall be based on DoD-approved activity models that document functional processes and associated data models that document data and information requirements, including integration of information from other functional areas.

g. The principle of fee-for-service shall govern the provisioning of information services and information technology capabilities, where possible.

h. Identification and validation of functional requirements and ensuring that satisfactory functional processes are implemented and operated shall be done by the OSD Principal Staff Assistants and the Chairman of the Joint Chiefs of Staff.

2. The ISs are planned, acquired, developed, and implemented from a DoD-wide perspective to ensure consistency of information and processes in and across functional areas, as follows:

a. Where possible and cost-effective, as seen from a DoD viewpoint:

(1) A centrally managed infrastructure for computing, communications, information security, and systems security shall be used.

(2) Approved DoD-wide methods, approaches, models, tools, data, information technology, and information services shall be used.

(3) Integration shall be achieved across functional areas while maintaining the ability to change processes within individual functional systems independently.

b. Standard DoD data definitions shall be used for all ISs, to include the interfaces between weapon systems and the ISs.

c. The ISs shall be based on a model of information needs that encompasses the creation, collection, processing, transmission, use, storage, dissemination, and disposition of information regardless of function or component level.

d. Security of information, commensurate with the risk and magnitude of harm resulting from loss, misuse, or unauthorized access to or modification of the information, shall be an integral part of all IS designs. The user shall apply risk analysis to validate IS designs for war scenario survivability.

e. IS development or modernization shall be based on sound business principles, incorporating the evaluation of costs and benefits to include the satisfaction of mission requirements; and consistency with life-cycle management policies and procedures and the following:

(1) Design by prototyping, in a generally defined strategy, as the preferred course for the rapid fielding of improved systems.

(2) Use DoD-wide IM methodologies supported by the application of DoD-approved support tools where available.

(3) Acquire, to the extent practical, information technology components from the centrally-managed DoD-wide information technology repository to reduce the time and costs of the ISs.

(4) Ensure maximum reuse of standard software components and use DoD-approved software engineering tool sets and metrics to provide for continuous quality improvement.

E. RESPONSIBILITIES

1. The Assistant Secretary of Defense for Command, Control, Communications, and Intelligence shall:

a. Serve as the Principal Staff Assistant for the DoD IM Program, in accordance with DoD Directive 5137.1, section C. (reference (a)). That includes development, and oversight of standard DoD-wide IM policies, procedures, strategic planning, methods, models, and tools, as well as appropriate IM performance measures and assessments.

b. As the DoD Senior IM official (subsection D.2. of reference (a)), issue policies and procedures to implement Pub. L. No. 96-511 (1980), OMB Circular A-130, and 41 CFR 201 (references (c) through (e)); executed by DoD Directive 7740.1 (reference (f)).

c. Issue policies and procedures for the design, development, deployment, operation, and acquisition of the AISs implemented by DoD Directive 7920.1 (reference (g)).

d. Promote integration of the policies in section D. and paragraphs E.1.a. through E.1.c., above, and the IM principles (enclosure 3) for all DoD activities and establish appropriate thresholds for application of implementing procedures in consultation with the DoD Components. Identify opportunities for the integration of IM strategic planning, processes, methods, approaches, activities, services, systems, and information across functional areas. Facilitate resolution of functional and technical integration issues across functional areas and forward unresolved functional issues to the Deputy Secretary of Defense.

e. Chair a senior-level DoD Information Policy Council, and establish appropriate boards to provide forums for functional and information managers to exchange a full range of views about DoD IM policies and to facilitate cross-function integration of IM functions, activities, data, the ISs, and information services.

f. Provide for the development and maintenance of an IM model(s) that presents an integrated top-level representation of DoD processes, information flows, and data, in consultation with the DoD Components.

g. As the DoD senior information security official (subsection D.4. of DoD Directive 5137.1, reference (a)), ensure the development and implementation of data, information, and IS security policies and procedures, to include the identification of threat.

h. Ensure the development, operation, and maintenance of a centrally managed DoD-wide IM infrastructure, to include repositories, computing, communications, information security, and systems security, where it is cost-effective from a DoD perspective.

i. Ensure the development and implementation of standard DoD-wide data; IM methods, models, and tools; and information technology and services (paragraph D.17.z. of reference (a)).

j. Assist, as necessary, the DoD Components in establishing programs for the development and retention of highly qualified IM professionals (subsection D.12. of reference (a)).

2. The Director of Administration and Management, Office of the Secretary of Defense, shall manage for the ASD(C3I) the execution of records management and privacy programs in the Department of Defense (subsection D.2. of reference (a)).

3. The Principal Staff Assistants of the Office of the Secretary of Defense and the Chairman of the Joint Chiefs of Staff, in executing their responsibility and authority for assigned functional areas, including the supporting ISs, shall:

a. Simplify and streamline the DoD operation by ensuring the application of sound business practices; policies in section D., above; and IM principles (enclosure 3).

b. Implement, execute, and exercise oversight for the evaluation and improvement of functional processes as well as the development of functional process performance measures and assessments.

c. Develop, integrate, implement, and maintain functional strategic plans, objectives, architectures, IS strategies, and related models and repository contents that support the functional missions.

d. Promote commonality of functional processes across the DoD Components. Resolve functional issues affecting IM and provide for the resolution of technical ISs integration issues in their functional areas.

e. Establish and chair, where feasible, a Functional Steering Committee, or in each functional area of responsibility, provide a DoD-wide forum for senior functional managers to exchange a full range of views.

f. Ensure preparation and validation of functional economic analyses (FEAs), as required.

g. Perform functional management control and oversight of their supporting ISs throughout the systems' life-cycles, ensuring functional leadership in all life-cycle phases.

h. Review funding requirements for IM and information technology programs during planning, programing, and budgeting system activities and recommend appropriate adjustments and allocations.

4. The Heads of the DoD Components shall:

a. Establish a Component IM program to integrate, implement, and oversee DoD IM principles, policies, procedures, programs, and standards.

b. Appoint a senior official (or a senior representative for the Defense Agencies, the Chairman of the Joint Chiefs of Staff, and the DoD Field Activities) reporting directly to the Heads of the DoD Components to be responsible for the DoD Component IM program.

c. Apply the policies in section D., above, the IM principles (enclosure 3), and strategic planning to functional processes under their cognizance and in functional process improvement efforts managed by responsible OSD Principal Staff Assistants.

d. Ensure that each new weapon system, or major change to an existing weapon system, is assessed for its interaction with, and integration into, the DoD IM infrastructure consistent with DoD Instruction 5000.2, subsections C.4. and C.7. (reference (h)), and:

(1) Ensure that all interfaces to the ISs are in compliance with DoD IM standards.

(2) Identify any unique IS support requirements and include their costs into the total life-cycle cost estimates of the weapon systems.

5. The Director, Defense Information Systems Agency, shall execute the responsibilities in DoD Directive 5105.19 (reference (i)) and:

a. Develop and execute, with DoD Component participation, integrated information technology standardization under the DoD Standardization Program (subsection Q.6. of DoD Instruction 5000.2, reference (h)).

b. Develop and manage the DoD Data Administration Program (DoD Directive 8320.1 (reference (j))).

c. Make available IM expertise and supporting technical services to the DoD Components on a competitive fee-for-service basis.

d. Develop and provide analytic support methods, models, and tools to the DoD Components.

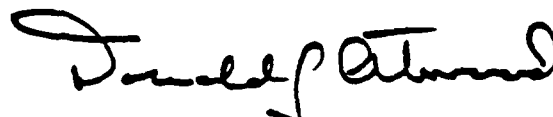
e. Plan for and provide value-added functions such as information and system security; survivability; technical and data standards; databases; directories; standard information technology products and services including reusable software modules; and a competitive DoD-wide infrastructure to include computing, communications, and data from a central information utility service. Resources shall be justified on the basis of revenue from fees.

f. Formulate and execute, with DoD Component participation, an acquisition program for central acquisition of DoD standard information technology products and services.

g. Consistent with the assigned responsibilities of, and in consultation with the Directors of the Defense Intelligence Agency and the National Security Agency, provide technology and services required to ensure the availability, reliability and maintainability, integrity, and security of defense information, commensurate with its intended use.

F. EFFECTIVE DATE AND IMPLEMENTATION

This Directive is effective immediately. The Heads of the DoD Components shall establish strict controls to ensure that implementing documents are kept to the absolute minimum, consistent with this Directive. Forward one copy of implementing documents to the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence within 180 days.



Donald J. Atwood
Deputy Secretary of Defense

Enclosures - 3

1. References
2. Definitions
3. IM Principles

DTIC QUALITY INSPECTED 4

Accession For	
NTIS GRA&I	<input checked="checked" type="checkbox"/>
DTIC TAB	<input type="checkbox"/>
Unannounced	<input type="checkbox"/>
Justification	
By _____	
Distribution/	
Availability Codes	
Dist	Avail and/or Special
A-1	

REFERENCES, continued

- (e) Title 41, Code of Federal Regulations, Part 201, "The Federal Information Resources Management Regulation," current edition
- (f) DoD Directive 7740.1, "DoD Information Resources Management Program," June 20, 1983
- (g) DoD Directive 7920.1, "Life-Cycle Management of Automated Information Systems (AISs)," June 20, 1988
- (h) DoD Instruction 5000.2, "Defense Acquisition Management Policies and Procedures," February 23, 1991
- (i) DoD Directive 5105.19, "Defense Information Systems Agency (DISA)," June 25, 1991
- (j) DoD Directive 8320.1, "DoD Data Administration," September 26, 1991
- (k) Public Law 99-591, "Paperwork Reduction Reauthorization Act of 1986" (40 U.S.C. 759 (a)(2))
- (l) Joint Pub 1-02, "Department of Defense Dictionary of Military and Associated Terms," December 1, 1989
- (m) DoD Instruction 7041.3, "Economic Analysis and Program Evaluation for Resource Management," October 18, 1972
- (n) DoD Directive 5200.28, "Security Requirements for Automated Information Systems (AIS)," March 21, 1988
- (o) DoD Directive 5025.1, "Department of Defense Directives System," December 23, 1988
- (p) Public Law 97-86, "Department of Defense Authorization Act, 1982" (10 U.S.C. 2315)

DEFINITIONS

1. Automated Data Processing Equipment (ADPE). Any equipment or interconnected system or subsystems 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 a Federal Agency, or under a contract with a Federal Agency, which requires the use of such equipment; or requires the performance of a service; or the furnishing of a product that is performed or produced making significant use of such equipment. Such term includes computers; ancillary equipment; software, firmware, and similar procedures; services, including support services; and related resources, as defined by the Administrator for General Services (Pub. L. No. 99-591 (1986), reference (k)).
2. Automated Information System (AIS). A combination of information, computer, and telecommunications resources, and other information technology and personnel resources that collect, record, process, store, communicate, retrieve, and display information (DoD Directive 7920.1, reference (g)).
3. Federal Information Processing (FIP) Resources. Any ADPE, as defined in definition 1., above (41 CFR 201, reference (e)).
4. Function. Appropriate or assigned duties, responsibilities, missions, tasks, functions, powers, or duties of an individual, office, or organization (Joint Pub 1-02, reference (l)). A functional area (e.g., personnel) is comprised of one or more functional activities (e.g., recruiting), each of which consists of one or more functional processes (e.g., interviews).
5. Functional Economic Analysis (FEA). A structured proposal that serves as the principal part of a decision package for enterprise leadership. It includes an analysis of functional process needs or problems; proposed solutions, assumptions, and constraints; alternatives; life-cycle costs; benefits and/or cost analysis; and investment risk analysis. It is consistent with, and amplifies, existing DoD economic analysis policy in DoD Instruction 7041.3 (reference (m)).
6. Information. Any communication or reception of knowledge such as facts, data, or opinions, including numerical, graphic, or narrative forms, whether oral or maintained in any medium, including computerized data bases, paper, microform, or magnetic tape (OMB Circular A-130, reference (d)).
7. Information Management (IM). The functional proponents creation, use, sharing, and disposition of data or information as corporate resources critical to the effective and efficient operation of functional activities consistent with IM guidance issued by the C3I. It includes the structuring of functional management improvement processes by the OSD Principal Staff Assistants to produce and control the use of data and information in functional activities; information resources management; and supporting information technology and information services.
8. Information Resources Management. The planning, budgeting, organizing, directing, training, promoting, controlling, and management activities associated with the burden, collection, creation, use, and dissemination of information by

Agencies and includes the management of information and related resources, such as FIP resources (Pub. L. No. 99-591 (1986), reference (k)).

9. Information Services. A range of IM activities typically provided from service suppliers to customers on a fee-for-service basis. Those activities include analysis, acquisition, test, delivery, operation, or management of hardware, software, and communications systems.

10. Information System (IS). The organized collection, processing, transmission, and dissemination of information, in accordance with defined procedures, whether automated or manual (DoD Directive 5200.28, reference (n)).

11. Information Technology. The hardware and software used for Government information, regardless of the technology involved, whether computers, communications, micrographics, or others (OMB Circular A-130, reference (d)).

12. OSD Principal Staff Assistants. The Under Secretaries of Defense; the Assistant Secretaries of Defense; the General Counsel of the Department of Defense; the IG, DoD; the Comptroller of the Department of Defense; the Assistants to the Secretary of Defense; and the OSD Directors, or equivalents, who report directly to the Secretary or the Deputy Secretary of Defense (DoD Directive 5025.1, reference (o)).

13. Weapon System. Items that can be used directly by the Armed Forces to carry out combat missions and that cost more than 100,000 dollars or for which the eventual total procurement cost is more than 10 million dollars. That term does not include commercial items sold in substantial quantities to the general public (Pub. L. No. 97-86 (1982), reference (p)).

PRINCIPLES OF INFORMATION MANAGEMENT (IM)

Implementation of the DoD IM Program shall be guided by the following principles:

1. Information shall be managed through centralized control and decentralized execution.
2. Simplification by elimination and integration is to be preferred to automation whether developing new or enhancing existing information systems (ISs).
3. Proposed and existing business methods must be subject routinely to cost-benefit analysis, which includes benchmarking against the best public and private sector achievement.
4. New business methods shall be proven or validated before implementation.
5. The ISs performing the same function must be common unless specific analysis determines they should be unique.
6. Functional management shall be held accountable for all benefits and all directly controllable costs of developing and operating their ISs.
7. The ISs shall be developed and enhanced according to a DoD-wide methodology and accomplished in a compressed timeframe to minimize the cost of development and achieve early realization of benefits.
8. The ISs shall be developed and enhanced in the context of process models that document business methods.
9. The computing and communications infrastructure shall be transparent to the ISs that rely on it.
10. Common definitions and standards for data shall exist DoD-wide.
11. Where practicable, information services shall be acquired through competitive bidding considering internal and external sources.
12. Data must be entered only once.
13. Access to information shall be facilitated, and/or controlled and limited, as required. Information must also be safeguarded against unintentional or unauthorized alteration, destruction, or disclosure.
14. The presentation between the user and system shall be friendly and consistent.

DEPARTMENT OF DEFENSE DIRECTIVE (DODD) 8000.1
DEFENSE INFORMATION MANAGEMENT (IM) PROGRAM

OFFICE OF THE DIRECTOR OF DEFENSE INFORMATION
ARLINGTON, VA

OCT 92