



DEFENSE INFORMATION SYSTEMS AGENCY

701 S. COURT HOUSE ROAD
ARLINGTON, VA 22204-2199

DIRECTOR'S POLICY LETTER 93-3

30 March 1993

DISA and OMNCS Information Management Policy

1. Purpose. The purpose of this policy letter is to establish the Defense Information Systems Agency (DISA) and Office of the Manager, National Communications System (OMNCS) framework for defining and managing DISA and OMNCS information resources and systems. (Note: As appropriate, reference to "DISA" includes the OMNCS.)

2. References. Listed in Enclosure 1.

3. Policy.

a. The underlying principle for management of the DISA Information System (DISA-IS) is that information will be treated as a critical resource within the Agency.

b. The DISA-IS will be centrally managed, using standards-based methodology, with distributed execution and operation of information systems resources.

c. The DISA-IS infrastructure will be centrally funded. Non-infrastructure components (e.g., premise equipment such as PCs, printers, etc.) will be funded by the using DISA organization.

d. Premise equipment connected to, or to be connected to, the DISA-IS infrastructure must meet Agency standards and must employ standard applications/products. Premise equipment, required and purchased by DISA using organizations as stand-alone resources, must also comply with standards established for the DISA-IS infrastructure.

e. When mission requirements dictate the use of non-standard systems to be interfaced with the DISA-IS infrastructure or as stand-alone resources, the requiring DISA office will submit formal requests for waivers, providing full justification, to HQ DISA/Chief Information Officer.

OPR: IA
DISTRIBUTION: A, B, J

f. DISA organizations will not connect/interface applications residing on systems or equipment to the DISA-IS infrastructure without prior approval of the responsible operations element.

g. New DISA organizations will transition their legacy systems to the DISA-IS architecture as soon as practical within resource constraints.

h. All DISA organizations will adhere to published DISA-IS policies, guidance, and standards.

i. The functions of Information Resources Management (IRM) in DISA will be performed consistent with public law and the directives of higher authorities.

4. Enclosure 2 expands and clarifies these policies. HQ DISA/IA will supplement existing guidelines and policy documents for DISA and OMNCS use.

- 2 Enclosures:
(1) References
(2) DISA and OMNCS Information Management Policy


ALONZO E. SHORT, JR.
Lieutenant General, USA

References:

- (a) OMB Circular A-130, "Management of Federal Information Resources," December 12, 1985
- (b) DoD Directive 8000.1, "Defense Information Management (IM) Program," October 27, 1992
- (c) DISA CIM, "DoD Technical Architecture Framework for Information Management," Volumes 1-5, October 21, 1992
- (d) DISA CIM, "DoD Technical Reference Model," version 1.2, (Vol 3), August 25, 1992
- (e) DISA CIM, "DoD Human Computer Interface Style Guide," version 1.0, February 12, 1992
- (f) Draft DISA CIM, "DoD Standards Based Architecture Planning Handbook," version 1.0, March 6, 1992
- (g) DoD Directive 7920.1 "Life Cycle Management of Automated Information Systems (AIS)," June 20, 1988 [Revision pending]
- (h) DoD Instruction 7920.2 "Automated Information Systems (AIS) Life Cycle Management Review and Milestone Approval Procedures," March 7, 1990 [Revision pending]
- (i) DoD Directive 5200.28, "Security Requirements for Automated Information Systems (AIS)," March 1988
- (j) DISA Instruction 630-230-19, "Security Requirements for Automated Information Systems (AIS)," August 1991
- (k) DoD Directive 7740.1, "DoD Resources Information Management Program," June 1983
- (l) DoD Directive 8320.1, "DoD Data Administration," September 26, 1991
- (m) Draft DoD 8320.1M, "DoD Data Administration Procedures," September 21, 1992
- (n) Draft DoD 8320.1M-1, "DoD Data Element Standardization Procedures," September 30, 1992
- (o) DoD Instruction 8020.1, "Functional Process Improvement Program," October 1, 1992
- (p) Draft DoD 8020.1-M, "Functional Process Improvement," August 1992
- (q) ITPB Guidance No 9148, and Working Draft DoDD 3405.1, "Software Management," November 1, 1992, version 4.
- (r) DoD Directive 7950.1, "Defense Automation Resources Management," September 1988
- (s) DoD 7950.1-M, "Defense Automation Resources Management Manual," September 1988
- (t) GSA, "Federal Information Resources Management Regulation (FIRMR)," 1990 Loose Leaf Edition

- (u) J.A. Zachman, IBM Systems Journal, "A Framework for Information Systems Architecture," Vol 26, Nr. 3, 1987
- (v) Integrated Computer Aided Software Engineering (ICASE) Usage Policy Memo, ODDI, February 1992

SUBJECT: DISA and OMNCS Information Management Policy

A. PURPOSE:

The purpose of this document is to establish the Defense Information Systems Agency (DISA) and Office of the Manager, National Communications System (OMNCS) policy framework for defining and managing DISA and OMNCS information resources and systems. Within this framework, DISA and OMNCS Instructions and subordinate operational and procedural documents will be implemented. (Note: For the remainder of this document, any reference to "DISA" includes the OMNCS, as appropriate).

B. DEFINITIONS:

1. Attachment 1 contains definitions from DoD and government references which apply to this policy.

2. However, the following paragraphs more clearly define key concepts as used in the context of DISA information management (IM) policy.

a. DISA Information Management: The planning, budgeting, organizing, directing, training, promoting, and controlling of internal DISA information as a corporate resource. Information systems, information technology, information services, and information resources management (IRM) are components and activities of DISA Information Management (DISA-IM).

b. DISA Information Systems: The organized collection, processing, transmission, and dissemination of internal DISA information, in accordance with defined procedures, whether automated or manual. The DISA Information System (DISA-IS) comprises all of the information and processes used by DISA personnel to accomplish their jobs. The DISA-IS includes all internal DISA systems that process and/or transmit voice/data/imagery signals. The DISA Network (DISANet) is one of the principal, and most visible, DISA automated information systems (AIS). Elements of the DISA-IS may have access to or interface with DISA mission, mission-support, or business systems; however, the DISA-IS does not include specific DISA mission systems, mission-support systems, or DoD business systems. Internal administrative systems identified as legacy systems, which are typically specific to DISA needs, are part of the DISA-IS until replaced by DoD migratory business systems.

c. DISA Information Technology: The hardware and software used to manage internal DISA information, regardless of the technology involved, whether computers, communications, micrographics, or others.

d. DISA Information Services: A range of internal DISA information management activities, typically provided by DISA service suppliers to internal DISA customers. These activities include analysis, acquisition, test, delivery, operation, or management of information technology. Examples include data administration, AIS security, IM review and oversight, operation and maintenance (O&M), requirements processing, business process improvement, etc.

e. DISA Information Resources Management (IRM): The planning, budgeting, organizing, directing, training, promoting, controlling, and management activities associated with the burden, collection, creation, use, and dissemination of information by the DISA. It includes the management of information and related resources, such as federal information processing (FIP) resources, as directed by public law.

f. DISA-IS Infrastructure: The centrally funded, electronic transport mechanisms and processors which connect and transfer information between DISA users and locations. It also includes the centrally funded, standard software applications, services, and utilities which satisfy DISA user requirements and Agency corporate needs.

g. DISA Premise Equipment: Automated hardware and software purchased to support DISA individual or organizational unique information processing requirements. Information technology equipment and services not provided as a part of the DISA-IS Infrastructure.

h. DISA-IS Architectures: Planning documents which describe the functional/technical capabilities and the physical configuration of the DISA-IS, necessary to meet Agency mission requirements and goals. They also normally include descriptions of the model DISA-IS and the roadmap/evolutionary changes needed to achieve the model.

i. DISA Mission Systems: Those information systems provided by DISA, primarily in support of customers external to the Agency. Examples include the Defense Information System Network (DISN), the Defense Message System (DMS), the Global Command and Control System (GCCS)/C4I for the Warrior, the Director for Defense Information Network (DDINet), etc.

j. DISA Mission Support Systems: Those information systems provided by DISA, primarily to support DISA component organizations in the accomplishment of their external missions. Examples include the Worldwide On-Line System (WWOLS), the Telecommunications Management System (TMS), test and evaluation systems, etc.

k. DISA Business Systems: Information systems and applications identified as a part of the CIM Initiative to

promote improved business practices within DoD. These systems will evolve into migratory systems from existing legacy systems currently operated by individual components of the DoD. Examples include Acquisition, Civilian Personnel, Finance, Material Resources, etc. Under DMRD, DISA/DITSO will become increasingly responsible for the implementation and operation of these business systems.

l. DISA Legacy Systems: Information systems or applications that perform functions within the areas identified by the CIM Initiatives to be replaced, in time, by DoD Business Systems. Legacy systems will be implemented, maintained, and operated as integral components of the DISA-IS until replaced by CIM migratory systems.

m. DISA Administrative Systems: Those information systems provided to DISA component organizations, primarily to facilitate the management and support of DISA resources. Examples include systems supporting the following functional (and mission) areas: finance, payroll accounting, logistics, transportation, enterprise-level support, acquisition, procurement processing, auditing, project management, etc.

n. DISA Repository: The aggregation and structure of data and information used by DISA personnel in the accomplishment of Agency goals and objectives.

o. DISA Operational Information (aka Action Officer Data): Information collected, stored, maintained, and manipulated by subordinate organizations and/or DISA personnel in the daily conduct of their assigned responsibilities.

p. DISA Component/Mission Information (aka Tactical Data): Information collected, stored, maintained, and manipulated in response to specific mission, mission-support, administrative, or organizational component functions.

q. DISA Corporate Information (aka Strategic Data): Information collected, stored, maintained, and manipulated to support enterprise-level (DISA Command Staff) information needs.

C. DESCRIPTION:

1. The DISA information management environment encompasses all DISA information systems, DISA information technology, DISA information services, and DISA information resources management functions.

2. The DISA-IS comprises all of the information and processes used by DISA personnel to accomplish their jobs. This includes the interface level of DISA-IS access with mission, mission-support, and business systems, but does not include

specific mission, mission-support, or business systems as an integral part of the DISA-IS.

a. The DISA-IS provides a physical infrastructure to support the activities of DISA personnel. The infrastructure consists of the hardware, software, and data systems that provide:

(1) The transportation of information within and between DISA sites, organizations, and personnel; and interfaces permitting the transportation and/or exchange of information to external organizations and personnel.

(2) The processing platforms that store, manage, communicate, manipulate, and present information to other processors or the end user.

(3) The standard applications software and services needed to create, manipulate, display, retrieve, and protect DISA information.

(4) A data administration framework for the efficient management of DISA information.

b. The DISA-IS infrastructure evolves from, and is the product of architectural planning, which is performed at two primary levels within DISA.

(1) The Functional Architecture provides a model and logical description of desired capabilities. It logically integrates the information/data, processes, and management practices used by DISA functions to accomplish the mission. It is based on the Agency's vision, business rules, culture, corporate requirements, user needs, and available/projected resources. It also considers government, DoD, and Agency standards and practices.

(2) The Technical Architecture provides a more specific description of the physical DISA-IS structure and services required to accomplish the Agency mission. It is managed within the DoD Information Systems Architecture and is driven by both the DISA-IS Functional Architecture and the DoD Technical Architecture Framework for Information Management (Reference c). The DISA-IS Technical Architecture is also standards-based and is composed of three elements:

(a) A technical architecture of computing platforms, communications networks, and support applications;

(b) An applications software architecture of operational DISA functions; and

(c) A data architecture of standard DISA data elements, shared DISA databases, data models of DISA functions, etc.

(3) The long range goal of the DISA-IS architecture is to more closely integrate the three major components of the systems environment. Figure C-1 illustrates the conventional or existing relationships; Figure C-2 illustrates the desired (target) relationship between these components.

c. The DISA-IS can also be described according to the levels at which DISA information and processes are managed.

(1) The DISA corporate leadership operates at the strategic level, providing guidance, reviewing strategic policies, monitoring progress, and evaluating data from the tactical environment with respect to DISA objectives and goals.

(2) The DISA Directorate heads, project directors, and program managers operate at the tactical level, directing mission tasks, managing resources, and providing detailed directions based on guidance from the strategic level and the requirements of day-to-day operations.

(3) The rest of the agency operates at the operational level, carrying out the individual tasks required to accomplish DISA's mission.

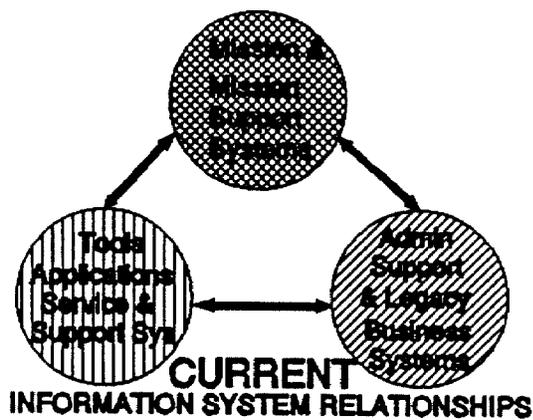


Figure C-1

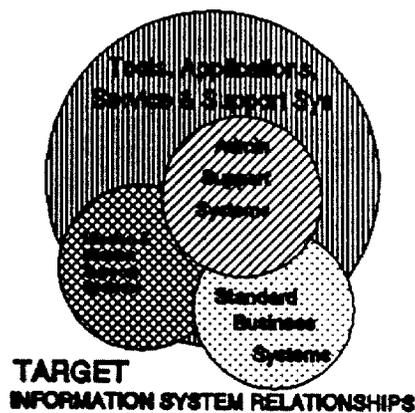


Figure C-2

d. Information and processes contained in the DISA-IS can be viewed from the perspective of control.

(1) Within the DISA-IS, there are three levels of control (see Figure C-3):

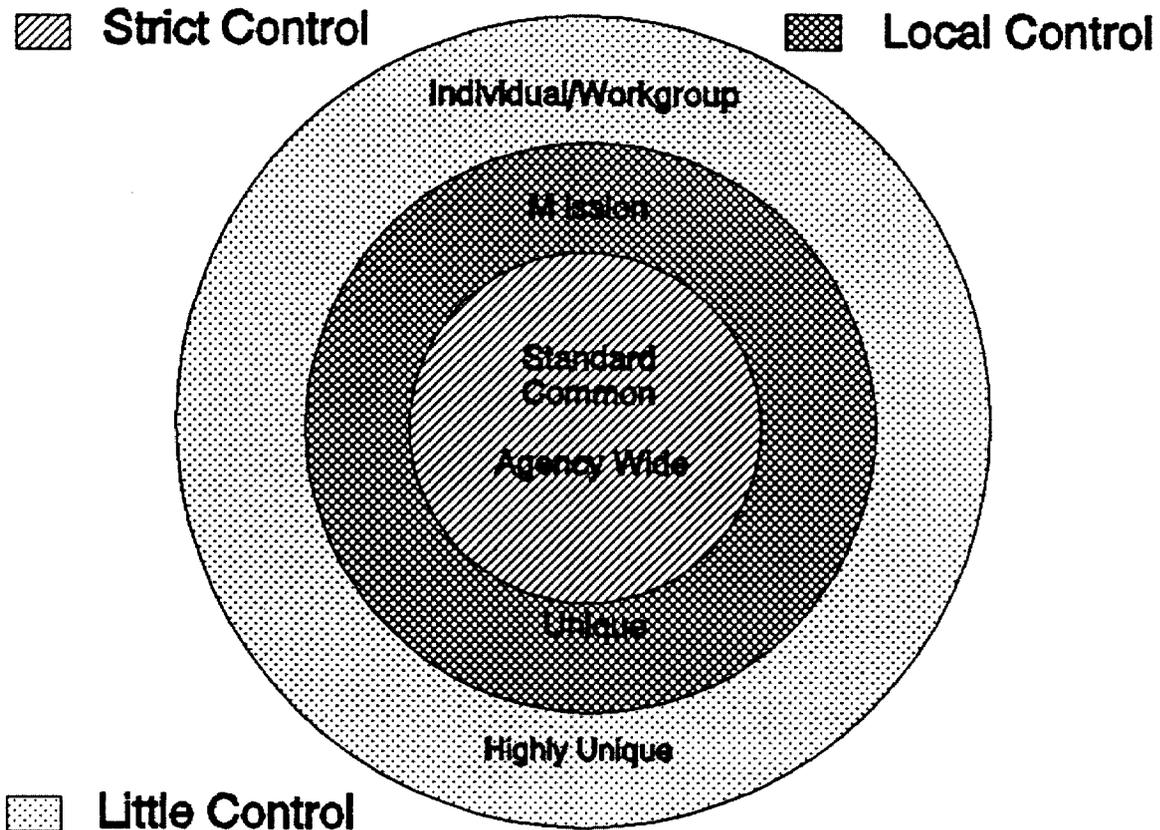


Figure C-3

(a) The inner-most level contains the information and processes that are standard, common, and available across the DISA-IS. This level contains the DISA-IS core resources and is tightly controlled. Management control is exercised by the Chief Information Officer (CIO) (functional requirements/logical architecture) and the Defense Systems Support Organization (DSSO) (technical architecture/operations/products). Examples of software applications or information managed at this level would be the Agency corporate management information, standard electronic mail package, DISA and Department of Defense (DoD) forms, the DISA telephone directory, and most of the office automation applications.

(b) The next level contains mission- or component-unique information and applications. These elements are

characterized by being unique and standard within the mission or component, but not necessarily unique or standard across the Agency. Examples would include the applications and data supporting the management of the Defense Information System Network (DISN) or the World Wide Military Command and Control System (WWMCCS) Incident Reporting System. Control over these elements is distributed to the DISA component assigned operational responsibility.

(c) The outermost level, or ring, of information or process supported by the DISA-IS contains highly unique, non-standard data or processes. Examples include individual databases with non-standard data elements, stand-alone applications, or software tailored for individual use; e.g., wordprocessing macros. These elements are characterized by minimum central control and maximum control by individuals or work groups.

(2) To the degree that any of these level elements are hosted on DISA-IS platforms or implemented as a part of the DISA-IS infrastructure, logical integration and high-level configuration management is exercised by the CIO. Configuration control of the physical DISA-IS infrastructure will reside with the DISA component assigned operational responsibility (e.g. DSSO, Defense Information Technology Services Organization (DITSO), etc.).

3. The aggregation and structure of information about the data and information used by DISA personnel in the accomplishment of Agency goals and objectives is the DISA Repository.

4. The DISANet is the automated information system supporting DISA-IS processes, products, and services used by the DISA personnel in performing their assigned duties and responsibilities. Thus, DISANet provides a backbone for linking DISA's diverse operational activities (both automated and manual). DISANet includes the hardware and software residing on and connected to the LANs and the communications networks linking DISA's locations. The endings of this network are embodied in the premise equipment provided by activities, both internal and external to DISA. The backbone of the network is a combination of leased/dedicated lines connecting LANs installed at DISA locations. The servers and mainframes of the DISANet are part of the physical environment which makes up the network, while the software running on these servers and mainframes provides the intelligence required to perform tasks and store/share data. In addition to the physical network, DISANet also includes applications and services that allow an operational activity to communicate with the network and with other operational activities' equipment and services.

a. The set of common functions and applications (enterprise wide) which are/will be supported by the DISA-IS includes the following:

- o Payroll
- o Electronic Mail
- o Database
- o Project Management
- o Graphics
- o Message Handling
- o Group-ware
- o Workflow
- o Directory Services
- o Translation Services
- o Suspense Tracking
- o Full Text Search
- o Reports Management
- o Acquisition Planning and Tracking
- o Decision-making and Management Support
- o Action Officer Teleconference
- o Time Keeping
- o Word Processing
- o Bulletin Boards
- o Video Teleconferencing
- o Financial Management
- o Calendar/Scheduling
- o Personnel Management
- o Forms Management
- o Library Services
- o Action Coordination
- o Common Shared Space
- o Spreadsheet Access
- o Records Management
- o System and Network Management
- o Dynamic Simulation
- o Document Management
- o External Database Access

b. These common applications and functional areas will expand/change as the DISA-IS evolves over time.

5. Primary management responsibilities for the DISA-IS architecture and infrastructure are assigned to the CIO and the DSSO. As the DISA organization evolves, infrastructure management responsibilities may be also tasked to other operational elements.

a. The CIO identifies, develops, establishes, and proposes Agency priorities for the functional requirements for corporate information systems and data to produce the DISA-IS functional architecture and master plans. In this role, the OCIO implements DISA information management policy as defined in the references and supplements this policy as necessary to meet DISA's mission.

b. The DSSO translates the functional requirements into physical solutions, executing the DISA-IS projects and programs in accordance with DISA-IS Review Board prioritization of requirements and consistent with the DISA-IS functional architecture. The DSSO designs, develops, and implements the technical DISA-IS architecture, selecting standard products and methods which best satisfy functional requirements. The DSSO (and other operational elements, as tasked) operates, manages, and maintains the physical DISA-IS. Within established policies and procedures, the CIO provides management oversight for accomplishing these functions.

6. Other DISA organizations provide collateral support to the DISA-IS in accordance with their primary mission areas of responsibility (e.g. the Joint Interoperability and Engineering Organization (JIEO) provides engineering support, the Defense Network Systems Organization (DNSO) provides communications and video teleconferencing expertise, the DISA Center for Information Management (CIM) provides DoD Corporate Information Management guidance and assistance, Defense Information Technology Procurement Organization (DITPRO) provides procurement support, DITSO provides operations, software development and maintenance support, and develops acquisition requirements and documentation for the Defense Information Infrastructure (DII)). As DISA evolves under DMRD, other DoD organizational elements will realign to DISA and may also provide technical support to the DISA-IS as DSSO does.

D. APPLICABILITY AND SCOPE:

1. This policy applies to all DISA activities/components and addresses the collection, creation, use, dissemination, disposition, and transport of data and information regardless of medium or intended use.

2. This policy will guide:

a. The design, development, test, implementation, operation, and maintenance of an Agency-wide information system infrastructure, providing standard services, applications, and consistent, user-friendly interfaces to authorized users worldwide.

b. The definition, development, and acquisition of common standard applications and services for the DISA-IS.

c. The acquisition of applications and services supporting DISA administrative and mission-support requirements.

d. The life-cycle review and management of all DISA Information Management Systems: mission, mission support, and administrative.

e. The corporate oversight of all information management programs within DISA.

E. POLICY:

1. The underlying principle for management of the DISA-IS is that information will be treated as a critical resource within DISA. Additionally, the "Principles of Information Management," outlined in Reference a, and attached as Attachment 2 to this enclosure, will be used as basic guidelines in the evolution of the DISA-IS.

2. The DISA-IS will be centrally managed, utilizing standards-based methodology in which the CIO will establish standard services, applications, and interfaces for the DISA-IS. DSSO establishes standard products for use on the DISA-IS infrastructure as well as designs, develops, acquires, operates, maintains, and manages the DISA-IS physical/technical infrastructure. This complies with legislative, Office of Management and Budget (OMB), General Services Organization (GSA), DoD, and CIM guidance and procedures that management of DISA's information resources and requirements be centralized, with execution and operation of information systems resources distributed. The CIO will follow established infrastructure, application, and data guidelines when establishing internal services, applications, and interfaces.

a. All DISA organizations will adhere to published DISA-IM policies, guidance, and standards.

b. When mission requirements dictate the use of non-standard systems to be interfaced with the DISA-IS infrastructure, DISA organizations will submit requests for waivers, providing full justification to the CIO.

c. DISA organizations will not connect/interface applications residing on systems or equipment to the DISA-IS infrastructure without prior approval of the responsible operations element (e.g., DSSO for the DISANet). If an application resides on a non-standard system, a waiver to the standard is required by the CIO.

d. Only the responsible operations element will connect equipment to the infrastructure; offending equipment will be removed, or the segment of the network to which the offending equipment is connected will be disconnected from the infrastructure.

e. Organizations which become DISA components as a result of DOD reorganizations or other initiatives will initially retain their legacy information systems as long as those systems can be integrated into the DISA-IS (through gateways, etc). However, new DISA organizations, with the assistance of the CIO, DSSO, and other appropriate DISA directorates, will plan and program transition of their legacy systems to the DISA-IS architecture as soon as resources permit.

3. The DISA-IS infrastructure will be centrally funded. The CIO will act as the Agency proponent in the POM process for the specification, justification, and management of the DISA-IS infrastructure funds. Allocated funds will be distributed at the beginning of the fiscal year to DISA organizations responsible for program execution in that fiscal year (e.g. DSSO).

4. DISA-IS systems and components which are not centrally funded as part of the infrastructure (e.g. premise equipment or other end items, such as PCs, printers, etc.) will be managed by the using DISA organization.

a. Premise equipment connected to, or to be converted to the DISA-IS infrastructure, must meet Agency standards and must employ standard applications/products, as published, but will be funded by the using organizations.

b. Premise equipment, applications, services, or tools required by DISA organizations as stand-alone capabilities will be funded by the using organization and must comply with standards established for the DISA-IS infrastructure, unless a waiver has been requested and obtained from the CIO.

c. Acquisition of all premise equipment and information processing resources is subject to IM regulatory legislation - Federal Information Resource Management Regulations (FIRMR) - and OMB/GSA/DoD/CIM guidance. All Federal Information Processing (FIP) requirements and purchase requests must be submitted to and approved by the CIO prior to acquisition and/or implementation, unless blanket procurement authority is delegated by the CIO.

5. The functions of IRM in DISA will be performed consistent with public law and with directives of higher authority. The methods and procedures implemented for IRM will be designed to enhance Agency mission and administrative performance through effective and economic acquisition, processing, and use of information resources and technology. The performance of each IRM function will be consistent with specific DISA policy specified in the DISA publication which implements that function.

6. The CIO will supplement existing guidelines and policy documents for DISA use including, but not limited to, the following:

- o DISA-IS Architecture
- o Requirements Processing
- o DISA-IS O&M Policy
- o Data Administration
- o Database Management Systems
- o AIS Security/Information Systems Security
- o Information Management Programs
- o Life Cycle Management of AISs
- o FIPR Acquisition
- o CIM Principles and Guidelines
- o Business Processes and Activities
- o Administrative Telecommunications Resources
- o Telecommunications and Network Resources
- o Contractor Administration/Access to Sensitive Unclassified Information Systems

Note: Any policy issued by the CIO will be additive and complementary to corporate (enterprise) DoD policy (e.g. in the form of internal DISA implementation policy/guidance).

F. PROCEDURES:

1. Implementation of this policy will set the framework and guiding principles for information systems management within DISA. As required, DISA components will develop operational procedures and subordinate documents to implement this policy under CIO oversight. Copies of implementation documents will be forwarded to the CIO.

2. Waiver processing procedures are as follows:

a. Organizations seeking deviation from this policy and its implementing documents are responsible for documenting their case.

(1) A waiver is requested and obtained from CIO based on a determination that:

(a) The requesting organization's requirement is unique and cannot be satisfied within the policies/standards established for the DISA-IS; and

(b) The acquisition would be cost-effective and would not adversely affect the cost-effectiveness of the DISA-IS.

(2) The justification for a waiver must address the special need that merits exception. At a minimum, the waiver request must provide a comprehensive, and comprehensible, description of the unique technical, functional, or performance requirements that justify the deviation.

b. Waiver requests shall be sent to the Office of the Chief Information Officer, ATTN: IR. Decisions by the CIO will be made on a case-by-case basis. The CIO will respond to requesting organizations within 20 working days.

G. RESPONSIBILITIES:

1. CIO: The CIO shall have the following responsibilities:

a. Serve as the DISA Senior IM Representative.

b. Implement and supplement, as necessary, higher level IM policies, procedures, and guidance within DISA.

c. Develop and establish corporate IS and data policies, procedures, and standards as guidance for corporate implementation.

d. Identify, develop, establish, and propose priorities for the functional requirements for DISA internal information processing (e.g., DISA information systems) and data. Insure the maximum possible level of functional user involvement in the defining of requirements through state-of-the-art modeling techniques, predominant user representation in decision making groups, and user review of requirements.

e. Produce the DISA-IS functional architecture and master plans.

f. Provide the secretariat function to the DIS/NCS Steering Group when it is meeting as the DISA-IS Review Board, which approves priorities set for the DISA-IS.

g. Exercise logical integration and high-level configuration management over the components of the DISA-IS.

h. Chair the Information Systems Working Group (ISWG) as an internal information systems and requirements working group to provide an Agency-wide forum for DISA information systems.

i. Analyze user requirements, Agency needs, and the availability of technology to develop, maintain, and integrate the logical architecture for the DISA-IS.

j. Act as the advocate in the Program Objective Memorandum (POM) process to budget funding for DISA-IS requirements; plan for and control the financial resources for DISA's internal information activities (DISA-IS), except for premise equipment and organization-specific functional management information systems requirements, in the CIO Future Years Corporate Plan (FYCP); and transfer control of funding to DSSO and other operational components at the beginning of the execution year.

k. Provide oversight management for all information system security aspects of the DISA-IS.

(1) Serve as the Designated Approving Authority (DAA) for the DISA-IS.

(2) Develop and establish DISA-IS security policies, procedures, and standards.

l. Serve as the DISA Data Administrator under the DoD Data Administrator (DA) program, establish and oversee a DISA DA program, develop DISA DA policies, and delegate operational

implementation/execution responsibilities to appropriate DISA elements. Specifically:

- (1) Prepare a Data Management Plan for DISA in accordance with DoD 8020.1-M.
- (2) Coordinate the DISA Data Model with the DoD Data Administration Program Management Office.
- (3) Follow the Integrated Computer Aided Software Engineering (ICASE) Usage Policy Memo, Office of Director of Defense Information (ODDI), February 1992.
- (4) Manage the DISA Repository as the Agency's Data Administrator.

m. As the DISA Senior IM Representative, maintain accountability for acquisitions conducted under the authority of the Brooks Act, including compliance with applicable IRM policies and regulations.

- (1) Develop and manage the FIRMR acquisition review process.
- (2) Delegate acquisition authority within the Agency.
- (3) Coordinate with GSA for Delegations of Procurement Authority and FIRMR approvals.
- (4) Coordinate with appropriate oversight agencies.
- (5) Ensure compliance with DISA-wide objectives and policies.
- (6) Review and approve agency Federal Information Processing Resources (FIPR) procurement requests.

n. Coordinate Automated Data Processing Resources management with the Defense Automation Resources Information Center (DARIC) in accordance with DoDD 7950.1

o. Coordinate the Technical Data Management Program and the Scientific and Technical Information Program (STIP) to ensure effective documentation of contract requirements and to eliminate duplicative work.

p. Develop, implement, and operate the DISA Forms and Reports Management Programs.

2. DSSO: The DSSO shall have the following responsibilities:

a. Design, develop, implement and maintain software as well as developing implementation plans and operational procedures for the day-to-day operation of DISA information systems.

b. Design, develop, acquire, operate, maintain, and manage the DISA-IS physical/technical infrastructure.

c. Acquire, or coordinate on the acquisition of, information management resources required to support individual component requirements; e.g. premise equipment.

d. Comply with DISA architecture guidance for IM systems and "Reuse, Refurbishment, and Replacement" guidelines.

e. Exercise integration and configuration management over the physical elements of the DISA-IS through the DSSO Configuration Control Board.

f. Operate a laboratory/testbed to identify products meeting functional requirements of the functional architecture and validate that they are compliant with standards and will operate on the DISANet without adverse impact on the net.

g. Evaluate and select products to meet functional requirements identified by the CIO.

h. Program and budget for resources required to operate and maintain the DISANet.

i. Develop and maintain a current technical architecture for the DISANet DISA-IS.

j. Establish and chair a DISANet Technical Configuration Management Board.

3. DNSO: The DNSO shall have the following responsibilities:

a. Provide electronic transport connectivity in accordance with approved DISA information system requirements.

b. Provide administrative voice capabilities to support DISA information resource management requirements.

c. Provide visual information (e.g., teleconferencing) support for the DISA-IS.

4. DITPRO: The DITPRO shall act as the procurement agent for the DISA-IS.

5. JIEO: The JIEO shall have the following responsibilities:

- a. Provide the head engineer for the DISA-IS.
- b. Provide engineering support to design, develop, implement, and test the DISA-IS.
- c. Review DISA-IS plans to ensure that DISA information systems plan for and accommodate access/interfaces with appropriate DoD mission/business systems.
- d. Review DISA-IS plans to ensure compliance with open systems architectures and standards.
- e. Develop, specify, certify, and enforce engineering standards required for the DISA-IS.
- f. Through the Defense Information Systems Security Program (DISSP) office, review the DISA AIS security program for compliance with DoD AIS security policies.

6. CIM: The CIM shall have the following responsibilities:

- a. Review DISA-IS plans for compliance with DoD data architecture and data administration guidance.
- b. Review DISA-IS plans for compliance with DoD software application architecture guidance.
- c. Review DISA-IS plans for compliance with DoD technical infrastructure architectural and acquisition guidance.
- d. Provide technical support as required to implement the DISA-IS.

7. DITSO: The DITSO shall have the following responsibilities:

- a. Operate and maintain any assigned elements of the DISA-IS.
- b. Provide training and operations enabling services for any assigned segments of the DISA-IS.

8. CAS: The Center for Agency Services (CAS) shall:

- a. Direct records, correspondence, libraries, publications management, mail management, reprographics, and micrographics operations in accordance with IRM policy and other higher echelon guidance, policy, and procedures.

b. As the DISA Property Management Officer (PMO):

(1) Maintain a central data base of all DISA property to include FIPR. The data base will contain a set of property accounting records that show, on a continuing basis, the item identification, gains and losses, on-hand balance, condition, and location of all property assigned to the property account.

(2) Serve as the Agency focal point to source office/premise equipment (such as PC's, printers, etc.) when needed on a temporary basis to support high priority requirements. Develop and publish a strategy for providing these services with assistance, as necessary, from the CIO (funding support/advocacy) and DSSO (technical support).

9. As users of DISA information systems, all DISA organizations are responsible for:

a. Participation in the definition, prioritization, review, and advocacy of DISA-IS infrastructure (centrally funded) requirements, including formal review and coordination of those which support their functional needs.

b. Identification, prioritization, and funding of information system premise equipment requirements.

c. Identification, prioritization, and funding of organization-specific functional information systems requirements, development, and implementation.

d. Compliance with policies, standards, and guidelines as set forth in this document.

H. EFFECTIVE DATE

This policy is effective immediately.

DEFINITIONS

AIS SECURITY / INFORMATION SYSTEMS SECURITY - Measures and controls that safeguard or protect an AIS against unauthorized (accidental or intentional) disclosure, modification, or destruction of AIs and data, and denial of service. AIS Security includes consideration of all hardware and/or software functions, characteristics, and/or features; operational procedures, accountability procedures, and access controls at the central computer facility, remote computer and terminal facilities; management constraints; physical structures and devices; personnel and communication controls needed to provide an acceptable level of risk for the AIS and for the data contained in the AIS (DISAI 630-230-19).

DATA ADMINISTRATION - The activity that assures the cost-effective availability of data to support the cost-effective operation of functions (DoD 8320.1M).

DATA REPOSITORY - A specialized type of database containing information about data, such as meaning, relationships to other data, origin, usage, and format, and including all the important information resources needed by an organization (DoD 8320.1M).

FEDERAL INFORMATION PROCESSING (FIP) RESOURCES - Automatic data processing equipment (ADPE) as defined in Public Law 99-500 (40 U.S.C. 759(a)(2) and set out in paragraphs (a) and (b) of this definition.

(a) 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--

(1) by a Federal agency, or

(2) under a contract with a Federal agency which-

(i) requires the use of such equipment, or

(ii) requires the performance of a service or the furnishing of a product which is performed or produced making significant use of such equipment.

(b) Such term includes--

(1) computers;

(2) ancillary equipment;

- (3) software, firmware, and similar procedures;
- (4) services, including support services; and
- (5) related resources as defined by regulations issued by the Administrator for General Services.

(c) The term, FIP resources, includes FIP equipment, software, services, support services, maintenance, related supplies, and systems (specific examples of what the term FIP resources includes and excludes are provided in FIRMR Bulletin A-1). These terms are limited by paragraphs (a) and (b) of the definition of FIP resources and are defined as follows:

(d) FIP equipment means any equipment or interconnected system or subsystems of equipment used in the automatic acquisition, storage, manipulation, management, control, display, switching, interchange, transmission, or reception of data or information.

(e) FIP maintenance means those examination, testing, repair, or part replacement functions performed on FIP equipment or software.

(f) FIP related supplies means any consumable item designed specifically for use with FIP equipment, software, services, or support services.

(g) FIP services means any service other than FIP support services, performed or furnished by using FIP equipment or software.

(h) FIP software means any software, including firmware, specifically designed to make use of and extend the capabilities of FIP equipment.

(i) FIP support services means any commercial nonpersonal, including FIP maintenance, used in support of FIP equipment, software, or services.

(j) FIP system means any organized combination of FIP equipment, software, services, support services, or related supplies. (Federal Information Resources Management Regulation (Amendment 1, October 1990))

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 Principle Staff Assistants to produce and control the use of data and information

Principles of Information Management

A. Principles of Information Management DoD 8000.1:

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 controlled costs of developing and operating their ISS.
7. The ISS shall be developed and enhanced according to 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 the system shall be friendly and consistent.

B. Additional DISA-IS Principles of Information Management:

1. The DISA-IS must be a standards-based, open systems architecture.

2. The DISA-IS must plan for and accommodate information and users at different levels of classification and sensitivity and need to know.

3. The DISA-IS should enhance interoperability development.

4. As much as possible, the system development should rely on common databases that similar applications draw on.

5. The DISA-IS should be a model information system that supports all common aspects of the DISA mission and is designed and developed using the DISA engineering process.

in functional activities; information resources management; and supporting information technology and information services (DoDD 8000.1).

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 (DoDD 8000.1).

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 (DoDD 8000.1).

INFORMATION SYSTEM (IS) - The organized collection, processing, transmission, and dissemination of information, in accordance with defined procedures, whether automated or manual (DoDD 5200.28).

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).

LIFE CYCLE MANAGEMENT (LCM) - A management process which is applied throughout the life of an automated information system (AIS). It bases all programmatic decisions on the anticipated mission-related and economic benefits derived over the life of the AIS (DoDI 7920.1).

REPOSITORY - A database of knowledge about an enterprise, it's goals, entities, records, organizational units, functions, processes, procedures, and application and information engineering. (A dictionary contains names and descriptions of data items, processes, data-handling facilities, etc.) A repository contains: (a) complete coded representations of plans, models, and designs with tools for cross-checking, correlation analysis, and validation and (b) many rules relating to knowledge stored and how to employ rule processing (the artificial intelligence technique) to help achieve accuracy, integrity, and completeness of the plans, models, and designs. Thus, it is a knowledge base that not only stores development information but also helps to control its accuracy and validity (DoD 8320.1M)

SENIOR INFORMATION MANAGEMENT REPRESENTATIVE - That designated individual assigned responsibility for the implementation and management of the agency Information Management Program in accordance with DoDD 8000.1.