Federal Emergency Management Agency

Information Resources Management Policy and Procedural Directive

FIRMPD

Electronic Version
December 29, 1999

Left blank intentionally

FOREWORD

The FEMA Information Resources Management (IRM) Policy and Procedural Directive (FIRMPD) provides, in a single source, the policies, responsibilities, authorities, and procedural guidance to plan, acquire, manage, and dispose of information systems.

This document is structured in two parts: Part I contains statements of policy for integration of agencywide information and information systems, and assigns responsibility for those policies. Part II contains the procedures and guidance for implementation of the policies identified in Part I.

Within Part II, chapters identify the main divisions of guidance associated with the policies, and the chapter title is shown at the top of each page. The main division of guidance may be subdivided to provide detailed information.

The FIRMPD is available by subchapter and title on FEMA's Email Bulletin Board under the CIO Bulletin Board. The appendices section of this document are identified by the chapter name and number, and the page sequence is identified by lower case alpha characters.

The top of each page identifies the policy or procedural division. The bottom of each page identifies the document, the organizational element responsible for its maintenance, the date, and the subchapter number followed by the page number. (Example: Part II, Subchapter 1-1.1, 1-1.2, 1-1..., 2-1.1, 3-1.1 through 3-1.4, etc.)

This document supersedes FEMA Instruction 1500.1, Management of Information Resources, dated May 9, 1995. The entire 1500 instruction series is revised and canceled by chapters of this document. On the reverse page of the Foreword, the canceled instructions and manuals are cross-referenced to the chapters of the FIRMPD. New or update chapters will be issued in their entirety and will be annotated and dated to reflect the change.

The Information Technology Services Directorate, Management Division, Policy and Requirements Branch (IT-MA-PR) acknowledges the contributions of all FEMA directorates, offices, and administrations that participated in the preparation of this document.

Suggestions can be forwarded, on the suggestion page included in this document, to IT-MA-PR, Room 252, or via E-mail on the CIO Bulletin Board.

Existing Instructions		New Policy & Procedural Directive
		Part I IRM Policy Directive
1500.1	**Mgmt of Information Resources**	**Chapters 1-5**
		Part II IRM Procedural Directive
1200.4	**Comm Security Policy**	**Chap 4-1 Info Sys Safeguards**
1200.5	**Safeguard & Contl of Comm Sec Material/Info**	**Chap 4-1 Info Sys Safeguards**
1500.2	**Information Systems Planning Program**	**Canceled**
1500.3	**Information Systems Policy**	**Chap 1-1 Strategic Planning**
1501.1	**ADP Documentation Standards (M)**	**Chap 5 Info Sys Standards**
1501.2	**Guidelns for Docmnt of Comp Prog (M)**	**Canceled**
1510.2	**Req for Access to Auto Info Sys**	**Chap 2-2 Access to IT for Ind w Disab**
1520.3	**Comp Inrct Displ, Entry & Rtrv Sys (M)**	**Canceled**
1520.4	**Radiological Def Monitor Station & Instru Inv PC Mgr Sys (M)**	**Canceled**
1520.5	**Radioactive Mat PC Mgr Sys (M)**	**Canceled**
1520.6	**Dams Inv Sys Retrieval Prog (M)**	**Canceled**
1520.7	**Gantt Chart Comp Term Users (M)**	**Canceled**
1520.8	**Mgmnt of Alerting Pagers & Beepers**	**Chap 3-1-4 Paging Devices & Cell Telepns**
1520.9	**Nat Fac Srv/Recp & Cr PC Mgr Sys (M)**	**Canceled**
1520.10	**Radiological Def Prog PC Mgr Sys (M)**	**Canceled**
1520.11	**Emergency Broadcast Sys (EBS) (M)**	**Chap 3-1 Communications Services**
1540.1	**Info Sys Security Policy**	**Chap 4-1 Information Sys Safeguards**
1540.2	**Automated IS (M)**	**Chap 5 Ofc Automation Sys and Serv**
1540.3	**Sec for FEMA Micros & WPs (M)**	**Chap 4-1 Information Sys Safeguards**
1550.1	**Telecomm Svc**	**Chap 3-1 Communications Services**
1550.3	**Sec Policy for Secure Telephone Unit III**	**Chap 2-3 Information Sys Safeguards**
1550.4	**Frequency Spectrum Mgt**	**Chap 3-1 Communications Services**
1550.5	**Comm Security Monitoring**	**Chap 4-1 Information Sys Safeguards**

PART I

INFORMATION RESOURCES MANAGEMENT POLICY DIRECTIVE

Left blank intentionally

Part I
Policy Contents

Chapter 4 Information Systems Safeguards

Chapter 5 Information Systems 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.

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.

- 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.

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.]

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

- 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.]

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.]

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.]

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.]

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.

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.

PART II

INFORMATION RESOURCES MANAGEMENT PROCEDURAL DIRECTIVE

Left blank intentionally

Part II
Procedural Contents

Appendices

Chapter 1

Information Systems Planning, Budgeting and Development

Left blank intentionally

1-1 Information Technology Planning Process

Overview

1. This chapter implements the procedures for the Federal Emergency Management Agency's (FEMA's) management of planning for strategic information resources management.

2. The purpose of the FEMA planning process is to ensure information technology (IT) resources are focused on providing the services needed to accomplish FEMA's goals and priorities; funding for individual program objectives is commensurate with the value delivered to the Agency in meeting those objectives; funding is provided to mission critical programs; and coherent, cohesive planning is performed to meet future Agency needs.

3. In addition to the responsibilities identified in Part I of the FIRMPD, the responsibilities below apply for information resource management planning.

Responsibility

1. The Information Resources Board (IRB) is responsible for reviewing and approving IT plans, standards, proposed IT projects, and policies. The IRB is responsible for the development of the IRM plans.

2. The Chief Information Officer (CIO) is responsible for ensuring that the regulatory requirements mandated in the Information Technology Management Reform Act of 1996 (ITMRA) and the Paper Work Reduction Act of 1995 (PRA) are supported by the planning processes identified in the Office of Management and Budget (OMB) Circular No. A-130. These planning processes include the creation and implementation of the Strategic IRM Plan, the Information Plan, the Management and Technical Architecture Framework, and the IT Operations Plan.

3. Associate Directors, Administrators, Regional Directors, and Office Directors are responsible for:

   - Providing representation to the IRB and the Information Systems Policy Advisory Group (ISPAG). These groups provide recommendations for the development of policies, standards, and architectures of the Agency. The ISPAG provides representation for the development of the IT Operations Plan.

   - Providing the IRB with information on major IT program plans and requirements.

   - Ensuring that the IT Operations Plan and Catalogue of FEMA Information Systems properly represent program plans and budget requirements for IT systems.

4. All FEMA employees will have access to these plans. It is the responsibility of all FEMA employees to ensure that their efforts are in concert with these plans.

Strategic Information Resources Management

1. The Strategic Information Resources Management section of OMB Circular A-130 identifies four planning documents which build upon each other to meet the full range of IRM planning needs for an agency. The Strategic IRM Plan, the Information Plan, the Management and Technical Architecture Framework and the IT Operations Plan are summarized below.

2. **The Strategic IRM Plan** reflects and supports the mission, goals, and objectives of the FEMA Strategic Plan, and has a 5- to 10-year focus. The Strategic IRM Plan addresses how management of IT meets the Agency mission; reflects and anticipates changes in the Agency's mission, policy direction, technological capabilities and resource levels; and describes the parameters of the Technical Framework. It will be updated to reflect changes in mission or other significant event. Included in the Strategic IRM Plan are: FEMA's IRM Mission, FEMA's IRM Vision, Strategic IRM Goals, and Strategic IRM Objectives.

3. **The Information Plan** analyzes the information needs of the Agency. The purpose of an Information Plan is to promote efficient use of information to maximize usefulness; minimize the information collection burden on the public; preserve integrity, availability and confidentiality of information; and, support the Information Collection Budget. This is updated to reflect changes in customer requirements, mission or other significant event. Included in the Information Plan are: Identification of Users of FEMA Information, Identification of Information Collection vehicles, Identification of Information Sources and Information Requirements.

4. **Management and Technical Architectures/Frameworks** drive operational planning and describe how the Agency intends to use information and information technology. The technical framework serves as a reference for updates to new and existing information systems. The management framework assures the integration of proposed IT projects into the technical framework in a manner that will ensure progress towards achieving an open systems environment. Management and technical frameworks provide strategies to move toward an open systems environment. These strategies consist of profiles based on the NIST Application Portability Profile in order to satisfy user requirements; accommodate agency standards; promote interoperability; and provide application portability and scalability by defining interfaces, services, protocols, and data formats. Included in the technical architecture are: IT standards, interoperability requirements, target technology, services, protocols, and data formats.

5. **The Information Technology Operations Plan** is a 1- to 5-year plan which includes:

    - list of existing and planned information systems;
    - list of planned information technology acquisitions;
    - how these systems relate to each other and the Agency mission; and
    - summary of computer security planning.

The IT Operations Plan links information technology to program and mission needs, reflects budget constraints, and forms the basis for budget requests. The IT Operations Plan serves as a mechanism for communicating to the public how the Agency's IT applications may affect them, including the vendor community, which may be interested in providing services to the Agency. Procurement information is not to be considered acquisition sensitive. The Plan identifies initiatives to reduce the information collection burden to the public, while making the public's dealing with the Government as "user-friendly" as possible. The IT Operations Plan is required to be updated and submitted annually to OMB.

Included in the IT Operations Plan are: Planned systems and upgrades; short descriptions of each system requirement and mission criticality; list of existing systems (Catalogue of Information Systems); planned budgets, including contractor support, services, operation and maintenance expenses; FEMA personnel support requirements; performance measures and implementation schedules.

Procedures

1. Program offices are responsible for identifying work processes which could be improved by creative uses of IT and that would enable the emergency management community to meet FEMA's strategic objectives. FEMA's external customers work with program offices or designated liaison officers to identify customer needs. The program office may perform a requirements analysis utilizing their own resources, or request assistance for this analysis from the Information Technology Services Directorate (ITS). ITS is available for consultation to provide consistency across the Agency. This analysis should determine whether other FEMA elements will be impacted by this effort or if information from existing FEMA systems is needed to perform the work process.

2. Once it is determined that a mission-critical process can be improved by use of IT, an analysis of alternatives is performed by the program office to determine if existing FEMA systems can support the requirement, or if a new system must be procured. The program office can make use of the Catalogue of FEMA Information Systems or ITS staff to determine if existing FEMA IT systems will meet their needs. The planned system is identified by the program office to the representative to the ISPAG for inclusion in the FEMA IT Operations Plan, which serves as a vehicle to provide input to the FEMA budget process.

3. If a new system must be developed to meet the requirement, the contract value, mission criticality, and funding availability determine the level of reviews and authorities needed to complete the implementation. Any system that will have a significant impact on other FEMA systems must be reviewed so that a determination can be made on whether the planned application is consistent with the FEMA IT architecture and whether the existing infrastructure can support the new application. Systems that are cross cutting must be presented to the Information Resources Board (IRB) for review and approval of the planned system requirement.

4. When there is a budget shortfall between planned IT requirements and available funding, the IRB is charged with the responsibility of ensuring that the funding is commensurate with mission impact.

5. The FEMA IT Operations Plan must be reviewed, updated, and evaluated beginning each January after the receipt of the President's Budget. By that time, the IRB is aware of shortfalls between funding requests and actual funding for the current fiscal year. The loss of funding for any key agencywide system or program that affects the implementation of the target IT architecture will be evaluated and presented to the IRB. New requirements and adjustments to planned efforts are incorporated into the revised FEMA IT Operations Plan.

6. Each program office is responsible for submitting new and updated IT plans, budget and resource requirements to their representative on the ISPAG. These representatives work with Policy and Requirements Branch, Management Division, ITS, (IT-MA-PR) to integrate these requirements into the IT Operations Plan. The IT Operations Plan development schedule is as follows:

   January: Receive President's Budget, program offices submit updated IT plans, budgets and resource requirements to their representatives. Initial meetings are held to begin the planning process.
   April: OMB Call/Initial Draft of new IT Operations Plan. IT-MA-PR provides additional information as requested by OMB.
   June: Submit to OMB.
   July: Provide to the Office of Financial Management for budget submissions.

Background

The Paperwork Reduction Act (44 U.S.C. Chapter 35), the Information Technology Management Reform Act of 1996 (ITMRA) and the Office of Management and Budget (OMB) Circular No. A-130 provide the policy and planning framework for Federal Information Resources Management (IRM). This guidance is provided in a series of policy areas. It is within the context of Strategic Information Resources Management that the planning processes for IT is delineated.

1-2 Report on Major IT Systems Budgets

Overview

1. This chapter implements the Federal Emergency Management Agency's (FEMA's) policy and procedures for meeting the budget collection and reporting requirements for obligations on data acquisition, operation, and use of information technology systems as a requirement of OMB A-130.

2. The provisions of this chapter are applicable to all FEMA's organizational elements in the headquarters, regions, and field establishments whose functions include the acquisition, operation, and use of information technology systems.

3. This chapter documents and supports compliance with the Chief Financial Officer's Act, and encompasses reporting requirements of budget estimates for information technology initiatives in any of the years (Past, Current, or Budget).

Responsibility

1. Associate Directors, Administrators, Regional Directors and Office Directors are responsible for the following:

   - Reporting actual and planned expenditures for information systems;

   - Conforming to Presidential, fiscal, and budgetary guidelines for reporting requirements for information technology systems; and

   - Submitting reports for information systems that provide information on workyears and obligations for: planning, including requirements, feasibility, and benefit-cost studies; system design, development, and acquisition; voice and data telecommunications requirements, regardless of whether or not they are associated with an information system's installation, operations, maintenance, and support.

2. The Associate Director, Information Technology Services Directorate, is responsible for implementing the reporting requirements for obligations on information technology systems FEMA-wide.

3. The Chief Financial Officer, Office of Financial Management, is responsible for verifying conformance and adherence to program estimates, appropriations, and budget submissions to Office of Management and Budget (OMB), as well as special reporting requirements for the high risk area.

Procedures

1. Submitting Reports. The Policy and Requirements Branch, Information Technology Services Directorate (IT-MA-PR) issues to each organizational element requests for submission of budget projections for each information technology acquisition with FEMA's annual strategic plan, Information Technology Operations Plan. Based on the data reported by the organizational elements, IT-MA-PR formulates and prepares, OMB Circular A-11, agencywide summary on obligations for information technology. Data not available from the plan submissions is solicited from the appropriate organizational element. Disaster funds used for information resources must be reported.

   The IT-MA-PR coordinates with the Office of Financial Management to ensure consistency of the Exhibit data with the latest budget decisions and with FEMA's operating plans. The Office of Financial Management transmits the final Exhibit data to OMB as part of FEMA's budget submission.

2. Reporting Requirements. OMB requires the data reported should include all automatic data processing equipment. Amounts will be shown in thousands of dollars. The data in the Exhibit should be consistent with the FEMA Information Technology Operations Plan. Organizational elements should retain the data for subsequent budget obligation projections and reports.

1-3 Life Cycle Management

Overview

1. This chapter implements procedures for the Federal Emergency Management Agency's (FEMA's) management of information systems life cycle. The procedures in this chapter, at this time, primarily emphasize life cycle acquisition guidance. The provisions of this directive are applicable to all organizational elements in headquarters, regions, and field establishments. Local acquisition offices must adhere to the same procedures as delineated for the Acquisition Services Division, Office of Financial Management.

2. Life Cycle Management (LCM) encompasses technical, budgetary, and programmatic areas of consideration to ensure that, as information systems progress through the stages of their life cycle, these areas are integrated into a unified management strategy that best meets FEMA's mission. LCM identifies and considers the true investment of information systems by recognizing the acquisition costs of hardware, software, and services, and the overhead costs of operations and maintenance, resources, facilities, and disposition.

3. The minimum set of phases in the LCM process include decision making, strategy, acquisition, and implementation.

    - Strategic Phase describes the future direction of the information system over the next 5 years.

    - Decision making Phase defines the alignment of information systems plans and budgets; the Agency's goals and objectives; and the programmatic plans and budgets.

    - IT Acquisition Phase consists of the requirements analysis and analysis of alternatives to satisfy information needs and an assessment of the alternatives for meeting the information requirements.

    - Implementation Phase consists of a synopsis of the key activities, milestones, and resources needed to implement the selected alternative from delivery through operations to disposition of the information system.

Responsibility

1. The Chief Information Officer (CIO) provides technical guidance for the information systems LCM process, and promotes LCM practices with agencywide policies, principles, standards, and guidelines. The CIO is responsible for ensuring effective and efficient use of information technology services within FEMA. The Clinger-Cohen Act of 1996 requires agencies to apply three critical questions for IT procurement. The CIO asks the following questions for any IT investment:

- Should the function to be supported be performed in the private sector rather than by an agency of the Federal Government? If so, should the component of the agency performing that function be converted from a governmental organization to a private sector organization?

- Should the function be performed by the executive agency? If so, should the function be performed by a private sector source under a contract entered into by the head of the executive agency, or should it be performed by executive agency personnel?

- Does the function to be supported need to be appropriately redesigned to improve its efficiency, or has it been?

2. Information Resources Board (IRB) - Information systems development and enhancements in excess of FEMA's procurement threshold of $250,000 must be presented to the IRB for conceptual review and oversight of system requirements. The IRB recommends concurrence or non-concurrence to the CIO. Submission of the Requirements Analysis, Analysis of Alternatives, and Risk Benefit Analysis documents will suffice as an alternative to a presentation to the IRB. Presentations may be scheduled with IT-MA.

3. Procurement Review Board (PRB) - Procurement plans for major information systems in excess of $1 million must be presented to the PRB for review. All acquisitions in excess of the FEMA threshold of $1 million must be approved in writing by the PRB before any contract can be signed or any in-house development efforts can begin. Acquisitions of $25,000 or greater require written approval of the Director, Acquisition Services Division, acting as the PRB Chairperson. Acquisitions costing less than $25,000 do not require approval by the PRB. However, all documentation must be retained in the files of the requester for auditing and management review.

4. Associate Directors, Administrators, Regional Directors, and Office Directors are responsible for the following:

    - Applying LCM concepts consistent with ITMRA, OMB Circular A-130, and FEMA regulations, policies, standards, and guidelines;

    - Appointing a Project Manager or group to apply the LCM process;

    - Providing information needed to support LCM information system planning and developing the related budget requests;

    - As part of the LCM, ensuring inclusion of the required analyses and the feasibility of reuse of information systems;

    - Ensuring determination and use of an LCM methodology early in the planning process that incorporates the full life cycle cost for the information system; and

- Overseeing the development of planning documents, such as Test Plan, Configuration Management Plan, etc., and updating the documents as needed throughout the LCM process.

Procedures

1. The information resources life cycle process begins with the determination of need for the information system and continues through the day-to-day operations of the installed system to the planning for its replacement. The requester is responsible for preparing a Requirements Analysis and Analysis of Alternatives for all information systems prior to the acquisition. The amount of documentation varies with the system size and complexity and is described in Chapter 1-4, Documentation Requirements. The format for these two documents is shown in figures 1 and 2.

2. OMB issues a data call annually for all Federal agencies to submit their strategic plans for information systems and technology. Strategic plans generally contain the following kinds of information: a description of the organization's program priorities and a discussion of how information technology is used to meet those priorities; a list of the organization's major information systems and the costs budgeted over a 5-year period; and a description of significant information technology initiatives.

3. Each organizational element must prepare and submit to IT-MA-PR its annual update of the 5-year IT Operations Plan that reflects the funding needed to support the investment decisions for the information systems. It is the requesting organization's responsibility to assure that the plan agrees with its budget submission. IT-MA-PR will review, analyze, and develop a consolidated 5-year Agency IT Operations Plan for reporting to the Office of Management and Budget. Whenever possible, all major procurements are reported in the plan.

4. Based on approved plans, organizational elements or program offices prepare and submit the Requirements Analysis, Analysis of Alternatives, and the Project Information Sheet or Form 40-19, Acquisition Strategy/Milestones, to IT-MA-PR and to the appropriate local acquisition office. For unplanned procurements, the Requirements Analysis, Analysis of Alternatives and Form 40-1, Requisition Commitment for Services/Supplies, or Form 60-1, Requisition for Supplies, Equipment and/or Services, must be submitted concurrently to IT-MA-PR and to the appropriate local acquisition office.

5. IT-MA-PR will assist program offices by coordinating information systems technical reviews, including any required computer security reviews. The requisition documents will be reviewed according to the type of information system and the dollar thresholds stated below. Selected identifying data from the documentation will be entered into a repository database to catalogue mission critical application systems. To encourage use of available resources to meet new requirements and to avoid duplication, the database will be made accessible for query throughout FEMA.

Information Systems Procurement Thresholds
Effective October 1999

Threshold Dollar Value	**Review/Approval Responsibility**
$0 - $10,000	Associate Directors, Administrators, Office Directors, Regional Directors
Greater than $10,000	CIO or Information Resources Board

Requirements Analysis Format

1. **Project Title:** **Give the title and a short descriptive sentence of the information systems needed (rather than the end product).**
2. **Overview:** **Brief description of requirements for resources as to the information systems and services needed by FEMA. Tailor this item and all others to the specific needs of this procurement.**
3. **Mission Needs:** **Description of FEMA and IRM mandates for emergency management services and support.**
4. **Information Needs:** **Provide a general description of information systems needs and the requirements to support those systems and their service flows. It is not the systems, but the flow of services in support of emergency management that is critical. This item should be more specific in terms of type, quantity, geographic coverage, security, et al.**
5. **Current Systems and Operations:** **Describe needs met and unmet by current operations, including personnel.**
6. **Requirements and Anticipated Unmet Needs:** **Describe the expected need that will not be met for defined system requirements, such as:**

   System Life
   Workload
   Compatibility, interoperability, integration of systems
   Interagency coordination
   Training
   NSEP functions
   Security/privacy
   Federal regulations and standards, et al.

7. **Legislative and Executive Mandates for IRM:** **Such as PRA, OMB Circular A-130, ITMRA, et al.**
8. **Formal Aggregation and Analysis of Requirements:** **List the specific functions that are required to meet those requirements defined above. Also, give the deficit in resources (including personnel and expertise) these functions will rectify. There must be a timeframe for the services.**

Figure 1

Analysis of Alternatives Format

1. **Restatement of Needs/Specific Functions: Write a brief description of the specific functions defined in the requirements analysis.**

2. **Preliminary Conclusion: The workload cannot be done with existing resources, expertise, and personnel levels. Describe why not. Issues that must be considered:**

   GSA Mandatory Programs
   Reuse of Existing Resources
   Sharing of Existing Resources
   Contracting for New Resources

3. **Select 3 Economical, Viable Alternatives: To fulfill these requirements, the proposed contract cannot be the only solution; therefore, evaluations of other possibilities must be provided that document an awareness of the aspects of the information systems contracted for and how those services might be delivered. For example:**

   Combine engineering and development with procurement
   Hire individual consultants as needed
   Compete each task separately
   Use other agencies' services

4. **Evaluate Factors in Each Alternative: List and price the benefits and costs for each proposal and how they differ by which alternative is selected. Benefits should include but not be limited to service flows, personnel skills, mission needs, timeliness, economies of scale, etc. Costs include price, risks, delays in implementation, responsiveness, turnaround, security, regulatory constraints, etc.**

5. **Select Most Advantageous Alternative: In procurement, as in the rest of life, cheapest is not always best; we get what we pay for. Therefore, analyze the full ramifications of prompt, secure, reliable services that are cost-efficient. FEMA must be concerned with procurements that are on-time, work effectively, and improve service, as well as, getting the lowest price; although the latter is never to be discounted.**

Figure 2

1-4 FEMA Documentation Requirements

Overview

1. The Federal Emergency Management Agency (FEMA) has established policy and procedures for developing documentation for information technology (IT) systems. Documentation complexity should reflect the complexity of the system and the needs of the users, operators, programmers, and system administrators who utilize the system. Documentation should support the life-cycle stages of system development including functional and data requirements; design, building, testing, and implementation stages; and operational and maintenance stages.

2. The quality of documentation should be such that at any time, a new development group could be brought in and immediately pick-up where the first group left off. Documentation of less quality will generate long term life-cycle problems as systems are upgraded and personnel change.

3. FEMA will often utilize system development models such as Spiral Development or Rapid System Prototyping, that differ from the classical model outlined below. However, these models have the same final documentation requirements as the classical model. They may occur in slightly different sequences as developers "refine requirements, build a little, test a little, and begin the cycle anew to refine requirements . . ." until the full development is completed.

Responsibility

It is the responsibility of FEMA program managers to ensure that system documentation is completed as appropriate per this procedure.

Procedures

1. Requirements and Planning Stage.

   The objective of the requirements and planning stage is to define the user's need for automated systems processing. During this phase, a Requirements Analysis and Analysis of Alternatives are developed. The Agency will then know the system capabilities and features it needs and the technical environment in which the system will operate (e.g., hardware, system software, telecommunications). The Agency will also have an estimate of the cost of the system, and will have entered this information into the budgeting cycle. The Agency may have already awarded a contract for a vendor to work with the government to develop the system, or the Agency may be developing the system. However, the documents developed in this phase act as a blue print for system objectives and requirements, which will be met and expanded upon in all subsequent stages.

2. Functional and Data Requirements Stage.

   The developer defines in detail the system requirements, including both the automated software and related manual activities and procedures. This phase is sometimes referred to as systems concept, conceptual design or logical design. There are two primary classes of requirements that must be documented.

   Functional requirements describe aspects such as:

   - the flows of data to, from and within the software or system
   - the sources and recipients of data
   - how the software manipulates or transforms the data
   - the workload volumes for data flows
   - performance requirements such as response times, for specific functional processes
   - the data contained in user interface/data entry screens and output reports, potentially including their physical layout.

   The functional requirements can be described by narrative, graphics such as dataflow or process flow diagrams, structured flowcharts, matrices or combinations.

   Data Requirements describe the data that the system will maintain. Data models may be developed and data normalized to eliminate unnecessary elements. Data dictionaries should be created, defining each element in terms of name, attributes (e.g. alphanumeric, logical), length, format, permissible values, ownership (i.e., who can create the data element, who can modify it).

3. Design Stage.

   In the General Design Stage, the developer defines how the system will achieve the requirements identified in earlier phases. The developer defines programs to carry out specific system functions and divides the data into data stores, files or databases. This information can be documented graphically using data or process flow diagrams or flowcharts.

   As the Detail Design Stage begins, the specifications are written for program and data files, providing the level of detail programmers need for coding. The documentation can take the form of hierarchical input-process-output (HIPO) charts, process action diagrams, Structured English, pseudo code or Warnier-Orr diagrams. Computer-Aided Software Engineering (CASE) tools can automate much of the general and detailed design activities.

   Written documentation should be developed to identify, goals and objectives, procedures, testing criteria and schedules for the Test Plan. A Requirements Traceability Matrix (RTM) that maps functional requirements to physical configuration items such as databases or programs should be developed. Then, whenever a software component is reviewed, audited or tested, the Agency can use the RTM to identify the related functional requirements.

4. Building Stage.

   During this phase, programmers write or generate the software code. These coded instructions control the various hardware, systems software, and telecommunications components. The programmers usually develop the software components in sections from smallest to largest: first program units, then modules supporting major processes, then interfaces among modules and with external systems. The programs are debugged and documented. Finally, the entire software system is made ready for testing.

   During this phase, training manuals for end users through system administrators are finalized. Step-by-step procedures should be developed to allow users and system administrators to perform any function on the system.

5. Testing Stage.

   Testing takes place in two major stages. First, the developers conduct their own test of the software. The developer conducts unit tests, integration tests and system tests, correcting errors as they are found. Regression testing should also be performed to ensure that the correction of a particular part of the software did not cause problems in other areas of the software. These test results and corrections should be documented.

   Secondly, FEMA will conduct an acceptance test of the software according to an acceptance test plan and procedures. The acceptance test plan and procedures may be prepared and performed by Agency personnel or an independent testing group then conducts tests according to the Test Plan. After these have been successfully completed, the Agency may bring in users to participate in the acceptance test to ensure that the system is ready for production. Those performing the acceptance testing should utilize the user manuals to demonstrate their effectiveness.

6. Implementation Stage.

   The implementation stage includes pre-installation activities such as site preparation and user training, installation of the software and hardware, and post installation activities such as converting data from old systems to the new.

7. Operation and Maintenance Stages.

   During this phase, gaps in documentation should be corrected, upgrades and modifications that are made to the software need to be documented.

8. ITMRA Evaluation Procedures.

The 1996 Information Technology Management Reform Act requires that any information technology project be planned and have quantifiable goals, objectives and performance measures identified before procurement or implementation. Once the system is delivered and becomes operational, the system is to be judged on actual versus projected performance. Performance management systems are to be put in place that will insure that cost, schedules, and technical aspects of the project are truly integrated. These management control systems provide a framework for defining work, assigning work responsibilities, establishing budgets, controlling costs, and summarizing, with respect to planned versus actual accomplishments, the detailed cost, schedule and related technical achievement information for management review. These issues have been defined in the Planning and Requirements Stages of the project. At completion of the development and through-out the life-cycle of the system, periodic reviews will be held to ensure that:

- Performance of the projects work scope, schedule, and cost objectives are met;
- Comparisons of actual resources used versus what were projected are measured; and
- Reliable reports of life-cycle performance versus projected performance are created for management review.

9. Documentation Examples for Systems of Four Levels of Complexity.

Level I. COTS Packages

Commercial-off-the-shelf (COTS) software packages often meet user requirements. Even those applications developed utilizing FEMA's standard suite of office automation software require documentation. The more complex the requirement being met, the more extensive the documentation required to support the system.

- Requirements and Planning Documentation.
- This high level document should describe the overall program office requirements for achieving mission objectives, and why this solution was reached, as opposed to any other approach, such as using existing FEMA systems or other already developed FEMA applications. Generally, for small or uncomplicated requirements, this should be a 1 - 2 page document.
- Functional and Requirements Documentation.

- This should clearly describe functional activities of the work to be automated. This document should be written in layman's terms to be readily understood by anyone wishing to understand what the system is to functionally perform. This document may be as short as one page for uncomplicated requirements.

- Standard vendor documentation:

  - User Guides
  - Quick Reference Guides
  - System Administrator and or Database Administrator Guides

- For applications developed around the COTS package.

- Descriptions of the data base design and structure, forms layouts and design, interfaces between data bases, and data maintenance procedures required for the application's data files.

- User Guides or User Procedures for the users of the application if the standard COTS documentation isn't sufficient for the users of the application.

Level II. Customized COTS

- All of the documentation listed above for using COTS packages.

- Source Code Document - A listing of the code for any software developed to augment the COTS software.

- Design Document - Documentation needed for any software developed to augment the COTS software that describes the modules of the software, the functions of each module and interfaces between modules.

- Interface Description - Describes interfaces between the COTS software and the user software developed to augment the COTS package.

- Test Plans and Test Procedures - Describes plans and procedures to be used to perform validation and verification testing of the software developed to augment the COTS package.

Level III. Major Projects

Major projects are systems with one basic application software system developed for FEMA such as the Teleregistration System.

- Requirements and Planning Documentation.

- A full Requirements Analysis and Analysis of Alternatives/ Business Case must be completed prior to any other activity. This document must answer questions required by the Information Technology Management Reform Act (ITMRA) such as: Should this function be performed by the Agency or outsourced? Is FEMA the right Agency to perform this function as opposed to other Agencies? Have we explored use of existing FEMA systems? and, Does the system comply with Government-wide regulatory requirements?

- User (FEMA) Requirements Document for the software system.

- MILSTD documents relating to the requirements specification phase of the software development:

  Functional Requirements Description
  Data Requirements Documents
  Interface Control Documents

- MILSTD documents relating to the software design phase of the software development:

  System Specifications
  Software Requirements Specifications
  Program Specifications
  Test Specifications
  Software Design Specifications
  Database Specifications
  Interface Design Specification

- Documents at the completion of the software development (after it has been 'built'):

  Source Code for all Program Modules
  'As Built' Detail Design specifications
  'As Built' Database Specifications
  'As Built' Interface Design Specification
  Users Manual(s)
  Program (System) Maintenance Manual
  Operations (System Administrator's) manual
  Installation Procedures
  Test Plan & Procedures for Validation and Verification testing
  Training Plan

Level IV. Major Projects Requiring Parallel Modular Development and Integration

Documentation for large projects apply a minimum of the level III complexity. Interface Control documents must address the interfacing of the software systems (modules) as well as the interfacing of the various components of each software system in detail.

Left blank intentionally

Chapter 2

Management and Use of Information

Left blank intentionally

2-1 Collections of Information

Overview

1. This chapter implements the provisions of the Paperwork Reduction Act of 1995 concerning collections of information by establishing procedures for the review, evaluation, control, and use of collections of information conducted or sponsored by the Agency. The guidance in this chapter is designed to reduce, minimize and control burdens on the public to provide or disclose information. It is also designed to maximize the practical utility and public benefit of the information created, collected, disclosed, maintained, used, shared, and disseminated by or for FEMA. FEMA organizations will, to the extent practicable, acquire, use, and manage information technology to improve the Agency's ability to efficiently and effectively perform its missions and functions while reducing information collection costs and burdens on the public.

2. Section 3506(c) of the Paperwork Reduction Act of 1995, directs Federal agencies to establish processes that are sufficiently independent of program responsibilities, that they can fairly evaluate whether proposed collections of information are necessary for the performance of agency functions and should be approved by the Office of Management and Budget (OMB). These processes include: a review of each collection of information for need; a functional description of the information to be collected; a plan for the collection of the information; a specific, objectively supported estimate of burden, as appropriate; a test of the collection of information through a pilot program (if used); and a plan for the efficient and effective management and use of the information to be collected, including necessary resources. The objectives of the review are: to ensure that proposed collections of information have practical utility; are the least burdensome to perform the Agency's functions; comply with legal requirements and achieve program objectives; do not duplicate of information otherwise accessible to FEMA; and minimizes the costs of collecting, processing, and using the information without shifting disproportionate costs or burdens on the public.

3. FEMA organizations may not conduct or sponsor a collection of information from more than 10 respondents unless the collection of information has been reviewed under the Agency's formal review process and approved by OMB.

4. OMB approved collections of information will be assigned an OMB control number and an expiration date.

5. All approved collections of information will display a currently valid OMB control number and expiration date. In addition, collections of information or their instructions, will inform potential respondents of the following: they do not have to respond to the collection of information unless it displays a currently valid OMB control number; the reasons the information is being collected, including how it will be used to further the proper performance of the Agency's functions; an estimate of the burden of the collection of information and a request for comments concerning the accuracy of the burden estimate and

suggestions for reducing the burden; whether responses are voluntary, required or obtain or retain a benefit, or mandatory; and the nature and extent of confidentiality to be provided to the information being requested.

6. Once a collection of information is approved by OMB, FEMA organizations may not make modifications to the collection of information unless the modification has been coordinated with the FEMA Information Collections Officer and submitted to OMB for review and approval.

7. FEMA organizations may not use collections of information that display an expired expiration date.

8. FEMA may not impose a penalty on any respondent for failing to comply with a collection of information if it does not display a currently valid OMB control number or fails to inform the potential person who is to respond to the collection of information that they are not required to respond unless it displays a currently valid OMB control number. When a collection of information is used to prove or satisfy a condition for the receipt of a benefit or the avoidance of a penalty, and does not display the OMB control number or inform respondents, the FEMA organization will not treat a person's failure to comply as grounds for withholding the benefit or imposing the penalty, but must permit respondents to prove or satisfy the legal conditions in any other reasonable manner.

Responsibility

1. The Chief Information Officer is responsible for:

   - Ensuring compliance with and implementation of information policies and information resources management responsibilities in this chapter to reduce information collection burdens on the public.

   - Ensuring a process to evaluate fairly whether proposed collections of information should be approved.

   - Designating the FEMA Information Collections Officer, under the direction of the Associate Director, Operations Support Directorate, to conduct such reviews and evaluations of and submit proposed collections of information and required certifications to OMB.

   - Improving the integrity, quality and utility of information to users within and outside the Agency.

   - Implementing common standards for the collection, storage, processing, and communications, including standards for security, interconnectivity, and interoperability.

2. The Associate Director, Operations Support Directorate, is responsible for:

   - Establishing and implementing Agency guidance for the collections of information review, submission and certification process; and

- Implementing guidelines and procedures to protect the privacy and security of information created, collected or maintained by the Agency.

3. The Office of General Counsel is responsible for establishing guidelines and procedures to protect the privacy information created, collected or maintained by the Agency.

4. The Associate Directors, Executive Associate Directors, Administrators, Executive Administrators, Inspector General, Regional Directors and other Office Directors are responsible for ensuring adherence to information collection policy and procedures.

Procedures

The FEMA Information Collections Officer will:

1. Conduct reviews and evaluations of all proposed collections of information consistent with the provisions of the Paperwork Reduction Act of 1995 and OMB regulation 5 CFR 1320.

2. Certify that proposed collections of information are necessary for performing the functions of the agency, and submitting the proposed collections and certifications to OMB for approval.

3. Assess proposed collections of information for excessive or disproportionate burdens on the public and develop an Agency plan to minimize such burdens.

4. Annually or as required, develop in conjunction with FEMA organizations the Agency's Information Collection Budget and manage the ICB and burden hours imposed on the public.

FEMA Organizations will:

1. Obtain OMB approval before conducting, or sponsoring the conduct of, a collection of information from ten or more respondents.

2. Follow the guidance and procedures in this chapter, and in FEMA Instruction 5300.1, FEMA Reports/Information Collections Management Program, to request OMB review and approval of a proposed collection of information.

3. Coordinate, in advance, proposed collections of information with the FEMA Information Collections Officer.

4. Plan well in advance for the development, use, design, printing and distribution of proposed new collections of information and for the continued need for and revisions to expiring collections of information to ensure timely review and processing by OMB. Under normal processing procedures, the OMB review and approval process takes a minimum of four months to complete. There are provisions for short-term approvals under OMB's "emergency" processing procedures. Unplanned, last minute requirements will delay your ability to use a proposed collection of information.

5. Provide notice to and otherwise consult with members of the public and affected agencies concerning each proposed collection of information to solicit comments. Use comments, as appropriate, to modify or otherwise finalize the proposed collection of information.

6. Conduct periodic evaluations of the need for the collection of information to:

   - Ensure that the information is necessary for the proper performance of the Agency's missions and functions;
   - Reduce or eliminate the collection of duplicative information;
   - Use information technology to reduce burden and improve data quality, agency efficiency, and responsiveness to the public; and,
   - Ensure that information collected is relevant, accurate, valid, and reliable, and the organization has the ability to process the information it collects in a useful and timely manner.

Definition and Descriptions of Collections of Information

1. "Burden" means the value of the time, effort and financial resources expended by persons to generate, maintain, retain, disclose or provide information to or for a Federal agency. This includes reviewing instructions; developing, acquiring, installing and utilizing technology and systems for any of these purposes: training personnel, searching data sources, collecting data, completing and reviewing information collections, and transmitting or otherwise disclosing information.

2. "Collection of information" means the obtaining, causing to be obtained, soliciting, or requiring the disclosure to third parties or the public, of facts or opinions by or for any agency, **regardless of form or format,** calling for either (1) answers to identical questions posed to, or identical reporting or recordkeeping requirements imposed on 10 or more persons or organizations. Collections of Information include, but are not limited to, any requirement for persons to obtain, maintain, retain, report, or publicly disclose information. Collections of information refer to the **act** of collecting or disclosing information, to the **information** to be collected or disclosed, or to a **plan or instrument** calling for the collection or disclosure of information. Examples include:

   - Report Forms
   - Application Forms
   - Schedules
   - Questionnaires
   - Surveys, including customer service and program evaluation surveys
   - Directives (Circulars, Instructions, Bulletins, Manuals)
   - Reporting or Recordkeeping Requirements
   - Contracts, Cooperative Agreements, Grants
   - Policy Statements
   - Plans
   - Rules or Regulations
   - Planning Requirements
   - Interview Guides
   - Oral communication

- Telegraphic, telephonic, or facsimile requests
- Requests for proposal or other procurement requirements
- Automated, electronic, mechanical or other technological collection techniques
- Standard questionnaires used to monitor compliance with Agency requirements
- Techniques or technological methods used to monitor compliance with agency requirements

Left blank intentionally

2-2 Access to Information Technology for Individuals with Disabilities

Overview

1. This chapter implements the procedures for the Federal Emergency Management Agency (FEMA) to establish an accessible information environment to ensure that individuals with disabilities may access and use information technology systems and services provided by FEMA for internal and external customers.

2. The establishment of accessible information environments is an important FEMA goal. Accessible information technology systems and services provides FEMA with a tool to:

    - Recruit the most qualified applicants;
    - Better utilize the skills of current employees; and
    - Improve the delivery of information services to all citizens.

3. Accessible information environments ensure that employees with disabilities receive equivalent and integrated information services, equipment, training, and technical support as those without disabilities. It also ensures that customers and citizens with disabilities will be able to access automated information services that are being developed by FEMA.

Responsibility

1. The Chief Information Officer (CIO) is responsible for ensuring that the requirements for accessibility to information technology, which is mandated in the Americans With Disabilities Act , 424 U.S.C. 12112 and related laws and regulations, are fully met by the Agency. The planning processes identified in Chapter 1-1 of this document must be supported. The CIO is responsible for:

    - Ensuring electronic office equipment access for current or prospective employees with disabilities;

    - Ensuring access of FEMA's public information resources to individuals with disabilities; and

    - Monitoring progress towards achieving electronic equipment accessibility goals.

2. Associate Directors, Administrators, Regional Directors, and Office Directors are responsible for:

    - Ensuring that employees are provided access to the information technology tools they require to perform their jobs, including access to FEMA information dissemination services such as the Intranet and electronic mail;

    - Ensuring that all employees are aware of the policy and procedures for providing accessibility to FEMA information technology resources;

- Providing adaptive technology hardware, software and upgrades for employees to retain compatibility with the standard office automation suite.
- Funding adaptive technology requirements for employees; and
- Funding application programming to accommodate adaptive technology requirements resulting from automated business processes that impose information access restrictions on FEMA employees or the public.

3. The General Counsel, Office of the General Counsel, is responsible for interpreting the requirements of the Americans With Disabilities Act and other pertinent legislation dealing with accessibility; and for ensuring that FEMA Offices, Administrations and Directorates fully understand and comply with these laws and regulations.
4. The Director, Office of Emergency Information and Media Affairs is responsible for ensuring that information available for use by the public is accessible to individuals with disabilities.
5. The Associate Director, Preparedness, Training and Exercises Directorate and the Administrator, U.S. Fire Administration are responsible for ensuring that:
   - Video-based media produced for instructional, training, or informational purposes will be captioned so the information presented is accessible to deaf and hard of hearing viewers;
   - Paper based training materials developed after November 1, 1996, are available in electronic and Braille formats for use by the blind and visually impaired.
6. The Executive Associate Director, Operations Support Directorate, is responsible for ensuring that publications developed after November 1, 1996 are available in electronic and Braille formats for use by individuals with disabilities.
7. System administrators, program developers, Internet Domain Webmasters and system designers are responsible for ensuring that the products they develop allow non-audio and non-graphical alternative accesses to information.

Procedures

1. At minimum, FEMA employees will have access to the standard FEMA office automation software, Intranet and Internet, telecommunications networks and telephone equipment and electronic mail systems. Employees with special requirements for sensory, cognitive, or mobility adaptive technology will be equipped with special peripherals or software that provide access to FEMA's information technology systems.
2. The Information Technology Services Directorate supports the use of the following services provided by other agencies:
   - Telecommunications devices for the deaf (TDD) numbers will be published in the FEMA Telephone Directory and made available to the General Services Administration for inclusion in the Federal TDD Directory.

- The General Services Administration's Federal Information Relay Service (FIRS) for providing voice to TDD relay services, allowing direct communications among those with and without speech, hearing, deaf and hard-of-hearing employees and public.

3. Requests for telecommunications related adaptive technology services will be made through the Local Ordering Official as outlined in Chapter 3-1, Purchasing via the Telecommunications Information Management Accounting and Control System. Requests are submitted on FEMA Form 85-51, Telecommunications Service Requests.

4. Requests for information systems related adaptive technology will be purchased through the 40-1 process as outlined in Chapter 3-7, Purchasing Standardization Program.

5. FEMA employees are encouraged to utilize GSA's Clearinghouse on Computer Accommodation (COCA) which provides assistance to agencies in all aspects of accessibility management, from demonstration of enhancement capabilities in a demonstration center to briefings that assist agencies establish their own support capabilities. COCA can be accessed at **http://www.gsa.gov/coca.**

Left blank intentionally

2-3 Records Maintenance and Electronic Recordkeeping

Overview

1. This chapter establishes the Agency's procedures for the creation, maintenance, use, dissemination and disposal of FEMA's official records, including electronic recordkeeping. The chapter also covers the safeguards to protect the accuracy, completeness, privacy and security of FEMA's electronic records. These procedures serve to supplement and support the policy and directives on records management implemented by the Associate Director for Operations Support.

2. Federal law requires FEMA to create and preserve official records documenting the Agency's organizations, functions, policy, and essential transactions, including those created and maintained on electronic media. Official records document and reflect the information necessary to ensure the management and accountability of agency programs and to protect both legal and financial rights of the Federal Government.

3. Government information and official records may be stored and retrieved in a variety of ways, but cost containment and public demand place increasing emphasis on the use of electronic media. FEMA's information systems, by definition, contain information that constitutes temporary or permanent agency records.

4. Federal policy for electronic data processing and recordkeeping now includes fostering public access to information maintained by and for Federal agencies. The policy extends to strengthening FEMA's partnerships with State and local governments by lessening their information burdens through improved dissemination and use of Federal data. The expanded responsibilities highlight the need for maximum uniformity and simplicity in maintaining and using agency records.

5. To help the public and agencies locate and access government information, the Executive Branch has established the Government Information Locator Service (GILS), consisting of decentralized agency-based information locator records and associated information services. FEMA must compile an inventory of its 1) locators that cover its information dissemination products, 2) automated information systems, and 3) Privacy Act systems of records. The inventories serve to increase the efficiency of the dissemination function and to avoid duplicative information collections. Inventories and locator aids are an important tool to identify the availability of public information and to assist agencies in carrying out their responsibilities to manage, schedule for disposition, and archive their official records. Records that are properly described in GILS will be properly described for records schedule, and vice versa.

Responsibilities

1. The Chief Information Officer is responsible for:

    - Minimizing the cost to the Agency for the creation, collection, maintenance, use, dissemination, and disposition of information.

- Strengthening the partnership between FEMA and the State and local governments by minimizing the burden and maximizing the utility of information created, collected, maintained, used, disseminated, and retained by or for the Federal Government.

- Enhancing public access to and dissemination of information, using electronic and other formats.

- Instituting information technology standards for the collection, storage, processing and dissemination of electronic records, including standards for security, interconnectivity, and interoperability.

- Implementing and enforcing procedures, including requirements for archiving information maintained in electronic format, particularly in the planning, design, and operation of information systems.

2. The Associate Director, Operations Support, is responsible for:

   - Formulating policy and procedures and exercising supervision over FEMA's records management program.

   - Initiating actions and standards as may be necessary to ensure maximum uniformity and simplicity in maintaining and using agency records, including records in electronic format.

   - Designating FEMA's Records Officer to serve as liaison with the National Archives and Records Administration (NARA) and to provide records management guidance and assistance to all organizational levels.

3. The Associate Directors, Executive Associate Directors, Administrator, Executive Administrator, Inspector General, Regional Directors, and other Office Directors are responsible for ensuring proper management and safeguards for Agency records by employees in their respective areas.

Procedures

1. Creation and Designation of FEMA's Official Records.

   - FEMA officials and personnel are responsible for the establishment and safeguarding the Agency's official temporary and permanent records, including those on electronic media.

   - The development of public information and official records shall be consistent with FEMA's policy and records management directives.

   - The FEMA Records Officer shall make the final determination as to whether or not particular information or files constitute official records.

- The FEMA Records Officer serves as liaison with NARA and other Federal departments and agencies relating to records management.

- The development and modification of all information systems shall incorporate the requirements and standards for records management, including the documentation of the information system itself.

2. Accessibility of FEMA's Public Information and Official Records.

   - Information collection and retention shall enhance public access and dissemination of records and Federal data.

   - Electronic records shall conform to agency and federal standards for interconnectivity and interoperability.

   - For compatibility, FEMA shall use standard network terminology and voluntary, international standards for information search and retrieval when disseminating information to the public.

   - Electronic records shall be labeled as to make the records accessible and convertible to a nonproprietary format.

   - Records shall be easily accessible to any organizational units that use them for official purposes.

   - FEMA's participation in the Government Information Locator Service (GILS) shall be used to manage FEMA's records, particularly electronic systems.

3. Maintenance of Temporary or Permanent Records.

   - Records management controls shall be maintained to reduce excess paperwork burdens or duplication of data.

   - FEMA officials and personnel shall implement appropriate records management practices to all records, irrespective of the media.

   - Electronic recordkeeping shall be designed to simplify the maintenance and to expand the use of Agency records and Federal data, and shall be designed and used only on NARA approved systems.

   - Records and files shall be maintained in accordance with applicable data integrity, security, privacy, and safety regulations, including the provision of duplicates or backup copies of electronic records.

   - Agency personnel shall review periodically all existing forms and reports (both those originated by the agency and those responded to by the agency but originated by another agency or branch of government) to determine if they need to be improved or canceled.

- Information systems managers shall maintain electronic records in a cost effective manner that allows the information to be retrieved quickly and reliably.

- System managers shall review electronic files and records regularly to determine that records are complete and that standards for accuracy, integrity, security and privacy are adequate.

- Employees electronic working files or temporary records shall be filed separately from Agency's official files.

4. Disposal and Archiving of Temporary and Permanent Records.

   - Unauthorized destruction or disposition of temporary or permanent records is prohibited by law, including those created and maintained on electronic media.

   - Records no longer current or active shall be retired and archived in conformance to Federal and FEMA guidelines. Electronic records shall be converted to an appropriate format and transmitted with appropriate labels.

   - Electronic records shall conform to the standards and controls for creating, maintaining, using, disseminating, preserving, and disposing of FEMA records as set by the Operations Support Directorate.

   - Employees may request transfers of records to other Federal Agencies.

   - No FEMA employee may remove classified records, including copies of classified documents.

   - Employees shall eliminate unnecessary duplicative or outdated convenience files, including those on electronic media in a timely manner.

   - Departing officials and employees shall contact the FEMA Records Officer and request a review of materials proposed for removal from FEMA, including any material on electronic media.

   - The Records Officer shall be informed of any threatened loss or removal of official records.

Chapter 3

Management and Use of Information Systems and Services

Left blank intentionally

3-1 Agencywide FEMA Systems

1. The Federal Emergency Management Agency (FEMA) requires extensive utilization of information resources and services in order to reduce the loss of life and property and protect our institutions from all hazards by supporting a risk-based emergency management program. Agencywide systems shall be utilized to support FEMA applications. Agencywide systems include, but are not limited to, the National Emergency Management Information System (NEMIS), the Integrated Financial Management Information System (IFMIS), the Logistics Information Management System II (LIMS II), the FEMA Wide Area Network (WAN), the FEMA Switched Network (FSN), the FEMA Internet/Intranet and FEMA Electronic Mail systems.

2. The National Emergency Management Information System (NEMIS) is the Agencywide disaster response and recovery system. The system provides FEMA, other Federal agencies, State and local emergency management and emergency services personnel with information related to all aspects and phases of emergency management. NEMIS includes hardware, software, telecommunications and application modules to support operations for:

   - Human Services
   - Infrastructure Support
   - Mitigation
   - Emergency Coordination
   - Emergency Support

   NEMIS integrates new technologies and capabilities with existing FEMA investments, including:

   - Enterprise Database
   - Data Warehouse
   - On-line Reference Libraries
   - Geographic Information Systems (GIS)
   - Imaging, storage and retrieval systems
   - Workflow management and action tracking
   - Electronic signatures and correspondence tracking
   - Interactive Voice Response system

   NEMIS interfaces and accesses other FEMA systems including:

   - Human Resources Management System
   - National Fire Incident Reporting System
   - National Flood Insurance Program (NFIP) database

Prior to development of new applications, all FEMA program offices are encouraged to discuss requirements with the NEMIS Program Management Group (PMG), to preclude duplication.

3. The Integrated Financial Management Information System (IFMIS) provides a single system for tracking and accounting for all FEMA financial transactions.

4. The Logistics Information Management System II (LIMS II) provides material management and inventory systems, maintenance scheduling and histories, and logistics readiness reporting.

5. The FEMA Wide Area Network (WAN) is comprised of an interconnected system of Local Area Networks through a centrally managed Wide Area Network which provides gateways for its users to FEMA's major IT assets and the other nodes on the network.

6. The FEMA Switched Network (FSN) is a switched circuit network that employs Integrated Services Digital Network (ISDN) for voice, data, and video communications required for emergency and day-to-day use. The FSN provides the circuitry infrastructure that supports the FEMA WAN.

7. The FEMA Internet provides access to the world's largest computer network, the Internet. Internet provides access to other Federal agency, State, local government and industry Internet networks. Internet technology is utilized to create the FEMA Intranet for internal FEMA usage.

8. FEMA Electronic Mail systems provide electronic mail capability for internal and external electronic communications.

9. FEMA Standardization Program for office automation provides hardware and software standards for all FEMA systems. The Standardization Program was enacted to ensure that FEMA systems remain interoperable and to build Agencywide core expertise in the FEMA application development software.

10. All Agencywide systems are mandatory for use. Specialized program office requirements, which cannot be met through the established Agencywide systems or standards, shall be approved by the Information Resources Board prior to development, implementation, operation, or procurement.

3-2 Telecommunications Systems and Services

Overview

1. This chapter establishes the Federal Emergency Management Agency's (FEMA's) procedures for telecommunications systems and services as a component of the Information Resources Management (IRM) Program, and assigns responsibilities for IT implementation. The provisions of this chapter apply to all FEMA organizational elements in headquarters, regions, and field establishments engaged in the acquisition, management, and use of voice and data communications. These provisions also apply to other Federal, State, and local government agencies, and contractors performing activities that meet FEMA mission requirements.

2. This chapter describes the overall consolidated procedures for requesting voice communications services, authorizing assignment of those services, managing, and using communications. The separate sections for telephone service, Telecommunications Information Management and Control System , voice mail, cellular telephones, pagers, and Telecommunications Service Priority (TSP) System delineate procedures for specific voice and data communications. Circuits carrying classified voice or record traffic, including military, and fire detection or other dedicated alarm circuits are excluded.

Responsibility

1. The Chief Information Officer (CIO), is responsible for overall management and operation of FEMA's communications services. ITS is responsible for the following:

   - Managing network services provided by FEMA, including evaluations of network utilization and system performance and reconfiguration of services to accommodate FEMA's emergency response requirements.

   - Providing network interoperability by performing technical reviews of all service requests, implementation plans, and procurements that will connect to or make use of FEMA Information Systems Telecommunications Program services.

   - Providing centralized network assistance to FEMA Switched Network nodes for matters relating to network services, operations, management or administration.

   - Administering and coordinating the National Security/Emergency Preparedness (NS/EP) invocations from FEMA, the States, or in support of the Federal Coordinating Officer, during an emergency; and coordinating with the National Communications System (NCS) to implement Telecommunications Service Priority (TSP) in support of NS/EP invocations.

   - Providing for submission of TSP requests to the Office of the Manager, NCS (OMNCS), for issuance of a TSP authorization code.

- Managing the centralized ordering of all communications services, which includes issuing, tracking, monitoring, and verifying completion of all communications service orders.
- Issuing telephone calling cards agencywide.

2. Associate Directors, Administrators, Inspector General, Regional Directors, Office Directors, Federal Coordinating Officers are responsible for and shall be held accountable for:
   - Implementing FEMA's communications policy and procedures,
   - Identifying organizational requirements and providing funding for procurement of telecommunications services, and
   - Designating the Administrative Telephone Officers (may also be identified as the Local Ordering Official) to support and provide services to users in the respective FEMA locations.
3. Administrative Telephone Officers are responsible for communications services and support at the respective FEMA locations.
4. LAN Administrators are responsible for local area network services and support to their respective organizations.
5. Authorized users are responsible for using communications resources for authorized business purposes only; to be familiar with the requirements as outlined in this document; and, to report suspected violations to their managers.

Authorized Use

1. FEMA procures, assigns and authorizes use of communications services to meet FEMA mission requirements. FEMA also requires compliance with government regulations on the authorized use and assignment of telecommunications resources. Descriptions of authorized use include FEMA personnel, FEMA contractors, and other Federal agency, State and local Government personnel who are performing FEMA directed activities. The guidance covers use of hardware, telecommunications services and personal calling. The term "Telecommunications Services" includes hardware and services for telephones, cellular phones, voice mail, FTS2000 telephone credit cards, pagers, data communications, facsimile systems, INMARSAT and other satellite services, and the FEMA Local Area and Wide Area Networks.
2. Those telecommunications services not covered under government guidelines for procurement purposes (radio, video and television equipment and services) will be administered by FEMA in the same mode as those covered services for the purpose of authorizing use and managing and reviewing programs and systems.

3. FEMA's implementation of these regulations follow:

   - The GSA Mandatory-for-Use Program. GSA requires that standard telecommunications services be supplied through the FTS2000 and local services programs. FEMA has developed network systems that integrate FTS2000, and FEMA's exempted services. The implementation and design of FEMA's integrated telecommunications network ensures that GSA's programs are fully utilized as required by the Mandatory-for-Use Program.

   - FEMA Mandatory-for-Use Program. FEMA has identified mandatory for use systems for telecommunications. Telecommunications are provided through the FEMA Switched Network, the FEMA LAN/WAN, and the FEMA Internet/Intranet. Mandatory use provisions will be met when ordering services through the FEMA System Administrators or Administrative Telephone Officers.

   - Eligibility for Authorized Assignment and Use. All FEMA employees, contractors, other Federal agencies, voluntary organization personnel, State and local government employees, who are assigned to FEMA facilities or who perform activities to meet FEMA mission requirements or while performing FEMA directed activities, may be authorized to use FEMA provided telecommunications services. The use of these services shall be deemed necessary for the performance of the jobs. An authorized FEMA official, such as an employee's supervisor or a contractor's Contracting Officer, shall certify eligibility and assign appropriate resources.

4. Authorized use of FEMA communications services is limited to the conduct of official Government business, and for the conduct of those activities the Agency determines are necessary and in the interest of the Government.

5. Official telecommunications service usage may include emergency telephone calls and other calls the agency determines are necessary and in the interest of the government. Personal calls may be authorized if they do not affect the performance of official duties; are of reasonable duration and frequency; and cannot be reasonably made at another time. Federal Register Vol. 32. No. 213, dated November 4, 1987 clarifies that this category of information system (IS) usage may include long distance calls and multiple calls as necessary. Examples of IS usage which may be authorized include:

   - Calls to home or to a doctor if an employee is injured or becomes sick at work.

   - An employee traveling on business is delayed by transportation problems and needs to notify family.

   - An employee traveling on business is allowed to make a brief call home, but not more than an average of one call home per day.

- An employee may make a brief daily call to speak to a spouse or minor children or those responsible for the children.
- An employee may make a brief call to locations within the local commuting area that can be reached only during working hours, such as a bank or physician.
- All FEMA service users are responsible for ensuring that authorized use of telecommunications services reflect the least cost to the Government. Therefore, users assigned cellular or satellite telephones may use these services only if lower cost alternatives are unavailable.

6. Willful and repetitive unauthorized use of telecommunications resources may result in appropriate administrative, civil or criminal actions. Appropriate administrative actions may extend up to and include suspension or dismissal, civil or criminal procedures. Examples of unauthorized use of communications resources includes:

   - Causing FEMA to incur costs associated with any activity that is not authorized, official FEMA business;
   - Making unauthorized long distance calls with the intent of later reimbursing the Government;[1]
   - Recording or listening-in on conversations except as exempted in the Privacy Act;
   - Making unauthorized use of call detail reporting data;
   - Using the telephone or other communications resource to threaten, harass or otherwise cause harm to another individual, group or facility;
   - Use of a modem on any system which is also connected to a FEMA network;
   - Accessing or attempting access to computer systems, voice mail systems or local area networks to which the caller is not an identified and authorized user; and,
   - Using FEMA provided communications resources to conduct personal commercial business is prohibited.

7. Collect calls for official business purposes are strongly discouraged. The Information Technology Services Directorate provides assistance in developing alternative services to collect calls, such as FTS2000 Credit Cards and 800 Service, should a toll-free calling capability be required.

[1]FEMA allows reimbursement of personal calls made on cellular telephones, when no other calling options are available. This exception is necessary due to the nature of disaster response environments. Prior coordination with the Telecommunications Support Staff is recommended.

8. Communications services usage information are collected on a monthly basis in the form of call detail reporting (CDR) and from billing statements submitted by service providers. This information is designed to provide managers with monthly organizational reports, down to the branch level, which provide detailed accounting for the cost of telephone services incurred by the respective organizations. These summary reports serve as the basis for the billing process of various FEMA and tenant organizations.

9. Requests for communications systems and services shall be made to the Administrative Telephone Officer unless otherwise noted.

10. All requests shall include a short justification of need for the service based on official duties and shall be signed by an authorizing official.

11. The Local Ordering Official shall periodically provide itemized bills for each user's review. Users shall verify that all charges are proper. If charges are listed that were not made by the user, report this to the Local Ordering Official.

12. FEMA may authorize personnel to utilize FEMA telecommunications assets from temporary facilities, such as Disaster Field Offices or the employee's home in order to perform temporary job assignments. This includes, but is not limited to assignment and use of cellular phones, calling cards, personal computers, remote Internet access and remote cc:Mail access. All asset assignment justifications for use at temporary facilities shall be reviewed by the authorizing official at a minimum of every 6 months for re-authorization.

13. All users shall return telecommunications systems and hardware to the Local Ordering Official upon completion of temporary facility assignments, upon request by an authorized official or upon terminating FEMA service.

Purchasing via the Telecommunications Information Management and Control System (TIMACS)

1. Telecommunications services and facilities shall be ordered through the FEMA TIMACS. In addition, all ordering and invoicing for moves, changes or disconnects of circuits, terminals, and interface equipment shall be processed through the system.

2. All requests for communication services shall be made through the Local Ordering Official. Requests are submitted on FEMA Form 85-51, Telecommunications Service Request; TSP requests are submitted on Standard Form 315, TSP Request for Service Users. Requests that cannot be entered into TIMACS are to be faxed to the NNOC/Contract Services Center, (540) 542-2628. The Local Ordering Officials are:

   - FEMA Headquarters: Headquarters Information Technology Service Center (ITSC) Staff;

   - Regional Element and MERS Detachments while at their respective Federal Regional Center: Information Systems Managers or Communications Managers;

- Mount Weather Emergency Assistance Center (MWEAC): NNOC/Contract Services Center, Bldg. 431; and
- National Emergency Training Center: Facilities Service Analyst.

3. In a presidentially declared disaster or special event, requests for telecommunications services shall be processed in accordance with the memorandum of understanding between FEMA and GSA that states FEMA assets are to be used first to the extent possible. Provisions of the TIMACS is to be followed to the extent practical during disasters. Requests for service and entry into TIMACS may be faxed to the MWEAC Help Desk, (540) 542-4000. A Federal Coordinating Officer (FCO) has the authority to assign and authorize the temporary use of any FEMA information asset to support specific disaster response efforts. Users, who may be assigned temporary use of FEMA information services and assets by the FCO, include FEMA, other Federal agencies, State and local governments, volunteer and contractor personnel working under the FCO's direction to support the disaster relief effort. The FCO shall ensure that the assigned services and assets are accounted for and returned to FEMA when their use is no longer necessary. When an FCO assigns temporary use of FEMA assets, the FCO shall ensure that the obligation documents and invoices for emergency communications support are provided to ITS. ITS shall maintain a record of all FEMA communications costs.
4. FEMA forms may be obtained from the Printing and Publications Division, Operations Support Directorate. Standard Forms may be reproduced as needed.

Telephone Calling Cards

1. Telephone calling cards are to be used for official government business long-distance calls in lieu of commercial calling whenever government services are not available. Telephone calling cards utilize the government FTS2000 network for call completion in compliance with GSA's mandatory use provisions.
2. All calling card requests shall include a short justification of need for the calling card based on official duties signed by the Local Ordering Official.
3. Requests for calling cards shall be directed to the NNOC/Contract Services Center, (540) 542-2628. The calling card shall be issued to the employee within 10 working days.
4. Telephone calling cards shall be used for the conduct of official government business only.
5. Telephone calling card numbers are subject to theft. Extra caution is required to safeguard the card to prevent the number from being seen or overheard by bystanders.
6. If a calling card is lost or stolen, report the incident to an Administrative Telephone Officer immediately. The Administrative Telephone Officer shall take action to void the card.
7. The Administrative Telephone Officer shall provide a monthly itemized bill for each user's review. Users are required to verify that all calls were proper. Report promptly to the Administrative Telephone Officer any billing for calls that were not made by the card holder.

8. Employees are reminded not to leave a calling card unattended at any time or leave the card exposed in a vehicle, restaurant, office, social event, plane or train.

9. Employees are prohibited from lending the card to anyone or allowing unauthorized use of the card.

10. Do not use the calling card when government telephones are available.

Paging Devices and Cellular Telephones

1. During normal operations, the requester contacts the Administrative Telephone Officer for the price of pager/beeper and cellular telephone to be requested. The FEMA Form 40-1 is prepared for the cost amount, cost for losses and upgrades, maintenance, and number required. The FEMA Form 40-1 is forwarded to the NNOC/Contract Services Center, Bldg. 431, Room 114, along with the Service Request for entry into TIMACS. The equipment is delivered to the Administrative Telephone Officer for acceptance, recording of identification numbers, and issuance.

2. During disaster/incident operations, the designated Administrative Telephone Officer shall be responsible for determining the number of pagers/beepers and cellular telephones required in support of the operations of the Disaster Field Office (DFO). The request is forwarded to the MWEAC Help Desk, or faxed to (540) 542-5430 for issuance from in-stock supply or ordering. If FEMA is unable to supply requested services, the Administrative Telephone Officer shall request assistance from the General Services Administration (GSA). GSA will pass the request to the FEMA TIMACS office. When equipment is received on site, it shall be inventoried and controlled through hand receipt. At the completion of operations of the DFO all equipment shall be accounted for and inventory forwarded to the TIMACS office for disposition instructions.

3. To initiate the funding and billing process, the respective office prepares FEMA Form 40-1 for purchasing, maintenance, and replacement of equipment that the office shall require at the beginning of the fiscal year. Requests for additional equipment required during the fiscal year shall be forwarded in memoranda to the Administrative Telephone Officer, if funds are in place, or by a FEMA Form 40-1, if funds are not in place. Invoices are sent monthly from TIMACS to the respective office for certification or noncertification. The office shall check each invoice for inaccuracies, which shall be noted and returned for challenge and correction.

Teleconference and Video Conference

1. FEMA provides several types of teleconferencing capabilities. These include both audio and video teleconferencing and combined conferences where some participants are an audio-only link while other participants use video links. Video conferences may utilize a variety of media including still image video, graphics, and motion video. Regional and Field facility staff are encouraged to contact their local Information Systems staff to ensure utilization of additional capabilities that may be available at the local site.

2. **Audio-Only Conferences**. These conferences consist of three or more sites (the number of participants at each site can vary) and can be accomplished using a variety of existing capabilities.

3. **Small Conferences**. The originators of conferences that involve three sites can establish the teleconference through the use of the conference feature on many of the office telephones within FEMA. To accomplish this, the following procedures should be followed:

    - The originator should dial the telephone number at the second site and establish the telephone call.
    - They should request the participants at the second site to mute their microphones if possible.
    - The originator should conference in the third site, using the procedures appropriate for the telephone set being used.
    - After the conference call is completed, all participants should hang up.

4. **Large Conferences**. FEMA has two types of conference bridge capabilities which may include operator assistance, when desired. Meet-Me conferences allows participants to meet via telephone at a predetermined time by calling a pre-established conference number. Operator-assisted conferences utilize FEMA Operators to connect users to the conference.

5. **Meet-Me conference** procedures are as follows:

    - The originator contacts the FEMA conference operator (202-566-1600, ext. 3340) and gives their name, date and time of the planned teleconference, the duration of the call, and the number of participants.
    - The operator will provide the originator with a unique conference identification (ID) number and the telephone number to call into the conference.

- The originator contacts the participants, notifies them of the date and time of the conference and provides them with the conference ID number and call-in number. The conference operator may perform this coordination, upon request if the originator provides all pertinent information to do so.

- On or just prior to the scheduled starting time of the conference call, the originator and all participants should call the conference bridge number. Once connected to the conference number, the callers will be required to enter the conference ID number. If the proper number is entered, the caller will be added to the conference. If an incorrect number is entered, the caller will default to the operator and will be manually put into the correct conference.

- If the caller experiences trouble, they should contact the operator at (202) 566-1600, ext. 3340, and ask for assistance.

- At the starting time, the originator or conference leader should begin the conference. Appropriate meeting courtesies and practices may be covered by the originator or designated conference leader. All participants should be encouraged to mute their microphones except when they are speaking.

- The conference leader is responsible for ensuring that the conference is completed on or before the predetermined completion time. (The conference bridge used for the conference may have been scheduled for another teleconference.) If additional time is required, the leader should contact the operator (202-566-1600, ext. 3340) to confirm additional availability.

6. **Operator-assisted teleconference** procedures are as follows:

   - The conference originator should contact the FEMA conference operator (202-566-1600, ext. 3340) and give their name, the date and time of the planned teleconference, the duration of the call, and the names and telephone numbers of the participants.

   - The originator will contact the participants and notify them of the date and time of the conference and provide them with the conference date and time. The conference operator may perform this coordination upon request.

   - At the appropriate time before the start of the conference, the operator will telephone the participants and add them to the conference bridge. When all the participants are on the bridge (targeted to be the predetermined starting time), the operator will add the originator, call the roll, and then give control of the conference to the originator or conference leader.

- At the starting time, the originator or conference leader should begin the conference. Appropriate meeting courtesies and practices may be covered by the originator or designated conference leader. All participants should be encouraged to mute their microphones except when they are speaking.

- During the conference, if a participant is disconnected or experiences any trouble, they should contact the operator at (202) 566-1600, ext. 3340, and ask for assistance.

- At the conclusion of the teleconference, the participants should hang up to conclude the call.

7. **EIDA Audio Conferences**. These conferences are originated from the EIDA conference room at Headquarters and may be associated with a video teleconference or other complex audio-visual and multimedia tools:

   - The conference originator should contact the FEMA conference operator (202-566-1600, ext. 3340) to coordinate a teleconference as noted above.

   - The conference coordinator must also contact the IT Service Center (202) 646-4357 to advise them of the date, time, and all pertinent conference information about the planned conference in the EIDA, so that technical support will be available if required.

   - At the start of the conference the conference leader should remind everyone to mute speakerphones except when talking.

   - The conference leader is responsible for ensuring that the conference is completed on or before the predetermined completion time. If additional time is required, the leader should notify the operator as soon as possible.

   - The operators will monitor all EIDA conference calls for performance problems in coordination with the ITS support technician present in the EIDA.

8. **Video Conferences**. Video conferences must occur at sites that have video teleconferencing equipment. Currently, the FEMA sites which have this capability include:

Location	FSN Video Number	FSN Voice Number
HQ EIDA	6-670-8801	6-651-3688
NECC, MWEAC	6-683-8801	6-631-6100
Maynard MERS VSAB	6-561-8801	6-531-5519
Maynard MERS Mobile	6-521-7250	6-531-5519
Thomasville MERS VSAB	6-564-8801	6-534-4770
Thomasville MERS Mobile	6-524-7251	6-534-4770
Denton MERS VSAB	6-566-8801	6-536-5321
Denton MERS Mobile	6-526-7252	6-536-5321
Denver MERS VSAB	6-568-8801	6-538-4828
Denver MERS Mobile	6-528-7253	6-538-4828
Bothell MERS VSAB	6-560-8801	6-530-4445
Bothell MERS Mobile	6-520-7254	6-530-4445
Kansas City, Reg. VII	6-587-8802	6-537-7508
Chicago, Reg. V	6-585-8802	6-535-5557
San Francisco, Reg. IX	6-589-8802	6-539-7150
MATTS Mobile	6-660-7255	6-631-6100
NETC, Emmitsburg	6-655-8802	6-653-1183
MWEAC Conf/Trng Center	6-654-8861	6-630-2266

Call NECC, MWEAC, for conferences of three or more users (6-631-6100):

- To establish a video teleconference with another site or sites within FEMA, the originator should contact the site video teleconferencing manager. They will assist the originator with the conference call.
- To establish a video teleconference with a site(s) outside FEMA, the originator must schedule a FEMA site through the site administrator. For a video conference involving three or more sites, a conference bridge must be used. FEMA's conference bridge is managed and operated by the National Emergency Coordination Center.
- For a two-site conference, the user should dial the remote video system's telephone number using the local site's video system.

All Division-level and higher conference calls will be monitored for quality and identification of extemporaneous noise. Any situation that results in negative customer service will be reported immediately to ITS.

Left blank intentionally

3-3 Voice Mail

Overview

Voice mail is implemented through the FEMA Switched Network (FSN). Voice mail features include, but are not limited to, the capability for telephone messages to be received, reviewed, saved, retrieved, and sent in a single call from any touch-tone telephone on a 24-hour basis. Each voice mail user is assigned a mailbox for storage of personal greetings and incoming messages. The voice mail can be customized to meet the unique needs of the users.

Procedures

1. Voice mail may be used in FEMA subject to the following criteria:

    - Staff will answer the telephone whenever possible.
    - Callers may be forwarded to voice mail after official duty hours.
    - Voice mail will not be used to screen calls.

2. FEMA staff shall be responsive to the public and thus may use voice mail as an enhancement to existing communication systems in providing the public rapid access to available Agency information or personnel. Voice mail may be used to make information available through voice bulletin boards and to make other public telecommunications announcements.

3. Initial service requests and voice mail capability requests shall be processed at the organizational component's location by the designated Administrative Telephone Officer.

4. Upon activation of voice mail, staff shall provide the following information on the personal greetings:

    - Identify yourself and your organizational element.
    - Give callers the option to speak directly to an individual.
    - Allow the caller to press "0" at any time during the call to speak to an individual.
    - Give length of expected absence.
    - Include a statement such as "Please leave a message at the tone."

5. Voice mail users shall be held accountable for checking their mailboxes regularly during duty hours to respond in a timely manner and to minimize the number of messages stored in the system.

6. Answering machines should not be utilized within FEMA when voice mail service is available.

Left blank intentionally

3-4 National Security/Emergency Preparedness (NS/EP) Program

Procedures

1. This section provides guidance and procedures for FEMA's usage of the TSP system. The provisions of this section apply to all FEMA elements.

2. The TSP system is the regulatory, administrative and operational system that establishes the framework for authorizing and enabling for the priority provisioning or restoration of NS/EP telecommunications services during crises. Only NS/EP telecommunications services are eligible for TSP assignments. NS/EP telecommunications services are those required to maintain a state of readiness or respond to and manage events or crises (local, national, or international), which cause or could cause:

    - Injury or harm to the population;
    - Damage to or loss of property; or
    - Degradation or threat to the NS/EP posture of the United States.

3. In the context of the TSP system, a telecommunications service is a communications capability specified by a user that can be restored or provisioned on a priority basis by the vendor providing the service. A TSP service shall meet the following requirements:

    - The service (e.g., circuits, antennas, etc.) qualifies as NS/EP and supports an NS/EP function;

    - The service may be provided by one or more prime vendors and each may have any number of subcontractors;

    - The service satisfies the requirements of a TSP category, subcategory, and criteria and is eligible for a priority; and

    - Users may request priority treatment on a service for which the selected vendor is capable of providing priority treatment.

4. TSP users include Federal, State, local, and foreign governments, volunteer organizations, and private industries that have NS/EP telecommunications functions for which TSP assignments have been requested or assigned. There is, however, one distinction in access to the TSP system between Federal Government users and other users. Federal Communications Commission (FCC) Report and Order 88-341 mandates that non-Federal users be sponsored by a Federal department or agency. The purpose of sponsorship is to ensure that an authorized Federal official confirms that a requirement merits a priority assignment. The NCS is responsible for sponsoring State and local government agencies.

5. The TSP system was established by the FCC in Report and Order FCC 88-341, dated November 17, 1988. The Report and Order established the TSP system for NS/EP as an amendment to Part 64 of the Commission's Rules and Regulations (Title 47 CFR, Chapter 1). Companion documents, National Communications System Directive (NCSD) 3-1 and

NCS Manual 3-1-1, July 5, 1990, prescribe policy, procedures, and provide guidance for all TSP users.

6. The TSP system comprises two distinct requirements:

   - Restoration. Restoration is the act of repairing or returning to service one or more telecommunications services that have experienced a service outage or are unusable for any reason, including a damaged or impaired telecommunications facility. Such repairs or returning to service may be done by patching, rerouting, substitution of component parts or pathways, and other means, as determined necessary by a vendor. A restoration requirement results in an Essential TSP request.

   - Provisioning. Provisioning is the act of supplying new telecommunications services to a user, including wiring, and equipment. Provisioning includes altering the state of an existing priority service or capability. (Wiring and equipment may not be provided by the carrier on a regulated basis.) A provisioning requirement normally results in an Emergency TSP request.

7. The TSP system includes two categories: Emergency and Essential.

   - Emergency. Emergency services are new services so critical as to be required to be provisioned at the earliest possible time without regard to the user's costs of obtaining them. Emergency services directly support or result from a specific NS/EP function, such as response to a Federal, State, or locally declared disaster or emergency.

   - Essential. Essential services are all other TSP services assigned either restoration or provisioning priorities within the TSP system. Essential services are generally applicable only to restoration priorities. Such services, however, may also be assigned provisioning priorities.

   - Essential Subcategories. Each of the following Subcategories has specific criteria defining the kinds of functions that a service shall support to qualify for the subcategory:

     * Subcategory A, National Security Leadership
     * Subcategory B, National Security Posture and U.S. Population Attack Warning
     * Subcategory C, Public Health, Safety, and Maintenance of Law and Order
     * Subcategory D, Public Welfare and Maintenance of National Economic Posture

8. Invocation. Invoking NS/EP treatment refers to notification to a vendor that a TSP service is so vital it needs to be expeditiously provisioned without regard to cost. Invocation is applicable only to provisioning; not to restoration. The first step in obtaining a provisioning priority is to obtain authorization to invoke NS/EP treatment from the designated invocation official.

9. Invocation Officials. TSP regulations state that invocation officials shall be the head or director of a Federal agency, commander of a specified military command, chief of a military service, commander of a major military command, or the delegates of any of the foregoing. The Director of FEMA is the Agency's designated Invocation Official for NS/EP TSP provisioning of telecommunications services. The Director has delegated invocation authority to the Associate Director and Deputy Associate Director, ITS. Neither FCOs nor FECCs have automatic invocation authority based on their assignment.

10. The following forms, which may be locally reproduced, are prescribed for use in the TSP system:

    - Standard Form (SF) 315, TSP Request for Service Users
    - SF 316, TSP Service Order Reporting
    - SF 317, TSP Action Appeal for Service Users
    - SF 320, NS/EP Invocation Report
    - Priority Action Notice (no form number)

11. FEMA TSP Procedures. The Information Technology Services Directorate, Operations Division (IT-OP) staff shall determine if the service meets NS/EP requirements; is eligible for a TSP assignment; and for which priority the service qualifies. This determination shall be based upon the TSP system categories, Subcategories, and criteria. If the requested service satisfies the TSP requirements, IT-OP staff completes SF 315, TSP Request, and forwards it to the NCS TSP Program Office for issuance of a TSP Authorization Number. Upon receipt of the TSP Authorization, IT-OP staff provides it to the appropriate vendor for service.

    - To invoke NS/EP treatment, the FCO submits the TSP request to the NNOC who will obtain authorization from the designated invocation official. The NNOC shall then request a provisioning priority from the NCS National Coordinating Center (NCC). After the NCC assigns the provisioning priority, the NNOC conveys it to the FCO, who notifies the vendor, either verbally or on a service order. The invocation occurs when the vendor receives the provisioning priority. Upon receiving the provisioning priority, the vendor shall make its best effort to meet the provisioning requirement.

12. Provisioning and Invocation.

    - Requirement. The user's first step in obtaining a provisioning priority is to obtain authorization to invoke NS/EP treatment from the designated invocation official. Invocation is applicable only to provisioning; not to restoration. If the user has been able to adequately plan for a service, the vendor (e.g., telephone company) can normally meet the service due date following normal business procedures. However, when the user requires a TSP service to be provisioned faster than the vendor's normal procedures allow, the user shall obtain invocation authority from the designated invocation official.

- Invoking. Invoking NS/EP treatment refers to notification to a vendor that a TSP service is so vital it needs to be expeditiously provisioned. To invoke NS/EP treatment, a service user shall first obtain authorization from the designated invocation official and then request a provisioning priority from the NCS National Coordinating Center (NCC). Once the NCC assigns the provisioning priority and the user receives it, the user conveys it to the vendor, either verbally or on a service order. The invocation occurs when the vendor receives the provisioning priority. Upon receiving the provisioning priority, the vendor shall make its best effort to meet the provisioning requirement.

3-5 Telecommunications Networks and Network Management

Overview

1. FEMA's telecommunications networks are managed through the National Network Operations Center (NNOC), a specialized operations center comprised of an information systems control staff and automated management systems. These management systems remotely administer, assess, and restore services for all FEMA communications networks, wide area networks, satellite systems, private branch exchanges (PBXs), T-1 multiplexors and network bandwidth management. The NNOC provides full time oversight of the operational status of FEMA's information system resources, i.e., telecommunications, wide area networks, warning, ADP systems and system connectivity. The NNOC directs system configuration or other actions as deemed necessary to compensate for critical losses until a failed system is restored. To facilitate restoration of critical capabilities, NNOC personnel recommend the dispersal of equipment, personnel, mobile units or other support as needed.

2. The NNOC serves as the point of contact between FEMA and the National Telecommunications System (NCS), National Coordinating Center (NCC) for NS/EP, for circuit initiation and restoration. The basic objective of the NNOC is to provide a central point from which FEMA's varied telecommunications, warning and ADP resources are effectively managed on a day-to-day basis as well as directed and controlled in crisis situations and national emergencies. This includes assistance as necessary or required to meet telecommunications and ADP resource needs of national, regional, State and local governments in crisis situations.

Responsibility

1. The National Network Operations Manager is responsible for the management, operations and maintenance of FEMA telecommunications networks.

2. Responsibilities of the NNOC include:

   - Centralized management of the FEMA Switched Network (FSN).
   - Management, administration and operation of the FEMA Wide Area Network (WAN) and router system.
   - Point of contact for operational status of FEMA information systems.
   - FEMA's network control for trouble-shooting, repair, and status of all FEMA information systems.
   - Centralized telecommunications service ordering for FEMA.

- Oversight for the following telecommunications services: T-1 bandwidth allocation, satellite connectivity, telephone services requests, billing, and central telephone operator services, including FEMA's information and location services to the public.
- Management and administration of FEMA's information systems billing and funding.
- Agencywide Help Desk for information systems support.

Procedures

1. All network management issues shall be referred and coordinated with the NNOC.
2. Requests for assistance for network and other information technology related issues are to be referred to the MWEAC Information Technology Services Center (ITSC) Help Desk by dialing FSN 630-4000 or (540) 542-4000.
3. The ITSC Help Desk shall either take care of the issue directly or refer the caller to the appropriate subject matter expert.
4. FEMA telecommunications users at Headquarters may call the Headquarters Services Branch at (202) 646-3635 during official duty hours for all telecommunications related issues. During non-duty hours, users may call the ITSC Help Desk at MWEAC for 24-hour assistance.

3-6 Local Area Networks and Network Management

Overview

1. This chapter establishes FEMA's procedures for the use and management of local area network (LAN) systems. The procedures herein apply to all organizational elements in headquarters, regions, and field establishments which use the FEMA LAN.

2. FEMA centrally manages the wide area network (WAN) through the National Network Operating Center. LANs are connected to the WAN to ensure agencywide connectivity. The individual offices, directorates, administrations and regions are responsible for managing their respective LANs, which support office automation, electronic mail and specialized applications.

3. The Information Technology Services Directorate provides LAN management and administration for those organizations who so request. The Headquarters Service Center provides these services to those located in Headquarters.

4. FEMA LANs are configured, operated, managed and maintained by designated System Administrators who coordinate their activities with the NNOC to ensure FEMA-wide interoperability through compliance to FEMA naming and addressing conventions, and hardware and software standards established by FEMA.

Procedures

1. Requests for LAN access will be made to the local System Administrator.

2. All requests shall include a short justification of need for the service based on official duties signed by the individuals' supervisor or other authorizing official.

3. All services on the FEMA LAN will be used for the conduct of official government business only.

4. Access to the FEMA LAN provides additional access to other FEMA systems through the WAN. FEMA's LANs are password protected. However, improper disclosure of user passwords may result in significant damage by unauthorized electronic intrusion. Therefore, users will comply with FEMA policy and procedures for computer security.

5. Employees are reminded not to leave a computer actively connected to sensitive information in an unattended mode.

6. The "lending" of passwords or the unauthorized use of LAN assets is prohibited.

Left blank intentionally

3-7 Automated Data Processing Systems and Services

Overview

1. This subchapter describes the overall consolidation procedures and guidelines for managing, procuring and using automated data processing systems and services (including office automation systems), authorizing assignment of those systems and services, and for assigning responsibilities for their implementation. Systems carrying operational classified data or record traffic are excluded.

2. The provisions apply to all FEMA organizational elements in headquarters, regions, and field establishments (including disaster field offices) engaged in the acquisition, management, and use of automated data processing (ADP) systems and services. These provisions also apply to other Federal, State, and local government agencies, and contractors using ADP systems and services in performing activities that meet FEMA missions or requirements.

3. In each organizational element, liaison staff will be designated as point of contact for information technology resources, including office automation software and hardware, software licensing accountability, and the information technology standardization program. These include network systems and stand-alone systems. At headquarters, an ITS designee will be designated liaison for each organizational element's system for which ITS has responsibility.

4. A current inventory will be maintained of all information technology resources (hardware, circuits, and software systems) in compliance with OMB Circular A-130. Included are programs operated agencywide or organizational element's own information technology equipment (including stand-alone PCs) as well as non-Agency equipment operated via teleprocessing at contractor facilities or at other Federal agencies.

5. Organizational elements are encouraged to affix protection seals on the processing units of PC/Workstations to provide for accountability and integrity of the information technology resources.

Responsibility

1. Associate Directors, Administrators, Inspector General, Regional Directors, and other Office Directors are responsible for:

   - Complying with FEMA's information technology procedures;
   - Ensuring that employees are aware of and understand their responsibilities;
   - Designating an information technology liaison to represent the local organization on information technology task forces and working groups; and

- Designating an information technology liaison (may be the system network or E-mail administrator) and alternates to support and provide IT maintenance for the organizational element, except for those organizational elements where ITS provides centralized service and maintenance.

2. Associate Director, Information Technology Services Directorate, is responsible for:

   - Overall management and operations of automated data processing systems, and the effective implementation of their application;

   - Coordination and maintenance of users' central systems; and

   - Overall functionality of agencywide systems in servicing, supporting, and monitoring system performance for load capacity and for database backups.

3. System Administrator is responsible for:

   - Support services, maintenance, and operation of enterprise-wide systems at the local level. These include user identification, passwords, installation of upgrades, and system functionality, performance, and backups.

   - Assessing the performance of computer equipment utilized on the LAN. Outdated or surplus computer equipment should be identified and disposed of as described in Subchapter 3-10.

4. Users are responsible for:

   - Using systems in an informed way,

   - Conforming to etiquette, customs, and courtesies, and

   - Complying with Federal regulations and FEMA's policies.

Procedures

1. FEMA procures, assigns and authorizes use of ADP systems and services to meet FEMA mission requirements. FEMA also requires compliance with government regulations on the authorized use and assignment of these resources. FEMA's implementation of these regulations follow:

   - Mandatory Programs. GSA requires that information systems and services comply with open systems standards, energy star programs and accessibility programs.

   - FEMA Mandatory Programs. FEMA has implemented several Agencywide systems which are mandatory for use. These mandatory use systems are the National Emergency Management Information System (NEMIS), the Integrated Financial Management System (IFMS), the Logistics Information Management System II (LIMS II), the FEMA Local Area Network/Wide Area Network (LAN/WAN), the FEMA Internet/Intranet and FEMA Electronic Mail systems.

- Eligibility for Authorized Assignment and Use. All FEMA employees, contractor, other Federal agency, State and local government employees assigned to FEMA facilities or performing activities to meet FEMA mission requirements or while performing FEMA directed activities are eligible for authorized use and assignment of FEMA provided ADP systems and services. The use of these services will be necessary for the performance of their job. An authorized FEMA official will certify eligibility and will assign appropriate resources.

Authorized Use

1. Authorized use of FEMA ADP systems and services is limited to the conduct of official Government business, and for those activities the agency determines are necessary and in the interest of the Government. Official usage may include writing a quick electronic mail message or memorandum to individuals or organizations that can be reached only through these media. Examples of those activities that the Agency determines as necessary and in the interest of the Government include writing an electronic mail message in order to coordinate activities while traveling or composing a short note to school officials explaining why a child was absent from school. All such activities will be short, necessary and very infrequent. All files and electronic records on FEMA office automation systems and services are the property of FEMA and can be accessed without notice by the employees' supervisor or other authorized official.

2. Unauthorized Use. Willful or repetitive unauthorized use of FEMA ADP systems and services may result in appropriate administrative, civil or criminal action. Unauthorized use includes:

   - Unauthorized use or malicious destruction of electronic files or records.
   - Misuse or unauthorized disclosure of electronic passwords.
   - Use of non-authorized software or services on FEMA office automation systems such as electronic game software, repetitive access of "hobby" or "social interest groups" through electronic networks, or display of any graphic or image which would threaten, embarrass or otherwise cause harm to another individual or group;
   - Actions that cause FEMA to incur costs associated with any activity that is not authorized, official FEMA business;
   - Costs associated with electronic media or services for unofficial use with the intent of later reimbursing the Government;
   - Access with the intent to read or copy electronic messages or files from other employees' systems without the direct permission of the employee, the employees' supervisor, or in association with an investigation by the Office of Inspector General;

- Unauthorized use of data or information received through FEMA office automation systems;
- Use of any office automation resource to threaten, harass or otherwise cause harm to another individual, group or facility;
- Use of a modem on a computer or system that is also connected to a FEMA network;
- Access or attempts to access computer systems, voice mail systems or local area networks to which the employee is not an identified and authorized user; and,
- Use of FEMA provided office automation resources to conduct personal commercial business is prohibited.

3. Reporting Requirements. Usage information may be collected from FEMA IT systems and services for a variety of management reporting or billing purposes.

4. Energy Star Program Requirements. FEMA ADP systems and services are to be turned off when not in use unless that system is critical to a network service and will remain operable. All monitors and printers with the capability, will be configured to "power down" after a maximum of 15 minutes of non-use.

5. Password Management. Employees will use passwords for most FEMA office automation requirements. Passwords will be protected as sensitive information and will not be shared. Passwords will be periodically changed according to frequency schedules outlined by the Information System Security Office. All information residing on FEMA systems is available for authorized use by FEMA. Personal and private information will reside only on those systems designated as official "Privacy Record Systems."

Purchasing via the Standardization Program

Overview

1. This subchapter sets forth the Agency's procedures for purchasing information technology through FEMA's Standardization Program, which is described in detail in Chapter 5 of this document. FEMA's objective in the acquisition of information technology resources are to:
   - Foster fully competitive procurements in compliance with OMB and GSA directives.
   - Rely on commercial-off-the-shelf (COTS) for information technology software and services to the maximum extent possible.

- Modernize information technology support to ensure system effectiveness and to preclude use of out-dated systems.
- Improve conformance with Federal and Agency standards.
- Document responsibility for the information technology budget.
- Promote effective use of information technology and encourage interoperability.

2. This guidance applies to all purchases or leases of telecommunications and computer software, hardware, and services. This covers new, upgraded or repair parts for computer hardware, software and services. It applies to purchases or leases under new, amended and modified contracts, including all credit card purchases, blanket purchase agreements, interagency agreements, and indefinite delivery indefinite quantity type procurements. The Acquisitions Office will require full adherence to these procedures prior to processing any requisition for procurements.

Procedures

1. Request for purchase of information technology resources will be reviewed by IT prior to submission to the Acquisition Office. ITS will use the agencywide inventory system and the Catalog of FEMA Information Systems as a basis by which to determine whether IT procurement requests for new information technology duplicate existing systems or capabilities.

2. All microcomputers, including personal computers and monitors, will be Energy Star compliant. The Energy Star low-power feature will already be activated when the computer equipment is delivered to the Agency and be of equivalent functionality of similar power managed models. The Energy Star compliant mandate does not apply to existing equipment.

3. All computers and software are required to comply with the Year 2000 Program. Existing systems will be reviewed and made compliant. New systems must be certified as compliant prior to procurement.

4. IT procurements required in the response phase of new disasters and emergencies are exempted **if** the information technology is not available in the Agency's centralized inventory. However, adherence to the Standardization Program is **not** exempted. Office automation hardware and software will be procured, at a minimum, based on the standard suite of baseline software and the standard baseline hardware specifications. Documentation will be submitted to IT following the procurement for accountability.

5. Organizational elements will prepare FEMA form 40-1, Request for Commitment for Services and Supplies, for procurement of information technology resources. When purchasing personal computers (PCs) or software for office automation use, the FEMA Standardization Program requirements will be used. In the project description section of the 40-1, indicate "Standardization Program" specifications. Cost estimates

may be obtained from the General Services Administration's (GSA) Schedule information listed from the Internet (http://www.gsa.gov). Where the Standardization Program cannot be used to procure PCs and office automation software, a complete and thorough justification will be written, including a cost estimate.

6. The 40-1 will include the appropriate concurrence signature lines as follows:

   - 40-1 amount less than $5,000 requires signature of Associate Director, Administrator, Office Director or Regional Director.

   - 40-1 amount greater than $5,000 requires the above signatures and the CIO.

7. Organizational elements will submit the 40-1 with appropriate documentation and signatures to the Information Technology Services Directorate for database processing and CIO signature.

8. ITS will ensure that the 40-1 information is recorded in the database. Any duplicate type IT system or systems that are not included in the Catalog of FEMA Information Systems will be annotated in the database. If the amount is greater than the simplified acquisition threshold, verify that the procurement has been presented to the Procurement Review Board and the IRB.

9. ITS will follow appropriate Integrated Financial Management Information System procedures, submit the 40-1 for appropriate signatures, forward through the Budget office for allocation of funds to the Acquisition office.

3-8 Internet and Intranet

This chapter prescribes guidelines and procedures for the access and use of Internet and Intranet technology at the Federal Emergency Management Agency (FEMA). It also describes responsibilities for its implementation. Guidance in this chapter is applicable to all organizational elements in headquarters, regions, and field establishments.

Overview

1. Internet is a worldwide electronic system of computer networks which provides telecommunications and resource sharing services to government employees, businesses, researchers, scholars, librarians, and students, as well as the general public. It offers access to State and local governments, public and private disaster support organizations, and permits flexibility for communicating public affairs information. The White House has endorsed the use of the Internet in order to make the federal government accessible to the public. FEMA supports the Administration's objectives and is actively pursuing methodologies to increase public access to information through the FEMA Internet server and through the use of electronic reading rooms that support Freedom of Information Act requirements. FEMA utilizes Internet technology to provide services to internal users. FEMA has established a Private Domain Server(s) (PvDS), a Public Domain Server(s) (PDS), Intranet Servers and an Interactive Forum Server (IFS), each with a full set of Internet services as depicted in figure 1.

2. The Private Domain Server has been implemented with a Firewall to provide:

   - secure gateway protection;
   - access to the PvDS and FEMA Intranets, is restricted to authorized FEMA users; and,
   - stringent protection mechanisms exist to preclude external Internet users from accessing FEMA's internal information systems, Intranets and networks.

   A Firewall can be described as components placed between two networks that control passage of only authorized traffic, and is itself immune to penetration. The Private Domain Server allows users within FEMA to access and obtain data internal and external to FEMA.

3. The Public Domain Server provides multi-media capability for exchange of information among Federal Government, State and local governments, private organizations, and the general public. This capability is vital for disseminating emergency information during emergencies and disasters, and for sharing plans and associated emergency management information day-by-day. FEMA information intended for the public, policy information and official FEMA positions are housed on the FEMA Public Domain Server.

4. The Interactive Forum Server (IFS) meets the requirements of program offices for fostering customer partnerships through discussion forums and pre-decisional chat sessions with external customers, and for gathering information or performing interactive functions that may be determined to be more appropriately completed on a server other than the FEMA Public Domain Server. Services include structured, password protected, closed user groups and open, real-time "chat sessions" and interactive forums. The IFS is intended to support program office and emergency community working level efforts that do not include dissemination of FEMA policy or other types of information intended for the general public.

5. Intranet servers are internal FEMA systems that utilize Internet technology to deliver services that are accessible only to those users who are behind the FEMA Firewall. The public, States and other Federal organizations do not have access to the FEMA Intranet. Intranet services are provided through FEMA Intranet Servers. Organizations are encouraged to utilize the Intranet to disseminate information to internal FEMA users. All organizational Intranet pages are to be accessed through the FEMA Intranet Master Index. Intranet pages will not duplicate information available through the FEMA home page.

6. Internet mail addresses are considered publicly available information, as are other employee access information such as work telephone numbers and postal mailing addresses. FEMA Internet Email addresses will be available via the Intranet and the FEMA Public Domain Servers.

7. The FEMA Internet network encompasses primary functions and services: World Wide Web browser, Internet electronic mail (Email), FTP - File Transfer Protocol and Telnet. These functions are bundled in the Internet software implemented at FEMA. The workstation/client software has been distributed to all local sites on the FEMA network with instructions for installation.

8. There is only one FEMA home page; there may be multiple satellite pages. The FEMA home page is resident on the Public Domain Server. Public access to FEMA on the World Wide Web is via http://www.fema.gov. Organizations are encouraged to utilize the FEMA home page for providing access to information about their programs. Some program office applications, such as the National Emergency Information Management System (NEMIS) and some FEMA regional offices, have large information sharing and distribution requirements, targeted to specific external or local audiences, that must be managed directly by the program office. The term "satellite page" is used to describe separate Internet capabilities that meet specific program office requirements of the Agency. FEMA satellite pages will be accessed through the Public Domain Server. Links will be established from the FEMA home page to satellite pages created by authorized program and regional offices. Satellite pages will not duplicate information available through other portions of the FEMA home page.

9. FEMA 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.

10. General guidance will be provided through the FEMA Internet Style Guide (Appendix 3-7.1.b) to ensure consistency in the "look and feel" of FEMA's Internet applications agencywide.

11. Internet and Intranet are for official government business only. "Personal home pages," links to personal home pages and other non-business use is prohibited.

World Wide Web (WWW) Browser

World Wide Web Browser software provides access to the Internet hyper media environment. It provides a capability to browse WWW information by merely pointing and clicking to view pictures, video clips, play sounds, read documents, and easily copy files to a workstation/personal computer (PC).

Internet Email

Internet Email message creation, use, maintenance and disposition must conform to FEMA's policies and procedures contained herein and in Part II, Chapter 3-8, Electronic Mail, of this document. Internet Email is fully integrated with the FEMA wide-area network. Features of the integrated system will place messages from the Internet Email system and from other Email systems into a single user mailbox. FEMA's old Internet Email address convention was "[userid]@fema.gov". The new address formula is:

Firstname.Lastname@fema.gov

(In the case of duplicate names, the middle initial will also be used.)

- Use a signature block at the bottom of Internet Email messages. Some Email systems strip header information from messages, including the sender's Email address. For example, the contents of a signature block: legal name, Email address, and telephone number or postal address.

FTP

File Transfer Protocol software (FTP) allows for connection to and transfer of files to FTP servers on the Internet. Access is often to an anonymous FTP server that allows the connectivity. When using FTP, users are also guests on another organization's systems and should follow basic guidelines:

- For anonymous FTP servers, Log-in as "anonymous" but provide your full Internet Email address where required.
- Avoid transferring large files during peak business hours for the remote system.
- Transfer files (download) to your network server, workstation's hard drive, or diskette, as soon as possible. Before using downloaded files, validate that the executable files do not carry viruses. Do not use infected files and adhere to the procedures described in Chapter 2-4, Information Systems Safeguards in this document.
- Respect copyright and licensing agreements of the files transferred.
- Some anonymous FTP servers require that the name of the firewall or proxy server be provided in order for a file transfer to be initiated. The FEMA firewall is not configured to provide its name. Transfers from these FTP sites may fail.

Telnet

Telecommunications Network (Telnet) software is one of the most powerful capabilities of the Internet. Workstations can be connected as terminals to any system on the Internet. To connect to and use remote computers on the Internet, special communications software must be installed on the user's workstation. When using Telnet to access remote computer systems, users should remember that they are guests on another organization's system and should observe basic courtesies:

- Log-off a remote computer system when finished - maintaining an open connection may prevent others from connecting to that system.
- Read or obtain documentation files when using a system for the first time.
- Be cognizant of the time and resource limitations for the remote system and adhere to IT restrictions.
- Be cognizant that personal opinions expressed in documents on Internet might be mistaken as FEMA's position. A disclaimer may be included in the document, e.g., "The opinions expressed here are my own and do not necessarily represent official policy of FEMA."

Services Available from FEMA Internet Servers					
Service/PC Application	**PvDS**	**PDS**	**Intra-Net**	**IFS**	**Function**
Internet Electronic Mail Software	√			√	**To transmit/receive messages.**
File Transfer Protocol (FTP) Software	√		√	√	**To transfer files via a protocol.**
Telnet Windows Software	√				**To access another computer remotely.**
World Wide Web (WWW) Browser Software	√	√	√	√	**To view, download, or print information in hyper text markup language (HTML) format.**
Interactive Forum Software				√	**Allows interactive electronic discussions between FEMA and emergency management and services organizations.**

Figure 1.

Responsibility

1. Chief Information Officer (CIO), is responsible for overall management and operations of the enterprise-wide Internet/Intranet system, and the effective implementation of IT applications. The National FEMA Webmaster will be designated by the CIO to oversee Internet/Intranet functions agencywide.

2. Associate Directors, Administrators, Inspector General, Regional Directors, and Office Directors are responsible for:

   - enforcing FEMA's Internet/Intranet policy and procedures;
   - ensuring that employees are aware of and understand their responsibility in using Internet/Intranet;
   - authorizing use of interactive forums, authorizing content and the creation of web based applications; and,
   - designating organizational (Domain) Webmasters and/or System Administrators and alternates to support and provide maintenance for the local area networks, except for those organizational elements where ITS provides centralized network service and maintenance.

3. Director, Office of Emergency Information and Media Affairs (EIMA) is responsible for the review of all information which is meant for release to the public on the Internet Public Domain Server, in accordance with established review procedures.

4. The FEMA National Webmaster, Operations Division, ITS is responsible for central coordination and maintenance of user identifications; for management, integration and distribution of Internet software upgrades; for coordination of Internet services and support; for monitoring Internet system performance for load capacity; and for Internet database backups. The National Webmaster is also responsible for the following:

    - Provide guidance to Domain Webmasters and System Administrators on Internet/Intranet implementation issues;
    - Ensure interoperability, integration and overall functionality of the agencywide Internet/Intranet system;
    - Ensure that the system complies with FEMA's policies and government laws and regulations; and,
    - Work with program offices and Domain Webmasters to identify opportunities to utilize Internet/Intranet to facilitate initiatives in the Agency.

5. System Administrators* are responsible for Internet support services, maintenance, and operation of the enterprise-wide Internet/Intranet at the local level. This includes user identification, installation of upgrades, and system functionality, performance, backups and all matters associated with the installation of Internet workstation software, and the operation and maintenance of Internet capabilities at the local site.

6. Domain Webmasters* are responsible for:

    - Working with end users to ensure that the application complies with the "look and feel" of Internet/Intranet interfaces as established by the Agency;
    - Ensuring that all Internet applications are accessible for users who require non-graphical and non-audio alternatives.
    - Ensuring that Internet/Intranet applications used by their organization meets the requirements and mission objectives of their respective organizations; and,
    - Ensuring that all Domain Webmaster mail receives timely responses.

7. Internet System Users are responsible for using Internet in a responsible and informed way, conforming to network etiquette, customs, and courtesies, and complying with Federal regulations and FEMA's policies and procedures.

* The Domain Webmaster and System Administrator may be a combined function.

Procedures

1. Organizational elements that have network connectivity with FEMA Internet addressing and naming conventions will be provided Internet access through the FEMA Firewall. Organizations without this connectivity will be provided access via a FEMA provided telecommunications server located and maintained at Mount Weather.

2. Each organizational element must designate a System Administrator and Domain Webmaster for Internet and Intranet support prior to the initiation of Internet account on the enterprise-wide network.

3. All pages on the Internet and Intranet will identify the responsible person and organization for ensuring accuracy and currency of the information content of the page by placing the person's name and organization in the non-visible code available by viewing the document source. This information may also be placed in the visible portion of the page when this information may be of value to the public.

4. All Internet and Intranet applications will have non-graphical alternatives for users who require adaptive technology. Appendix 3-7.a provides guidance in creating non-graphical and non-audio alternatives. The following developmental rules apply to all FEMA Internet and Intranet applications:

   - Every graphic image will have associated text.
   - Image maps will have an alternate method of selecting options.
   - Include detailed descriptive "comments" with all images.
   - Text transcriptions or descriptions will be provided for all audio clips.

   Internet applications will be developed for use by at least the three largest commercially utilized Browsers and the Agency standard. FTP sites are to be used for disseminating large files and documents.

To Obtain Internet Access

1. Employees may obtain Internet access to meet the requirements of their job. System Administrators will establish the Internet directory information, including user name, voice telephone number, organization identifier, and any associated computer interpretable electronic address that will allow appropriately equipped Federal employees in other agencies to send messages to FEMA employees. The Internet directory must be consistent with the E-Mail directory information. The directory will also include the System Administrator's name and voice telephone number. The directory information will be incorporated into the local FEMA telephone directory.

2. The System Administrator/Domain Webmaster will activate the User Account and will provide the directory information to the National Webmaster for agencywide notification and coordination. Once the user account is established, an Internet address will be designated. Users will have access to Internet address information for employees FEMA-wide and for employees in other Federal agencies. Users must identify themselves with their full Internet address or legal name when using any Internet service.

To Implement Page Access

1. Organizational elements that wish to create their own Internet/Intranet pages or other Internet/Intranet applications must document their requirements and gain authorization for content. General informational pages are to be approved at the Deputy Associate Directorate level (or official designee) for content, and reviewed for technical consistency by the Domain Webmaster prior to posting on the Intranet or on closed user group areas of the IFS. In addition, Internet and IFS postings intended for the public must be reviewed by EIMA.

2. Users may create pages using software contained in the FEMA standard office automation suite. This software will convert word documents, spreadsheets, and other applications into HTML documents that can be uploaded for posting on Internet/Intranet. The users will create the page(s) and save the files to a diskette or to a working directory on the network for uploading by the Domain Webmaster/System Administrator. Users will be expected to maintain and keep current any pages that they create.

3. Internet/Intranet requirements that intend to take advantage of database queries or search engine capabilities are required to undergo a technical review of the requirement prior to beginning any developmental work. Users will submit the requirements to the ITS Engineering Division (IT-SE) for a technical analysis. IT-SE will assist the user with the cost benefit analysis and the life cycle operations and maintenance costs. The requisition for procurement support must be submitted through IT-SE to the CIO for approval and recording into the CIO IT database.

4. Applications that require contractor support or other IT expenditures must be submitted in accordance with the CIO information technology review process.

5. Applications which are cross-cutting in the Agency must undergo review by the Information Resources Board.

To Use Internet/Intranet

1. Employees are cautioned how they represent themselves while on the Internet since what they say or do could be interpreted as FEMA opinion or policy. Users should be aware that their conduct reflects upon the reputation of FEMA. Internet access and use are a privilege, not a right, which may be revoked at any time for inappropriate conduct. In addition to those items listed in the Authorized Use section of Chapter 3-6, examples of permissible and non-permissible use of Internet are as follows:

2. Internet/Intranet may be used only for Agency business. Penalties for other use may include any of the following: loss of Internet privileges, and other disciplinary actions up to and including employment termination.

3. Internet/Intranet may be used to transmit official business messages and data/documents between Agency personnel. It may also be used to transmit official business messages between FEMA and external organizations such as other government agencies, private voluntary organizations, contractors, vendors, and universities.

4. Internet/Intranet may not be used to convey information on subjects protected under the provisions of the Privacy Act. This includes personal information from personnel files, adverse actions, grievances, workers' compensation, credit cards, etc. Such information is shared within the Agency on a need-to-know basis and is required to be safeguarded.

5. Unlawful or malicious activities, and abusive or objectionable language must not be conveyed through the Internet/Intranet. This includes any message or other communications, files, or programs that contain offensive or harassing statements, including comments based upon race, national origin, sex, sexual orientation, age, disability, religion or political beliefs and sexually orientated messages or images.

6. Internet/Intranet must not be used for national security classified, Limited Official Use and unclassified sensitive correspondence.

7. Messages sent through the Internet travel on FEMA's Electronic Stationary, and as such, are the same thing as paper messages sent on FEMA letterhead through the US Mail.

8. Take precautions against the importation of computer viruses as required in Chapter 4 of this document.

9. Do not post items to newsgroups, bulletin boards, etc. that do not reflect the policies of FEMA.

10. Users are cautioned that messages sent through the Internet/Intranet, either through the Browser or through Email, could be read by system administrators at each point where the message is routed. In other words, assume that you are using a Post Card when you prepare and send a message. Anyone who handles the mail could read the message on a post card sent through US Mail.

11. Users must also be aware that postings to news groups or other Internet listing services are routinely indexed by commercial search engine organizations and made available through name or keyword searches for perusal by the public.

12. For security purposes, an audit trail of all Internet accesses is automatically logged by the system. These records may be used by system administrators and FEMA managers in the same manner as telephone call detail records.

13. Courts (both state and federal) have ruled that all messages are the property of the agency/organization and may be subject to Freedom of Information Act requests and disclosures.

14. Access to all permissible Internet services from a FEMA networked computer must be performed via the FEMA Firewall. Bypassing the Firewall via a modem on a FEMA networked computer to connect to a 3rd party provider (i.e., America On-line) is prohibited. Waivers for these procedures must be authorized, in writing, by the Computer Security Office, Configuration Management Branch, Management Division, ITS.

Webmaster Advisory Group

A Webmaster Advisory Group (WAG) is established, Chaired by the National Webmaster with participation of each organizational Domain Webmaster. The WAG performs as a subgroup to act in a technical advisory capacity through the existing ISPAG. IT-OP and IT-EN ISPAG members will actively participate and take the lead on group activities according the operational and architectural issues. The ISPAG will continue to support the CIO and IRB with coordination facilitated by IT-MA.

3-9 Electronic Mail

Overview

1. This chapter establishes FEMA's procedures for the use and management of electronic mail (E-Mail) systems. The procedures herein apply to all organizational elements in headquarters, regions, and field establishments which use E-Mail systems. A distinction is made between E-Mail systems and message systems that carry classified information. E-Mail procedures do not apply to such messaging systems.

2. The cc:Mail software is a LAN-based E-Mail system. cc:Mail operates through the FEMA LAN which uses the FEMA Switched Network (FSN) capability for the wide area network (WAN) connectivity. Other existing E-Mail systems may continue to be used.

3. Guidance contained herein applies to the following types of electronic mail systems that exist in FEMA:

    - cc:Mail - cc:Mail Remote - cc:Mail Mobile
    - FTS2000 Mail (X.400)
    - Internet Mail (Pine)

4. Each organizational element using E-Mail will either designate an employee or request the National E-Mail System Administrator to serve as local E-Mail System Administrator. The System Administrator is responsible for the proper installation and operation of E-Mail. The administrator will be thoroughly familiar with the established FEMA LAN/WAN cc:Mail System Administrator's Guide, dated 9/22/94, Version 1, (provided with the software) and will be an active user of E-Mail.

5. E-Mail post office and mailbox names will be setup in accordance with FEMA's naming conventions. Each organizational element will establish and maintain the post office directory of FEMA employees who are equipped for E-Mail use. E-Mail directory information may be made available to other Federal agencies via an appropriate interagency mechanism. Likewise, FEMA will make directory information from other Federal agencies available so that staff can locate and send messages to Federal employees in other agencies.

6. For use in disasters and emergencies, FEMA will adhere to the standard post office node names and user identification (ID) names that have been established for use across the network. All DFO post offices will be coordinated through the National E-Mail System Administrator. This standard is established to ensure consistency, accurate routing, and rapid mail delivery.

7. Organizational elements will protect their systems with both physical and password security according to the guidelines set out in Chapter 2-3, Information Systems Safeguards. The virus protection software provided by the Policy and Oversight Division, Information Technology Services Directorate, will be installed and used on both the network file servers and the network personal computers used for E-Mail communications.

Responsibility

1. Associate Directors, Administrators, Inspector General, Regional Directors, and other Office Directors are responsible for enforcing FEMA's E-Mail policy and procedures, and for designating the E-Mail System Administrator to support and provide maintenance for the E-Mail nodes.

2. The Associate Director, Information Technology Services Directorate, is responsible for overall installation, management, and operations of the FEMA E-Mail system and the effective implementation of IT applications.

3. National E-Mail System Administrator is responsible for:

   - Centrally coordinating and controlling naming conventions;
   - Maintaining and monitoring E-Mail licenses;
   - Designating the routing path to all DFO post offices;
   - Managing, integrating and distributing E-Mail software upgrades; and,
   - Operating functionality of the agencywide E-Mail system (exclusive of the local E-Mail system).

4. E-Mail System Administrators are responsible for:

   - The E-Mail services and support at each FEMA local site;
   - Propagating upgrades, enhancements, bulletin boards, and other local network services;
   - Establishing the size limitation for message transmission;
   - Monitoring E-Mail system performance for adherence to policy and procedures; and,
   - E-Mail database backups.

5. E-Mail Users are responsible for:

   - Complying with policy and procedures;
   - Ensuring retention of E-Mail that constitutes official records in the same manner that paper documents are retained; and
   - Adhering to prescribed practices and protocols when using E-Mail.

Procedures

Permissible Use

1. E-Mail will be used only for Agency business. Penalties for other use may include any of the following: loss of E-Mail privileges, billing the employee for the cost to the government of the unofficial use, and other disciplinary actions up to and including removal.

2. E-Mail may be used to transmit official business messages, data, or documents between Agency personnel. It may also be used to transmit official business messages between FEMA and external organizations such as other government agencies, private voluntary organizations, contractors, vendors, and universities.

3. E-Mail may be used as informal correspondence to convey Agency business in the same manner as telephone communications.

4. E-Mail will not be used to convey information on subjects protected under the provisions of the Privacy Act. These include personal information from personnel files, adverse actions, grievances, workers' compensation, credit cards, etc. Such information is shared within the Agency on a need to know basis and is required to be safeguarded.

5. Employees will be cognizant of the size (message length and number of attachments) of E-Mail correspondence. E-Mail must not exceed 4000 kilobytes (KB) including attachments. Contact your local Network Server Administrator for transferring larger files. If you have problems, please contact the National E-Mail System Administrator.

6. E-Mail will not be used for national security classified, Limited Official Use and sensitive but unclassified correspondence.

Bulletin Boards

1. E-Mail Bulletin Boards will be used for widespread electronic dissemination of information where users may post information of general interest.

2. ITS will establish and maintain a national E-Mail Bulletin Board Directory to ensure the uniform propagation of all bulletin boards on the network that may be accessed throughout FEMA. The directory will be made available for access agencywide. Requests to propagate bulletin boards nationally will be made to the National Systems Administrator for coordination of content and input, and for notification to all the local post offices. Requests will include bulletin board names, duration, and names of the users-owners responsible for content of the board. Bulletin Board messages will not exceed 1000KB per message.

3. The FEMA E-Mail system is configured for decentralized administration. Bulletin boards will be accessible to all users on the local post office (file server), but they may not be automatically accessible to other post offices on the network. Each local System Administrator will create bulletin boards upon requests from users, and will administer owner and user accounts and privileges on the bulletin board. It is important that local System Administrators adhere to the procedures in the System Administrator's Guide for creating, updating, maintaining, and deleting bulletin boards.

E-Mail Internet

FEMA's Internet is a government asset and will be used only for official business. Any and all use of Internet will be FEMA related. Internet Mail message creation, use, maintenance and disposition will conform to FEMA's guidance contained herein and Chapter 3-8, Internet.

Freedom of Information Access

E-Mail messages and files will be subject to, and available for, examination in connection with authorized official Agency reviews (e.g., Office of Inspector General, etc.) and for other official Agency purposes. E-Mail messages and files will be subject to the disclosure provisions of reviews and may be requested by law enforcement officials, the Inspector General or other appropriate authorities. Messages may also be subject to disclosure under provisions of the Freedom of Information Act. Federal policy governing E-Mail has been formulated by the Office of Management and Budget and National Archives and Records Administration (NARA).

Privacy Access

While reasonable efforts will be made to ensure confidentiality and privacy of information contained in E-Mail correspondence, employees are reminded:

- Messages that they prepare may be forwarded by the recipient to others without the knowledge of the originator.
- System managers and other managers may have access to the text of messages for legitimate government purposes.
- There will be no routine review of electronic messages by E-Mail Systems Administrators, management, or other third parties. Casual and non-authorized reading of other person's messages by these or any other individuals is prohibited.

Retention of E-Mail Messages

1. E-Mail messages will be retained electronically for at least 30 days on all file servers and other shared hardware platforms. A purge cycle will be established on all system networks and users will be apprised of system maintenance schedules and procedures.

2. The E-Mail originator will determine whether a message is to be retained. For those E-Mail messages to be retained, they will be archived from the shared device platform to the originators personal computer (PC) storage media. Users are encouraged to exercise judgment in retaining E-Mail in the same manner as they would in retaining paper documents. Employees may retain E-Mail messages indefinitely on their assigned PCs.

3. E-Mail databases (including messages marked for purging) will be erased or backed-up in accordance with internal procedures and the cc-Mail System Administrators Handbook.

4. E-Mail messages that qualify as "official records" shall be printed out with transmittal data and kept as part of the paper-based recordkeeping system (see FEMA Manual 5400.1).

E-Mail Etiquette

1. Messages in UPPER CASE ONLY are hard to read. In some cases all upper case is needed for clarification, but not for everything.

2. The tone of E-Mail messages will correspond to the tone of written documents. What may sound funny in speech can sound aggressive, abrupt, or just plain rude in E-Mail.

3. Coarse, crude, vulgar or suggestive text is prohibited. Not only are these kinds of expressions rarely approved in the work place, but you're putting them on electronic paper, they become permanent records.

4. Messages not fit and proper for sending via memoranda are not fit and proper for E-Mail.

5. Expressions of anger via E-Mail yield the same consequence as anger expressed via memoranda. Accordingly, such expressions will be avoided. Think about how you are going to respond before you send the message. Remember that E-Mail may stay around for a long time.

Procedures

1. E-Mail System Administrators will establish the E-Mail directory information, including user name, voice telephone number, organization identifier, post office name, and any associated computer interpretable electronic address that will allow appropriately equipped Federal employees in other agencies to send messages to FEMA employees. The directory will also include the E-Mail System Administrator's name and voice telephone number. The directory information will be incorporated into the local FEMA telephone directory.

2. To ensure propagation across the network, each E-Mail post office directory will be provided to the National E-Mail System Administrator for Agencywide notification and coordination. Once the E-Mail directories are propagated, users will have access to E-Mail address information for employees FEMA-wide and for employees in other Federal agencies.

3. Users of the E-Mail post offices will select addressee names from the directory when they create messages. If the E-Mail addressee is served by the same post office as the originator, that post office delivers the mail directly. If the E-Mail addressee is served by a different post office (remote), the originator's post office transmits the outgoing mail to the addressee via the addressee's post office. (Another post office is considered "remote," even if it is located in the same building or organization.) The addressee's post office holds the mail until the addressee signs onto the system.

4. Users of E-Mail will contact their E-Mail System Administrator for both local and Agencywide services, including the establishment of bulletin boards. The E-Mail System Administrator will broadcast notices of changes to the National E-Mail System Administrator for updating directory entries. The National E-Mail System Administrator will handle the propagation of all directory and bulletin board updates to local post offices.

5. All current and newly established E-Mail post offices will be registered through the National E-Mail System Administrator at the MWEAC, FSN 6-630-2228, or (540) 542-2708.

6. The E-Mail System Administrator will establish and configure E-Mail post offices and mailboxes in accordance with the conventions established in the electronic mail attachment included in this document.

7. Users of E-Mail will exercise the same judgment and restraint in creating and disseminating electronic correspondence as they do with paper forms of correspondence. For example, E-Mail correspondence that may result in any type of assignment, tasking, or requirement levied on regional offices will be coordinated with the Office of Regional Operations and other appropriate organizational elements prior to dissemination.

8. E-Mail is a transmission media, and requirements for reports and forms management and directives remain in effect. Where retention is required, documents will be printed and the hard copy retained in accordance with procedures identified in Part II, Chapter 2-4, Record Maintenance and Electronic Recordkeeping or FEMA Manual 5400.2, Records Management, Files Maintenance and Records Disposition.

9. Where an actual signature is required by law, regulation, or directive, E-Mail transmission without confirming paper copy will not be deemed acceptable.

3-10 Electronic Data Interchange

To Be Provided

Left blank intentionally

3-11 Disposition of Excess and Surplus Hardware

Overview

1. This instruction establishes FEMA's policy and procedures under Executive Order 12999 for disposition of excess and surplus educationally useful equipment. This shall emphasize the donation of such equipment to schools and nonprofit educational organizations located in Federal enterprise and empowerment zones.

2. The provisions of this instruction apply to all organizational elements in headquarters, regions, and field establishments.

3. This instruction encompasses office automation information systems, such as personal computer systems, word processors, typewriters, printers, communications modems, related peripheral equipment, and local area network equipment. Due to vendor licensing requirements, this instruction does NOT apply to individually purchased commercial-off-the-shelf software programs.

4. The term, information processing equipment, is used herein to denote office automation information systems.

Responsibility

1. The Chief Information Officer (CIO), is responsible for assisting the Operations Support Directorate in ensuring that programs and data are properly removed from TEMPEST equipment prior to donating surplus or excess equipment.

2. Associate Directors, Administrators, Regional Directors, Heads of Field Establishments, and Office Directors are responsible for:

   - Ensuring that existing information processing equipment is routinely assessed for obsolescence, sharing, reuse, and disposal in accordance with Agency procedures; and,

   - Ensuring the integrity of the inventory process.

3. The Associate Director, Operations Support Directorate, is responsible for:

   - Establishing, implementing and managing a program to ensure proper disposition of excess and surplus equipment;

   - Managing, and maintaining the Agency's centralized inventory process for information processing equipment;

   - Notifying the participants in the FEMA Partnership in Education Program located in Federal enterprise and empowerment zones of the availability of excess information processing equipment and coordinating the transfer of the equipment.

4. The Accountable Property Officer, as designated in FEMA Manual 6150.1, is responsible for:

   - Maintaining the individual inventory process, including receipts and dispositions, for information processing equipment; and,

   - Recording and disposing of the equipment in accordance with the procedures established in this instruction.

Procedures

1. The Custodial Officer, or Project Officer who originally procured the computer equipment, may reassign the property elsewhere in the organization, or transfer it to the Accountable Property Officer for agencywide notification of the excess computer equipment. The original hand receipt is to be removed from the property record and returned to the individual releasing the property. The excess computer will be publicized agencywide as available excess property. Internal transfer of the computer equipment follows established procedures. If, after 7 days there are no requests for the excess property, the computer may be donated as described herein.

2. To be eligible to receive excess information processing equipment, the Principle of the school must make the request for receiving donations in writing. These letters should be addressed or forwarded to the Accountable Property Officer.

3. Requests for donations shall be divided into two categories by the Accountable Property Officer into those from schools and nonprofit organizations located in Federal enterprise zones, and those located outside.

4. Requests from schools and nonprofit educational organizations located in Federal enterprise zones will be met on a first come, first served basis.

5. Requests from schools and nonprofit educational organizations located outside Federal enterprise zones will be met on a first come, first served basis, after all requests have been met from schools and nonprofit educational organizations located within Federal enterprise zones.

6. The Accountable Property Officer for each FEMA facility maintains discretion on the quantity of hardware that will be provided to each requester, subject to the limitations outlined in this Directive.

7. Each organizational element will work with the Accountable Property Officer to prepare a letter of transfer conveying the excess information processing equipment to the receiving schools and will list the equipment by item, type (make and model), and serial number. A copy of the letter of transfer will be kept by the Accountable Property Officer as documentation for the appropriate property records.

8. Transfers of excess information processing equipment will be coordinated with the information technology office for technical validation of the systems operating capabilities.

9. The transfer of excess education-useful information processing equipment is an exception to the procedures described in Chapter 7-2, Disposition of Excess Property, FEMA Manual 6150.1.

10. Disposition of excess TEMPEST equipment will be made by the ITS, Mount Weather Emergency Assistance Center. ITS has the capability to modify the equipment for reuse or to destroy unrepairable equipment. Each organizational element will transfer TEMPEST equipment to ITS according to established procedures for relocating secure equipment.

Authority

Executive Order (E.O.) 12999 of April 21, 1996, *Educational Technology: Ensuring Opportunity for All Children in the Next Century*

Background

E.O. 12999 requires compliance by all Federal agencies, to the extent possible, to:

(a) identify and protect educationally useful Federal equipment that is in excess or surplus to current and anticipated needs;

(b) efficiently transfer educationally useful Federal equipment "…giving highest preference to schools and nonprofit organizations, including community-based educational organizations ("schools and nonprofit organizations")…", while giving "… particular preference to schools and nonprofit organizations located in the Federal enterprise communities and empowerment zones established in the Omnibus Reconciliation Act of 1993, Public Law 103-66"; and,

(c) assist teachers by training them to use computer hardware in teaching, connecting America's classrooms to the National Information Infrastructure, and providing ongoing maintenance and technical support for the educationally useful Federal equipment transferred to educational and nonprofit organizations.

EO 12999 defines the following:

(a) "Schools" means individual public or private education institutions encompassing prekindergarten through twelfth grade, as well as public school districts.

(b) "Community-based educational organizations" means nonprofit entities that are engaged in collaborative projects with schools or that have education as their primary focus.

(c) "Educationally useful Federal equipment" means computers and related peripheral tools (e.g., printers, modems, routers, and servers), including telecommunications and research equipment that are appropriate for use in prekindergarten, elementary, middle, or secondary education. It shall also include computer software, where the transfer of licenses is permitted…."

Omnibus Reconciliation Act of 1993, Public Law (PL) 103-66 provides details of "Empowerment Zones, Enterprise Communities, and Rural Development Investment Areas" in Section 13301, pages 107 Stat. 543 through 107 Stat. 555. PL 103-66 defines on page 107 Stat. 548, "…Empowerment Zone; Enterprise Community.—For purposes of this title, the terms 'empowerment zone' and 'enterprise community' mean areas designated as such under section 1391…", entitled Designation Procedure.

Under PL 103-66, the Secretary of Housing and Urban Development (HUD) may designate up to 65 nominated urban communities and the Secretary of Agriculture may designate up to 30 rural communities, for a total of 95 enterprise communities. A total of 9 empowerment zones may be designated; up to 6 by the Secretary of HUD in urban areas and up to 3 by the Secretary of Agriculture in rural areas. Designations are limited to a period of ten years, and according to guidelines in PL103-66 that include size, location, population, poverty, and unemployment of the areas.

3-12 Telecommuting

To Be Provided

Left blank intentionally

Chapter 4

Information Systems Safeguards

Left blank intentionally

4-1 Information Systems Safeguards

Overview

1. This chapter specifies security safeguards for the protection of FEMA's information systems. The security controls, procedures, and documentation standards establish the MINIMUM requirements for safeguarding classified and unclassified information technology hardware and software assets. The increased use of electronic media to store, process and transmit information adds a new dimension of complexity to traditional security concerns.

2. Managers at every level play lead roles in information security. Even program or functional managers, who do not oversee general support systems or major applications, have responsibility for providing information safeguards: managerial, operational, and technical. Integrating security safeguards into every phase of the program's life cycle is essential for protecting the confidentiality, integrity, and availability of information resources used in support of FEMA's mission.

3. As in other aspects of sound management, cost containment is a major part of information security. Experience has shown that costs are lower and risks are lessened when information safeguards are incorporated into the design and development of information systems. However, incorporating information safeguards into the design specifications does not negate the need for periodic assessments as threats change over time, and subsequent systems updates may alter the nature of the security environment.

Responsibility

1. The Chief Information Officer is responsible for:

   - Overseeing FEMA's information systems security policy, procedures, and practices.
   - Identifying and affording security protections commensurate with the risk and magnitude of the harm that may result from the loss, misuse, or unauthorized access to or modification of information collected or maintained by or on behalf of the Agency.
   - Appointing FEMA's Enterprise Security Manager.
   - Overseeing development and implementation of FEMA's information security training program.
   - Approving recommendations for application systems security accreditation.

2. Executive Associate Director, Information Technology Services Directorate is responsible for:

   - Developing and implementing applicable information systems policy, procedures, standards, and guidelines on privacy, confidentiality, security, disclosure, and sharing of information collected, processed, transmitted, or maintained by or for the Agency.

   - Coordinating with the Executive Associate Director, Operations Support Directorate, on all security matters pertaining to classified and sensitive unclassified information systems.

3. Associate Directors, Administrators, Executive Associate Directors, Regional Directors, and Office Directors are responsible for:

   - Ensuring FEMA's information systems security policy, requirements, and guidelines are followed in developing system specifications and contracts for the acquisition or operation of information systems, associated resources, and facilities.

   - Issuing, for programs and functions under their purview, information systems safeguards beyond the Agency's minimum stated requirements, as required.

   - Assigning security personnel, Site Mangers/Administrators and/or Network Administrators, as required.

   - Conducting effective security certification and accreditation for major, mission critical, high risk, financial, or classified information systems.

   - Authorizing information systems and by implication accepting the risks extant in the systems.

   - Implementing controls consistent with the criticality, value, and sensitivity of the information being handled.

   - Ensuring that employees are made aware of all information security policies and procedures and that security training is available for users, custodians, and owners of sensitive FEMA information assets.

4. The Inspector General is responsible for:

   - Performing independent audits relating to information systems security, including assessing compliance with information systems security and privacy legislation, regulations, and requirements.

- Assisting the CIO and the Director, Security Division of the Operations Support Directorate, in information systems security investigations; or as appropriate, conducting criminal investigations and making referrals to the United States Department of Justice.

5. The FEMA Enterprise Security Manager is responsible for:

- Approving the acquisition, configuration and installation of routers, switches, firewalls and other network-related equipment.
- Assuring FEMA information assets are used only for FEMA purposes.
- Assuring compliance with all applicable State and Federal laws and administrative policies.
- Assuring compliance with security policies and procedures established by the owners of the information assets and by the FEMA CIO.
- Advising the owner of information and the CIO of any vulnerability presenting a threat to information assets, and for providing specific means of protecting that information.
- Notifying the owner of information and the CIO of any actual or attempted violations of security policies, practices or procedures.
- Approving the addition of Local Area Network (LAN) or Wide Area Network (WAN) devices that impact Internet or Intranet services.
- Establishing and approving the security configuration control of all network devices.
- Developing or assisting with the development of operational procedures.
- Assuring adherence to all FEMA WAN-naming conventions.
- Developing or assisting with the development of operational procedures.
- Assuring adherence to all FEMA WAN-naming conventions.
- Providing support for the issuance of hardware tokens and maintenance of authentication databases.
- Evaluating vendor security products and apprising the Agency of approved Information Technology (IT) security products and techniques.
- Developing security accreditation guidelines and procedures for new application development.

- Participating as technical security advisor on in-house system development projects and assisting with security control implementations.
- Performing independent audits relating to information systems security, including assessing compliance with information systems security and privacy legislation, regulations and requirements.
- Conducting pre-production security tests to ensure compliance with FEMA security practices for new applications and devices.
- Investigating reports of information systems security compromises, violations or breaches, and recommending or implementing security countermeasures or corrective actions, as appropriate.
- Performing other security duties as assigned.

6. The Site Manager/Administrator has overall responsibility for:
   - Managing the local networks at a location where there are multiple local area networks with different Network Administrators.
   - Ensuring security, integrity, availability, and confidentiality of local information systems and network services for the site.
   - Presenting security orientations to current employees and new hires.
   - Processing newly arriving and departing employees to ensure compliance with security procedures, as required in Chapter 4-4 under “Personnel Security and Control” and “Access Control” headings.
7. The Network Administrator is responsible for:
   - Establishing and maintaining configuration, operation and security of the local system.
   - Maintaining the configuration management of all hardware and software connected to the local network.
   - Ensuring that system/network users comply with IT security policies and procedures.
   - Reviewing and auditing the information system/network on a regular basis to determine that the network remains secure.
   - Reporting any suspected security incidents to FEMA’s Information Technology Service Center (ITSC) at Mt. Weather (540) 542-4000 or directly to the ESM.

- Ensuring the integrity of program data through regularly scheduled system backups and any required restorations.

8. The Information Technology Service Center (ITSC), which is located at Mt. Weather, is responsible for:

   - Providing 24-hour-a-day, 7-day-a-week help desk for users of FEMA's information systems during declared disasters. At other times, the ITSC operates 16 hours a day. The ITSC can be reached on (540) 542-4000.

   - Taking reports on and processing suspected or actual network security problems.

   - Notifying the ESM and appropriate system/network administrator immediately following the reported incident.

Procedures

The procedures for information systems safeguards cover three levels of activities: user requirements, general support systems requirements, and applications systems.

1. User requirements describe the information safeguards to be practiced by users needed for routine administrative and program activities within an office environment. As the procedures represent only the minimal security safeguards, FEMA managers are authorized to impose additional safeguards if the sensitivity of the data warrants additional protection.

2. A general support system is defined as an interconnected set of information resources under the same direct management control; the systems provide processing or communications support or some combination thereof. For purposes of this directive, FEMA network administrators shall adhere to the security safeguards listed in Chapter 4-3 for general support systems.

3. Applications systems require additional security measures and oversight throughout their life cycles. A major application is defined as a large investment, mission critical, cross cutting or high risk use of information and information technology to satisfy a specific set of agency requirements. A major application requires management attention to security due to the risk and magnitude of harm that would result from loss, misuse, or unauthorized access to or modification of the information in the application.

Left blank intentionally

4-2 System User Security Requirements

Overview

1. This chapter specifies security safeguards for the protection of FEMA's information systems. The security controls, procedures, and documentation standards establish the MINIMUM requirements for safeguarding classified and unclassified information technology hardware and software assets. The increased use of electronic media to store, process and transmit information adds a new dimension of complexity to traditional security concerns.

2. Managers at every level play lead roles in information security. Even program or functional managers, who do not oversee general support systems or major applications, have responsibility for providing information safeguards: managerial, operational, and technical. Integrating security safeguards into every phase of the program's life cycle is essential for protecting the confidentiality, integrity, and availability of information resources used in support of FEMA's mission.

3. As in other aspects of sound management, cost containment is a major part of information security. Experience has shown that costs are lower and risks are lessened when information safeguards are incorporated into the design and development of information systems. However, incorporating information safeguards into the design specifications does not negate the need for periodic assessments as threats change over time, and subsequent systems updates may alter the nature of the security environment.

4. 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.

5. 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.

Responsibility

1. The Chief Information Officer is responsible for:

   - Overseeing FEMA's information systems security policy, procedures, and practices.

- Identifying and affording security protections commensurate with the risk and magnitude of the harm that may result from the loss, misuse, or unauthorized access to or modification of information collected or maintained by or on behalf of the Agency.
- Appointing FEMA's Enterprise Security Manager.
- Overseeing development and implementation of FEMA's information security training program.
- Approving recommendations for application systems security accreditation.

2. Executive Associate Director, Information Technology Services Directorate is responsible for:

   - Developing and implementing applicable information systems policy, procedures, standards, and guidelines on privacy, confidentiality, security, disclosure, and sharing of information collected, processed, transmitted, or maintained by or for the Agency.
   - Coordinating with the Executive Associate Director, Operations Support Directorate, on all security matters pertaining to classified and sensitive unclassified information systems.

3. Associate Directors, Administrators, Executive Associate Directors, Regional Directors, and Office Directors are responsible for:

   - Ensuring FEMA's information systems security policy, requirements, and guidelines are followed in developing system specifications and contracts for the acquisition or operation of information systems, associated resources, and facilities.
   - Issuing, for programs and functions under their purview, information systems safeguards beyond the Agency's minimum stated requirements, as required.
   - Assigning security personnel, Site Mangers/Administrators and/or Network Administrators, as required.
   - Conducting effective security certification and accreditation for major, mission critical, high risk, financial, or classified information systems.
   - Authorizing information systems and by implication accepting the risks extant in the systems.
   - Implementing controls consistent with the criticality, value, and sensitivity of the information being handled.

- Ensuring that employees are made aware of all information security policies and procedures and that security training is available for users, custodians, and owners of sensitive FEMA information assets.

4. The Inspector General is responsible for:

   - Performing independent audits relating to information systems security, including assessing compliance with information systems security and privacy legislation, regulations, and requirements.

   - Assisting the CIO and the Director, Security Division of the Operations Support Directorate, in information systems security investigations; or as appropriate, conducting criminal investigations and making referrals to the United States Department of Justice.

5. The FEMA Enterprise Security Manager is responsible for:

   - Coordinating the provision of security for Agency automated information systems and networks.

   - Security, integrity, and availability of information system services and networks that support FEMA operations.

   - Assessing security risks and vulnerability threats to FEMA information assets and providing specific means of protecting those information systems.

   - Evaluating vendor security products and apprising the Agency of approved IT security products and techniques.

   - Obtaining and assessing information systems security accreditation evidence as the basis for recommending security accreditation to the CIO.

   - Ensuring that appropriate security controls are installed, operated, and maintained to protect FEMA information assets.

   - Investigating reports of information systems security compromises, violations, or breaches, and recommending security countermeasures or corrective actions in coordination with the Operations Support Directorate and the Office of Inspector General.

   - Reviewing the configurations of all Agency information systems hardware and software.

   - Ensuring that network security complies with applicable State and Federal laws and regulations, and with Agency policies and procedures.

- Participating as technical security advisor on in-house system development projects and assisting with security control implementations.
- Establishing and reviewing security configurations of all network devices.
- Assisting with the development of operational security practices.
- Ensuring adherence to all FEMA network-naming conventions.
- Providing support for the issuance of hardware tokens and maintenance of authentication databases.

6. The Site Manager/Administrator has overall responsibility for:

   - Managing the local networks at a location where there are multiple local area networks with different Network Administrators.
   - Ensuring security, integrity, availability, and confidentiality of local information systems and network services for the site.
   - Presenting security orientations to current employees and new hires.
   - Processing newly arriving and departing employees to ensure compliance with security procedures, as required in Chapter 4-4 under “Personnel Security and Control” and “Access Control” headings.

7. The Network Administrator is responsible for:

   - Establishing and maintaining configuration, operation and security of the local system.
   - Maintaining the configuration management of all hardware and software connected to the local network.
   - Ensuring that system/network users comply with IT security policies and procedures.
   - Reviewing and auditing the information system/network on a regular basis to determine that the network remains secure.
   - Reporting any suspected security incidents to FEMA’s Information Technology Service Center (ITSC) at Mt. Weather (540) 542-4000 or directly to the ESM.
   - Ensuring the integrity of program data through regularly scheduled system backups and any required restorations.

8. The Information Technology Service Center (ITSC), which is located at Mt. Weather, is responsible for:

   - Providing 24-hour-a-day, 7-day-a-week help desk for users of FEMA's information systems during declared disasters. At other times, the ITSC operates 16 hours a day. The ITSC can be reached on (540) 542-4000.
   - Taking reports on and processing suspected or actual network security problems.
   - Notifying the ESM and appropriate system/network administrator immediately following the reported incident.

Procedures

Workstation Controls

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, lack of controls may result in the unauthorized disclosure, modification, or destruction of data resident on the system.

1. Protect workstations against unauthorized access. Use appropriate access control measures and follow established control procedures. Physical access controls are essential when authorized personnel cannot effectively monitor equipment.
2. Ensure that unauthorized personnel are not able to view sensitive data displayed at a workstation.
3. Monitor the printer to prevent unauthorized disclosure when printing sensitive data.
4. Remove sensitive output from the printer or other output device connected to the system as soon as possible. Delay may lead to unauthorized access.

Software & Data Controls

The following administrative control requirements are applicable to all users operating workstations in unclassified environments:

1. Do not originate, process, store, or transmit classified data on a system designated for unclassified use.
2. Do not use the workstation for personal business or entertainment.
3. Do not copy software from FEMA's workstations for use on privately owned computers, unless allowed by the software license, used only for official business, and authorized by management.

4. Do not copy FEMA data for use on privately owned computers unless authorized by management.

5. Do not install or use privately owned software on a workstation or upload privately owned software to software directories on a file server unless specifically authorized by the Enterprise Security Manager, checked for computer viruses, and used only for official business.

6. Do not process or store privately owned data on a workstation or file server.

7. Use proprietary software and related documentation in conformance with copyright restrictions, licenses, and other legal agreements. The duplication of proprietary software and documentation, except for backup purposes, is prohibited, unless permitted by the license and authorized by management.

8. Obtain written authorization before removing hardware, software, or documentation from a FEMA facility.

9. Report theft, damage, misuse, and unauthorized access of hardware, software, or data.

Downloading and Storing Data at Workstations

1. Safeguard data when downloading data from a FEMA file server for local use and storage at a workstation. Data that may be adequately protected on a file server may be extremely vulnerable to unauthorized access when stored on a fixed disk at a workstation.

2. Safeguard networks, hardware, software, and data when downloading executable programs or data from the Internet for local use and storage at a workstation. For computer virus protection see below.

3. For sensitive data, store data on removable media and physically protect the media from unauthorized access by storing the media in a locked desk, locked cabinet, safe, or other secure location.

Storage Media Protection

1. Protect diskettes and other types of removable storage media against unauthorized access, loss, and destruction.

2. Store diskettes and other types of removable storage media containing sensitive or critical data in locked desks, locked cabinets, safes, or locked rooms.

3. Label all removable storage media used at a workstation.

4. Use SF 710, Unclassified Label, to label unclassified removable media when unclassified and classified media are used or stored in the same [room or container] area.

5. Identify data stored on the media and indicate the sensitivity of data (e.g., Privacy Act data), if appropriate.

6. Exercise care when handling diskettes. Read and follow proper handling procedures for storage media.

7. Dispose of old or unwanted diskettes and tape cassettes that contain sensitive data by cutting into small pieces, shredding, burning, or using other methods of destruction that prevent unauthorized disclosure of data.

Backup

Each user is responsible for making and safeguarding backup copies of files residing on local storage media used at workstations. Current and reliable backup copies of word processing files and data files provide insurance against the loss of valuable or critical information system assets.

1. Make regular and systematic backup copies of word processing and data processing files resident on local storage media at workstations.

2. Comply with backup requirements specified by management.

3. Label and date all backup media used at a workstation so backup data can be readily identified and loaded when needed.

4. Protect backup media in the same manner as media containing original word processing and data files.

Computer Viruses on PCs and LANs

1. Protect workstations against computer viruses by using antivirus software tested and issued by the Information Technology Services Directorate, Operations Division.

2. Contact the ITS Operations Division for assistance in using the antivirus software or to report problems with the software package.

3. Do not install any software on a workstation or file server unless the software has been authorized and tested for virus infection. Public domain software, shareware, freeware, computer games, and software copied from a home system or another user's system may be infected with a virus or contain other malicious code that may infect a workstation or the entire network.

4. Report virus incidents immediately whenever any unusual activity occurs at a workstation or a computer virus is suspected or detected.

Left blank intentionally

4-3 General Support Systems Safeguards

Overview

1. This chapter specifies security safeguards for the protection of FEMA's information systems. The security controls, procedures, and documentation standards establish the MINIMUM requirements for safeguarding classified and unclassified information technology hardware and software assets. The increased use of electronic media to store, process and transmit information adds a new dimension of complexity to traditional security concerns.

2. Managers at every level play lead roles in information security. Even program or functional managers, who do not oversee general support systems or major applications, have responsibility for providing information safeguards: managerial, operational, and technical. Integrating security safeguards into every phase of the program's life cycle is essential for protecting the confidentiality, integrity, and availability of information resources used in support of FEMA's mission.

3. As in other aspects of sound management, cost containment is a major part of information security. Experience has shown that costs are lower and risks are lessened when information safeguards are incorporated into the design and development of information systems. However, incorporating information safeguards into the design specifications does not negate the need for periodic assessments as threats change over time, and subsequent systems updates may alter the nature of the security environment.

4. One major aspect of computer system security is controlling access to FEMA systems, networks, files and databases. Access to a system is strictly controlled to prevent the unauthorized disclosure, modification, or destruction of data and program files resident on the system storage devices. To protect against unauthorized access, FEMA assigns unique user identifiers (user IDs) and passwords to identify and authenticate authorized users. User IDs also play a key role in authorizing and controlling access to programs and data resident on the system, as well as ensuring individual user accountability on the system.

5. Standards and naming conventions for developing and assigning unique user IDs will be provided in Chapter 5 of this directive. The following sections describe FEMA standard practices in controlling these areas.

Responsibility

1. The Chief Information Officer is responsible for:

   - Overseeing FEMA's information systems security policy, procedures, and practices.

- Identifying and affording security protections commensurate with the risk and magnitude of the harm that may result from the loss, misuse, or unauthorized access to or modification of information collected or maintained by or on behalf of the Agency.
- Appointing FEMA's Enterprise Security Manager.
- Overseeing development and implementation of FEMA's information security training program.
- Approving recommendations for application systems security accreditation.

2. Executive Associate Director, Information Technology Services Directorate is responsible for:

   - Developing and implementing applicable information systems policy, procedures, standards, and guidelines on privacy, confidentiality, security, disclosure, and sharing of information collected, processed, transmitted, or maintained by or for the Agency.
   - Coordinating with the Executive Associate Director, Operations Support Directorate, on all security matters pertaining to classified and sensitive unclassified information systems.

3. Associate Directors, Administrators, Executive Associate Directors, Regional Directors, and Office Directors are responsible for:

   - Ensuring FEMA's information systems security policy, requirements, and guidelines are followed in developing system specifications and contracts for the acquisition or operation of information systems, associated resources, and facilities.
   - Issuing, for programs and functions under their purview, information systems safeguards beyond the Agency's minimum stated requirements, as required.
   - Assigning security personnel, Site Mangers/Administrators and/or Network Administrators, as required.
   - Conducting effective security certification and accreditation for major, mission critical, high risk, financial, or classified information systems.
   - Authorizing information systems and by implication accepting the risks extant in the systems.
   - Implementing controls consistent with the criticality, value, and sensitivity of the information being handled.

- Ensuring that employees are made aware of all information security policies and procedures and that security training is available for users, custodians, and owners of sensitive FEMA information assets.

4. The Inspector General is responsible for:

   - Performing independent audits relating to information systems security, including assessing compliance with information systems security and privacy legislation, regulations, and requirements.

   - Assisting the CIO and the Director, Security Division of the Operations Support Directorate, in information systems security investigations; or as appropriate, conducting criminal investigations and making referrals to the United States Department of Justice.

5. The FEMA Enterprise Security Manager is responsible for:

   - Approving the acquisition, configuration and installation of routers, switches, firewalls and other network-related equipment.

   - Assuring FEMA information assets are used only for FEMA purposes.

   - Assuring compliance with all applicable State and Federal laws and administrative policies.

   - Assuring compliance with security policies and procedures established by the owners of the information assets and by the FEMA CIO.

   - Advising the owner of information and the CIO of any vulnerability presenting a threat to information assets, and for providing specific means of protecting that information.

   - Notifying the owner of information and the CIO of any actual or attempted violations of security policies, practices or procedures.

   - Approving the addition of Local Area Network (LAN) or Wide Area Network (WAN) devices that impact Internet or Intranet services.

   - Establishing and approving the security configuration control of all network devices.

   - Developing or assisting with the development of operational procedures.

   - Assuring adherence to all FEMA WAN-naming conventions.

   - Developing or assisting with the development of operational procedures.

- Providing support for the issuance of hardware tokens and maintenance of authentication databases.
- Evaluating vendor security products and apprising the Agency of approved Information Technology (IT) security products and techniques.
- Developing security accreditation guidelines and procedures for new application development.
- Participating as technical security advisor on in-house system development projects and assisting with security control implementations.
- Performing independent audits relating to information systems security, including assessing compliance with information systems security and privacy legislation, regulations and requirements.
- Conducting pre-production security tests to ensure compliance with FEMA security practices for new applications and devices.
- Investigating reports of information systems security compromises, violations or breaches, and recommending or implementing security countermeasures or corrective actions, as appropriate.

6. The Site Manager/Administrator has overall responsibility for:

   - Managing the local networks at a location where there are multiple local area networks with different Network Administrators.
   - Ensuring security, integrity, availability, and confidentiality of local information systems and network services for the site.
   - Presenting security orientations to current employees and new hires.
   - Processing newly arriving and departing employees to ensure compliance with security procedures, as required in Chapter 4-4 under “Personnel Security and Control” and “Access Control” headings.

7. The Network Administrator is responsible for:

   - Establishing and maintaining configuration, operation and security of the local system.
   - Maintaining the configuration management of all hardware and software connected to the local network.
   - Ensuring that system/network users comply with IT security policies and procedures.

- Reviewing and auditing the information system/network on a regular basis to determine that the network remains secure.
- Reporting any suspected security incidents to FEMA's Information Technology Service Center (ITSC) at Mt. Weather (540) 542-4000 or directly to the ESM.
- Ensuring the integrity of program data through regularly scheduled system backups and any required restorations.

8. The Information Technology Service Center (ITSC), which is located at Mt. Weather, is responsible for:
   - Providing 24-hour-a-day, 7-day-a-week help desk for users of FEMA's information systems during declared disasters. At other times, the ITSC operates 16 hours a day. The ITSC can be reached on (540) 542-4000.
   - Taking reports on and processing suspected or actual network security problems.
   - Notifying the ESM and appropriate system/network administrator immediately following the reported incident.

Procedures

Access Control - System Accounts

1. In order to obtain a user account on any FEMA computer system, a request will be submitted through the supervisor to the Network Administrator who reviews the levels of system and database access. Both the Network Administrator and the appropriate application Data Base Administrator will implement such requests. Further reference material for Disaster Field Office's Network Administrator is provided in Appendix 4.3.c, "Disaster Field Officer's Network Administrators Guide."
2. Telephone discussions involving sensitive or classified U.S. Government Information must be conducted using a Secure Telephone Unit "STU-III" and the proper safeguards provided in FEMA Manual 1550.3.
3. Up-to-date account information must be maintained and monitored for inactivity. Account inactivity exceeding 30 days should warrant an inquiry. Failure to respond to a revalidation inquiry should justify account suspension.
4. Group accounts or shared passwords are prohibited. Any variance from this standard practice must be documented and waived by the Network Administrator in coordination with the Enterprise Security Manager and program or system manager.

Access Control - Account Termination

1. Accounts may be frozen due to extended leaves of absence, investigations, temporary assignments, etc.

2. Accounts must be terminated when an employee leaves FEMA, is reassigned, or no longer requires access. Supervisors are required to notify the cognizant Network Administrator when an employee no longer requires access.

Access Control - Password Management

1. Never disclose passwords to anyone or write them down on any medium accessible to others. Users are responsible for actions and events resulting from the disclosure of personal passwords.

2. Never store the network log-in command or a server attach command along with a user ID and password in a batch file on a workstation or in a user log-in script stored on a file server. This practice constitutes a serious vulnerability; it creates an easily accessible path for unauthorized access.

3. Report suspected password compromises.

4. Comply with the following requirements if the security system permits users to change personal passwords:

    - Change passwords at least every ninety (90) days to protect against undetected password compromise;

    - Change passwords whenever password compromises are suspected;

    - Avoid choosing passwords that incorporate personal information (e.g., users' names, children's names, dates of birth, addresses, telephone numbers, etc.); Passwords must NOT be related to the user's job or personal life, or words found in the dictionary. For example, car license plate number, spouse's name, address, proper names, places, and slang terms should not be used.

    - Choose passwords that are at least eight alphanumeric characters in length with at least one non-alphabetic character such as a numeral (0-9) or punctuation character. One recommended format for passwords is CVCNNCVC, where C is a consonant, V is a vowel, and N is a numeral (e.g., BAT56ZAM).

5. If system generated passwords are used, they must be generated using the low order bits of the system clock or some other unpredictable source. So that users can more easily remember them, and so that users will not need to write them down; all system-generated

passwords for end-users must be pronounceable. Passwords or Personal Identification Numbers (PINs) that are generated by a computer system must be issued immediately after they are generated. Regardless of the form they take, unissued passwords and PINs must never be stored on the computer systems unless they are encrypted.

6. Initial passwords issued by a Network Administrator will be valid only for the user's first on-line session. Users will be automatically notified and required to change their passwords at least once every ninety (90) days.

7. Consecutive entry of the incorrect password will be strictly limited. After three (3) unsuccessful attempts to enter a password, the user ID will be either (a) suspended until reset by the Network Administrator, (b) temporarily disabled for not less than three (3) minutes, or (c) if dial-up or other external network connections are involved, disconnected.

8. When the system is compromised or there is a suspicion of compromise, the Network Administrator will immediately change every password on the system. A trusted version of the operating system and all security-related software must also be reloaded. All recent changes to user and system privileges should be reviewed for unauthorized modifications.

9. When an employee who had system privileges and access to password files leaves FEMA or is no longer in a position of trust, all systems to which the employee had access must be notified and passwords must be changed.

Log-in Process

1. All users must be identified prior to being able to use any multi-user computer or communications system resources. All users must have their identity verified with a user-ID and a private password or by other means that provide equal or greater security-prior to being permitted to use FEMA computers connected to a network.

2. Remote access to FEMA systems via dial-in modems will require the use of a strong authentication system employing a hardware token when they become available. The use of the hardware token applies to all dial-in connections. The hardware token will be used to generate a one-time password unique to that log-in session.

3. All log-in banners on network-connected FEMA computer systems will require the user to log-in, providing prompts as needed. Specific information about the organization, the computer operating system, the network configuration, or other internal matters must not be provided in the log-in banner until a user has successfully provided both a user-ID and a password. When logging into a FEMA computer or data communications system, if any part of the log-in sequence is incorrect, the user will not be given specific feedback indicating the source of the problem. Instead, the user will be informed that the log-in process was incorrect after all of the log-in information has been entered.

4. The log-in process on multi-user computers will include a special notice: (1) the system is to be used only by authorized users, (2) this session may be monitored by FEMA management, and (3) by continuing to use the system, the user represents that he/she is an authorized user.

5. Users will be given information reflecting the last log-in time and date, which will allow detection of unauthorized system usage.

Log-off Process

1. Users must not leave their microcomputer (PC), workstation, or terminal unattended without first logging-out.

2. Inactivity on a computer terminal, workstation, or microcomputer for ten (10) minutes will cause the system to automatically blank the screen and suspend the session. Re-establishment of the session must take place only after the user has provided the proper password.

Privilege Control - Level of Access

1. The computer and communications system privileges of all users, systems, and programs will be based on the need-to-know. All computer-resident information that is either private, restricted, or sensitive will have system access controls to ensure that it is not improperly disclosed, modified, deleted, or rendered unavailable.

2. Access controls should be consistent with the information being protected and the computer system hosting the data. Access controls typically consist of Access Control Lists or other mechanisms that limit users' ability to read, modify, or delete information in accordance with their need-to-know.

3. Firewalls should protect servers that store and process sensitive data because the unauthorized modification, deletion, or release of sensitive data would have severe consequences. Refer to Appendix 4-3.A, Firewall Management and Administration, for further information.

Privilege Control - Logging and Auditing

1. System logs and audit trails, appropriate for the value of the system protected, will be maintained for each FEMA information asset to correct problems encountered due to intentional or inadvertent misuse.

2. All production application systems that handle private, restricted or sensitive FEMA information must generate logs that show every addition, modification, and deletion to such sensitive information. Any systems that do not support such logging capabilities must maintain a documented requirements analysis, approved by the applicable program manager, that justifies such operation. Mechanisms to detect and record significant computer security events must be resistant to attacks. These attacks include attempts to deactivate, modify, or delete the logging software and/or the logs themselves.

3. All FEMA computer systems connected to networks will securely log all significant computer security relevant events. Examples of computer security relevant events include: password guessing attempts, attempts to use privileges that have not been authorized, modifications to production application software, and modifications to system software. Logs of computer security relevant events must provide sufficient data to support comprehensive audits of the effectiveness of, and compliance with security measures.

4. All commands issued by computer system operators will be traceable to specific individuals via the use of comprehensive logs. Logs of major computer security relevant events must be retained for at least three (3) months. During this period, logs must be secured such that they cannot be modified, and such that only authorized persons can read them. All system and application logs must be securely maintained and accessible only on a need-to-know basis.

5. To allow proper remedial action, computer operations or information security staff must review records reflecting security relevant events in a periodic and timely manner. The Network Administrator and Enterprise Security Manager must review logs on a weekly basis. Where incidents of misuse or abuse are detected, procedures defined for incident reporting and handling must be followed.

Virus Prevention and Detection

1. A computer virus is an unauthorized program that replicates itself and spreads onto various data storage media (floppy disks, magnetic tapes, disk drives, etc.) and/or across a network. The symptoms of virus infection include much slower computer response time, inexplicable loss of files, changed modification dates for files, increased file sizes, and total failure of computers.

2. FEMA employees are cautioned to be especially careful when downloading software from electronic bulletin board systems, external communication networks, or other systems outside FEMA, to include the Internet and the World Wide Web. This caution is necessary because such software may contain viruses and may damage FEMA information and systems. All new software to be introduced into the FEMA system must be scanned for viruses.

3. Every computer connected to a FEMA network will use virus detection software that will automatically scan upon startup, floppy disk insertion, and on any file storage operation. FEMA's agency-wide standard anti-virus software product must be installed on computer systems.

System Backups

1. All critical system software and data should be backed up onto removable media on a regular basis. The back-up media should then be stored off-site.

2. Incremental and full backups and protected backup storage will be maintained at the local level.

3. Sufficient server storage space or portable backup equipment will be provided to support end users.

Software Usage

The introduction of unauthorized or unlicensed software into FEMA's information processing environment is prohibited.

1. All FEMA employees must honor licenses, copyright laws and other measures designed to protect legitimate proprietary interests in computer software and data.

2. Users must not possess or use software or hardware tools that can be used to break security mechanisms. Examples of such tools are those that facilitate illegal copying of copy-protected software, that are used to discover secret passwords, or that are used for unauthorized decipherment of encrypted data.

Network Configuration Control

1. If a security breach occurs or a computer virus is discovered, the Network Administrator will identify and isolate the source of the problem and notify the ESM directly or through the ITSC.

2. The Network Administrator will maintain information detailing the current inventory, configuration, and connectivity of all equipment in their system(s). No network equipment will be added, removed or modified; and no computer connections to FEMA networks will be made without review and approval by the Network Administrator.

Remote Access (Dial-in and Dial-out)

1. Access to the FEMA enterprise network via the commercial dial phone system is a significant security risk. The connection of modems to the network without a security risk assessment and configuration control is prohibited.

2. No modem will be connected to any portion of the FEMA network without prior approval. Refer to Appendix 4-3.b, Remote Access using Hardware Tokens and TACACS, for detailed information.

3. All modems on the network will be under the configuration control of the National ITSC at Mt. Weather.

Left blank intentionally

4-4 Application Systems Life-Cycle Security Requirements

Overview

1. This chapter specifies safeguards for all major FEMA applications systems, that are by definition, large investments, mission critical, cross cutting, or 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 system. These needs frequently extend beyond the scope of security procedures documented in this chapter. The procedures and controls discussed below present the minimum level of safeguards to be adopted.

2. 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.

3. OMB Circular A-130, Appendix III, "Security of Federal Automated Information Systems," requires Federal agencies to establish security controls in parallel with the application systems life-cycle process. The goal of these security controls is to ensure appropriate safeguards are incorporated into all new applications and into significant modifications to existing applications. The following safeguards include OMB Circular A-130 security control topics: assigning responsibility for security, security planning, review of security controls, and management authorization. The procedures also detail safeguards for ensuring security throughout the application systems life cycle. For more assistance or technical guidance, contact the FEMA Enterprise Security Manager.

Responsibility

1. The Chief Information Officer is responsible for:

   - Overseeing FEMA's information systems security policy, procedures, and practices.
   - Identifying and affording security protections commensurate with the risk and magnitude of the harm that may result from the loss, misuse, or unauthorized access to or modification of information collected or maintained by or on behalf of the Agency.
   - Appointing FEMA's Enterprise Security Manager.
   - Overseeing development and implementation of FEMA's information security training program.
   - Approving recommendations for application systems security accreditation.

2. Executive Associate Director, Information Technology Services Directorate is responsible for:

   - Developing and implementing applicable information systems policy, procedures, standards, and guidelines on privacy, confidentiality, security, disclosure, and sharing of information collected, processed, transmitted, or maintained by or for the Agency.

   - Coordinating with the Executive Associate Director, Operations Support Directorate, on all security matters pertaining to classified and sensitive unclassified information systems.

3. Associate Directors, Administrators, Executive Associate Directors, Regional Directors, and Office Directors are responsible for:

   - Ensuring FEMA's information systems security policy, requirements, and guidelines are followed in developing system specifications and contracts for the acquisition or operation of information systems, associated resources, and facilities.

   - Issuing, for programs and functions under their purview, information systems safeguards beyond the Agency's minimum stated requirements, as required.

   - Assigning security personnel, Site Mangers/Administrators and/or Network Administrators, as required.

   - Conducting effective security certification and accreditation for major, mission critical, high risk, financial, or classified information systems.

   - Authorizing information systems and by implication accepting the risks extant in the systems.

   - Implementing controls consistent with the criticality, value, and sensitivity of the information being handled.

   - Ensuring that employees are made aware of all information security policies and procedures and that security training is available for users, custodians, and owners of sensitive FEMA information assets.

4. The Inspector General is responsible for:

   - Performing independent audits relating to information systems security, including assessing compliance with information systems security and privacy legislation, regulations, and requirements.

- Assisting the CIO and the Director, Security Division of the Operations Support Directorate, in information systems security investigations; or as appropriate, conducting criminal investigations and making referrals to the United States Department of Justice.

5. The FEMA Enterprise Security Manager is responsible for:

- Approving the acquisition, configuration and installation of routers, switches, firewalls and other network-related equipment.
- Assuring FEMA information assets are used only for FEMA purposes.
- Assuring compliance with all applicable State and Federal laws and administrative policies.
- Assuring compliance with security policies and procedures established by the owners of the information assets and by the FEMA CIO.
- Advising the owner of information and the CIO of any vulnerability presenting a threat to information assets, and for providing specific means of protecting that information.
- Notifying the owner of information and the CIO of any actual or attempted violations of security policies, practices or procedures.
- Approving the addition of Local Area Network (LAN) or Wide Area Network (WAN) devices that impact Internet or Intranet services.
- Establishing and approving the security configuration control of all network devices.
- Developing or assisting with the development of operational procedures.
- Assuring adherence to all FEMA WAN-naming conventions.
- Developing or assisting with the development of operational procedures.
- Assuring adherence to all FEMA WAN-naming conventions.
- Providing support for the issuance of hardware tokens and maintenance of authentication databases.
- Evaluating vendor security products and apprising the Agency of approved Information Technology (IT) security products and techniques.
- Developing security accreditation guidelines and procedures for new application development.

- Participating as technical security advisor on in-house system development projects and assisting with security control implementations.
- Performing independent audits relating to information systems security, including assessing compliance with information systems security and privacy legislation, regulations and requirements.
- Conducting pre-production security tests to ensure compliance with FEMA security practices for new applications and devices.
- Investigating reports of information systems security compromises, violations or breaches, and recommending or implementing security countermeasures or corrective actions, as appropriate.
- Performing other security duties as assigned.

6. The Site Manager/Administrator has overall responsibility for:

   - Managing the local networks at a location where there are multiple local area networks with different Network Administrators.
   - Ensuring security, integrity, availability, and confidentiality of local information systems and network services for the site.
   - Presenting security orientations to current employees and new hires.
   - Processing newly arriving and departing employees to ensure compliance with security procedures, as required in Chapter 4-4 under “Personnel Security and Control” and “Access Control” headings.

7. The Network Administrator is responsible for:

   - Establishing and maintaining configuration, operation and security of the local system.
   - Maintaining the configuration management of all hardware and software connected to the local network.
   - Ensuring that system/network users comply with IT security policies and procedures.
   - Reviewing and auditing the information system/network on a regular basis to determine that the network remains secure.
   - Reporting any suspected security incidents to FEMA’s Information Technology Service Center (ITSC) at Mt. Weather (540) 542-4000 or directly to the ESM.

- Ensuring the integrity of program data through regularly scheduled system backups and any required restorations.

8. The Information Technology Service Center (ITSC), which is located at Mt. Weather, is responsible for:

   - Providing 24-hour-a-day, 7-day-a-week help desk for users of FEMA's information systems during declared disasters. At other times, the ITSC operates 16 hours a day. The ITSC can be reached on (540) 542-4000.

   - Taking reports on and processing suspected or actual network security problems.

   - Notifying the ESM and appropriate system/network administrator immediately following the reported incident.

Procedures

Personnel Security and Control

1. Separation of Duties.

   Structure the application systems development or maintenance environment where possible, to implement the control principle of separating duties. This practice provides a system of checks and balances and minimizes opportunities for any one individual to circumvent established security controls and adversely affect an application system while it is under development or maintenance.

2. Privileges.

   - Include security-related responsibilities in job descriptions and performance plans for personnel involved in application systems development and maintenance.

   - Implement the principle of least privilege in the application systems development or maintenance environment (i.e., grant each individual only the minimum physical and system access privileges needed to perform assigned duties).

3. Personnel Security.

   - Ensure that adequate personnel security measures are implemented in the application systems development or maintenance environment by complying with applicable procedures of the Security Division of the Operations Support Directorate.

   - Depending on the sensitivity of the application system under development or maintenance, required security measures may include personnel security clearances, normal access authorizations, and access privileges and restrictions based on need to know or need to use.

4. Security Awareness Training.

   - Provide basic security awareness training to personnel involved in the development or maintenance of an application system. Relevant system and application security issues, threats, vulnerabilities, requirements, and responsibilities should be emphasized.

   - Develop application-specific security awareness training material as a security feature of the application system.

   - All personnel associated with the application system should be aware of the basics of information systems security and application-specific security issues, threats, vulnerabilities, countermeasures, and personal security responsibilities.

   - The Computer Security Act of 1987 requires all personnel involved with sensitive automated information systems, including managers, operators, and end-users, to receive basic awareness training in information systems security.

   - All FEMA end users and other personnel associated with FEMA systems are required to read and sign a security agreement. By signing the agreement, personnel acknowledge they have received, read, and understood FEMA information security policy, procedures, and practices.

   - Failure by personnel to comply with FEMA's security policies, procedures, and practices will be grounds for disciplinary action up to and including termination of employment or contracts.

Security Plan

1. Establish an application system security policy and plan for protecting each application system and its resources throughout the systems life cycle.

2. Define application system security and control objectives in the security policy and establish rules for accessing and using application system functions, data, and other resources based on the application's sensitivity, identified threats, vulnerabilities, and risks.

3. Establish a security plan for each sensitive application system. Follow OMB Bulletin No. 90-08, Guidance for Preparation of Security Plans for Federal Computer Systems that Contain Sensitive Information. Consult the FEMA Enterprise Security Manager to obtain additional guidance.

4. Document and maintain the application system security policy and plan as a permanent part of the application system documentation library.

Sensitivity Analysis

1. Perform application system sensitivity analysis early in the system development or maintenance process.
2. Analyze the nature and characteristics of application functions and data to determine the application's level of sensitivity in the areas of confidentiality, integrity, and availability.
3. Identify sensitive, critical, or powerful application system functions as the basis for defining functional access control and separation of duty requirements.
4. Review application data elements independently, in combination, and in the aggregate to determine the sensitivity or classification level of data processed by the application system as the basis for defining data access control requirements.
5. Consider the regulatory and policy framework surrounding the application to determine special requirements related to confidentiality, integrity, or availability.
6. Document the results of sensitivity analysis and maintain the documentation as a permanent part of the application system's documentation library.

Access Control

1. Define and document the access control security features of the application. Given identified subjects (users) or groups of subjects and given named objects (e.g., application functions, programs, transactions, accounts, data files, records, etc.), provide comprehensive predefined rules to determine which subjects or groups may be permitted access to a specific application object. Security clearance, formal access approval, and need to know or need to use must be considered in granting access to classified application systems and application objects. Need to know or need to use should be criteria in granting access to unclassified application systems and objects.
2. Incorporate an automated access control feature into the application's security design to assist in enforcing the access control policy. Physical and administrative control measures may be required to supplement automated controls.
3. Establish an access control level for the application commensurate with the sensitivity level of application functions and data. Some applications may require access control only at the program and data file level, while more sensitive applications may require intra-program functional access control or data access control at the record or field level.

4. Provide an access control mechanism that is capable of the following:

    - Denying access to all non-privileged users by default (i.e., denying access to all users initially and then permitting access to selected application users by authorized exception);

    - Supporting the principle of least privilege (i.e., supporting the capability of granting each user no more access to application functions and data than is absolutely necessary to perform assigned duties); and,

    - Supporting the principle of separating sensitive or critical application system duties, so no one individual user can have complete control over the application, adversely affect application resources, or use the application for personal gain. For instance, sensitive financial management system transactions should be independently originated, authorized, executed, and reconciled.

5. Integrate access control modes into the application security structure when necessary to provide a finer grain of control over application programs and data files.

6. Include documented, application-specific access control guidelines as a security feature of the application system to assist system managers, security administrators, and application managers in establishing an adequate access control structure for the application in an operational environment. Guidelines should identify sensitive or critical application functions, programs, and data objects requiring access restrictions on the basis of security clearance, formal access approval, need to know, or separation of duties. Additionally, guidelines should provide the detailed technical information that is necessary to configure the access control mechanism and enforce the application's access control policy.

7. Do not provide any application system feature or function that permits bypassing or requires disabling the access control mechanism.

8. Protect the access control mechanism and related data files from unauthorized access by non-privileged application users and other unauthorized personnel.

9. Access control for major mission-critical, cross cutting, or high-risk FEMA information systems should include the following procedures:

    - Develop a process whereby a user or a supervisor from a functional area such as a FEMA Directorate, Office, etc., enters and submits an automated system access request for approval by the appropriate supervisor.

    - Provide automated access for supervisors to approve or deny requests from users or supervisors under their purview.

- Provide for functional areas to designate authorizing officials with duties to review and approve or deny on behalf of the functional area requests for system access.
- The designated system administrator receives and reviews access requests, creates accounts, and notifies the functional areas, supervisors, and users.
- It is required that the functional area authorizing officials designate user accounts that are no longer required when their status changes and to certify at least quarterly to the system administrator that each user account is still needed.

The system administrator disables user accounts that are no longer required upon notification from functional area authorizing official's Risk Assessment.

1. Perform a basic risk assessment of each application system's processing and teleprocessing environment in light of the results of the application system sensitivity analysis. These results and the results of the risk assessment should provide the foundation for formulating application-specific security requirements (i.e., definitions of security features, both manual and automated, required to adequately protect application system resources).
2. Perform threat and vulnerability analysis as a means of assessing application system risks. Identify and assess the nature and extent of potential threat agents, threat effects on the application (e.g., unauthorized disclosure, modification, destruction of application software or data, hardware damage, delay or total denial of service, etc.), and vulnerabilities in the application's physical, system, and telecommunications environment.
3. Document the results of risk assessment and maintain the documentation as a permanent part of the application system's documentation library.

Security Requirements

1. Define application system security requirements during the requirements analysis and definition phase of the system's life-cycle process, or when major system change or enhancement requirements are formulated for an existing application system.
2. Consider the following when defining application system security requirements:
   - The nature and characteristics of application functions and data;
   - The results of application sensitivity analysis and risk assessment;
   - Federal laws, regulations, and standards, as well as FEMA policies and directives applicable to the application system's functionality, data, and level of sensitivity;
   - National security directives and FEMA information security policies and requirements when the application involves classified data processing, storage, or transmission; and

- Baseline application systems security feature requirements outlined in this document.

3. Document application system security requirements and maintain the documentation permanently in the application system's documentation library.

4. Submit security requirements to the application management for review and approval prior to beginning application system design.

Security Specifications

1. Define functional security specifications for the application system during the design phase of the system's life-cycle process. OMB Circular A-130 defines security specifications, as detailed descriptions of the safeguards required to protect an application.

2. Integrate security design specifications into the overall design of the application system.

3. Document security design specifications and maintain the documentation as a permanent part of the application system's documentation library. Security specification documentation should clearly relate design specifications to application security objectives and requirements to provide management assurance that specifications satisfy objectives and requirements.

4. Submit security design specifications to application management for review and approval prior to beginning formal development (programming) of the application system. OMB Circular A-130 requires security design reviews and management approval of application security design specifications.

System Protection

1. Base the extent of security control in the system development or maintenance environment on the sensitivity of the application system under development or maintenance. The more sensitive application functionality and/or data, the more essential it is to exercise continuous control over the system development or maintenance environment.

2. Ensure application system source code, object code, and authorized development or maintenance personnel can only access programming utilities resident on the system. Application code on the development or maintenance system should be protected against unauthorized disclosure, modification, and destruction through an access control mechanism that permits access only to identified, authenticated, and authorized personnel.

3. Conduct all system development or maintenance activities under closed shop or protective conditions. The development or maintenance system, system environment, and associated operations, as well as software and documentation products should be positively controlled with access granted only to authorized personnel. As noted above, the principle of least privilege should govern all access authorizations and activities.

4. Define and document system backup strategy and related procedures and assign backup responsibilities to protect software modules while under development or maintenance. Restrict backup and restore operations to a minimum number of authorized personnel and grant only authorized personnel physical access to areas used to store backup media.

Application System Design and Development

1. Use structured software engineering methodologies and techniques during system design, development, and maintenance to provide a controlled software-engineering environment resulting in reliable, maintainable, secure application system software. The use of structured techniques can produce modular software that supports security by isolating sensitive application system functions, which can be secured through an access control mechanism.

2. Do not design or program the application or any function in a way that permits system-level security controls to be circumvented or requires those controls to be disabled.

3. Do not design or program any mode of entry into the application system for maintenance, support, or operation that violates system or application-level security control features or permits bypassing those features (e.g., a trap door or back door designed to permit system development or maintenance personnel to bypass established access controls).

4. Do not design or program any mode of entry into the application system for maintenance, support, or operation unless it is an approved and documented feature of the application system.

5. Use structured walk-through (peer reviews) to identify and resolve potential security flaws in program design and code and to locate and remove trap doors or back doors and malicious code (computer viruses, time bombs, logic bombs, Trojan horses, etc.).

6. Do not hard code passwords or encryption keys in clear-text form in application system programs or data files.

7. Document and protect security-related code. This includes code that implements security features or mechanisms, code that performs highly sensitive or critical processing, and code that accesses highly sensitive or critical data during execution.

8. Review all changes to application system functional requirements, data requirements, and design specifications throughout the system's life-cycle process to determine whether corresponding changes are required in application system security requirements and specifications.

Audit and User Accountability

1. Incorporate an audit trail facility into the security design of the application to provide individual user auditability and accountability while on the system and operating within the application. The audit trail should be capable of associating and recording unique user IDs

with actions taken by individual application system users. For many applications, the audit trail facility provided by the operating system may be sufficient to provide application auditability and user accountability. Some applications, however, may require significantly enhanced audit capabilities (e.g., a financial management system). When additional audit capabilities are required, the application system itself or supporting software such as a database management system (DBMS) must address the requirement for an enhanced audit facility.

2. Provide an audit trail facility that is capable of the following:

   - Recording events and violations related to system log on, log off, and all changes to the security status of the system and application (i.e., all actions related to creating, modifying, or deleting data in system and application security files, including the audit trail file itself);

   - Selectively auditing and recording application events and violations related to application files opened for reading, opened for modification, renamed, or deleted, and application programs or procedures executed; and,

   - Recording the following information about events and violations: date, time, and user ID associated with events and violations recorded, type of event or violation (e.g., unauthorized attempt to open a file for modification), and descriptions of modifications made to security mechanisms and related data files.

3. Provide documented, application-specific guidelines for configuring and using the audit trail facility to monitor application system security and maintain individual user accountability.

4. Provide guidelines for reviewing and analyzing application audit trail data. Guidelines should include translations of programmer-defined application program and data file names into user-recognizable application functions and data names. This will assist in using the audit facility to detect unauthorized application access attempts, highly unusual patterns of authorized activity, or other anomalies that may indicate actual or potential security problems within the application.

5. Do not provide any application system feature or function that permits bypassing or requires disabling the audit trail mechanism.

6. Protect the audit trail facility and associated data files from access by non-privileged application users or other unauthorized personnel.

Input Controls

1. Design manual or automated input controls for the application system to ensure only authorized, valid, complete, and accurate source data is entered into the application system

database. Reliable input controls protect data integrity by ensuring authorized data is accurately converted into machine-readable form, not suppressed or lost, added to, duplicated, or otherwise improperly modified. Safeguards that reduce the potential for harmful effects from data entry errors or accidents (as opposed to deliberate acts) are a first step toward reducing opportunities for deliberate acts such as fraud or intentional misuse. An application that tolerates frequent errors is a fertile field for deliberate, malicious activities that can be masked as errors. Examples of input controls are:

- Source document preparation, review, and authorization procedures;
- Automated data validation techniques such as input screen validity checks, edit routines, or use of data dictionaries; and
- Manual or automated input reconciliation controls or procedures (e.g., comparing and reconciling system generated totals to manual control totals after data entry sessions).

2. Provide appropriate control procedures to protect sensitive application system source documents, if such documents are required by an application. For classified applications, protective measures for source documents must satisfy security requirements specified in FEMA Manual 1230.1.

Output Controls

1. Design security mechanisms and procedures to control output generated by the application system. Application output refers to printed reports and listings, the results of inquiries, displays on system terminals or workstations, and application data recorded on magnetic media or other types of storage media. Sensitive application system output should be appropriately controlled by manual or automated means to prevent unauthorized disclosure.

2. Provide application system security controls and procedures for producing, marking, handling, distributing and storing highly sensitive unclassified or classified application system output on electronic storage media, paper, or displayed on terminals or workstations.

Transmission Controls

1. Incorporate transmission security and control features into the application system's security design when the sensitivity of application data requires protection during transmission. Protection must be commensurate with the risk of disclosure, loss, misuse, alteration, destruction, or otherwise unavailable application system data.

2. Protect classified application data during transmission in accordance with communications security requirements specified in FEMA Manual 1200.5.

3. Employ encryption or other protection techniques, (message authentication, electronic certification or signature, etc.) approved by the National Institute of Standards and Technology, when unclassified data requires more than minimum protection to ensure data confidentiality or integrity during transmission.

Backup and Recovery

1. Provide a documented backup strategy and related procedures to protect against the loss or destruction of application software and data in the operational environment. Adequate application system backups of software and data are required to ensure the continuity of application system operations.

2. Design recovery features and provide associated procedures to permit recovery after system or application failure. If application system integrity and availability requirements dictate an increased level of protection in this area, incorporate automated recovery mechanisms such as those provided by DBMS technology (e.g., marking quiet points in the database, keeping a journal of before-and-after images, and using roll back and roll forward techniques to restore the integrity and availability of the application database).

3. Provide documented policies and procedures on archiving, retaining, and destroying application system data. In some application system areas, Federal or FEMA regulations may generate specific application systems requirements in these areas.

Contingency Planning

1. Develop, document, and maintain a contingency plan for the application system. A contingency plan consists of plans, procedures, arrangements, and required actions necessary to ensure the continuity of critical application system operations and the availability of application functions and data. OMB Circular A-130 requires a contingency plan as a security feature of each application system to ensure application users can continue to perform essential functions in the event that information technology support for the application is interrupted.

2. Address procedures and activities in the plan that ensure application system hardware, software, data, documentation, and other necessary application system items are readily available in backup form, should primary resources be damaged, lost, or destroyed.

3. Ensure the application system contingency plan is consistent with the disaster recovery or continuity of operations plan formulated for the facility or facilities where the application will be installed.

Security Tests

1. Test all security features incorporated into the application system. OMB Circular A-130 requires security testing prior to placing an application system into operation to ensure security controls function as designed and are operationally adequate.

2. Conduct security testing as part of the normal systems life-cycle testing process for new applications (i.e., during program or unit testing, system integration testing, and system acceptance testing).

3. Conduct security testing when an existing application is significantly modified or enhanced. Application system regression testing should include testing all existing security controls to ensure application changes and enhancements have not affected the functionality or reliability of these controls.

4. Conduct security testing in support of the OMB Circular A-130 requirement for application systems security certification. Security certification testing should be conducted as part of system testing or user acceptance testing for a new application or an existing application that has been significantly modified. Three types of testing are required in support of security certification:

    - Security feature functional testing to determine that specified security features exist, satisfy requirements and design specifications, and function properly;

    - Security feature performance testing to assess factors such as security feature reliability, availability, accuracy, response time, maintainability, ease of use, etc.; and,

    - Security feature penetration resistance testing to assess resistance against breaking or circumventing application system security controls.

5. Prepare security certification test documentation to include a security test plan, test scripts, and a test analysis report.

6. Maintain security certification test documentation as a permanent part of the application system documentation library.

Security Certification and Accreditation

1. Submit the application system to FEMA's Enterprise Security Manager for formal security certification and accreditation. Certification is the process of collecting, generating, and evaluating technical evidence as the basis for certifying that application system security features meet applicable Federal policies, regulations, and standards, and that test results demonstrate installed security safeguards are adequate for the application. Security certification is the technical basis for application system accreditation or formal management approval for operation in light of established security controls and residual risks.

2. Prepare a security certification report for the application system. Guidance on preparing the certification report is provided in FIPS PUB 102, Guideline for Computer Security Certification and Accreditation.

3. Maintain the security certification report as a permanent part of the application system documentation library.

4. Submit the security certification report and supporting application system security documentation to FEMA's Enterprise Security Manager for certification review prior to placing the application into operation. The Enterprise Security Manager shall evaluate application system security certification and conduct independent security reviews and assessments if additional certification evidence is required. If the application meets applicable Federal policies, regulations, and standards, and if security design reviews and test results demonstrate that security controls are adequate for the application; the Enterprise Security Manager shall recommend security accreditation to FEMA's Chief Information Officer.

Security Review and Recertification

1. Conduct security reviews or audits as the basis for recertification and reaccreditation of the application system. OMB Circular A-130 requires periodic review and recertification to evaluate the continued adequacy of implemented safeguards, to ensure all are still functioning properly, to identify new or modified threats and vulnerabilities, and to assist with the implementation of new security features where required.

2. Conduct security reviews or audits for recertification and reaccreditation:

   - At least every 3 years, or whenever an application system is significantly modified;
   - Whenever there are major changes in application system requirements, including changes in Federal or FEMA security policies or in user requirements related to security and control (as in the need to process data of a higher sensitivity or classification level); or
   - Whenever an application system security compromise, violation, audit, or risk assessment calls into question a prior security certification and accreditation.

3. Update the application system certification report and other security related documentation during the recertification process.

4. Maintain recertification documentation as a permanent part of the application system's documentation library.

5. Submit the recertification report and updated application security documentation package to the Enterprise Security Manager for recertification review and reaccreditation.

Configuration Management

1. Establish a configuration management system to authorize, control, and document changes to the application system hardware, software, and documentation baseline.

2. Maintain the configuration management system throughout the systems life-cycle process as prescribed in the FIRMPD, Chapter 2-4, Configuration Management.

3. Use the configuration management system to support security by ensuring application modifications and enhancements do not degrade the security posture of the application system.

Left blank intentionally

Chapter 5

Information Systems Standards

Left blank intentionally

5-1 Standardization Programs

Overview

1. Standards provide for the uniformity of information, software, and hardware and thus facilitate the interoperability and transportability of Information Systems resources. In addition they provide a common frame of reference for the interchange of information, ideas, and resources by Agency personnel. To take advantage of these benefits, FEMA will implement and maintain standardization in its information systems resources.

2. As required by OMB Circular A-130, FEMA will adhere to Federal Information Processing Standards (FIPS) except where it can be demonstrated that the costs of using a standard exceed the benefits of the standard or will impede the Agency in accomplishing its mission.

3. The remainder of Chapter 5 presents specific FEMA Information Systems and Information Technology standards. Software standards are identified in three categories: office automation software standards are described in Chapter 5-2, software application standards are described in Chapter 5-3, and Geographical Information Systems (GIS) standards are described in Chapter 5-6. Hardware standards for office automation are identified in two categories: office automation hardware standards (which are presented in three configurations: Desktop Computers [new], Laptop Computers [new], and 486 Upgrades) are described in Chapter 5-4, and hardware standards for servers and central processors are described in Chapter 5-5.

4. Each following Chapter contains a discussion of the identified software or hardware standard and an appendix containing the current FEMA baseline configuration standard. As baseline configurations standards are changed, the appropriate appendix will be replaced to reflect the change.

Responsibility

1. Associate Directors, Administrators, Regional Directors, and Office Directors are responsible for ensuring compliance with FEMA standards.

2. The IRB is responsible for approving standards based upon recommendation of the IRB-sponsored Information Systems Policy Advisory Group (ISPAG).

3. The Preparedness, Training and Exercises (PT&E) Directorate is responsible for user training courses based upon FEMA standards.

4. The Chief Information Officer is responsible for:

    - Waiving the standards in those instances where compliance with the standards would have an adverse impact on the accomplishment of the Agency's missions;

- Defining, documenting, and disseminating all agencywide information systems standards; and,
- Maintaining enterprise licenses and support services for the FEMA standards agencywide.

5. The ISPAG, in concert with the ITS Software Control and Integration Center, will conduct periodic reviews of updated release versions of the office automation software standards to determine the appropriateness of the updated versions to FEMA's requirements.
6. Federal Coordinating Officers and Emergency Support Team Directors have the authority to assign and authorize temporary use of FEMA information technology assets to support the disaster and emergency effort, to ensure compliance with FEMA's hardware and software standards.

5-2 Office Automation Software Standards

Overview

1. FEMA's Information Resources Board (IRB), which is responsible for overseeing consistency and integration of information systems on an agencywide corporate basis, has established the software standards listed below in accordance with FEMA's standardization program and the Federal Acquisition Regulations. These standards are integral to the automated systems modernization plan, which was identified in the FEMA 1995 Information Technology Operations Plan.

2. The office automation software standards are effective for purchases of information systems that require product features as described for those standards. Procurements in response to disasters are **not** exempt.

Procedures

Standards

Specific Office Automation Software Baseline Configuration Standards are given in Appendices at the end of this manual. These specific baseline configuration standards do not preclude the use of other existing software. However, this standard requires that subsequent information systems purchases support the current baseline configuration standards. A request for exemption from the baseline configuration standards must be approved by the IRB.

Implementation

1. Requisitions for office automation software and/or information systems (via FEMA Form 40-1 and FEMA Form 60-1, or by credit card and blanket purchase order purchases) must be submitted to ITS. IT requisitions must be submitted to ITS for procurements in excess of $5,000. Requisitions under the threshold are to be submitted to ITS for informational purposes. This will facilitate the planning and funding for enterprise licenses, the associated maintenance and support, and agencywide training. Requests for waivers also are to be submitted through ITS to the IRB.

2. The Acquisition Operations Division will, in the interest of the government, use the office automation hardware standards to negotiate the most appropriate contract vehicle for the procurement. It is anticipated that information needed for such procurements will be posted on the FEMA electronic mail bulletin board.

3. Reviews of the acquisition of information systems will be conducted by ITS to ensure compliance with FEMA's office automation software standards. Refer to Chapter 3-6 Purchasing via the Standardization Program.

Left blank intentionally

5-3 Application Software Standards

Overview

1. FEMA establishes software application standards in order to ensure that application development is consistent across the agency so that data can be shared among applications. FEMA will be developing a data warehouse architecture in the future. Standardization in data formatting and data dictionaries are critical to this effort.

2. Compliance to software application standards is required for all systems. Procurements and developments in response to disasters are **not** exempt.

Procedures

Standards

Specific application standards are given in Appendices at the end of this manual. These standards will be expanded as defined and approved by the Information Resources Board. Current application standards include:

Year 2000 Compliant Date Fields

When developing information systems which will be required to perform date/time processing involving dates subsequent to December 31, 1999, FEMA will ensure that solicitations, contracts and internal developments:

- Require that the system be Year 2000 compliant; or
- Require that non-compliant information technology be upgraded to be Year 2000 compliant prior to the earlier of (1) the earliest date on which the system may be required to perform date/time processing involving dates later than December 31, 1999, or (2) December 31, 1999.

Stand-alone legacy systems may meet Year 2000 compliance by a variety of measures. It is critical that data exchange formats for dates be standardized. All FEMA applications must comply with the National Institute of Standards Technology for date fields for data exchange.

Left blank intentionally

5-4 Office Automation Hardware Standards

Overview

1. FEMA's Information Resources Board (IRB), which is responsible for overseeing consistency and integration of information systems on an agencywide, corporate basis, has established the hardware standards listed below in accordance with FEMA's standardization program and the Federal Acquisition Regulations. These standards are integral to the information technology modernization plan, which is identified in the FEMA Information Technology Operations Plan.

2. The office automation hardware standards for desktop and laptop computers are effective for purchases of information technology that require product components as described for those standards. Procurements made in response to disasters are **not** exempt.

3. FEMA's office automation hardware standards are categorized in two (2) configurations: purchases of new desktop computers, and purchases of new laptop computers. FEMA's policy for disposition of obsolete computers, including sharing and reuse, is outlined in Chapter 3-10 of the FIRMPD.

Procedures

Standards

1. Specific Office Automation Hardware Baseline Configuration Standards are given in the Appendix at the end of this manual. These specific baseline configuration standards do not preclude the use of other existing hardware. However, these standards require that future purchases of computer components and of desktop and laptop computers be in compliance with the baseline configuration standards, both hardware and software. Software pre-loaded on newly purchased computers, including operating systems, must comply with FEMA's software baseline configuration standards. For example, computers purchased new must be preloaded with the standard operating systems. Requests for exemption from the standards must be approved by the IRB chair or the IRB's designee.

2. The hardware baseline standards are to be understood as the minimum acceptable configuration and can be exceeded with program office justifications. The standards do not preclude the use of other existing hardware as long as the existing hardware can support the standard software. However, the established hardware baseline standards do require that future purchases of computer components and of desktop and laptop computers be in compliance with the standards, both hardware and software. Software pre-loaded on newly purchased computers, including operating systems, must comply with FEMA's baseline software standards. Requests for exemption from the standards must be approved by the IRB chair or the IRB's designee.

Implementation

Requisitions for information systems and components (via FEMA Form 40-1 and FEMA Form 60-1, or by credit card and blanket purchase order purchases) must be submitted to ITS. Guidance requires that all requisitions for IT purchases be submitted to ITS. This will facilitate the planning and funding for FEMA's information technology modernization plan, and the associated maintenance and support. Requests for waivers also are to be submitted to the CIO.

When preparing requisitions for microcomputer hardware, requesters will specify whether the requirement is for desktop or laptop units, and the quantity and cost of the units. Submission of hardware configuration specifications will no longer be required. The Acquisition Office will, in the interest of the government, use the office automation hardware standards to negotiate the most appropriate contract vehicle for the procurement. It is anticipated that information needed for such procurements will be posted on the FEMA electronic mail bulletin board.

5-5 Hardware Standards for Servers and Central Processors

To Be Provided

Left blank intentionally

5-6 Geographical Information Systems Standards

Overview

FEMA's Information Resources Board (IRB), which is responsible for overseeing consistency and integration of information systems on an agencywide corporate basis, has established MapInfo Professional as the Agency standard for Desktop GIS in accordance with FEMA's standardization program and the Federal Acquisition Regulations. FEMA will continue to support multiple vendor GIS software in server and modeling applications. Server and model software must interface with the desktop standard. These standards are integral to the National Emergency Management Information System and other agencywide systems.

Procedures

The GIS Desktop software standard is effective for purchases of information systems that require product features as described for those standards. Procurements in response to disasters are **not** exempt.

Left blank intentionally

APPENDICES TO CHAPTERS

IRM REGULATORY REFERENCE GUIDE

GLOSSARY

Left blank intentionally

Appendix to 3-8 Writing Accessible HTML Documents

Because of the structured nature of HTML, the WWW provides tremendous power and flexibility in presenting information in multiple formats (text, audio, video, graphic, etc.). However, the features that provide power and elegance for some users present potential barriers for others. For example, servers which require the viewing of graphic images are inaccessible to blind users. Careful design and coding of information can alleviate access barriers. The following technical guidelines should be followed in designing and coding accessible HTML documents.

It is important to note that implementing these guidelines does not compromise the aesthetics or functionality of the server.

Guideline: Every graphic image should have associated text.

Rationale:

If the person viewing the information is using a character-based program (e.g. Lynx) or has graphics turned off in other browsers, the link will be lost.

Strategy:

Use *ALT* attribute in image reference anchors and include selection text within the anchor.

Example of inaccessible code:

On January 20, 1993, William Jefferson Clinton
<A HREF="/images/raw/bill-portrait.gif" >
<IMG SRC="/images/small/bill-portrait.gif" > < /A >
was sworn in as the 42nd President of the United States, and moved into the White House with his wife.
< A HREF="/images/raw/hillary-portrait.gif" > < IMG SRC="/images/small/hillary-portrait.gif" > < /A >
Hillary Rodham Clinton and their daughter Chelsea.

In this example, the graphics convey no information about the link. A user with a character-based application would not know the nature of the link.

Accessible code would look like this:

Example of accessible code:

On January 20, 1993,
<A HREF="/images/raw/bill-portrait.gif" >
<IMG SRC="/images/small/bill-portrait.gif" alt="**Picture of President Clinton...**" >
William Jefferson Clinton < /A > was sworn in as the 42nd President of the United States, and moved into the White House with his wife, < A HREF="/images/raw/hillary-portrait.gif"

> < IMG SRC="/images/small/hillary-portrait.gif" **Alt="Picture of Hillary Rodham Clinton and their daughter Chelsea."** > Hillary Rodham Clinton and their daughter Chelsea. < /A >

This example adds both the "alt" image expression and a text descriptor within the anchor.

Guideline: If image maps are used, there should be an alternate method of selecting options.

Rationale:

If the person viewing the information is using a character-based program (e.g. Lynx) or is using a computer which is not capable of displaying graphics, the image will be completely lost; there will be no way to select options.

Example of inaccessible code:

< TITLE > Map of Washington, DC. < /TITLE > < H1 > Click on a building below < /H1 > < A HREF="http://www.whitehouse.gov/img/dcmap" > < IMG SRC="http://www.whitehouse.gov/images/large/DC_map.gif" ISMAP > < /A >

In this example, the entire page is lost for character-based viewers. An alternative way to handle this would be to present an option for a list of buildings. This would give all viewers a better understanding of what information was available.

Example of accessible code:

< TITLE > Map of Washington, DC. < /TITLE > < H1 > Click on a building in the map below or select from < A HREF="http://www.whitehouse.gov/dcmap_list.html" > list of buildings < /A >< /H1 > < A HREF="http://www.whitehouse.gov/img/dcmap" > < IMG SRC="http://www.whitehouse.gov/images/large/DC_map.gif" ISMAP alt=map of Washington"> < /A >

In this example, the user is given the choice of an alternate page "dcmap_list.html" which might look something like this:

< TITLE > Buildings in Washington, DC. < /TITLE >
<H1> Select from the list of buildings below </H1 >
<UL>
<LI> <A HREF="http://www.doc.gov"> Department of Commerce </A > 16th St. N.W
< LI > < A HREF="http://www.DOI.gov/Parks/Washington_Monument.html" > Washington Monument < /A > Between 15th and 17th south of Constitution Ave.< LI > < A HREF="http://www.doi.gov">
Department of Interior < /A > 14th St. N.W < LI >
...
< LI > ...
< /UL >

There are two ways to implement this guideline. The first way is to modify every page which contains an ISMAP so that on each page the user is offered a choice of graphic or text selection. Another method however, is to offer the user a choice at the home page. With this method if the user selects “no graphics” at the home page, a separate set of pages with no ISMAPs will be selected.

Inclusion of a second home page would allow the user to select “no graphics” The code would look like this:

Select <A HREF="http://www.whitehouse.gov/Welcome-no_graphics.html" > no graphics < /A > if you would like to browse without pictures.

Guideline: Include detailed descriptive “comments” with all JPEG images.

Rationale:

Although JPEG files are used for high resolution images, there is still useful information that can be conveyed to blind users. One example of this would be JPEG images of pages in a manuscript. In this case, a full transcript of text contained in the image should be included.

Strategy:

Use a JPEG file editor to include information in the “comments” section of the JPEG file. Alternatively, a separate “text” file could be linked to the image.

Guideline: Provide text transcriptions or descriptions for all audio clips.

Rationale:

Audio clips are of no use to users with hearing impairments or who are connecting through systems which do not support audio.

Inaccessible code:

The President asked
< A HREF="http://www.whitehouse.gov/images/raw/al-portrait.gif" >
< IMG SRC="http://www.whitehouse.gov/images/small/al-portrait.gif" >
Vice President Gore < /A > to head up the
< A HREF="http://www.npr.gov/" > National Performance Review (NPR)
< /A > a project to make government work better and cost less.
< A HREF="http://www.whitehouse.gov/Sounds/Gore.au" >
< IMG SRC="http://www.whitehouse.gov/icons/audio.gif"> < /A >

This code has two problems. First, the sound clip icon does not have associated text and therefore can not be seen with text browsers. Second, the link is of no use to users who are hearing impaired or do not have sound equipped viewers.

Suggested code:

The President asked
< A HREF="http://www.whitehouse.gov/images/raw/al-portrait.gif" >
< IMG SRC="http://www.whitehouse.gov/images/small/al-portrait.gif"
alt="Picture of Al Gore" >
Vice President Gore < /A > to head up the
< A HREF="http://www.npr.gov/" > National Performance Review (NPR)
< /A > a project to make government work better and cost less.
< A HREF="http://www.whitehouse.gov/Sounds/Gore.au" > You can hear
< IMG SRC="http://www.whitehouse.gov/icons/audio.gif" alt="audio icon">
< /A > or < A HREF="http://www.npr.gov/Al_N

Authored by Paul Fontaine
Center for Information Technology Accommodation
General Services Administration
Washington, DC. USA

http://www.gsa.gov/coca/

June 5, 1995 DRAFT

Appendix to 3-9 Electronic Mail Naming Convention Standard

cc:Mail Naming Conventions

To provide for user name recognition in the cc:Mail directory and for ease of user access, the naming conventions use the minimum number of characters that are functionally descriptive. The naming structure includes a dash (-) that separate data within a field and the fields are separated by a slash. User names may contain up to a maximum of 25 contiguous characters (spaces are not valid). Comment entries may contain up to 17 contiguous characters that will display with the page/screen width without scrolling.

The FEMA cc:Mail directory standards for User Names and Post Office Names are identified in figures 1 and 2 respectively. The cc:Mail standards to be used in conjunction with the Federal Response Plan (FRP) are identified as follows:

FRP Emergency Support Functions Matrix
FRP Name Addressing Scheme
Group 1, Primary and Support Government Agencies
Group 2, Primary ESFs & EST Positions at FEMA Headquarters
Group 3, Primary ESFs & Positions at an established DFO
Group 4, Emergency Response Team ESFs in Transition
Group 5, Primary ESFs & Positions at ROC AND EOC

The cc:Mail directory (mailing list) display includes the following:

Name	*Loc*	*Last Checked In*	*Comment*

where: Name is the User Name and FRP Name.
Loc is the location of the file server to the user performing the name search.
Last Checked In is the date and time that the user last logged into cc:Mail.
Comment is the area for descriptive information.

cc:Mail User Naming Convention

The User Name is entered into the directory as follows:

LastName, Firstname (Optional Middle Initial)

Examples: Happygo, Lucky

Each User Name should be listed in the directory in the manner in which the user wishes to be addressed. If a nickname, such as "Luck," is used for business purposes, that nickname may supplant either the lastname, firstname or middle initial. FEMA employees must be identified in the Comment area.

Example: Happygo, Luck

An acronym which is based upon a function may be entered into the cc:Mail directory as a user name. The acronym must have a comment entry which defines its function and the location of its post office.

Examples: NNOC, SCIC, EICC

User Name Comment Field. Enter "FEMA" must be preceded by the Office Symbol for all FEMA employees as follows:

FEMA/Office Symbol

Office symbol is the user's current office designation. It may be followed by any additional comments to identify specific groups, or contractor support personnel.

Format: FEMA/XX-YY-ZZ
where: XX is the directorate level, YY is the Division level, ZZ is the Branch level.

Examples: FEMA/RR-DA-IA
OS-AQ-PE/Contractor ABC

A comment entry for a User Name acronym must define its function and/or location.

Examples: NNOC, National Network Operation Center
SCIC, Software Control and Integration Center
EICC, Emergency Information Coordination Center

Figure 1

SITE CODES

Site	Site Code
Headquarters	HQ
Special Facility	SF
NETC, Emmitsburg	EM
Olney, MD	FS
Charlottesville, VA	CV
Region 1	R1
Region 1 FRC	F1
Region 2	R2
Region 3	R3
Region 4	R4
Region 4 FRC	F4
Region 5	R5
Region 5 FRC	F5
Region 6	R6
Region 7	R7
Region 8	R8
Region 9	R9
Region 10	R0
Nat'l Warning Center	NW
Nat'l Teleregistration Center	NT
Bluegrass, SC	BL
Palo Pinto, TX	PP
DFO1	D1
DFO2	D2
DFO3	D3
FEMA Switched Network	-

cc:Mail Naming Convention for Federal Response Plan Addressing

The Federal Response Plan (FRP) identifies the primary support agencies' functions, the Emergency Support Function (ESF) numbers, the agency names, and agency acronyms or abbreviations as described on the following page.

The FRP ESF and Emergency Support Team (EST) addressing scheme is categorized into five groups of use as the naming convention in cc:Mail.

Group 1	Primary and Support Government Agencies
Group 2	Primary ESFs and EST Positions at FEMA Headquarters
Group 3	Primary ESFs and EST Positions at an established DFO
Group 4	Emergency Response Team ESFs in Transition
Group 5	Primary ESFs and Positions at ROC and EOC locations

Group 1 Where the primary and support agencies are assigned at their base location:
HQ-(Agency Abbreviation/Acronym)-(opt)

Group 2 Where the EST (a constant) and ESF 2-digit number or positions symbol (i.e., DIR=Director, LOG=Logistics, OPS=Operations, FIN=Finance) are located at FEMA headquarters:

EST-ESF(##)/Position Symbol-(opt)

Group 3 Where the Emergency Support Function is located at a State Disaster Field Office (DFO) and the DFO unique number is assigned:

(State Abbreviation)-DFO(xxxx)-ESF(##)/Position Symbol

Group 4 Where the Emergency Response Team (ERT) is located at a State locality:

(State Abbreviation)-(Locality Name)-ERT-ESF(##)

Group 5 Where the Emergency Support Function is located at a Regional Operating Center (ROC) or an Emergency Operating Center (EOC):

(Regional Site Code)-ROC-ESF(##)/Position Symbol

or

(Regional State Abbreviation)-EOC-(State Abbreviation covered by region)

Emergency Support Function Matrix

Emergency Support Function	ESF Number	Primary Support Agency	Acronym/Abbreviation
Transportation	ESF01	Department of Transportation	DOT
Communications	ESF02	National Communications System	NCS
Public Works and Engineering	ESF03	DOD, US Army Corps of Engineers	DOD-USACE
Firefighting	ESF04	USDA, Firefighting Division	USDA-FS
Information and Planning	ESF05	Federal Emergency Management Agency	FEMA
Mass Care	ESF06	American Red Cross	ARC
Resource Support	ESF07	General Services Administration	GSA
Health and Medical Services	ESF08	Health and Human Services	DHHS
Urban Search and Rescue	ESF09	Federal Emergency Management Agency	FEMA
Hazardous Materials	ESF10	Environmental Protection Agency	EPA
Food	ESF11	USDA, Food and Nutrition Services	USDA-FNS
Energy	ESF12	Department of Energy	DOE
	ESF13	Nuclear Regulatory Commission	NRC

Group 1
Primary and Support Government Agencies

Group 1 Naming Standard Formula

HQ-AGY-EXP
where, AGY=Agency Abbreviation/Acronym
EXP=Expansion ID for further grouping (Optional)

Example 1: HQ-DOD-USACE is the Department of Defense, Army Core of Engineers Division, at their home base location in Washington, DC.

Group 1 Naming Standard Formula

1. AID
2. AID-OFDA
3. ARC
4. DHHS
5. DHUD
6. DLA
7. DOC
8. DOD-USACE
9. DOD-DOMS
10. DOE
11. DOED
12. DOI
13. DOJ-FBI
14. DOL
15. DOS
16. DOT
17. EPA
18. FEMA
19. FCC
20. GSA
21. ICC
22. NASA
23. NIST
24. NCS
25. NRC
26. OPM
27. TREAS
28. TVA
29. USCG
30. USDA-FNS
31. USDA-FS
32. USGS
33. USPS
34. VA
35. WHITEHOUSE

Note: Numbers 1-34 represent the Primary and Support agencies listed in the FRP.

Additional agencies and departments of agencies may be added as connectivity occurs.

Group 2
Primary ESFs and EST Positions at FEMA Headquarters

Group 2 Naming Standard Formula

(1) EST-ESF#-EXP or EST-Position-ESP
where, #= ESF Number as defined in the FRP (2 digits: 01-12)
EXP=Expansion ID for further grouping (Optional)
Position=Function IDs as follows:

DIR - Director
LOG - Logistics
OPS - Operations
FIN - Finance
EXT - External Affairs

Example 1: EST-ESF01 is the Department of Transportation desk at FEMA Headquarters

Example 2: EST-DIR is the EST Director at FEMA Headquarters

Example Listing of Group 2 Names

1. EST-ESF01
2. EST-ESF02
3. EST-ESF03
4. EST-ESF04
5. EST-ESF05
6. EST-ESF06
7. EST-ESF07
8. EST-ESF08
9. EST-ESF09
10. EST-ESF10
11. EST-ESF11
12. EST-ESF12
13. EST-ESF13
13. EST-DIR
14. EST-LOG
15. EST-OPS
16. EST-FIN
17. EST-EXT

Note: Numbers 13 through 17 indicate 13 additional addresses utilized by the EST at FEMA Headquarters, EICC.

Further expansions will be used to indicate separate workstations for each function and to mandate use of unique user IDs. For example, if the Logistics desk has three additional workstations besides the primary Chief of Logistics workstation, the IDs EST-LOG-A, EST-LOG-B, EST-LOG-C may be established. Additional workstation IDs will be determined by the support function chief and reported to the FEMA cc:Mail National System Administrator.

Group 3
Primary ESFs and Positions at an established DFO location

Group 3 Naming Standard Formula

(1) State-DFOxxxxESF# or (2) State-DFOxxxx-Position
where,

State=Abbreviation
xxxx=Unique Disaster or Emergency Number assigned by White House
#=ESF Number as defined in the FRP
Position=Function IDs as follows:

- FCO - Federal Coordinating Officer
- OPS – Operations
- LOG – Logistics
- FIN – Finance
- DCO - Defense Coordinating Officer
- EXT - External Affairs

Example 1: FL-DFO9999-ESF01 is the Department of Transportation position at the declared DFO number 9999 site in Florida.
Example 2: FL-DFO9999-FCO is the Federal Coordinating Officer for the declared DFO number 9999 site in Florida.

Example Listing of Group 3 Names

4. FL-DFOxxxx-ESF01
5. FL-DFOxxxx-ESF02
6. FL-DFOxxxx-ESF03
7. FL-DFOxxxx-ESF04
8. FL-DFOxxxx-ESF05
9. FL-DFOxxxx-ESF06
10. FL-DFOxxxx-ESF07
11. FL-DFOxxxx-ESF08
12. FL-DFOxxxx-ESF09
13. FL-DFOxxxx-ESF10
14. FL-DFOxxxx-ESF11
15. FL-DFOxxxx-ESF12
16. FL-DFOxxxx-FCO
17. FL-DFOxxxx-OPS
18. FL-DFOxxxx-LOG
19. FL-DFOxxxx-FIN
20. FL-DFOxxxx-DCO
21. FL-DFOxxxx-EXT

Note: Numbers 13-18 indicate the primary addresses utilized for sending mail to DFO Point of Contacts other than the ESFs at the DFO location.

Group 4
Emergency Response Team ESFs in Transition

Group 4 Naming Standard Formula
State-EXP-ERT-ESF#
where,

State	=Abbreviation
EXP	=Expansion ID for further grouping to indicate specific location
#	=ESF Number as defined in the FRP

Example: HI-OAHU-ERT-ESF1 is the DOT ERT at Oahu, Hawaii, for Iniki
or
UT-ERT-ESF1 is the DOT ERT in Utah for Response 93

Group 4 Names

1. HI-OAHU-ERT-ESF1
2. HI-OAHU-ERT-ESF2
3. HI-OAHU-ERT-ESF3
4. HI-OAHU-ERT-ESF4
5. HI-OAHU-ERT-ESF5
6. HI-OAHU-ERT-ESF6
7. HI-OAHU-ERT-ESF7
8. HI-OAHU-ERT-ESF8
9. HI-OAHU-ERT-ESF9
10. HI-OAHU-ERT-ESF10
11. HI-OAHU-ERT-ESF11
12. HI-OAHU-ERT-ESF12

Note: Group 4 names will be used when an Emergency Response Team is first deployed. These names are for temporary use until a DFO is formally established.

Group 5
Primary ESFs at ROC and EOC locations

Group 5 Naming Standard Formula
(1) R*-ROC-ESF#-EXP or (2) R*-ROC-Position-EXP
where, *=FEMA Region Number (1-10)
EXP=Expansion ID for further groupings
# =ESF Number as defined in the FRP
Function IDs as follows:
FCO - Federal Coordinating Officer
OPS – Operations
LOG – Logistics
FIN – Finance
DUTYOFF - Duty Officer
or (3) State-EOC-EXP

where,

State	=State Abbreviation
#	=ESF Number as defined in the FRP
EX	=Expansion ID for further groupings

Example: R2-ROC-ESF1 is the ID used for the Regional Operating Center for DOT at FEMA Region 2. NY-EOC is the ID used for the Emergency Operating Center for the state of New York

Group 5 Names

1. R1-ROC-ESF01
2. R1-ROC-ESF02
3. R1-ROC-ESF03
4. R1-ROC-ESF04
5. R1-ROC-ESF05
6. R1-ROC-ESF06
7. R1-ROC-ESF07
8. R1-ROC-ESF08
9. R1-ROC-ESF09
10. R1-ROC-ESF10
11. R1-ROC-ESF11
12. R1-ROC-ESF12
13. R1-ROC-FCO
14. R1-ROC-OPS
15. R1-ROC-LOG
16. R1-ROC-FIN
17. R1-ROC-DUTYOFF

18-23. MA-EOC (and -ME,-NH,-CT,-VT,-RI)
24-27. NY-EOC (and -NJ,-PR,-VI)
28-33. PA-EOC (and -MD,-DE,-WV,-VA,-DC)
34-40. GA-EOC (and -TN,-NC,-SC,-FL,-MS,-KT)
41-46. IL-EOC (and -MI,-MN,-IN,-OH,-WI)
47-51. TX-EOC (and -NM,-OK,-AK,-LA)
52-55. MO-EOC (and -IO,-KS,-NE)
56-61. CO-EOC (and -UT,-WY,-MT,-ND,-SD)
62-65. CA-EOC (and -NV,-AZ,-HI)
66-69. WA-EOC (and -AL,-OR,-ID)

Note: Numbers 13-17 indicate the primary addresses utilized for sending mail to ROC Point of Contacts other than the ESFs.+++

Appendix to 4-3.A Firewall Management and Administration Guidelines

This document outlines the management and tasking for Firewall Administration. At minimum, the Firewall Administration tasks relate to Firewall hardware and software, particularly in the following subject areas:

- File management
- System backups
- System restores
- Disk management
- User login accounts (if any)
- Security administration
- System documentation
- Assistance with Internet service conditions
- Addition or deletion of IP subnets
- Maintaining a file of change requests

System ("root") passwords will be held only by the designated Agency Firewall Administration personnel (i.e., Firewall Administrator and Backup Administrator) and filed with CIO.

Internal firewalls used to protect Agency information systems must support access restriction by network segment or domain (packet filtering) as well as access restrictions by service (FTP vs. Telnet etc.). Internal firewalls will also provide session and traffic logging, event alarms, and support of centralized management.

Internal firewalls or filtering routers provide strong access control and support for auditing and logging for any systems hosting FEMA critical applications. These controls will be used to segment the internal FEMA network to support the access policies developed by the designated owners of information.

System passwords will be changed as often as needed in order to maintain the highest level of system security and data integrity. At minimum, "root" passwords will be changed every 60-90 days. To maintain security, password rotation schedules will not be published.

System Changes. All changes, modifications, upgrades, enhancements to the FEMA Internet firewall will be made in response to a known cause or vendor-released patch, and will be reviewed, in advance and in writing (Email is acceptable) by the Firewall Administration personnel. Only the Firewall Administration personnel may make changes.

System Documentation and Logs. All changes upgrades, enhancements and modifications to the hardware, software and peripherals will be recorded, in as much detail as possible, in a Firewall Administration Log. The log may be handwritten or electronic and will be furnished to Firewall Administration's management. An up-to-date "working copy" of the log will be retained on-site for auditing purposes. A second copy of the log will be stored off-site.

The proxies, kernels and authentication management system automatically write information to the logs. Every night, the "cron daemon" runs a shell script that rotates compresses and removes the log files. By default, the system retains the logs for fourteen (14) days, though this number can be adjusted. The daily script rotates the reports and compresses older log files. Also by default, the firewall keeps seven (7) days of logs in ASCII format and the previous seven (7) days in compressed format. The types of information that the kernel logs, as well as the contents of the log can also be customized.

- Firewall Log Retention - Logs will be retained for a rolling period of at least sixty (60) days.

- Firewall Log Distribution - Neither raw system logs nor extracts from the logs may be provided to any person other than the Firewall Administration personnel without the specific written authorization of the CIO.

System Reports. The firewall contains several reporting mechanisms that sort through the log files and summarize information. These are broken into two (2) main types of reports:

- Service Summary Reports. This report includes both daily and weekly usage and user information on a service basis. Each night or once a week, the firewall can mail the reports. The firewall does not store the daily or weekly reports.

- Exception Reports. This report, by default, defines a list of items that are not noteworthy and ignores such entries in the logs. For example, the firewall default is to ignore successful authentication when parsing the log file. Successful authentication attempts are a normal part of firewall activity, while unsuccessful authentication attempts could be a sign of a potential attack. Therefore, the exception report includes all unsuccessful authentication attempts from the logs. Any item that the firewall has not specifically been told to ignore, it reports. The nightly script summarizes all of the noteworthy items in the log files since the last time it created a report and, by default. The exception report is not stored by the system.

Reports can be custom configured for the events the firewall will ignore in the Exception Report, for the report recipient, enable and disable daily and weekly Service Summary reports, enable and disable Exception reports and customize the Exception reporting interval.

Subnet Proxies. FEMA subnets are proxies to the firewall in order that the internal IP addresses will not be publicized on the public side of the firewall. By configuration of the netstart table, all subnets passing through the firewall proxy take on the firewalls outside IP address. This reduces the risk that a "hacker" could breach the firewall security by masquerading as an internal machine.

Suspected Intrusion. If compromise is suspected, the netperm table will be modified to deny access from all hosts for all applications until the logs can be reviewed and appropriate countermeasures, as needed, have been installed and tested. Only the Firewall Administration personnel will execute such action.

Internal Site Managers and Network administrations shall report any suspicions concerning intrusions and Internet-borne viruses, with as much supporting documentation as possible, to the Enterprise Security Manager and to the Email address established for this purpose:

firewall@fema.gov.

Testing. Attack tests will be performed on an irregular schedule, to simulate as rigorously as possible a real hacking attack, including but not limited to IP spoofing, denial of service and other known and emerging attack modes.

Auditing. The system will be audited on a regular unpublished schedule. Audits will include, but are not limited to, documentation, process and quality controls. Results of these types of audits will be presented to management of the Information Technology Services Directorate.

Physical Security. The current firewall system is secured in a FEMA protected computer room. The firewall administration personnel will conduct periodic inspections to determine if any undocumented attempts to circumvent the devices have occurred. This will include a visual inspection of wiring hubs, cables, switches and other devices that provide connection to the system. Each inspection will be documented.

Left blank intentionally

Appendix to 4-3.B Remote Access Using Hardware Tokens and TACACS

The three major components of network security are authentication, authorization, and accounting (AAA). To address the remote access aspects of network security, FEMA has implemented the Terminal Access Controller Access Control (TACACS) protocol coupled with hardware tokens. The access device challenges users immediately for a user identification and password; utilizes the TACACS protocol the Access Server to forward the user name and one time password information to a centralized authentication server. If the user identification and password are valid, the Access Server allows the remote connection into the network. If either the user identification or the password is incorrect the Access Server immediately hangs up the modem.

Authentication. Determines whether a valid user has attempted access and if the user will be allowed access to the network. It allows Network Administrators to bar intruders from their networks. Simple authentication methods use a database of user names and passwords while more complex methods use one-time passwords.

Authorization. Determines what users are allowed to do. Authorization allows Network Administrators to limit network services available to each user to that which is minimally essential. This approach limits the exposure of the internal network to outside callers and simplifies the view of the network for the less technical remote access user. Authorization allows mobile users to connect to the closest local connection and still have the same access privileges of their local networks. This also may restrict a Network Administrator to issuing specific commands on predetermined network devices.

Accounting. Keeps track of who did what, when, and where. Network Administrators may need to recreate a session at a later time. Accounting provides logs of connection times and bytes transferred. Accounting can also be used to track suspicious connection attempts to the network.

Central management of access security servers is required for FEMA. The client/ server architecture of TACACS allows all security information to be located in a single, centralized database, instead of being scattered around a network in many different devices. Changes to the database are made in a few security servers instead of in every access point in the network. This type of design allows for easy scalability and extendibility.

All TACACS user names shall be registered and maintained through the National Help Desk. Users shall be assigned a hardware token for one time password generation at that time. Users are responsible for the hardware tokens; if they are lost, users must notify the National Help Desk immediately.

Dial-in Access:

When hardware tokens become available all users who access the FEMA system shall come in through dial-in connections using TACACS and hardware tokens. The Enterprise Security Manager must approve systems that provide direct dial-in connections to FEMA production systems. All in-bound modem access shall be via a modem server controlled by the National ITSC at Mt. Weather. The use of desktop modems to support dial-in access to FEMA systems is prohibited.

Information regarding access to FEMA computer and communication systems, such as dial-up modem phone numbers, is considered restricted. This information must NOT be posted on electronic bulletin boards, listed in telephone directories, placed on business cards, or otherwise made available to third parties without the advance written permission of the ESM. The ESM shall periodically scan direct dial-in lines to monitor compliance with policies and may periodically change the telephone numbers, after providing 30-day advance notice to users, to make it more difficult for unauthorized parties to locate FEMA communications numbers.

Dial-out Access:

All users who need to access systems external to FEMA via dial-out modems must do so through modem services approved by the ESM and controlled by the National ITSC at Mt. Weather. The use of desktop modems to support dial-out access to external systems is prohibited for machines connected to a LAN or WAN.

Appendix to 4-3.C Disaster Field Office's Network Administrators Guide

A Disaster Field Office (DFO) network has some unique characteristics. This office is typically set up quickly; is staffed by personnel drawn from throughout the agency plus local hires; has other Federal, State, and local personnel intermixed in the network environment; and suffers frequent staff turnover. Network administration security policy, procedures, and practices apply to and shall be the responsibility of the DFO Network Administrator. Due to these unique circumstances, special attention must be applied to the DFO network.

This appendix is intended to be a concise reference for the DFO Network Administrator who shall refer to the FEMA Information Resources Management Policy and Procedural Directive (FIRMPD) for additional detail. The Network Administrator shall refer any security questions or requests for assistance directly to the Enterprise Security Manager (ESM) or through the national Information Technology Service Center at Mt. Weather (540) 542-4000.

Password Management:

- All passwords shall be at least six characters in length and include at least one numeric or special character.
- Passwords must be changed at least every 90 days.
- After three consecutive failed log-in attempts, login shall be temporarily disabled.

Virus Control:

- Virus detection software shall be installed and run on all computers, clients and servers that are connected to FEMA networks.
- FEMA currently recommends the use of Command Systems' FPROT software. Any Network Administrator that chooses to use a different software package is responsible for maintaining up to date virus signature files.
- Virus controls must be applied to all downloads from the Internet or World Wide Web.

Remote Access:

- Desktop modems are prohibited without a waiver from the Enterprise Security Manager.
- All dial-in access is prohibited except via Terminal Access Controller Access Control Systems (TACACS) approved by the ESM and operated by the ITS directorate.
- No connection to external networks is allowed without written approval from the Enterprise Security Manager.
- Internet Access is available to the DFO via the connection to the FEMA Enterprise Network. Any other connection to Internet (either directly or through a state connection) is prohibited.

Incident Detection:

- The Network Administrator shall review all system logs and audit trails on a weekly basis.
- The Network Administrator shall promptly report all suspected security incidents to the national Information Technology Service Center at Mt. Weather (540)-542-4000.
- Break-ins must be reported to the Office of Inspector General.

Personal Accountability:

- The Network Administrator is responsible for all computers, software, and communications equipment connected to the LAN.
- The Network Administrator is responsible for any LAN operations that disrupt FEMA WAN operations. Failure to restore operations promptly or to avoid repeated disruptions is grounds for disciplinary action up to and including dismissal.

Modems:

- Dial-in Access. In the DFO, modem dial-in access is prohibited unless approved by the ESM. The Enterprise Security Manager must approve systems, which provide direct dial-in connections to FEMA production systems. All in-bound modem access shall be via a modem server administered by the national ITSC. ***The use of desktop modems to support dial-in access to FEMA systems is prohibited unless waived by the ESM.***

- Dial-out Access. All users who need to access systems external to FEMA via dial-out modems must do so through approved modem services approved by the ESM and controlled by the national ITSC. The use of desktop modems to support dial-out access to external systems is prohibited unless waived by the ESM. For further information of FEMA's dial-out capability contact the national ITSC at (540)-542-4000.

Left blank intentionally

Appendix to 5-2 Office Automation Software Baseline Configuration Standard

The software baseline standards listed below are effective for purchases of information systems that require product features as described for those standards. Procurements in response to disasters are **not** exempt.

Standards

FEMA's software baseline standards are categorized as follows:

Software Category	Software Product
1. Multi-user Data Base	Oracle Relational Data Base Management System
2. Information Access Strategy	Client-Server processing platform
3. Network Operating System	Novell NetWare
4. Desktop Environment	Microsoft Windows Operating System, including Windows 95*, and Windows NT.
5. Desktop Office Automation	Microsoft Office Professional Suite (Includes Word - word processor, Excel - spreadsheet, Access - database, and Powerpoint – graphics, etc.)
6. Geographic Information System	MapInfo
7. Internet/Intranet	Microsoft Explorer preferred Browser. Netscape and AirMosaic Browsers will be supported.
8. Electronic Mail	Microsoft Exchange/Outlook
9. Virus Software	F-PROT Professional
10. Project Management	Microsoft Project (complex projects - full feature) Kick Start (small and less complex projects)

* FEMA has decided not to upgrade to Windows 98 at this time since we are currently in the process of migrating to Microsoft Exchange/Outlook and installing NEMIS agency-wide. Once these initiatives have been completed, Windows 98 (or other environments) will be considered.

Left blank intentionally

Appendix to 5-3 Application Software Standard

The application software standards listed below are effective for development of information systems used within FEMA. Procurements in response to disasters are **not** exempt.

Standards

FEMA's application software baseline standard

Application Category	Standard
Year 2000 Compliant Date Fields	yyyymmdd

Left blank intentionally

Appendix to 5-4 Office Automation Hardware Baseline Configuration Standard

The **minimum** hardware standards for desktop computers are as follows:

Components	**Desktop Configuration Minimum - New Purchases**
Processor	333MHz* Pentium Intel CPU or greater PCI local bus with minimum of 3 PCI slots 2 ISA 16-bit expansion slots
Memory	64MB RAM with minimum of 3 memory slots with 2, at a minimum, of the slots available for future expansion. 512K L2 Cache
Data Storage & Input/Output Media	8.0GB enhanced IDE Hard Drive mode 4 type 3.5" Built-in Diskette Drive EIDE hard drive/floppy disk controller 101/104 Keyboard PS 2 button serial mouse CD ROM
Video Display	17" Color Monitor with .28 dot/75 Hz scan rate PCI bus Video Accelerator Card with 32 bit processor 4MB VRAM
Ports	Serial port with 16550 UART support Parallel port with enhanced bi-directional capabilities
Network Interface Card	Driver support for Novell NetWare 32 Bit Intel equivalent 10Base-T connection IEEE 802.3 standard
Conservation	Energy Star Compliant system unit that powers down below 60 watts total when in idle mode
All Components	Year 2000 compliant

* 350MHz and higher CPU systems will provide a 100MHz system bus instead of a 66MHz system bus generally available with 333MHz CPU. When speed is a consideration, 350MHz (or higher) CPU with 100MHz system bus is recommended.

The hardware standards for Laptop/Notebook computers are as follows:

Components	**Laptop/Notebook Configuration Minimum - New Purchases**
Processor	233MHz Pentium Intel CPU or greater 2 Type II & Type III PCMCIA slots 56K Built-in (or PMCIA Slot) Modem 10/100 PCMCIA NIC
Memory	32MB RAM or greater 256K L2 Cache
Data Storage & Input/Output Media	3.0GB Hard Drive or greater 3.5" Built-in Diskette Drive Hard drive/floppy disk controller 87 Keys, Windows 95 ready Built-in mouse, J-Pointer, or Touchpad 20x CD ROM Needed/Required to load s/w and data display
Video Display	10" Active matrix Color Monitor 32-Bit Local Bus Video/2MB Video RAM
Ports	External ports for mouse, keyboard and monitor
Conservation	Lithium ion cell battery with a minimum 2-3 hour battery life
All Components	Year 2000 compliant

Appendix to 5-5 Office Automation Standards for Servers and Central Processors

The hardware standards for Server computers are as follows:

Components	**Server Configuration Minimum - New Purchases**
Processor	400MHz Pentium II processor w/512K Cache
Memory	128MB EDO RAM or greater
Data Storage & Input/Output Media	1X6 Hot Pluggable Backplane Expandable RAID Controller w/32MB RAM RAID 5 Configuration 5 each 4.5GB Ultra-wide SCSI hard drives 3.5" Built-in Diskette Drive 20GB DAT Tape Back-up system w/software 101/104 Keyboard PS 2 button serial mouse 24X CD ROM
Video Display	17" Color Monitor with .28 dot/75 Hz scan rate PCI bus Video Accelerator Card with 32 bit processor 2MB VRAM, Diamond Stealth equivalent
Ports	Serial port with 16550 UART support Parallel port with enhanced bi-directional capabilities
Network Interface Card	10/100 Ethernet, PCI Adapter, Twisted Pair
Conservation	Energy Star™ Compliant system unit that powers down below 60 watts total when in idle mode
All Components	Year 2000 compliant

The hardware standards for Central Processors are as follows: TO BE PROVIDED

Components	**Central Processor Configuration Minimum – New Purchases**
Processor	
Memory	
Data Storage & Input/Output Media	
Video Display	
Ports	
Conservation	
All Components	

Appendix A-1 IRM Regulatory Authorities Guide

Authorities

1. Public Law 96-511, The Paperwork Reduction Act of 1980, as amended.
2. Public Law 99-500, The Paperwork Reduction Reauthorization Act of 1995.
3. Public Law 100-235, Computer Security Act of 1987.
4. Public Law 100-503, Computer Matching and Privacy Protection Act of 1988.
5. Executive Order 12472, Assignment of National Security and Emergency Preparedness Telecommunications Functions, April 3, 1984.
6. Public Law 104-208, Section 808 , Title VIII of the Omnibus Consolidated Appropriations Act (Clinger-Cohen Act of 1996).
7. Executive Order 12656, Assignment of Emergency Preparedness Responsibilities, November 18, 1988.
8. CFR Part 201; et al., National Communications System; Final Rule, December 11, 1990.

Left blank intentionally

Appendix A-2 IRM Regulatory Reference Guide

References

1. Office of Management and Budget Circular A-76, Policies for Acquiring Commercial or Industrial Products and Services Needed by the Government, dated March 3, 1966, as revised and amended.

2. Office of Management and Budget Circular A-109, Major Systems Acquisitions, dated April 5, 1976.

3. Office of Management and Budget Circular A-130, Management of Federal Information Resources.

4. Office of Management and Budget Circular A-11, Preparation and Submission of Budget Estimates, Exhibits 43A and 43B.

5. FEMA Instruction 1610.5, Procurement Review Board/Procurement Planning System.

6. FEMA Instruction 1610.13, Information Resources Board.

7. FEMA Manual 6150.1, Personal Property Management Program.

8. Federal Information Processing Standards Publications (FIPS PUBS) Index List 58.

9. An Introduction to Computer Security: The NIST Handbook, NIST Special Publications 800-12, National Institute of Standards and Technology, Gaithersburg, MD 1995.

10. National Institute of Standards and Technology, Glossary of Computer Security Terminology, NISTIR 4659, September 1991.

11. Defense Intelligence Agency Manual 50-3, Physical Security Standards for Construction of Sensitive Compartmented Information Facilities, February 1990.

12. Director of Central Intelligence Directive 1/6, Security Policy for Uniform Protection of Intelligence Processed in Automated Information Systems and Networks (U), July 19, 1988.

13. Security Administration of Unclassified LANs a handbook for system managers.

14. Everything You Always Wanted to Know About Computer Security But Were Afraid to Ask, a handbook for all users of FEMA computer systems.

15. Computer Security - Management's Responsibility, a handbook for all managers of computer systems users.

Appendix B-1 Definitions

A

Access control. The process of limiting access to the resources of a system to authorized users, programs, processes, or other systems (in computer networks).

Access to information. The function of providing to members of the public, upon their request, the government information to which they are entitled under law.

Accreditation. Official authorization granted to an information system to process sensitive information in its operational environment based on comprehensive security evaluation of the system's hardware, firmware, and software security design, configuration, and implementation of other system, procedural, administrative, physical, TEMPEST, personnel, and communications security controls.

Agency procurement request (APR). A request by a Federal agency for General Services Administration (GSA) to acquire Federal information processing (FIP) resources or for GSA to delegate the authority to acquire FIP resources.

Application systems manager. The FEMA employee responsible for establishing a management control process over application systems development and maintenance.

Application systems security manager. The FEMA employee responsible for managing and establishing application systems life-cycle security requirements, application security control process required by OMB Circular A-130, reviewing and testing reliable security features incorporated into application systems, serving as the focal point for issues and actions involving application systems security, defining and establishing application specific security requirements based on application system data sensitivity.

Audit trail. A series of records of computer events, about an operating system, an application, or user activity.

Authentication. Proving to some reasonable degree that users are who they claim to be.

Automated data processing (ADP). See automatic data processing.

Automated information system. An organized collection, processing, transmission, and dissemination of information in accordance with defined procedures that is automated.

Automated information system (AIS) security. Measures and controls that protect an AIS against denial of service and unauthorized (accidental or intentional) disclosure, modification, or destruction of AISs and data. See computer security (COMPUSEC).

Automatic data processing (ADP). One or more devices that use common storage for all or part of a computer program, and also for all or part of the data necessary for execution of the program; that execute user-written or user-designated programs; that perform used-designated

symbol manipulation, such as arithmetic operations, logic operations, or character-string manipulations; and that can execute programs that modify themselves during their execution. Automatic data processing may be performed by a standalone unit or by several connected units.

B

Burden. The total time, effort, or financial resources required to respond to a collection of information.

C

Certification. Comprehensive evaluation of the technical and nontechnical security features of an information system and other safeguards made in support of the accreditation process that establishes the extent to which a particular system design and implementation meet specified security requirements.

Chief Information Officer (CIO). FEMA executive who serves as principal advisor to the Director and other senior managers regarding the acquisition of IT and management of information resources.

Collection of information. The obtaining or soliciting of information from 10 or more persons by means of identical questions, identical reporting or recordkeeping requirement, or requirements to obtain, maintain, retain, report, or publicly disclose information, whether mandatory, voluntary, or required to obtain a benefit. The term "collection of information" refers to the act of collecting information, to the information to be collected, and to a plan and/or an instrument calling for the collection of information.

Commercial-off-the-shelf (COTS) software. Computer applications and programs that have been designed and developed for sale to the general public.

Common-use software. Software that deals with applications common to many agencies, that would be useful to other agencies, and is written in such a way that minor variations in requirements can be accommodated without significant programming effort.

Communications. A method or means of conveying information of any kind from one person or process to other person(s) or process(es) by a telecommunication medium.

a. **Data communications**. A communications technique that passes information encoded as discrete, on-off pulses, by a telecommunication medium.

b. **Voice communications**. A communications technique that uses a continuous signal varied by amplification to transmit voice from one person to another by a telecommunication medium.

Communications link. The physical means of connecting one location to another for the purpose of transmitting and receiving information.

Communications security (COMSEC). The protection resulting from all measures designed to deny unauthorized persons information of value which might be derived from the possession and study of telecommunications, or to mislead unauthorized persons in their interpretation of the results of such possession and study. Communications security includes: (a) cryptosecurity; (b) transmission security; (c) emission security; and (d) physical security of communications security materials and information.

Computer. (1) A device capable of accepting and processing information and supplying the results. It usually consists of input, output, storage, arithmetic, logic, and control units. (2) A functional unit that can perform substantial computation, including numerous arithmetic operations or logic operations, without intervention by a human operator during a run. Computers have been loosely classified into microcomputers, minicomputers, and main-frame computers, based on their size.

Computer accommodation. The acquisition or modification of information technology to minimize the functional limitations of employees in order to promote productivity and to ensure access to work-related information resources.

Computer Security (COMPUSEC). Synonymous with automated information system (AIS) security.

Computer system. A functional unit, consisting of one or more computers and associated software, that uses common storage for all or part of a program and also for all or part of the data necessary for the execution of the program; executes user-written or user-designated programs; performs user-designated data manipulation, including arithmetic operations and logic operations; and that can execute programs that modify themselves during their execution. A computer system may be a standalone unit or may consist of several interconnected units. Synonymous with ADP system.

Computer virus. A common type of malicious computer program written to disrupt or damage computer systems or associated resources. Most viruses copy themselves to other computer programs, thereby infecting them, and then execute malicious instructions programmed by the author. Computer viruses 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.

Contingency plan. A plan for emergency response, backup operations, and disaster recovery maintained to ensure the availability of critical system resources and facilitate continuity of operations in an emergency situation. Also disaster recovery plan or continuity of operations plan (COOP).

D

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

Data communications. The transfer of data between functional units by means of data transmission according to a protocol. The transmission, reception, and validation of data.

Delegation of procurement authority (DPA). The General Services Administration (GSA) delegates its procurement authority to executive agencies, and it grants those delegations to the designated official when GSA determines that such officials are sufficiently independent of program responsibility and have sufficient experience, resources, and ability to fairly and effectively carry out procurements under GSA's authority as provided by 40 U.S.C. 759(b)(3).

Electronic form. A form that consists of electronic print images and resides on magnetic or optical media.

Electronic record. Any information that is recorded in a form that only a computer can process and that satisfies the definition of a Federal record in 44 USC 3301. Electronic records include numeric, graphic and text information, which may be recorded on any medium capable of being read by a computer and which satisfies the definition of a record. This includes, but is not limited to, magnetic media, such as tapes and disks, and optical disks.

Environmental control. Established safeguards to protect system hardware, software, and storage media against damage from unreliable or poor quality power, airborne contaminants, fire, water, temperature, and humidity.

F

Federal information processing (FIP) resources. Automatic data processing equipment (ADPE) as defined in Public Law 99-500 (40 U.S.C. 759(a)(2)). The term, FIP resources, includes FIP equipment, software, services, support services, maintenance, related supplies, and systems. These terms are limited by paragraphs (a) and (b) of the definition of FIP resources and are defined as follows:

(1) **FIP equipment**. Any equipment or interconnected system or subsystems of equipment used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information.

(2) **FIP maintenance**. Those examination, testing, repair, or part replacement functions performed on FIP equipment or software.

(3) **FIP related supplies**. Any consumable item designed specifically for use with FIP equipment, software, services, or support services.

(4) **FIP services**. Any service, other than FIP support services, performed or furnished by using FIP equipment or software.

(5) **FIP software**. Any software, including firmware, specifically designed to make use of and extend the capabilities of FIP equipment.

(6) **FIP support services**. Any commercial nonpersonal services, including FIP maintenance, used in support of FIP equipment, software, or services.

(7) **FIP system**. Any organized combination of FIP equipment, software, services, support services, or related supplies.

Federal telecommunications system (FTS). The umbrella of local and long distance telecommunications services, including FTS2000 long distance services, provided, operated, managed, or maintained by GSA for the common use of all Federal agencies and other authorized users.

Functional manager. Required to provide adequate physical security for workstations and other system components located in the functional area. Must assume responsibility for safeguarding data stored locally on devices and media used at system workstations.

Firewall. Secure gateway that blocks or filters access between two networks. Secure gateways allow internal users to connect to external networks and at the same time prevent malicious hackers from compromising the internal systems.

G

Government information. Information created, collected, processed, disseminated, or disposed of by or for the Federal Government.

H

Hardware. Any physical equipment or device used in the configuration and operation of an information system.

I

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, microfilm, or magnetic tape.

Information accessibility. The application or configuration of FIP resources in a manner that accommodates the functional limitations of individuals with disabilities so as to promote productivity and provide access to work-related or public information resources.

Information collection. See collection of information.

Information management. Planning, budgeting, manipulating, and controlling of information throughout its life cycle.

Information processing. Data processing, integrated with processes such as office automation and data communication.

Information processing system. A system that performs data processing integrated with processes such as office automation and data communication. See also data processing system.

Information resources. Includes both government information and information technology.

Information resources management. The process of managing information resources to accomplish agency missions. The term encompasses both information itself and the related resources, such as personnel, equipment, funds, and information technology.

Information system. The organized collection, processing, transmission, and dissemination of information in accordance with defined procedures, whether automated or manual.

Information systems security administrator (ISSA). Depending on circumstances or the local threat environment, assesses physical vulnerabilities and establishes additional controls for workstations, e.g., disposal of hard disks or return hard disks to a vendor for maintenance or replacement, when needed. Provide technical security assistance to system users, functional managers, and system managers/administrators, as well as ensuring the implementation of information systems security requirements.

Information systems security officer (ISSO). Is responsible for promoting information systems security and ensuring the implementation of information systems security requirements in his/her organizational element.

Information systems security manager (ISSM). Implements physical access controls to protect network servers, auxiliary disk storage subsystems, workstations with backup devices, and removable storage media.

Integrity. information security characteristic that ensures information security resources operate correctly and data in system data bases are inviolate. The characteristic protects against deliberate or inadvertent unauthorized modifications. This characteristic applies to hardware, software, firmware, and data bases used by a system.

Intrusion detection. Refers to the process of identifying attempts to penetrate a system and gain unauthorized access.

Information systems security (INFOSEC). A composite of factors necessary to protect FIP systems and the information they process to prevent exploitation through interception, unauthorized electronic access, or related technical intelligence threats, and to ensure authenticity.

Information technology. The hardware and software operated by a Federal agency or by a contractor of a Federal agency or other organization that processes information on behalf of the Federal Government to accomplish a Federal function, regardless of the technology involved, whether computers, telecommunications, or others. It includes automatic data processing equipment.

Information technology system. The hardware, software, and other resources used for the collection, processing, transmission, and dissemination of information in accordance with established procedures. Information technology systems include non-financial, financial, and mixed systems, as defined below.

a. **Non-financial system**. A system that supports non-financial functions of an agency or agency sub-component, and has little or no financial functions.

b. **Financial system**. A financial system encompasses procedures, controls, data, hardware, software, and associated support personnel. A system, comprised of one or more applications, that is used for (1) collecting, processing, maintaining, transmitting, and disseminating data about events having financial consequences (e.g., receipt of appropriations or other financial resources, acquisition of goods and services, payments or collections, recognition of guarantees, benefits to be provided, other potential liabilities, and other discrete financial transactions); (2) providing financial and related information about the operations of an agency or agency sub-component; (3) supporting financial planning or budgeting activities.

c. **Mixed system**. A system that supports both financial and non-financial functions, where financial functions are significant.

Interoperability. The ability of FIP resources to provide services to and accept services from other FIP resources and to use the services so exchanged to enable them to operate effectively together.

L

Life cycle management (LCM). The stages through which information resources progress from the decision making, analyses, operations and maintenance through disposition. LCM encompasses the (1) decision making steps necessary to describe the purpose and size of an acquisition or in-house development in terms of explanation and cost estimates; (2) requirements analysis and analysis of alternative steps to justify and document the decision making, milestones, and key activities needed for delivery and acceptance; (3) operations and maintenance steps which provide for the manipulation and maintenance of information resources in support of the decision making; and (4) disposition steps to determine when the information resources no longer serve a useful purpose to the Federal government.

a. **Information life cycle**. The stages through which information passes, typically characterized as creation or collection, processing, dissemination, use, storage, and disposition.

b. **Information system life cycle**. The phases through which an information system passes, typically characterized as initiation, development, operation, and termination.

M

Major information system. An information system that requires special continuing management attention because of its importance to an agency mission; its high development, operating or maintenance costs; or its significant impact on the administration of agency programs, finances, property, or other resources.

Major system. That combination of elements that will function together to produce the capabilities required to fulfill a mission need. The elements may include, for example, hardware, equipment, software, construction, or other improvements or real property. Major system acquisition programs are those programs that (1) are directed at and critical to fulfilling an agency mission, (2) entail the allocation of relatively large resources, and (3) warrant special management attention.

Management information system (MIS). A communication process in which data are recorded in some fashion and processed for operational purposes in support of processes for identifying and isolating problems for higher-level decision making.

Messaging service. In Integrated Services Digital Network (ISDN), an interactive telecommunications service that allows information transfer between users by means of store-and-forward, electronic mail, or message-handling functions.

Media degaussing. Clearing or erasing of stored sensitive data prior to release for reuse, maintenance, or replacement by any individual or organization outside the system environment.

N

National security and emergency preparedness (NSEP). Those physical, technical, and administrative characteristics of FIP systems that will ensure a prescribed level of survivability in times of national or other emergencies up to and including nuclear attack. Government common-use telecommunications systems are designed, built, tested, and maintained to meet the defined emergency mission needs of the Government entities that use them.

O

Obsolescence. The state of FIP hardware or software that is either in a degenerative condition, which if not corrected will render the resource useless, or has become technologically outmoded compared to other hardware or software being sold.

Office automation (OA). The techniques and means used for the automation of office activities, in particular, the processing and communication of text, images, and voice.

Open system. A system whose characteristics comply with specified, publicly maintained, readily available standards and that therefore can be connected to other systems that comply with these same standards.

Operating system. Software that controls the execution of programs; and that provides services such as resource allocation, scheduling, input/output control, and data management. Usually, operating systems are predominantly software, but partial or complete hardware implementations are possible.

Outdated equipment. Any Federal information processing equipment over eight years old, based on the initial commercial installation date of that model of equipment, and that is no longer in current production.

P

Personal computer. A stand-alone computer equipped with all the system, utility, and application software, and the input/output devices and other peripherals that an individual needs to perform one or more tasks.

Physical control. Use of locks, guards, badges, alarms, barriers, control procedures, or similar measures to limit access to information resources.

R

Records. All books, papers, maps, photographs, machine readable materials, or other documentary materials, regardless of physical form or characteristics, made or received by an agency of the United States Government under Federal law or in connection with the transaction of public business and preserved, or appropriate for preservation, by that agency or its legitimate successor, as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of the Government or because of the informational value of data in them.

Records disposition. Any activity with respect to disposal of temporary records no longer necessary for the conduct of business by destruction or donation; transfer of records to Federal agency storage facilities or records centers; transfer to the National Archives of the United States of records determined to have sufficient historical or other value to warrant continued preservation; or transfer of records from one Federal agency to any other Federal agency.

Records management. Planning, controlling, directing, organizing, training, promoting, and other managerial activities involved with respect to records creation, records maintenance and use, and records disposition in order to achieve adequate and proper documentation of the policies and transactions of the Federal Government and effective and economical management of agency operations.

Records maintenance and use. Any activity involving location of records of a Federal agency; storage, retrieval, and handling of records kept at office file locations by or for a Federal agency; processing of mail by a Federal agency; or selection and utilization of equipment and supplies associated with records and copying.

Risk management. Process of identifying, controlling, eliminating or minimizing uncertain events that may degrade information systems resources. It includes risk analysis, cost/benefit analysis, and the selection, evaluation, and implementation of cost-effective safeguards.

S

Safeguards. Protective devices, actions, procedures, techniques or measures prescribed to meet the security requirements specified for an information system. Safeguards include, but are not limited to: hardware and software security features, operational controls, accountability procedures, access and distribution controls, administrative constraints, personal security, and physical control structures areas, or devices.

Security policy. Basic information systems security requirements that safeguards all unclassified information as a valuable resource or asset and implemented in every unclassified systems environment without exception.

Sensitive. Is synonymous with important or valuable. In general, the more important a system is to the mission of the agency, the more sensitive it is.

Sensitivity assessment. Looks at the value of both the information and the system itself. The assessment considers legal implications, organization policy, and the functional needs of the system.

Software. A term that applies to computer programs or sets of computer instructions and automated procedures; for example, operating systems, applications programs, programming languages, compilers, security programs, various utility-type programs, etc. The term is used in contrast with hardware.

Specific make and model specification. A description of the Government's requirement for FIP resources that is so restrictive that only a particular manufacturer's products will satisfy the Government's needs, regardless of the number of suppliers that may be able to furnish that manufacturer's products.

Storage media protection. Proper safeguards and handling of storage media such as diskettes, tape cassettes, fixed hard disks, and removable hard disks in the loss of valuable software or data, or unauthorized disclosure or modification of data.

System analysis. A systematic investigation of a real or planned system to determine the functions of the system and how they relate to each other and to any other system.

System and data access control. Established safeguards to prevent the unauthorized disclosure, modification, or destruction of word processing and data processing files resident on the system storage devices. Protects against unauthorized access, unique user identifies (user IDs) and passwords are used to identify and authenticate authorized users.

System description. Documentation that describes the system design and that defines the organization, essential characteristics, and the hardware and software requirements of the system.

System design. A process of defining the hardware and software architecture, components, modules, interfaces, and data for a system to satisfy specified requirements.

System design concept. An idea expressed in terms of general performance, capabilities, and characteristics of hardware and software oriented either to operate or to be operated as an integrated whole in meeting a mission need.

System development. A process that begins with requirements analysis and includes system design, implementation, and documentation.

System documentation. The collection of documents that describe the requirements, capabilities, limitations, design, operation, and maintenance of an information processing system.

System life cycle. The course of developmental changes through which a system passes from its conception to the termination of its use; for example, the phases and activities associated with the analysis, acquisition, design, development, test, integration, operation, maintenance, and modification of a system. See life cycle management.

Systems security requirements. Establishment, implementation, and use of safeguards for Federal Emergency Management (FEMA) application systems, local area networks (LAN), mini and mainframe computer systems and personal computers (PC). The minimum security controls, procedures, and documentation products specified for safeguarding classified and unclassified computer hardware and software systems implemented into the life-cycle process provide reliable security features to protect the confidentiality, integrity, and availability of computer hardware and software resources used in support of FEMA's mission.

Systems specification. Specifications which include the delineation of the objective which the system is intended to accomplish, and the data processing requirements underlying that accomplishment.

T

Telecommunications. Any transmission, emission, or reception of signs, signals, writing, images and sounds or intelligence of any nature by wire, radio, optical or other electromagnetic systems.

Telecommunications device for the deaf (TDD). A machine that uses typed input and output, usually with a visual text display, to enable individuals with hearing or speech impairments to communicate over a telecommunications network.

Telecommunications facilities. Equipment used for such modes of transmission as telephone, data, facsimile, video, radio, audio, and such corollary items as switches, wire, cable, access arrangements, and communications security facilities.

Telecommunications resources. Telecommunications equipment, facilities, and services.

Telecommunications service priority (TSP). A regulated service provided by a telecommunications provider, such as an operating telephone company or a carrier, for NSEP telecommunications.

Telecommunications services. The transmission, emission, or reception of signals, signs, writing, images, sounds, or intelligence of any nature, by wire, cable, satellite, fiber optics, laser, radio, or any other electronic, electric, electromagnetic, or acoustically coupled means. The term includes the telecommunications facilities necessary to provide such services.

U

Used computer equipment. Mainframe, minicomputer, microcomputer (personal computer), and associated peripheral equipment that has been previously installed. This term includes reconditioned, refurbished or remanufactured equipment.

User. An organizational or programmatic entity that receives service from an information technology facility. A user may be either internal or external to the agency organization responsible for the facility, but normally does not report either to the manager or director of the facility or to the same immediate supervisor.

V

Vulnerability. Refers to a weakness in automated system security procedures, administrative controls, internal controls, and so forth, that could be exploited by a threat to gain unauthorized access to information or disrupt critical processing.

Y

Year 2000 compliant. Defined as information technology that accurately processes date/time data (including, but not limited to, calculating, comparing, and sequencing) from, into, and between the twentieth and twenty-first centuries, and the years 1999 and 2000 and leap year calculations. Furthermore, Year 2000 compliant information technology, when used in combination with other information technology, shall accurately process date/time data if the other information technology properly exchanges date/time data with it.

Appendix C-1 Acronyms

A

ADP	Automatic Data Processing/Automated Data Processing
ADPE	Automatic Data Processing Equipment
AIS	Automated Information Systems
APR	Agency Procurement Review

C

CIO	Chief Information Officer
COMM	Communications
COMPUSEC	Computer Security
COMSEC	Communications Security
COTS	Commercial-off-the-shelf

D

DAR	Designated Agency Representative
DEC	Director's Executive Council
DPA	Delegation of Procurement Authority

E

E-mail	Electronic Mail

F

FAR	Federal Acquisition Regulation
FAX	Facsimile
FED-STD	Federal Standard
FIP	Federal Information Processing
FIPS	Federal Information Processing Standards
FIPS PUBS	Federal Information Processing Standards Publications
FIRMR	Federal Information Resources Management Regulation
FOIA	Freedom of Information Act
FPMR	Federal Property Management Regulations
FSN	FEMA Switched Network
FTS	Federal Telecommunications System

G

GAO	General Accounting Office
GSA	General Services Administration

I

INFOSEC	Information Systems Security
INTERCOM	Intercommunications
IRB	Information Resources Board
IRM	Information Resources Management
IRPMR	Information Resources Procurement and Management Review
IS	Information Systems
ISP	Information Systems Plan
IT	Information Technology
ITMRA	Information Technology Management Reform Act of 1996

L

LCM	Life Cycle Management

M

MIS	Management Information System
MOU	Memorandum of Understanding

N

NIST	National Institute of Standards and Technology
NSEP	National Security and Emergency Preparedness
NTIS	National Technical Information Service

O

OA	Office Automation
OMB	Office of Management and Budget

P

PRA	Paperwork Reduction Act

T

TDD	Telecommunications Device for the Deaf
TELECOMM	Telecommunications
TSP	Telecommunications Service Priority