

PART I  
INFORMATION RESOURCES  
MANAGEMENT  
POLICY DIRECTIVE

INFORMATION RESOURCES MANAGEMENT POLICY DIRECTIVE

Left blank intentionally

## **Part I Policy Contents**

### **Overview**

### **General Policy**

### **Responsibilities**

Chief Information Officer (CIO)  
FEMA Information Resources Board (IRB)  
FEMA Procurement Review Board (PRB)  
Associate Directors, Executive Associate Directors, Administrators, Regional Directors,  
and Office Directors  
Director, Management Division, IT-MA  
Director, Acquisition Support Division, FM-AS  
Director, Program Services Division, OS-PS  
Office of General Counsel (OGC)

### **Chapter 1 Information Systems Planning, Budgeting and Development**

- [1-1](#) Information Technology Planning Process
- [1-2](#) Report on Major IT Systems Budgets
- [1-3](#) Life-Cycle Management (LCM)
- [1-4](#) FEMA Documentation Requirements

### **Chapter 2 Management and Use of Information**

- [2-1](#) Information Collections
- [2-2](#) Access to Information Technology for Individuals with Disabilities
- [2-3](#) Records Maintenance and Electronic Recordkeeping

### **Chapter 3 Management and Use of Information Systems and Services**

- [3-1](#) Agencywide FEMA systems
- [3-2](#) Telecommunications Systems and Services
- [3-3](#) Voice Information Processing Systems (Voice Mail)
- [3-4](#) National Security/Emergency Preparedness Program
- [3-5](#) Telecommunications Networks and Network Management
- [3-6](#) Local Area Networks and Network Management
- [3-7](#) Automated Data Processing Systems and Services
- [3-8](#) Internet and Intranet
- [3-9](#) Electronic Mail
- [3-10](#) Electronic Data Interchange
- [3-11](#) Disposition of Obsolete Hardware and Software
- [3-12](#) Telecommuting

**Chapter 4 Information Systems Safeguards**

- [4-1](#) Information Systems Safeguards
- [4-2](#) System User Security Requirements
- [4-3](#) General Support Systems Safeguards
- [4-4](#) Application Systems Life-Cycle Security Requirements

**Chapter 5 Information Systems Standards**

- [5-1](#) Standardization Programs
- [5-2](#) Office Automation Software Standards
- [5-3](#) Application Software Standards
- [5-4](#) Office Automation Hardware Standards
- [5-5](#) Hardware Standards for Servers and Central Processors
- [5-6](#) Geographical Information Systems (GIS) Standards

## Overview

1. This document prescribes the policy for management of information resources within the Federal Emergency Management Agency (FEMA), and assigns responsibility for its implementation.
2. This document establishes the Information Resources Management (IRM) Program which supports FEMA's mission by promoting a vision for information resources by encouraging users to think on a broad scale of the relationships among their systems and the organization, and by managing information resources as an integrated process. The FEMA IRM Program constitutes the cornerstone and provides a single source for policies and management oversight.
3. The provisions of this document are applicable to all FEMA organizational elements in the headquarters, regions, and field establishments. This guidance includes all current and planned acquisitions, uses, and dispositions of information resources, regardless of source, in support of FEMA's mission critical systems.

## General Policy

It is FEMA's policy to establish an Information Resources Management (IRM) Program that uses information and information technology (IT) as a strategic resource for achieving the mission of the Agency. FEMA shall plan, manage and utilize information and IT to ensure information needs of our customers are met; IT resources are focused on providing the services needed to accomplish FEMA's goals and priorities; funding for individual IT program objectives are commensurate with the value delivered to the Agency in meeting those objectives; funding is provided to mission critical IT programs; and coherent, cohesive planning is performed to meet future Agency needs. The objectives of the IRM Program are designed to support FEMA's organizational elements and customers by providing them effective and high-quality information resources. The major policies governing implementation of the FEMA IRM Program are described in the chapters herein.

## Responsibilities

1. FEMA's Associate Director for Information Technology Services serves as the Agency's Chief Information Officer (CIO) and reports directly to the Director of FEMA. The CIO is responsible for carrying out the Agency's information resources management functions, for overseeing Agency compliance with applicable Federal regulations and legislative requirements, and for accrediting information systems under the Computer Security Act. The CIO provides leadership in improving the management of information systems within the Agency and is responsible for centralized day-to-day operations of the FEMA Information Resources Management Program. In addition, the CIO serves as official liaison between the Agency and any external organization regarding information resources management. The CIO is also responsible for providing guidance to the emergency management community for use of information technology.

## INFORMATION RESOURCES MANAGEMENT POLICY DIRECTIVE

2. The FEMA Information Resources Board shall provide broad, high-level recommendations to the CIO for management of information systems consistent with the mission of the Agency, as prescribed in FEMA Instruction 1610.13, Information Resources Board.
3. The FEMA Procurement Review Board shall approve or disapprove planned acquisitions of information systems as prescribed in FEMA Instruction 1610.5, Procurement Review Board/Procurement Planning System.
4. Associate Directors, Administrators, Regional Directors, and Office Directors are responsible for:
  - Appointing and supporting participation of senior staff members in the work of the Information Resources Board and the Procurement Review Board;
  - Appointing staff to serve as IRM representatives and the organizational element's points of contact for IRM activities;
  - Preparing and submitting information requirements and budget justifications in the organizational element's information systems plan;
  - Preparing and submitting requests for procurement of information systems to the CIO for review;
  - Operating and maintaining information systems in conformance with Federal guidelines;
  - Assisting in the formal reviews of information systems activities; and
  - Reporting actual and planned expenditures for information systems.

[The following are applicable to the Regions]

- Appointing and supporting Regional Information Systems Manager (Communications Officer/Local Ordering Official/Telephone Administrative Officer), and
  - Ensuring that the following functions are carried out:
    - Freedom of Information
    - Information Systems Security
    - System Administration
    - Management of Office Automation and Services
5. The Director, Management Division ITS, is responsible for:
    - Developing and promulgating policies, procedures, standards, and technical guidance for the acquisition, management, and use of information systems.
    - Directing the information systems planning, computer security programs, and the life-cycle process for information systems.
    - Implementing information systems standards conforming with Federal policy, law, and regulations.

## INFORMATION RESOURCES MANAGEMENT POLICY DIRECTIVE

- Performing technical guidance with the customers for information systems requirements analysis, and for information systems acquisition plans and requests.
  - Monitoring agencywide adherence to information systems security policy and guidance.
  - Reviewing internal and external IRM documents for conformance with established policies, procedures, and guidance.
  - Overseeing FEMA's catalogue of information systems.
  - Consolidating Agency reporting on information systems to meet requirements established by OMB, General Accounting Office, and other requesters.
6. Director, Acquisition Services Division, FM, is responsible for providing agencywide procurement support services in accordance with FEMA's acquisition management program, OMB, and the Federal Acquisition Regulation.
  7. Director, Program Services Division, OS, is responsible for records management, which includes the creation, maintenance, and use of official records, and for collection and dissemination of information resources in accordance with FEMA's Information Collection Management Program and the Federal Property Management Regulation.
  8. The Office of General Counsel is responsible for compliance of information systems with the Freedom of Information Act, the Computer Matching and Privacy Protection Act of 1988, and the Computer Matching and Privacy Protection Amendments of 1990.

INFORMATION RESOURCES MANAGEMENT POLICY DIRECTIVE

Left blank intentionally

## Chapter 1 Information Systems Planning, Budgeting and Development

1-1 Information Technology Planning Process. FEMA shall establish and maintain a 5-year strategic planning process for acquiring and operating information systems to meet program and mission needs, as prescribed in the Paperwork Reduction Act, the Information Technology Management and Reform Act (ITMRA) and OMB Circular A-130. The IT Planning Process includes four related planning documents which build upon each other to produce the foundation of an operational capability from which to use technology to meet mission needs. These plans are as follows:

- The Strategic IRM Plan, a 5-to 10-year, high-level plan that identifies strategies to use information technology in order to better meet the goals and priorities of the Agency's Strategic Plan;
- The Information Plan, a 5-to-10 year requirements plan that identifies the types of information needed by the Agency and emergency management community to perform their missions; and identifies information needs of Congress, the White House and the public;
- The Management and Technical Architecture, a 5-to-10 year plan that links the strategic IRM objectives, and the information requirements, technology and standards into a cohesive, integrated architecture which serves as a blue print for IT development; and
- The IT Operations Plan, a 1-to 5-year detailed tactical plan for implementing the objectives of the Strategic IRM Plan, using the Technical Architecture as a guide for development and integration of these systems. The IT Operations Plan must be updated annually and submitted to OMB. It includes an approved means for describing the Agency's requirements, budgets, and plans for information systems for each organizational element. Each information system requirement and accompanying budget initiative shall relate to the mission of the Agency. User requirements must be translated into realistic, cost-effective, and well-coordinated plans that tie together common requirements into a cohesive agencywide plan. FEMA shall ensure that acquisitions of information systems are in accordance with the updated IT Operations Plan.

All other planning documents are updated as requirements or mission changes require. [Refer to Part II, Chapter 1-1, for details.]

1-2 Report on Major IT Systems Budgets. FEMA must report on major information technology systems plans to fulfill the requirements of OMB Circular A-11, and to ensure that Obligations for Information Technology Systems, Exhibits 43 and 300, accompany FEMA's initial budget submission. [Refer to Part II, Chapter 1-2, for details.]

## INFORMATION RESOURCES MANAGEMENT POLICY DIRECTIVE

1-3 Life-Cycle Management (LCM). FEMA shall establish and adhere to the LCM concept, as described in OMB Circular A-130 and in the ITMRA. FEMA shall ensure that the information systems plan, requirements analysis, and request documents are reviewed to determine whether the proposed system duplicates other FEMA information systems, whether the requirements are subject to provisions of the ITMRA. The LCM process must document the requirements that each information system is intended to provide, and ensure agencywide use of LCM concepts to:

- Establish and promote thorough planning at every level of effort, and develop detailed plans that identify and validate FEMA information systems that meet the needs of the user;
- Conduct periodic reviews of the requirements over the life of the information system to determine whether the requirements continue to exist and whether the system continues to meet the purpose for which it was originally acquired;
- Explore alternate system design concepts before developing new systems to ensure effective development and operation at the lowest cost through consideration of alternatives, costs, risks, and impacts;
- Ensure that appropriate requirements for information systems are identified and acquisition strategies are documented early in the development process; and
- Maintain a catalogue repository of information systems to preclude system duplication and to provide for system accountability in accordance with Section 3506(c) of the Paperwork Reduction Act.

[Refer to Part II, Chapter 1-3, for details.]

1-4 FEMA Documentation Requirements. FEMA shall establish and adhere to the standard system development documentation guidelines. [Refer to Part II, Chapter 1-4, for details.]

## Chapter 2 Management and Use of Information

2-1 Information Collections. FEMA shall collect only that information necessary for the proper performance of Agency functions and that has practical utility. The information shall be collected in the most effective, efficient, and economical manner that will not place a disproportionate burden on the respondent. FEMA shall use electronic collection techniques where such techniques reduce burden on the public, increase efficiency of the Agency programs, reduce costs to the Government and the public, and provide better service to the public. FEMA organizations may not conduct or sponsor a collection of information unless the collection of information has been reviewed under the Agency's formal review process and approved by OMB. [Refer to Part II, Chapter 2-1, for details.]

2-2 Access to Information Technology for Individuals with Disabilities. FEMA shall provide for current or prospective employees, and for others with disabilities, equivalent access to electronic office equipment (which includes access to Federal public information resources), to the extent both present and future needs for such access are determined by the Agency. FEMA shall comply with Federal law to ensure that current or prospective employees with disabilities and others with disabilities who use Agency information resources can produce information and data, and have access to information and data, regardless of the type of medium, comparable to the information and data and access, respectively, of individuals without disabilities, to the extent both present and future needs for such access are determined by the Agency. FEMA shall, through the use of adaptive computer and telecommunications devices or equally effective means, remove communication and information barriers that impede access to the Agency's information resources by persons with disabilities to the extent both present and future needs for such access are identified in requirements analyses. [Refer to Part II, Chapter 2-2, for details.]

1. In accordance with Section 711 of The Communications Act, 57 U.S.C. 611, FEMA produced or funded public service video announcements will include closed captioning of the verbal content of the video announcement.
2. All FEMA employees with adaptive technology needs will be provided with tools necessary to have office automation capabilities equivalent to the standard FEMA office automation suite in order to perform their job functions.
3. FEMA will design information technology systems to adhere to the policy:
  - Ensure that people with disabilities can access and use the same data bases and application programs as other people;
  - Ensure that people with disabilities shall be supported in manipulating data and related information resources to attain equivalent end results as other people; and

## INFORMATION RESOURCES MANAGEMENT POLICY DIRECTIVE

- Ensure that when electronic office equipment is part of a telecommunications system, that people with disabilities can transmit and receive messages in a manner that supports their disability related needs and provides the capability to communicate with other users of the system.

2-3 Records Maintenance and Electronic Recordkeeping. It is FEMA's policy to ensure adequate and proper documentation of Agency activities through efficient, economical, and effective controls over the creation, maintenance, disposition, and preservation of all records, including those created by or maintained on electronic media. All records, including electronic mail messages, must be maintained and disposed of in accordance with the Agency's approved records retention schedules. FEMA's Records Management Program provides guidance for the implementation of this policy. [Refer to Part II, Chapter 2-3, for details.]

## Chapter 3 Management and Use of Information Systems and Services

3-1 Agencywide FEMA Systems. All information systems and services that have been deemed mandatory for use within the agency shall be utilized unless waivers are received by the IRB and the CIO. [Refer to Part II, Chapter 3-1, for details.]

3-2 Telecommunications Systems and Services. All telecommunications services shall be authorized and documented in accordance with Federal regulations and standards, including radio frequency (RF) spectrum. Funding for telecommunications services shall be provided by the requesting office.

- Assignment of communications services shall be authorized at the organizational level, and during emergencies at the Federal Coordinating Officer level. FEMA components must coordinate with the Operations Division, Information Technology Services Directorate, any plans for, responses to, or recovery from emergencies involving local connections to FEMA Networks.
- Telephones shall be provided to staff for the conduct of official business. The installation of listening-in circuits, transmitter cutoff switches (switches located in areas of high background noise and in secure areas are exempted), and other devices for recording or listening to telephone conversations at any FEMA activity shall be prohibited.
- Telephone calling cards (credit cards) shall be chargeable to FEMA, and authorized and issued when staff makes official telephone calls while on official travel status or when absent from the office.
- Paging devices and cellular telephones shall be used in connection with emergency activities and in operating situations where an employee must be reachable at all times. Cellular telephones shall be used in situations where normal telephone service is unavailable and in operating situations where an employee must have immediate access to voice communications at all times while away from the office.

[Refer to Part II, Chapter 3-2, for details.]

3-3 Voice Information Processing Systems (Voice Mail) are made available to FEMA employees on a limited basis only through the FEMA Switched Network (FSN). During duty hours, all telephone calls shall be answered by an individual where possible. Voice mail must not be used to screen calls. [Refer to Part II, Chapter 3-3 for details.]

3-4 National Security/Emergency Preparedness Program. Operation of National Security/Emergency Preparedness (NS/EP) program services and systems shall be in accordance with applicable rules, regulations, and procedures promulgated by the Federal Communications Commission and/or the Office of the Manager, National Communications System, as supplemented by FEMA procedures. [Refer to Part II, Chapter 3-4, for details.]

## INFORMATION RESOURCES MANAGEMENT POLICY DIRECTIVE

3-5 Telecommunications Networks and Network Management. The National Network Operations Center (NNOC) shall establish a specialized operations center necessary for the management and operations of FEMA telecommunications networks and network related equipment. [Refer to Part II, Chapter 3-5, for details.]

3-6 Local Area Networks and Network Management. FEMA manages its wide area network (WAN) through the NNOC. Local Area Networks (LANs) shall be managed and administered by individual Offices, Directorates, Administrations and Regions to support office automation, electronic mail and specialized applications. The Information Technology Services Directorate shall provide LAN management and administration for those organizations who so request through the Headquarters Information Technology Service Center. [Refer to Part II, Chapter 3-6, for details.]

3-7 Automated Data Processing Systems and Services. Requests for information systems services, equipment, facilities, or changes to existing services, equipment, and facilities shall be justified, funded, and documented over its life cycle by the requesting organizational elements. Existing and planned information systems shall not duplicate those systems available in FEMA or those systems available in other Federal agencies. Where feasible, optimal use shall be made of commercial-off-the-shelf (COTS) software. [Refer to Part II, Chapter 3-7, for details.]

3-8 Internet and Intranet. Internet and Intranet shall be used within FEMA for the conduct of official Agency business. Any and all uses of Internet/Intranet must be FEMA related. FEMA's Internet implementation shall comply with OMB Circular A-130 requirements for electronic release of information. FEMA shall also adhere to the Agency's guidance on the exchange of information and correspondence with external sources including the general public as described in the FEMA Instructions and Manuals. For example, signature authority for paper correspondence is applicable for signature authority of electronic correspondence. Internet shall be accessible to employees through an Internet Firewall which provides protection of internal FEMA data and programs from "external to FEMA" intrusion. Internet and Intranet applications will be designed for accessibility. In support of the Americans With Disabilities Act of 1990 and other laws and regulations pertaining to access to Americans with disabilities, non-graphical and non-audio alternatives will be available for accessing information from FEMA Internet and Intranet services. All employees will have access to primary functions and services on the Internet and Intranet through the FEMA enterprise-wide network. Staff may be provided enhanced Internet access based upon job functions and access requirements as determined by directorate and office level management. [Refer to Part II, Chapter 3-8, for details.]

## INFORMATION RESOURCES MANAGEMENT POLICY DIRECTIVE

3-9 Electronic Mail. Electronic mail (E-mail) must be used only to conduct Agency business. FEMA reserves the right to look at E-mail on any Agency systems. Government office protocol, etiquette, and ethics must be observed for all E-mail information and correspondence. E-mail correspondence shall be treated in the same manner as paper correspondence that is subject to provisions of the privacy, security, and record retention regulations and the Freedom of Information Act. [Refer to Part II, Chapter 3-9, for details.]

3-10 Electronic Data Interchange. It is FEMA's policy to migrate to a government-wide electronic commerce for acquisition as Federal regulations are developed. [Refer to Part II, Chapter 3-10, for details.]

3-11 Disposition of Obsolete Hardware and Software. FEMA shall provide for the disposition of obsolete office automation equipment, if appropriate, through central points of coordination to ensure adherence to Federal statutory guidance, and FEMA property management guidance. FEMA shall establish guidelines for distribution of outdated or excess office automation equipment through the FEMA Sponsors in Education Program, and in accordance with Section 303 of Public Law 102-245, American Technology Preeminence Act of 1991. [Refer to Part II, Chapter 3-11, for details.]

3-12 Telecommuting. FEMA has implemented a telecommuting program for accommodating temporary requirements of employees and the Agency. Telecommuting programs for individuals and positions must be authorized by the Office of Human Resources Management. Decisions to implement authorized telecommuting programs is the discretion of the manager. [Refer to Part II, Chapter 3-12, for details.]

INFORMATION RESOURCES MANAGEMENT POLICY DIRECTIVE

Left blank intentionally

## Chapter 4 Information Systems Safeguards

4-1 Information Systems Safeguards. The Agency's information systems are valuable assets and, as such, FEMA shall establish and maintain an effective Information Systems Security program in accordance with national authorities and guidelines. FEMA information systems data, which are Federal assets, shall be protected in accordance with the Computer Security Act of 1987. Information systems, facilities, and services shall be used solely for conducting official Government business. Employees must be made aware of what constitutes proper and improper use of FEMA's information systems in accordance with the organizational element's program requirements. Constant vigilance must be maintained to ensure that effective administrative, physical, and technical controls are in place, and to ensure the availability, integrity, and confidentiality of information systems assets. [Refer to Part II, Chapter 4-1, for details.]

4-2 System User Security Requirements. Magnetic media and other types of media used to store software and data at user workstations must be protected. Inadequate protection or improper handling of storage media such as diskettes, tape cassettes, fixed hard disks, and removable hard disks may result in the loss of valuable software or data, or lead to unauthorized disclosure or modification of data. Computer viruses represent a serious computer security problem that can cause a wide variety of disruptive or destructive actions on systems. For instance, viruses may corrupt or totally destroy data residing on storage media or cause computer hardware or software damage. In view of the increasing risk of computer viruses, all FEMA PCs and networked PCs shall be tested for and protected against viral infection. [Refer to Part II, Chapter 4-2, for details.]

4-3 General Support Systems Safeguards. Information security encompasses basic physical protection for resources entrusted to users care. Inadequate physical security may lead to theft, damage, or the destruction of hardware, software, and storage media. Additionally, physical access control vulnerabilities may result in the unauthorized disclosure, modification, or destruction of data resident on the system. [Refer to Part II, Chapter 4-3, for details.]

4-4 Application Systems Life-cycle Security Requirements. This chapter specifies safeguards for major applications systems that are, by definition, high risk. Managers of major applications systems need to devote special attention to security due to the risk and magnitude of harm that could result from the loss, misuse, or unauthorized access to or modification of information in the application. The procedures and controls discussed below present the minimum level of safeguards to be adopted. All systems and applications require some level of security. The information systems safeguards presented in this chapter stress sound management controls. Technical and physical controls support sound management practices by extending the necessary security protection to systems and data. Security safeguards apply to both classified and unclassified information systems. [Refer to Part II, Chapter 4-4, for details.]

INFORMATION RESOURCES MANAGEMENT POLICY DIRECTIVE

Left blank intentionally

## Chapter 5 Information Systems Standards

5-1 Standardization Programs. It is FEMA's policy to require strict application of Federal standards for system interoperability, system access, and system sharing when acquiring new systems or updating existing systems. Standards for information technology systems, such as the Federal Information Processing Standards (FIPS), Federal Telecommunications Standards (FED-STD), and other approved standards shall be enforced as a means of increasing the transportability of the Agency's data and software and providing compatibility and interchangeability of hardware in an open systems environment. [Refer to Part II, Chapter 5, for details.]

All organizational elements of FEMA and contractors performing on behalf of FEMA shall promote the full utilization of the standards.

- Conformance to the standards is required in the acquisition, development, use, management, and operation of Agency systems unless an exception is granted by the IRB.
- To overcome vendor-specific barriers, Open Data Base Connectivity (ODBC) compliant standards must be enforced for all information systems to be procured or developed in-house.
- The designated FEMA preferred relational database management system must be enforced for all information systems developments.
- Site (enterprise) licenses for the desktop baseline software in sufficient quantity for all FEMA employees shall be contracted and centrally maintained.
  - Support services, including problem resolution, repairs and integration will be provided only for those specifically identified as standard in Part II, Chapter 5.
  - Compliance with the Federal Information Processing Standards (FIPS), the Federal Standard (FED-STD), and the standards established herein is required.

5-2 Office Automation Software Standards. All FEMA mission critical information technology systems were made Year 2000 compliant by March 31, 1999. All other FEMA information technology systems are required to be Year 2000 compliant by December 31, 1999. The managers of all FEMA information technology systems will maintain the systems' Year 2000 compliance.

5-3 Application Software Standards. All information technology systems must comply with application software standards. Waivers must be requested through the CIO staff.

## INFORMATION RESOURCES MANAGEMENT POLICY DIRECTIVE

5-4 Office Automation Hardware Standards. All information technology systems must comply with office automation hardware standards. Waivers must be requested through the CIO staff.

5-5 Hardware Standards for Servers and Central Processors. All information technology systems must comply with the hardware standards for servers and central processors. Waivers must be requested through the CIO staff.

5-6 Geographical Information Systems Standards (GIS). All information technology systems must comply with the GIS standards. Waivers must be requested through the CIO staff.