

# Chapter 3

## Management and Use of Information Systems and Services

# INFORMATION RESOURCES MANAGEMENT PROCEDURAL DIRECTIVE

Left blank intentionally

# INFORMATION RESOURCES MANAGEMENT PROCEDURAL DIRECTIVE

## 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

## INFORMATION RESOURCES MANAGEMENT PROCEDURAL DIRECTIVE

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.

## INFORMATION RESOURCES MANAGEMENT PROCEDURAL DIRECTIVE

- 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.

## INFORMATION RESOURCES MANAGEMENT PROCEDURAL DIRECTIVE

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.

## INFORMATION RESOURCES MANAGEMENT PROCEDURAL DIRECTIVE

- 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;<sup>1</sup>
  - 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.

---

<sup>1</sup>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.

## INFORMATION RESOURCES MANAGEMENT PROCEDURAL DIRECTIVE

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;

## INFORMATION RESOURCES MANAGEMENT PROCEDURAL DIRECTIVE

- 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.

## INFORMATION RESOURCES MANAGEMENT PROCEDURAL DIRECTIVE

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.

# INFORMATION RESOURCES MANAGEMENT PROCEDURAL DIRECTIVE

## 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.

## INFORMATION RESOURCES MANAGEMENT PROCEDURAL DIRECTIVE

- 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.

## INFORMATION RESOURCES MANAGEMENT PROCEDURAL DIRECTIVE

- 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:

## INFORMATION RESOURCES MANAGEMENT PROCEDURAL DIRECTIVE

<b>Location</b>	<b>FSN Video Number</b>	<b>FSN Voice Number</b>
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.

# INFORMATION RESOURCES MANAGEMENT PROCEDURAL DIRECTIVE

Left blank intentionally

# INFORMATION RESOURCES MANAGEMENT PROCEDURAL DIRECTIVE

## 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.

# INFORMATION RESOURCES MANAGEMENT PROCEDURAL DIRECTIVE

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

## INFORMATION RESOURCES MANAGEMENT PROCEDURAL DIRECTIVE

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.

## INFORMATION RESOURCES MANAGEMENT PROCEDURAL DIRECTIVE

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.

## INFORMATION RESOURCES MANAGEMENT PROCEDURAL DIRECTIVE

- 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.
1. 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.

## INFORMATION RESOURCES MANAGEMENT PROCEDURAL DIRECTIVE

- 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.

# INFORMATION RESOURCES MANAGEMENT PROCEDURAL DIRECTIVE

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

## INFORMATION RESOURCES MANAGEMENT PROCEDURAL DIRECTIVE

- 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.

## INFORMATION RESOURCES MANAGEMENT PROCEDURAL DIRECTIVE

- 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;

## INFORMATION RESOURCES MANAGEMENT PROCEDURAL DIRECTIVE

- 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.

## INFORMATION RESOURCES MANAGEMENT PROCEDURAL DIRECTIVE

- 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

## INFORMATION RESOURCES MANAGEMENT PROCEDURAL DIRECTIVE

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.

# INFORMATION RESOURCES MANAGEMENT PROCEDURAL DIRECTIVE

## 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.

## INFORMATION RESOURCES MANAGEMENT PROCEDURAL DIRECTIVE

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.

## INFORMATION RESOURCES MANAGEMENT PROCEDURAL DIRECTIVE

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:

## INFORMATION RESOURCES MANAGEMENT PROCEDURAL DIRECTIVE

- 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.”

# INFORMATION RESOURCES MANAGEMENT PROCEDURAL DIRECTIVE

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

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.

## INFORMATION RESOURCES MANAGEMENT PROCEDURAL DIRECTIVE

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.

# INFORMATION RESOURCES MANAGEMENT PROCEDURAL DIRECTIVE

## 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.

## INFORMATION RESOURCES MANAGEMENT PROCEDURAL DIRECTIVE

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:

## INFORMATION RESOURCES MANAGEMENT PROCEDURAL DIRECTIVE

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.

## INFORMATION RESOURCES MANAGEMENT PROCEDURAL DIRECTIVE

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.

# INFORMATION RESOURCES MANAGEMENT PROCEDURAL DIRECTIVE

## 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.

# INFORMATION RESOURCES MANAGEMENT PROCEDURAL DIRECTIVE

## 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.

# INFORMATION RESOURCES MANAGEMENT PROCEDURAL DIRECTIVE

## 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.

## INFORMATION RESOURCES MANAGEMENT PROCEDURAL DIRECTIVE

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.

## INFORMATION RESOURCES MANAGEMENT PROCEDURAL DIRECTIVE

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.

## INFORMATION RESOURCES MANAGEMENT PROCEDURAL DIRECTIVE

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**

# INFORMATION RESOURCES MANAGEMENT PROCEDURAL DIRECTIVE

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.

## INFORMATION RESOURCES MANAGEMENT PROCEDURAL DIRECTIVE

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.

## INFORMATION RESOURCES MANAGEMENT PROCEDURAL DIRECTIVE

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...."

## INFORMATION RESOURCES MANAGEMENT PROCEDURAL DIRECTIVE

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.

INFORMATION RESOURCES MANAGEMENT PROCEDURAL DIRECTIVE

**3-12 Telecommuting**

**To Be Provided**

# INFORMATION RESOURCES MANAGEMENT PROCEDURAL DIRECTIVE

Left blank intentionally