

# INFORMATION RESOURCES MANAGEMENT PROCEDURAL DIRECTIVE

## APPENDICES TO CHAPTERS

Writing Accessible HTML Documents.....	<a href="#">Appendix to 3-8</a>
Electronic Mail Naming Convention Standard .....	<a href="#">Appendix to 3-9</a>
Firewall Management and Administration Guidelines .....	<a href="#">Appendix to 4-3.A</a>
Remote Access Using Hardware Tokens and TACACS .....	<a href="#">Appendix to 4-3.B</a>
Disaster Field Office's Network Administrators Guide.....	<a href="#">Appendix to 4-3.C</a>
Office Automation Software Baseline Configuration Standard.....	<a href="#">Appendix to 5-2</a>
Application Software Standard .....	<a href="#">Appendix to 5-3</a>
Office Automation Hardware Baseline Configuration Standard.....	<a href="#">Appendix to 5-4</a>
Office Automation Standards for Servers and Central Processors.....	<a href="#">Appendix to 5-5</a>

## IRM REGULATORY REFERENCE GUIDE

Authorities .....	<a href="#">Appendix A-1</a>
References .....	<a href="#">Appendix A-2</a>

## GLOSSARY

Definitions.....	<a href="#">Appendix B-1</a>
Acronyms.....	<a href="#">Appendix C-1</a>

# INFORMATION RESOURCES MANAGEMENT PROCEDURAL DIRECTIVE

Left blank intentionally

## Appendix to 3-8 Writing Accessible HTML Documents

Because of the structured nature of HTML, the WWW provides tremendous power and flexibility in presenting information in multiple formats (text, audio, video, graphic, etc.). However, the features that provide power and elegance for some users present potential barriers for others. For example, servers which require the viewing of graphic images are inaccessible to blind users. Careful design and coding of information can alleviate access barriers. The following technical guidelines should be followed in designing and coding accessible HTML documents.

It is important to note that implementing these guidelines does not compromise the aesthetics or functionality of the server.

**Guideline: Every graphic image should have associated text.**

### **Rationale:**

If the person viewing the information is using a character-based program (e.g. Lynx) or has graphics turned off in other browsers, the link will be lost.

### **Strategy:**

Use *ALT* attribute in image reference anchors and include selection text within the anchor.

### **Example of inaccessible code:**

On January 20, 1993, William Jefferson Clinton  
<A HREF="/images/raw/bill-portrait.gif" >  
<IMG SRC="/images/small/bill-portrait.gif" > </A >  
was sworn in as the 42nd President of the United States, and moved into the White House with his wife.  
< A HREF="/images/raw/hillary-portrait.gif" > < IMG SRC="/images/small/hillary-portrait.gif" >  
> </A >  
Hillary Rodham Clinton and their daughter Chelsea.

In this example, the graphics convey no information about the link. A user with a character-based application would not know the nature of the link.

Accessible code would look like this:

### **Example of accessible code:**

On January 20, 1993,  
<A HREF="/images/raw/bill-portrait.gif" >  
<IMG SRC="/images/small/bill-portrait.gif" alt="Picture of President Clinton..." >  
William Jefferson Clinton </A > was sworn in as the 42nd President of the United States, and moved into the White House with his wife, < A HREF="/images/raw/hillary-portrait.gif"

## INFORMATION RESOURCES MANAGEMENT PROCEDURAL DIRECTIVE

```
> < IMG SRC="/images/small/hillary-portrait.gif" Alt="Picture of Hillary Rodham Clinton and their daughter Chelsea." > Hillary Rodham Clinton and their daughter Chelsea. < /A >
```

This example adds both the "alt" image expression and a text descriptor within the anchor.

**Guideline: If image maps are used, there should be an alternate method of selecting options.**

### **Rationale:**

If the person viewing the information is using a character-based program (e.g. Lynx) or is using a computer which is not capable of displaying graphics, the image will be completely lost; there will be no way to select options.

### **Example of inaccessible code:**

```
< TITLE > Map of Washington, DC. < /TITLE > < H1 > Click on a building below < /H1 > < A HREF="http://www.whitehouse.gov/img/dcmap" > < IMG SRC="http://www.whitehouse.gov/images/large/DC_map.gif" ISMAP > < /A >
```

In this example, the entire page is lost for character-based viewers. An alternative way to handle this would be to present an option for a list of buildings. This would give all viewers a better understanding of what information was available.

### **Example of accessible code:**

```
< TITLE > Map of Washington, DC. < /TITLE > < H1 > Click on a building in the map below or select from < A HREF="http://www.whitehouse.gov/dcmap_list.html" > list of buildings < /A >< /H1 > < A HREF="http://www.whitehouse.gov/img/dcmap" > < IMG SRC="http://www.whitehouse.gov/images/large/DC_map.gif" ISMAP alt="map of Washington"> < /A >
```

In this example, the user is given the choice of an alternate page "dcmap\_list.html" which might look something like this:

```
< TITLE > Buildings in Washington, DC. < /TITLE >
< H1 > Select from the list of buildings below < /H1 >
< UL >
< LI > < A HREF="http://www.doc.gov" > Department of Commerce < /A > 16th St. N.W
< LI > < A HREF="http://www.DOI.gov/Parks/Washington_Monument.html" > Washington
Monument < /A > Between 15th and 17th south of Constitution Ave.< LI > < A
  HREF="http://www.doi.gov" >
  Department of Interior < /A > 14th St. N.W < LI >
...
< LI > ...
< /UL >
```

## INFORMATION RESOURCES MANAGEMENT PROCEDURAL DIRECTIVE

There are two ways to implement this guideline. The first way is to modify every page which contains an ISMAP so that on each page the user is offered a choice of graphic or text selection. Another method however, is to offer the user a choice at the home page. With this method if the user selects "no graphics" at the home page, a separate set of pages with no ISMAPs will be selected.

Inclusion of a second home page would allow the user to select "no graphics" The code would look like this:

```
Select <A HREF="http://www.whitehouse.gov/Welcome-no_graphics.html" > no graphics </A  
> if you would like to browse without pictures.
```

**Guideline: Include detailed descriptive "comments" with all JPEG images.**

### **Rationale:**

Although JPEG files are used for high resolution images, there is still useful information that can be conveyed to blind users. One example of this would be JPEG images of pages in a manuscript. In this case, a full transcript of text contained in the image should be included.

### **Strategy:**

Use a JPEG file editor to include information in the "comments" section of the JPEG file. Alternatively, a separate "text" file could be linked to the image.

**Guideline: Provide text transcriptions or descriptions for all audio clips.**

### **Rationale:**

Audio clips are of no use to users with hearing impairments or who are connecting through systems which do not support audio.

### **Inaccessible code:**

The President asked

```
< A HREF="http://www.whitehouse.gov/images/raw/al-portrait.gif" >  
< IMG SRC="http://www.whitehouse.gov/images/small/al-portrait.gif" >  
Vice President Gore </A > to head up the  
< A HREF="http://www.npr.gov/" > National Performance Review (NPR)  
</A > a project to make government work better and cost less.  
< A HREF="http://www.whitehouse.gov/Sounds/Gore.au" >  
< IMG SRC="http://www.whitehouse.gov/icons/audio.gif"> </A >
```

This code has two problems. First, the sound clip icon does not have associated text and therefore can not be seen with text browsers. Second, the link is of no use to users who are hearing impaired or do not have sound equipped viewers.

## INFORMATION RESOURCES MANAGEMENT PROCEDURAL DIRECTIVE

### Suggested code:

The President asked

```
< A HREF="http://www.whitehouse.gov/images/raw/al-portrait.gif" >
```

```
< IMG SRC="http://www.whitehouse.gov/images/small/al-portrait.gif"
alt="Picture of Al Gore" >
```

Vice President Gore </A > to head up the

```
< A HREF="http://www.npr.gov/" > National Performance Review (NPR)
```

```
</A > a project to make government work better and cost less.
```

```
< A HREF="http://www.whitehouse.gov/Sounds/Gore.au" > You can hear
```

```
< IMG SRC="http://www.whitehouse.gov/icons/audio.gif" alt="audio icon">
```

```
</A > or < A HREF="http://www.npr.gov/Al_N
```

Authored by Paul Fontaine

Center for Information Technology Accommodation

General Services Administration

Washington, DC. USA

<http://www.gsa.gov/coca/>

**June 5, 1995 DRAFT**

# INFORMATION RESOURCES MANAGEMENT PROCEDURAL DIRECTIVE

## Appendix to 3-9 Electronic Mail Naming Convention Standard

cc:Mail Naming Conventions

To provide for user name recognition in the cc:Mail directory and for ease of user access, the naming conventions use the minimum number of characters that are functionally descriptive. The naming structure includes a dash (-) that separate data within a field and the fields are separated by a slash. User names may contain up to a maximum of 25 contiguous characters (spaces are not valid). Comment entries may contain up to 17 contiguous characters that will display with the page/screen width without scrolling.

The FEMA cc:Mail directory standards for User Names and Post Office Names are identified in figures 1 and 2 respectively. The cc:Mail standards to be used in conjunction with the Federal Response Plan (FRP) are identified as follows:

- FRP Emergency Support Functions Matrix
- FRP Name Addressing Scheme
- Group 1, Primary and Support Government Agencies
- Group 2, Primary ESFs & EST Positions at FEMA Headquarters
- Group 3, Primary ESFs & Positions at an established DFO
- Group 4, Emergency Response Team ESFs in Transition
- Group 5, Primary ESFs & Positions at ROC AND EOC

The cc:Mail directory (mailing list) display includes the following:

<i>Name</i>	<i>Loc</i>	<i>Last Checked In</i>	<i>Comment</i>

- where:
- Name is the User Name and FRP Name.
  - Loc is the location of the file server to the user performing the name search.
  - Last Checked In is the date and time that the user last logged into cc:Mail.
  - Comment is the area for descriptive information.

**cc:Mail User Naming Convention**

**The User Name is entered into the directory as follows:**

*LastName, Firstname (Optional Middle Initial)*

**Examples: Happygo, Lucky**

Each User Name should be listed in the directory in the manner in which the user wishes to be addressed. If a nickname, such as "Luck," is used for business purposes, that nickname may supplant either the lastname, firstname or middle initial. FEMA employees must be identified in the Comment area.

**Example: Happygo, Luck**

An acronym which is based upon a function may be entered into the cc:Mail directory as a user name. The acronym must have a comment entry which defines its function and the location of its post office.

**Examples: NNOC, SCIC, EICC**

**User Name Comment Field. Enter "FEMA" must be preceded by the Office Symbol for all FEMA employees as follows:**

*FEMA/Office Symbol*

Office symbol is the user's current office designation. It may be followed by any additional comments to identify specific groups, or contractor support personnel.

**Format: FEMA/XX-YY-ZZ**

**where: XX is the directorate level, YY is the Division level, ZZ is the Branch level.**

**Examples: FEMA/RR-DA-IA  
OS-AQ-PE/Contractor ABC**

**A comment entry for a User Name acronym must define its function and/or location.**

**Examples: NNOC, National Network Operation Center  
SCIC, Software Control and Integration Center  
EICC, Emergency Information Coordination Center**

Figure 1

# INFORMATION RESOURCES MANAGEMENT PROCEDURAL DIRECTIVE

## SITE CODES

Site	Site Code
Headquarters	HQ
Special Facility	SF
NETC, Emmitsburg	EM
Olney, MD	FS
Charlottesville, VA	CV
Region 1	R1
Region 1 FRC	F1
Region 2	R2
Region 3	R3
Region 4	R4
Region 4 FRC	F4
Region 5	R5
Region 5 FRC	F5
Region 6	R6
Region 7	R7
Region 8	R8
Region 9	R9
Region 10	R0
Nat'l Warning Center	NW
Nat'l Teleregistration Center	NT
Bluegrass, SC	BL
Palo Pinto, TX	PP
DFO1	D1
DFO2	D2
DFO3	D3
FEMA Switched Network	-

# INFORMATION RESOURCES MANAGEMENT PROCEDURAL DIRECTIVE

## **cc:Mail Naming Convention for Federal Response Plan Addressing**

The Federal Response Plan (FRP) identifies the primary support agencies' functions, the Emergency Support Function (ESF) numbers, the agency names, and agency acronyms or abbreviations as described on the following page.

The FRP ESF and Emergency Support Team (EST) addressing scheme is categorized into five groups of use as the naming convention in cc:Mail.

Group 1	Primary and Support Government Agencies
Group 2	Primary ESFs and EST Positions at FEMA Headquarters
Group 3	Primary ESFs and EST Positions at an established DFO
Group 4	Emergency Response Team ESFs in Transition
Group 5	Primary ESFs and Positions at ROC and EOC locations

Group 1      Where the primary and support agencies are assigned at their base location:  
HQ-(Agency Abbreviation/Acronym)-(opt)

Group 2      Where the EST (a constant) and ESF 2-digit number or positions symbol (i.e.,  
DIR=Director, LOG=Logistics, OPS=Operations, FIN=Finance) are located at  
FEMA headquarters:

EST-ESF(##)/Position Symbol-(opt)

Group 3      Where the Emergency Support Function is located at a State Disaster Field Office  
(DFO) and the DFO unique number is assigned:

(State Abbreviation)-DFO(XXXX)-ESF(##)/Position Symbol

Group 4      Where the Emergency Response Team (ERT) is located at a State locality:

(State Abbreviation)-(Locality Name)-ERT-ESF(##)

Group 5      Where the Emergency Support Function is located at a Regional Operating Center  
(ROC) or an Emergency Operating Center (EOC):

(Regional Site Code)-ROC-ESF(##)/Position Symbol

or

(Regional State Abbreviation)-EOC-(State Abbreviation covered by region)

**INFORMATION RESOURCES MANAGEMENT PROCEDURAL DIRECTIVE**

**Emergency Support Function Matrix**

Emergency Support Function	ESF Number	Primary Support Agency	Acronym/Abbreviation
Transportation	ESF01	Department of Transportation	DOT
Communications	ESF02	National Communications System	NCS
Public Works and Engineering	ESF03	DOD, US Army Corps of Engineers	DOD-USACE
Firefighting	ESF04	USDA, Firefighting Division	USDA-FS
Information and Planning	ESF05	Federal Emergency Management Agency	FEMA
Mass Care	ESF06	American Red Cross	ARC
Resource Support	ESF07	General Services Administration	GSA
Health and Medical Services	ESF08	Health and Human Services	DHHS
Urban Search and Rescue	ESF09	Federal Emergency Management Agency	FEMA
Hazardous Materials	ESF10	Environmental Protection Agency	EPA
Food	ESF11	USDA, Food and Nutrition Services	USDA-FNS
Energy	ESF12	Department of Energy	DOE
	ESF13	Nuclear Regulatory Commission	NRC

# INFORMATION RESOURCES MANAGEMENT PROCEDURAL DIRECTIVE

## Group 1

### Primary and Support Government Agencies

#### Group 1 Naming Standard Formula

HQ-AGY-EXP

where, AGY=Agency Abbreviation/Acronym

EXP=Expansion ID for further grouping (Optional)

Example 1: HQ-DOD-USACE is the Department of Defense, Army Core of Engineers Division, at their home base location in Washington, DC.

#### Group 1 Naming Standard Formula

- |     |           |     |            |
|-----|-----------|-----|------------|
| 1.  | AID       | 18. | FEMA       |
| 2.  | AID-OFDA  | 19. | FCC        |
| 3.  | ARC       | 20. | GSA        |
| 4.  | DHHS      | 21. | ICC        |
| 5.  | DHUD      | 22. | NASA       |
| 6.  | DLA       | 23. | NIST       |
| 7.  | DOC       | 24. | NCS        |
| 8.  | DOD-USACE | 25. | NRC        |
| 9.  | DOD-DOMS  | 26. | OPM        |
| 10. | DOE       | 27. | TREAS      |
| 11. | DOED      | 28. | TVA        |
| 12. | DOI       | 29. | USCG       |
| 13. | DOJ-FBI   | 30. | USDA-FNS   |
| 14. | DOL       | 31. | USDA-FS    |
| 15. | DOS       | 32. | USGS       |
| 16. | DOT       | 33. | USPS       |
| 17. | EPA       | 34. | VA         |
|     |           | 35. | WHITEHOUSE |

Note: Numbers 1-34 represent the Primary and Support agencies listed in the FRP.

Additional agencies and departments of agencies may be added as connectivity occurs.

# INFORMATION RESOURCES MANAGEMENT PROCEDURAL DIRECTIVE

## Group 2

### Primary ESFs and EST Positions at FEMA Headquarters

#### Group 2 Naming Standard Formula

(1) EST-ESF#-EXP or EST-Position-ESP

where, #= ESF Number as defined in the FRP (2 digits: 01-12)

EXP=Expansion ID for further grouping (Optional)

Position=Function IDs as follows:

- DIR - Director
- LOG - Logistics
- OPS - Operations
- FIN - Finance
- EXT - External Affairs

Example 1: EST-ESF01 is the Department of Transportation desk at FEMA Headquarters

Example 2: EST-DIR is the EST Director at FEMA Headquarters

#### Example Listing of Group 2 Names

- |     |           |     |         |
|-----|-----------|-----|---------|
| 1.  | EST-ESF01 | 13. | EST-DIR |
| 2.  | EST-ESF02 | 14. | EST-LOG |
| 3.  | EST-ESF03 | 15. | EST-OPS |
| 4.  | EST-ESF04 | 16. | EST-FIN |
| 5.  | EST-ESF05 | 17. | EST-EXT |
| 6.  | EST-ESF06 |     |         |
| 7.  | EST-ESF07 |     |         |
| 8.  | EST-ESF08 |     |         |
| 9.  | EST-ESF09 |     |         |
| 10. | EST-ESF10 |     |         |
| 11. | EST-ESF11 |     |         |
| 12. | EST-ESF12 |     |         |
| 13. | EST-ESF13 |     |         |

Note: Numbers 13 through 17 indicate 13 additional addresses utilized by the EST at FEMA Headquarters, EICC.

Further expansions will be used to indicate separate workstations for each function and to mandate use of unique user IDs. For example, if the Logistics desk has three additional workstations besides the primary Chief of Logistics workstation, the ID's EST-LOG-A, EST-LOG-B, EST-LOG-C may be established. Additional workstation IDs will be determined by the support function chief and reported to the FEMA cc:Mail National System Administrator.

# INFORMATION RESOURCES MANAGEMENT PROCEDURAL DIRECTIVE

## Group 3

### Primary ESFs and Positions at an established DFO location

#### Group 3 Naming Standard Formula

(1) State-DFOxxxxESF# or (2) State-DFOxxxx-Position  
where,

State=Abbreviation

xxxx=Unique Disaster or Emergency Number assigned by White House

#=ESF Number as defined in the FRP

Position=Function IDs as follows:

FCO - Federal Coordinating Officer

OPS – Operations

LOG – Logistics

FIN – Finance

DCO - Defense Coordinating Officer

EXT - External Affairs

Example 1: FL-DFO9999-ESF01 is the Department of Transportation position at the declared DFO number 9999 site in Florida.

Example 2: FL-DFO9999-FCO is the Federal Coordinating Officer for the declared DFO number 9999 site in Florida.

#### Example Listing of Group 3 Names

4. FL-DFOxxxx-ESF01
5. FL-DFOxxxx-ESF02
6. FL-DFOxxxx-ESF03
7. FL-DFOxxxx-ESF04
8. FL-DFOxxxx-ESF05
9. FL-DFOxxxx-ESF06
10. FL-DFOxxxx-ESF07
11. FL-DFOxxxx-ESF08
12. FL-DFOxxxx-ESF09
13. FL-DFOxxxx-ESF10
14. FL-DFOxxxx-ESF11
15. FL-DFOxxxx-ESF12
16. FL-DFOxxxx-FCO
17. FL-DFOxxxx-OPS
18. FL-DFOxxxx-LOG
19. FL-DFOxxxx-FIN
20. FL-DFOxxxx-DCO
21. FL-DFOxxxx-EXT

Note: Numbers 13-18 indicate the primary addresses utilized for sending mail to DFO Point of Contacts other than the ESFs at the DFO location.

# INFORMATION RESOURCES MANAGEMENT PROCEDURAL DIRECTIVE

## Group 4

### Emergency Response Team ESFs in Transition

#### Group 4 Naming Standard Formula

State-EXP-ERT-ESF#

where,

State =Abbreviation  
EXP =Expansion ID for further grouping to indicate specific location  
# =ESF Number as defined in the FRP

Example: HI-OAHU-ERT-ESF1 is the DOT ERT at Oahu, Hawaii, for Iniki  
or  
UT-ERT-ESF1 is the DOT ERT in Utah for Response 93

#### Group 4 Names

1. HI-OAHU-ERT-ESF1
2. HI-OAHU-ERT-ESF2
3. HI-OAHU-ERT-ESF3
4. HI-OAHU-ERT-ESF4
5. HI-OAHU-ERT-ESF5
6. HI-OAHU-ERT-ESF6
7. HI-OAHU-ERT-ESF7
8. HI-OAHU-ERT-ESF8
9. HI-OAHU-ERT-ESF9
10. HI-OAHU-ERT-ESF10
11. HI-OAHU-ERT-ESF11
12. HI-OAHU-ERT-ESF12

Note: Group 4 names will be used when an Emergency Response Team is first deployed. These names are for temporary use until a DFO is formally established.

## Group 5

### Primary ESFs at ROC and EOC locations

#### Group 5 Naming Standard Formula

(1) R\*-ROC-ESF#-EXP or (2) R\*-ROC-Position-EXP

where, \*=FEMA Region Number (1-10)

EXP=Expansion ID for further groupings  
# =ESF Number as defined in the FRP

Function IDs as follows:

FCO - Federal Coordinating Officer  
OPS – Operations  
LOG – Logistics  
FIN – Finance  
DUTYOFF - Duty Officer  
or (3) State-EOC-EXP

## INFORMATION RESOURCES MANAGEMENT PROCEDURAL DIRECTIVE

where,

State =State Abbreviation  
# =ESF Number as defined in the FRP  
EX =Expansion ID for further groupings

Example: R2-ROC-ESF1 is the ID used for the Regional Operating Center for DOT at FEMA Region 2.  
NY-EOC is the ID used for the Emergency Operating Center for the state of New York

### Group 5 Names

1.	R1-ROC-ESF01	18-23.	MA-EOC (and -ME,-NH,-CT,-VT,-RI)
2.	R1-ROC-ESF02	24-27.	NY-EOC (and -NJ,-PR,-VI)
3.	R1-ROC-ESF03	28-33.	PA-EOC (and -MD,-DE,-WV,-VA,-DC)
4.	R1-ROC-ESF04	34-40.	GA-EOC (and -TN,-NC,-SC,-FL,-MS,-KT)
5.	R1-ROC-ESF05	41-46.	IL-EOC (and -MI,-MN,-IN,-OH,-WI)
6.	R1-ROC-ESF06	47-51.	TX-EOC (and -NM,-OK,-AK,-LA)
7.	R1-ROC-ESF07	52-55.	MO-EOC (and -IO,-KS,-NE)
8.	R1-ROC-ESF08	56-61.	CO-EOC (and -UT,-WY,-MT,-ND,-SD)
9.	R1-ROC-ESF09	62-65.	CA-EOC (and -NV,-AZ,-HI)
10.	R1-ROC-ESF10	66-69.	WA-EOC (and -AL,-OR,-ID)
11.	R1-ROC-ESF11		
12.	R1-ROC-ESF12		
13.	R1-ROC-FCO		
14.	R1-ROC-OPS		
15.	R1-ROC-LOG		
16.	R1-ROC-FIN		
17.	R1-ROC-DUTYOFF		

Note: Numbers 13-17 indicate the primary addresses utilized for sending mail to ROC Point of Contacts other than the ESFs.+++

## INFORMATION RESOURCES MANAGEMENT PROCEDURAL DIRECTIVE

### Appendix to 4-3.A Firewall Management and Administration Guidelines

This document outlines the management and tasking for Firewall Administration. At minimum, the Firewall Administration tasks relate to Firewall hardware and software, particularly in the following subject areas:

- File management
- System backups
- System restores
- Disk management
- User login accounts (if any)
- Security administration
- System documentation
- Assistance with Internet service conditions
- Addition or deletion of IP subnets
- Maintaining a file of change requests

System (“root”) passwords will be held only by the designated Agency Firewall Administration personnel (i.e., Firewall Administrator and Backup Administrator) and filed with CIO.

Internal firewalls used to protect Agency information systems must support access restriction by network segment or domain (packet filtering) as well as access restrictions by service (FTP vs. Telnet etc.). Internal firewalls will also provide session and traffic logging, event alarms, and support of centralized management.

Internal firewalls or filtering routers provide strong access control and support for auditing and logging for any systems hosting FEMA critical applications. These controls will be used to segment the internal FEMA network to support the access policies developed by the designated owners of information.

System passwords will be changed as often as needed in order to maintain the highest level of system security and data integrity. At minimum, “root” passwords will be changed every 60-90 days. To maintain security, password rotation schedules will not be published.

System Changes. All changes, modifications, upgrades, enhancements to the FEMA Internet firewall will be made in response to a known cause or vendor-released patch, and will be reviewed, in advance and in writing (Email is acceptable) by the Firewall Administration personnel. Only the Firewall Administration personnel may make changes.

System Documentation and Logs. All changes upgrades, enhancements and modifications to the hardware, software and peripherals will be recorded, in as much detail as possible, in a Firewall Administration Log. The log may be handwritten or electronic and will be furnished to Firewall Administration’s management. An up-to-date “working copy” of the log will be retained on-site for auditing purposes. A second copy of the log will be stored off-site.

## INFORMATION RESOURCES MANAGEMENT PROCEDURAL DIRECTIVE

The proxies, kernels and authentication management system automatically write information to the logs. Every night, the “cron daemon” runs a shell script that rotates compresses and removes the log files. By default, the system retains the logs for fourteen (14) days, though this number can be adjusted. The daily script rotates the reports and compresses older log files. Also by default, the firewall keeps seven (7) days of logs in ASCII format and the previous seven (7) days in compressed format. The types of information that the kernel logs, as well as the contents of the log can also be customized.

- Firewall Log Retention - Logs will be retained for a rolling period of at least sixty (60) days.
- Firewall Log Distribution - Neither raw system logs nor extracts from the logs may be provided to any person other than the Firewall Administration personnel without the specific written authorization of the CIO.

System Reports. The firewall contains several reporting mechanisms that sort through the log files and summarize information. These are broken into two (2) main types of reports:

- Service Summary Reports. This report includes both daily and weekly usage and user information on a service basis. Each night or once a week, the firewall can mail the reports. The firewall does not store the daily or weekly reports.
- Exception Reports. This report, by default, defines a list of items that are not noteworthy and ignores such entries in the logs. For example, the firewall default is to ignore successful authentication when parsing the log file. Successful authentication attempts are a normal part of firewall activity, while unsuccessful authentication attempts could be a sign of a potential attack. Therefore, the exception report includes all unsuccessful authentication attempts from the logs. Any item that the firewall has not specifically been told to ignore, it reports. The nightly script summarizes all of the noteworthy items in the log files since the last time it created a report and, by default. The exception report is not stored by the system.

Reports can be custom configured for the events the firewall will ignore in the Exception Report, for the report recipient, enable and disable daily and weekly Service Summary reports, enable and disable Exception reports and customize the Exception reporting interval.

Subnet Proxies. FEMA subnets are proxies to the firewall in order that the internal IP addresses will not be publicized on the public side of the firewall. By configuration of the netstart table, all subnets passing through the firewall proxy take on the firewalls outside IP address. This reduces the risk that a “hacker” could breach the firewall security by masquerading as an internal machine.

## INFORMATION RESOURCES MANAGEMENT PROCEDURAL DIRECTIVE

Suspected Intrusion. If compromise is suspected, the netperm table will be modified to deny access from all hosts for all applications until the logs can be reviewed and appropriate countermeasures, as needed, have been installed and tested. Only the Firewall Administration personnel will execute such action.

Internal Site Managers and Network administrations shall report any suspicions concerning intrusions and Internet-borne viruses, with as much supporting documentation as possible, to the Enterprise Security Manager and to the Email address established for this purpose:

[firewall@fema.gov](mailto:firewall@fema.gov).

Testing. Attack tests will be performed on an irregular schedule, to simulate as rigorously as possible a real hacking attack, including but not limited to IP spoofing, denial of service and other known and emerging attack modes.

Auditing. The system will be audited on a regular unpublished schedule. Audits will include, but are not limited to, documentation, process and quality controls. Results of these types of audits will be presented to management of the Information Technology Services Directorate.

Physical Security. The current firewall system is secured in a FEMA protected computer room. The firewall administration personnel will conduct periodic inspections to determine if any undocumented attempts to circumvent the devices have occurred. This will include a visual inspection of wiring hubs, cables, switches and other devices that provide connection to the system. Each inspection will be documented.

# INFORMATION RESOURCES MANAGEMENT PROCEDURAL DIRECTIVE

Left blank intentionally

## INFORMATION RESOURCES MANAGEMENT PROCEDURAL DIRECTIVE

### Appendix to 4-3.B Remote Access Using Hardware Tokens and TACACS

The three major components of network security are authentication, authorization, and accounting (AAA). To address the remote access aspects of network security, FEMA has implemented the Terminal Access Controller Access Control (TACACS) protocol coupled with hardware tokens. The access device challenges users immediately for a user identification and password; utilizes the TACACS protocol the Access Server to forward the user name and one time password information to a centralized authentication server. If the user identification and password are valid, the Access Server allows the remote connection into the network. If either the user identification or the password is incorrect the Access Server immediately hangs up the modem.

Authentication. Determines whether a valid user has attempted access and if the user will be allowed access to the network. It allows Network Administrators to bar intruders from their networks. Simple authentication methods use a database of user names and passwords while more complex methods use one-time passwords.

Authorization. Determines what users are allowed to do. Authorization allows Network Administrators to limit network services available to each user to that which is minimally essential. This approach limits the exposure of the internal network to outside callers and simplifies the view of the network for the less technical remote access user. Authorization allows mobile users to connect to the closest local connection and still have the same access privileges of their local networks. This also may restrict a Network Administrator to issuing specific commands on predetermined network devices.

Accounting. Keeps track of who did what, when, and where. Network Administrators may need to recreate a session at a later time. Accounting provides logs of connection times and bytes transferred. Accounting can also be used to track suspicious connection attempts to the network.

Central management of access security servers is required for FEMA. The client/ server architecture of TACACS allows all security information to be located in a single, centralized database, instead of being scattered around a network in many different devices. Changes to the database are made in a few security servers instead of in every access point in the network. This type of design allows for easy scalability and extendibility.

All TACACS user names shall be registered and maintained through the National Help Desk. Users shall be assigned a hardware token for one time password generation at that time. Users are responsible for the hardware tokens; if they are lost, users must notify the National Help Desk immediately.

## INFORMATION RESOURCES MANAGEMENT PROCEDURAL DIRECTIVE

### Dial-in Access:

When hardware tokens become available all users who access the FEMA system shall come in through dial-in connections using TACACS and hardware tokens. The Enterprise Security Manager must approve systems that provide direct dial-in connections to FEMA production systems. All in-bound modem access shall be via a modem server controlled by the National ITSC at Mt. Weather. The use of desktop modems to support dial-in access to FEMA systems is prohibited.

Information regarding access to FEMA computer and communication systems, such as dial-up modem phone numbers, is considered restricted. This information must NOT be posted on electronic bulletin boards, listed in telephone directories, placed on business cards, or otherwise made available to third parties without the advance written permission of the ESM. The ESM shall periodically scan direct dial-in lines to monitor compliance with policies and may periodically change the telephone numbers, after providing 30-day advance notice to users, to make it more difficult for unauthorized parties to locate FEMA communications numbers.

### Dial-out Access:

All users who need to access systems external to FEMA via dial-out modems must do so through modem services approved by the ESM and controlled by the National ITSC at Mt. Weather. The use of desktop modems to support dial-out access to external systems is prohibited for machines connected to a LAN or WAN.

## INFORMATION RESOURCES MANAGEMENT PROCEDURAL DIRECTIVE

### **Appendix to 4-3.C Disaster Field Office's Network Administrators Guide**

A Disaster Field Office (DFO) network has some unique characteristics. This office is typically set up quickly; is staffed by personnel drawn from throughout the agency plus local hires; has other Federal, State, and local personnel intermixed in the network environment; and suffers frequent staff turnover. Network administration security policy, procedures, and practices apply to and shall be the responsibility of the DFO Network Administrator. Due to these unique circumstances, special attention must be applied to the DFO network.

This appendix is intended to be a concise reference for the DFO Network Administrator who shall refer to the FEMA Information Resources Management Policy and Procedural Directive (FIRMPD) for additional detail. The Network Administrator shall refer any security questions or requests for assistance directly to the Enterprise Security Manager (ESM) or through the national Information Technology Service Center at Mt. Weather (540) 542-4000.

#### Password Management:

- All passwords shall be at least six characters in length and include at least one numeric or special character.
- Passwords must be changed at least every 90 days.
- After three consecutive failed log-in attempts, login shall be temporarily disabled.

#### Virus Control:

- Virus detection software shall be installed and run on all computers, clients and servers that are connected to FEMA networks.
- FEMA currently recommends the use of Command Systems' FPROT software. Any Network Administrator that chooses to use a different software package is responsible for maintaining up to date virus signature files.
- Virus controls must be applied to all downloads from the Internet or World Wide Web.

## INFORMATION RESOURCES MANAGEMENT PROCEDURAL DIRECTIVE

### Remote Access:

- Desktop modems are prohibited without a waiver from the Enterprise Security Manager.
- All dial-in access is prohibited except via Terminal Access Controller Access Control Systems (TACACS) approved by the ESM and operated by the ITS directorate.
- No connection to external networks is allowed without written approval from the Enterprise Security Manager.
- Internet Access is available to the DFO via the connection to the FEMA Enterprise Network. Any other connection to Internet (either directly or through a state connection) is prohibited.

### Incident Detection:

- The Network Administrator shall review all system logs and audit trails on a weekly basis.
- The Network Administrator shall promptly report all suspected security incidents to the national Information Technology Service Center at Mt. Weather (540)-542-4000.
- Break-ins must be reported to the Office of Inspector General.

### Personal Accountability:

- The Network Administrator is responsible for all computers, software, and communications equipment connected to the LAN.
- The Network Administrator is responsible for any LAN operations that disrupt FEMA WAN operations. Failure to restore operations promptly or to avoid repeated disruptions is grounds for disciplinary action up to and including dismissal.

## INFORMATION RESOURCES MANAGEMENT PROCEDURAL DIRECTIVE

### Modems:

- Dial-in Access. In the DFO, modem dial-in access is prohibited unless approved by the ESM. The Enterprise Security Manager must approve systems, which provide direct dial-in connections to FEMA production systems. All in-bound modem access shall be via a modem server administered by the national ITSC. ***The use of desktop modems to support dial-in access to FEMA systems is prohibited unless waived by the ESM.***
- Dial-out Access. All users who need to access systems external to FEMA via dial-out modems must do so through approved modem services approved by the ESM and controlled by the national ITSC. The use of desktop modems to support dial-out access to external systems is prohibited unless waived by the ESM. For further information of FEMA's dial-out capability contact the national ITSC at (540)-542-4000.

# INFORMATION RESOURCES MANAGEMENT PROCEDURAL DIRECTIVE

Left blank intentionally

# INFORMATION RESOURCES MANAGEMENT PROCEDURAL DIRECTIVE

## Appendix to 5-2 Office Automation Software Baseline Configuration Standard

The software baseline standards listed below are effective for purchases of information systems that require product features as described for those standards. Procurements in response to disasters are **not** exempt.

### Standards

FEMA's software baseline standards are categorized as follows:

Software Category	Software Product
1. Multi-user Data Base	Oracle Relational Data Base Management System
2. Information Access Strategy	Client-Server processing platform
3. Network Operating System	Novell NetWare
4. Desktop Environment	Microsoft Windows Operating System, including Windows 95*, and Windows NT.
5. Desktop Office Automation	Microsoft Office Professional Suite (Includes Word - word processor, Excel - spreadsheet, Access - database, and Powerpoint – graphics, etc.)
6. Geographic Information System	MapInfo
7. Internet/Intranet	Microsoft Explorer preferred Browser. Netscape and AirMosaic Browsers will be supported.
8. Electronic Mail	Microsoft Exchange/Outlook
9. Virus Software	F-PROT Professional
10. Project Management	Microsoft Project (complex projects - full feature) Kick Start (small and less complex projects)

\* FEMA has decided not to upgrade to Windows 98 at this time since we are currently in the process of migrating to Microsoft Exchange/Outlook and installing NEMIS agency-wide. Once these initiatives have been completed, Windows 98 (or other environments) will be considered.

# INFORMATION RESOURCES MANAGEMENT PROCEDURAL DIRECTIVE

Left blank intentionally

# INFORMATION RESOURCES MANAGEMENT PROCEDURAL DIRECTIVE

## Appendix to 5-3 Application Software Standard

The application software standards listed below are effective for development of information systems used within FEMA. Procurements in response to disasters are **not** exempt.

### Standards

FEMA's application software baseline standard

Application Category	Standard
Year 2000 Compliant Date Fields	yyyymmdd

# INFORMATION RESOURCES MANAGEMENT PROCEDURAL DIRECTIVE

Left blank intentionally

# INFORMATION RESOURCES MANAGEMENT PROCEDURAL DIRECTIVE

## Appendix to 5-4 Office Automation Hardware Baseline Configuration Standard

The **minimum** hardware standards for desktop computers are as follows:

Components	Desktop Configuration Minimum - New Purchases
Processor	333* MHz Pentium Intel CPU or greater PCI local bus with minimum of 3 PCI slots 2 ISA 16-bit expansion slots
Memory	64MB RAM with minimum of 3 memory slots with 2, at a minimum, of the slots available for future expansion. 512K L2 Cache
Data Storage & Input/Output Media	8.0GB enhanced IDE Hard Drive mode 4 type 3.5" Built-in Diskette Drive EIDE hard drive/floppy disk controller 101/104 Keyboard PS 2 button serial mouse CD ROM
Video Display	17" Color Monitor with .28 dot/75 Hz scan rate PCI bus Video Accelerator Card with 32 bit processor 4MB VRAM
Ports	Serial port with 16550 UART support Parallel port with enhanced bi-directional capabilities
Network Interface Card	Driver support for Novell NetWare 32 Bit Intel equivalent 10Base-T connection IEEE 802.3 standard
Conservation	Energy Star Compliant system unit that powers down below 60 watts total when in idle mode
All Components	Year 2000 compliant

\* 350 MHz and higher CPU systems will provide a 100 MHz system bus instead of a 66 MHz system bus generally available with 333 MHz CPU. When speed is a consideration, 350 MHz (or higher) CPU with 100 MHz system bus is recommended.

## INFORMATION RESOURCES MANAGEMENT PROCEDURAL DIRECTIVE

The hardware standards for Laptop/Notebook computers are as follows:

<b>Components</b>	<b>Laptop/Notebook Configuration Minimum - New Purchases</b>
Processor	233MHz Pentium Intel CPU or greater 2 Type II & Type III PCMCIA slots 56k Built-in (or PCMCIA Slot) Modem 10/100 PCMCIA NIC
Memory	32MB RAM or greater 256KB L2 Cache
Data Storage & Input/Output Media	3.0GB Hard Drive or greater 3.5" Built-in Diskette Drive Hard drive/floppy disk controller 87 Keys, Windows 95 ready Built-in mouse, J-Pointer, or Touchpad 20x CD ROM Needed/Required to load s/w and data display
Video Display	10" Active matrix Color Monitor 32-Bit Local Bus Video/2MB Video RAM
Ports	External ports for mouse, keyboard and monitor
Conservation	Lithium ion cell battery with a minimum 2-3 hour battery life
All Components	Year 2000 compliant

# INFORMATION RESOURCES MANAGEMENT PROCEDURAL DIRECTIVE

## Appendix to 5-5 Office Automation Standards for Servers and Central Processors

The hardware standards for Server computers are as follows:

<b>Components</b>	<b>Server Configuration Minimum - New Purchases</b>
Processor	400 MHz Pentium II processor w/512K Cache
Memory	128MB EDO RAM or greater
Data Storage & Input/Output Media	1X6 Hot Pluggable Backplane Expandable RAID Controller w/32MB RAM RAID 5 Configuration 5 each 4.5 Gigabyte Ultra-wide SCSI hard drives 3.5" Built-in Diskette Drive 20 Gigabyte DAT Tape Back-up system w/software 101/104 Keyboard PS 2 button serial mouse 24X CD ROM
Video Display	17" Color Monitor with .28 dot/75 Hz scan rate PCI bus Video Accelerator Card with 32 bit processor 2MB VRAM, Diamond Stealth equivalent
Ports	Serial port with 16550 UART support Parallel port with enhanced bi-directional capabilities
Network Interface Card	10/100 Ethernet, PCI Adapter, Twisted Pair
Conservation	Energy Star™ Compliant system unit that powers down below 60 watts total when in idle mode
All Components	Year 2000 compliant

## INFORMATION RESOURCES MANAGEMENT PROCEDURAL DIRECTIVE

The hardware standards for Central Processors are as follows: TO BE PROVIDED

<b>Components</b>	<b>Central Processor Configuration Minimum – New Purchases</b>
Processor	
Memory	
Data Storage & Input/Output Media	
Video Display	
Ports	
Conservation	
All Components	

# INFORMATION RESOURCES MANAGEMENT PROCEDURAL DIRECTIVE

## Appendix A-1 IRM Regulatory Authorities Guide

### Authorities

1. Public Law 96-511, The Paperwork Reduction Act of 1980, as amended.
2. Public Law 99-500, The Paperwork Reduction Reauthorization Act of 1995.
3. Public Law 100-235, Computer Security Act of 1987.
4. Public Law 100-503, Computer Matching and Privacy Protection Act of 1988.
5. Executive Order 12472, Assignment of National Security and Emergency Preparedness Telecommunications Functions, April 3, 1984.
6. Public Law 104-208, Section 808 , Title VIII of the Omnibus Consolidated Appropriations Act (Clinger-Cohen Act of 1996).
7. Executive Order 12656, Assignment of Emergency Preparedness Responsibilities, November 18, 1988.
8. CFR Part 201; et al., National Communications System; Final Rule, December 11, 1990.

# INFORMATION RESOURCES MANAGEMENT PROCEDURAL DIRECTIVE

Left blank intentionally

# INFORMATION RESOURCES MANAGEMENT PROCEDURAL DIRECTIVE

## Appendix A-2 IRM Regulatory Reference Guide

### References

1. Office of Management and Budget Circular A-76, Policies for Acquiring Commercial or Industrial Products and Services Needed by the Government, dated March 3, 1966, as revised and amended.
2. Office of Management and Budget Circular A-109, Major Systems Acquisitions, dated April 5, 1976.
3. Office of Management and Budget Circular A-130, Management of Federal Information Resources.
4. Office of Management and Budget Circular A-11, Preparation and Submission of Budget Estimates, Exhibits 43A and 43B.
5. FEMA Instruction 1610.5, Procurement Review Board/Procurement Planning System.
6. FEMA Instruction 1610.13, Information Resources Board.
7. FEMA Manual 6150.1, Personal Property Management Program.
8. Federal Information Processing Standards Publications (FIPS PUBS) Index List 58.
9. An Introduction to Computer Security: The NIST Handbook, NIST Special Publications 800-12, National Institute of Standards and Technology, Gaithersburg, MD 1995.
10. National Institute of Standards and Technology, Glossary of Computer Security Terminology, NISTIR 4659, September 1991.
11. Defense Intelligence Agency Manual 50-3, Physical Security Standards for Construction of Sensitive Compartmented Information Facilities, February 1990.
12. Director of Central Intelligence Directive 1/6, Security Policy for Uniform Protection of Intelligence Processed in Automated Information Systems and Networks (U), July 19, 1988.
13. Security Administration of Unclassified LANs a handbook for system managers.

## INFORMATION RESOURCES MANAGEMENT PROCEDURAL DIRECTIVE

14. Everything You Always Wanted to Know About Computer Security But Were Afraid to Ask, a handbook for all users of FEMA computer systems.
15. Computer Security - Management's Responsibility, a handbook for all managers of computer systems users.

# INFORMATION RESOURCES MANAGEMENT PROCEDURAL DIRECTIVE

## Appendix B-1 Definitions

### A

**Access control.** The process of limiting access to the resources of a system to authorized users, programs, processes, or other systems (in computer networks).

**Access to information.** The function of providing to members of the public, upon their request, the government information to which they are entitled under law.

**Accreditation.** Official authorization granted to an information system to process sensitive information in its operational environment based on comprehensive security evaluation of the system's hardware, firmware, and software security design, configuration, and implementation of other system, procedural, administrative, physical, TEMPEST, personnel, and communications security controls.

**Agency procurement request (APR).** A request by a Federal agency for General Services Administration (GSA) to acquire Federal information processing (FIP) resources or for GSA to delegate the authority to acquire FIP resources.

**Application systems manager.** The FEMA employee responsible for establishing a management control process over application systems development and maintenance.

**Application systems security manager.** The FEMA employee responsible for managing and establishing application systems life-cycle security requirements, application security control process required by OMB Circular A-130, reviewing and testing reliable security features incorporated into application systems, serving as the focal point for issues and actions involving application systems security, defining and establishing application specific security requirements based on application system data sensitivity.

**Audit trail.** A series of records of computer events, about an operating system, an application, or user activity.

**Authentication.** Proving to some reasonable degree that users are who they claim to be.

**Automated data processing (ADP).** See automatic data processing.

**Automated information system.** An organized collection, processing, transmission, and dissemination of information in accordance with defined procedures that is automated.

**Automated information system (AIS) security.** Measures and controls that protect an AIS against denial of service and unauthorized (accidental or intentional) disclosure, modification, or destruction of AISs and data. See computer security (COMPUSEC).

**Automatic data processing (ADP).** One or more devices that use common storage for all or part of a computer program, and also for all or part of the data necessary for execution of the program; that execute user-written or user-designated programs; that perform used-designated

## INFORMATION RESOURCES MANAGEMENT PROCEDURAL DIRECTIVE

symbol manipulation, such as arithmetic operations, logic operations, or character-string manipulations; and that can execute programs that modify themselves during their execution. Automatic data processing may be performed by a standalone unit or by several connected units.

### **B**

**Burden**. The total time, effort, or financial resources required to respond to a collection of information.

### **C**

**Certification**. Comprehensive evaluation of the technical and nontechnical security features of an information system and other safeguards made in support of the accreditation process that establishes the extent to which a particular system design and implementation meet specified security requirements.

**Chief Information Officer (CIO)**. FEMA executive who serves as principal advisor to the Director and other senior managers regarding the acquisition of IT and management of information resources.

**Collection of information**. The obtaining or soliciting of information from 10 or more persons by means of identical questions, identical reporting or recordkeeping requirement, or requirements to obtain, maintain, retain, report, or publicly disclose information, whether mandatory, voluntary, or required to obtain a benefit. The term "collection of information" refers to the act of collecting information, to the information to be collected, and to a plan and/or an instrument calling for the collection of information.

**Commercial-off-the-shelf (COTS) software**. Computer applications and programs that have been designed and developed for sale to the general public.

**Common-use software**. Software that deals with applications common to many agencies, that would be useful to other agencies, and is written in such a way that minor variations in requirements can be accommodated without significant programming effort.

**Communications**. A method or means of conveying information of any kind from one person or process to other person(s) or process(es) by a telecommunication medium.

- a. **Data communications**. A communications technique that passes information encoded as discrete, on-off pulses, by a telecommunication medium.
- b. **Voice communications**. A communications technique that uses a continuous signal varied by amplification to transmit voice from one person to another by a telecommunication medium.

**Communications link**. The physical means of connecting one location to another for the purpose of transmitting and receiving information.

## INFORMATION RESOURCES MANAGEMENT PROCEDURAL DIRECTIVE

**Communications security (COMSEC).** The protection resulting from all measures designed to deny unauthorized persons information of value which might be derived from the possession and study of telecommunications, or to mislead unauthorized persons in their interpretation of the results of such possession and study. Communications security includes: (a) cryptosecurity; (b) transmission security; (c) emission security; and (d) physical security of communications security materials and information.

**Computer.** (1) A device capable of accepting and processing information and supplying the results. It usually consists of input, output, storage, arithmetic, logic, and control units. (2) A functional unit that can perform substantial computation, including numerous arithmetic operations or logic operations, without intervention by a human operator during a run. Computers have been loosely classified into microcomputers, minicomputers, and main-frame computers, based on their size.

**Computer accommodation.** The acquisition or modification of information technology to minimize the functional limitations of employees in order to promote productivity and to ensure access to work-related information resources.

**Computer Security (COMPUSEC).** Synonymous with automated information system (AIS) security.

**Computer system.** A functional unit, consisting of one or more computers and associated software, that uses common storage for all or part of a program and also for all or part of the data necessary for the execution of the program; executes user-written or user-designated programs; performs user-designated data manipulation, including arithmetic operations and logic operations; and that can execute programs that modify themselves during their execution. A computer system may be a standalone unit or may consist of several interconnected units. Synonymous with ADP system.

**Computer virus.** A common type of malicious computer program written to disrupt or damage computer systems or associated resources. Most viruses copy themselves to other computer programs, thereby infecting them, and then execute malicious instructions programmed by the author. Computer viruses can cause a wide variety of disruptive or destructive actions on systems. For instance, viruses may corrupt or totally destroy data residing on storage media or cause computer hardware or software damage.

**Contingency plan.** A plan for emergency response, backup operations, and disaster recovery maintained to ensure the availability of critical system resources and facilitate continuity of operations in an emergency situation. Also disaster recovery plan or continuity of operations plan (COOP).

### **D**

**Data.** Representation of facts, concepts, or instructions in a formalized manner suitable for communication, interpretation, or processing by humans or by automatic means. Any representations such as characters or analog quantities to which meaning is or might be assigned.

## INFORMATION RESOURCES MANAGEMENT PROCEDURAL DIRECTIVE

**Data communications.** The transfer of data between functional units by means of data transmission according to a protocol. The transmission, reception, and validation of data.

**Delegation of procurement authority (DPA).** The General Services Administration (GSA) delegates its procurement authority to executive agencies, and it grants those delegations to the designated official when GSA determines that such officials are sufficiently independent of program responsibility and have sufficient experience, resources, and ability to fairly and effectively carry out procurements under GSA's authority as provided by 40 U.S.C. 759(b)(3).

**Electronic form.** A form that consists of electronic print images and resides on magnetic or optical media.

**Electronic record.** Any information that is recorded in a form that only a computer can process and that satisfies the definition of a Federal record in 44 USC 3301. Electronic records include numeric, graphic and text information, which may be recorded on any medium capable of being read by a computer and which satisfies the definition of a record. This includes, but is not limited to, magnetic media, such as tapes and disks, and optical disks.

**Environmental control.** Established safeguards to protect system hardware, software, and storage media against damage from unreliable or poor quality power, airborne contaminants, fire, water, temperature, and humidity.

### **F**

**Federal information processing (FIP) resources.** Automatic data processing equipment (ADPE) as defined in Public Law 99-500 (40 U.S.C. 759(a)(2)). The term, FIP resources, includes FIP equipment, software, services, support services, maintenance, related supplies, and systems. These terms are limited by paragraphs (a) and (b) of the definition of FIP resources and are defined as follows:

- (1) **FIP equipment.** Any equipment or interconnected system or subsystems of equipment used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information.
- (2) **FIP maintenance.** Those examination, testing, repair, or part replacement functions performed on FIP equipment or software.
- (3) **FIP related supplies.** Any consumable item designed specifically for use with FIP equipment, software, services, or support services.
- (4) **FIP services.** Any service, other than FIP support services, performed or furnished by using FIP equipment or software.
- (5) **FIP software.** Any software, including firmware, specifically designed to make use of and extend the capabilities of FIP equipment.

## INFORMATION RESOURCES MANAGEMENT PROCEDURAL DIRECTIVE

(6) **FIP support services**. Any commercial nonpersonal services, including FIP maintenance, used in support of FIP equipment, software, or services.

(7) **FIP system**. Any organized combination of FIP equipment, software, services, support services, or related supplies.

**Federal telecommunications system (FTS)**. The umbrella of local and long distance telecommunications services, including FTS2000 long distance services, provided, operated, managed, or maintained by GSA for the common use of all Federal agencies and other authorized users.

**Functional manager**. Required to provide adequate physical security for workstations and other system components located in the functional area. Must assume responsibility for safeguarding data stored locally on devices and media used at system workstations.

**Firewall**. Secure gateway that blocks or filters access between two networks. Secure gateways allow internal users to connect to external networks and at the same time prevent malicious hackers from compromising the internal systems.

### **G**

**Government information**. Information created, collected, processed, disseminated, or disposed of by or for the Federal Government.

### **H**

**Hardware**. Any physical equipment or device used in the configuration and operation of an information system.

### **I**

**Information**. Any communication or reception of knowledge such as facts, data, or opinions, including numerical, graphic, or narrative forms, whether oral or maintained in any medium, including computerized data bases, paper, microfilm, or magnetic tape.

**Information accessibility**. The application or configuration of FIP resources in a manner that accommodates the functional limitations of individuals with disabilities so as to promote productivity and provide access to work-related or public information resources.

**Information collection**. See collection of information.

**Information management**. Planning, budgeting, manipulating, and controlling of information throughout its life cycle.

**Information processing**. Data processing, integrated with processes such as office automation and data communication.

## INFORMATION RESOURCES MANAGEMENT PROCEDURAL DIRECTIVE

**Information processing system.** A system that performs data processing integrated with processes such as office automation and data communication. See also data processing system.

**Information resources.** Includes both government information and information technology.

**Information resources management.** The process of managing information resources to accomplish agency missions. The term encompasses both information itself and the related resources, such as personnel, equipment, funds, and information technology.

**Information system.** The organized collection, processing, transmission, and dissemination of information in accordance with defined procedures, whether automated or manual.

**Information systems security administrator (ISSA).** Depending on circumstances or the local threat environment, assesses physical vulnerabilities and establishes additional controls for workstations, e.g., disposal of hard disks or return hard disks to a vendor for maintenance or replacement, when needed. Provide technical security assistance to system users, functional managers, and system managers/administrators, as well as ensuring the implementation of information systems security requirements.

**Information systems security officer (ISSO).** Is responsible for promoting information systems security and ensuring the implementation of information systems security requirements in his/her organizational element.

**Information systems security manager (ISSM).** Implements physical access controls to protect network servers, auxiliary disk storage subsystems, workstations with backup devices, and removable storage media.

**Integrity.** information security characteristic that ensures information security resources operate correctly and data in system data bases are inviolate. The characteristic protects against deliberate or inadvertent unauthorized modifications. This characteristic applies to hardware, software, firmware, and data bases used by a system.

**Intrusion detection.** Refers to the process of identifying attempts to penetrate a system and gain unauthorized access.

**Information systems security (INFOSEC).** A composite of factors necessary to protect FIP systems and the information they process to prevent exploitation through interception, unauthorized electronic access, or related technical intelligence threats, and to ensure authenticity.

**Information technology.** The hardware and software operated by a Federal agency or by a contractor of a Federal agency or other organization that processes information on behalf of the Federal Government to accomplish a Federal function, regardless of the technology involved, whether computers, telecommunications, or others. It includes automatic data processing equipment.

## INFORMATION RESOURCES MANAGEMENT PROCEDURAL DIRECTIVE

**Information technology system.** The hardware, software, and other resources used for the collection, processing, transmission, and dissemination of information in accordance with established procedures. Information technology systems include non-financial, financial, and mixed systems, as defined below.

- a. **Non-financial system.** A system that supports non-financial functions of an agency or agency sub-component, and has little or no financial functions.
- b. **Financial system.** A financial system encompasses procedures, controls, data, hardware, software, and associated support personnel. A system, comprised of one or more applications, that is used for (1) collecting, processing, maintaining, transmitting, and disseminating data about events having financial consequences (e.g., receipt of appropriations or other financial resources, acquisition of goods and services, payments or collections, recognition of guarantees, benefits to be provided, other potential liabilities, and other discrete financial transactions); (2) providing financial and related information about the operations of an agency or agency sub-component; (3) supporting financial planning or budgeting activities.
- c. **Mixed system.** A system that supports both financial and non-financial functions, where financial functions are significant.

**Interoperability.** The ability of FIP resources to provide services to and accept services from other FIP resources and to use the services so exchanged to enable them to operate effectively together.

### **L**

**Life cycle management (LCM).** The stages through which information resources progress from the decision making, analyses, operations and maintenance through disposition. LCM encompasses the (1) decision making steps necessary to describe the purpose and size of an acquisition or in-house development in terms of explanation and cost estimates; (2) requirements analysis and analysis of alternative steps to justify and document the decision making, milestones, and key activities needed for delivery and acceptance; (3) operations and maintenance steps which provide for the manipulation and maintenance of information resources in support of the decision making; and (4) disposition steps to determine when the information resources no longer serve a useful purpose to the Federal government.

- a. **Information life cycle.** The stages through which information passes, typically characterized as creation or collection, processing, dissemination, use, storage, and disposition.
- b. **Information system life cycle.** The phases through which an information system passes, typically characterized as initiation, development, operation, and termination.

# INFORMATION RESOURCES MANAGEMENT PROCEDURAL DIRECTIVE

## M

**Major information system.** An information system that requires special continuing management attention because of its importance to an agency mission; its high development, operating or maintenance costs; or its significant impact on the administration of agency programs, finances, property, or other resources.

**Major system.** That combination of elements that will function together to produce the capabilities required to fulfill a mission need. The elements may include, for example, hardware, equipment, software, construction, or other improvements or real property. Major system acquisition programs are those programs that (1) are directed at and critical to fulfilling an agency mission, (2) entail the allocation of relatively large resources, and (3) warrant special management attention.

**Management information system (MIS).** A communication process in which data are recorded in some fashion and processed for operational purposes in support of processes for identifying and isolating problems for higher-level decision making.

**Messaging service.** In Integrated Services Digital Network (ISDN), an interactive telecommunications service that allows information transfer between users by means of store-and-forward, electronic mail, or message-handling functions.

**Media degaussing.** Clearing or erasing of stored sensitive data prior to release for reuse, maintenance, or replacement by any individual or organization outside the system environment.

## N

**National security and emergency preparedness (NSEP).** Those physical, technical, and administrative characteristics of FIP systems that will ensure a prescribed level of survivability in times of national or other emergencies up to and including nuclear attack. Government common-use telecommunications systems are designed, built, tested, and maintained to meet the defined emergency mission needs of the Government entities that use them.

## O

**Obsolescence.** The state of FIP hardware or software that is either in a degenerative condition, which if not corrected will render the resource useless, or has become technologically outmoded compared to other hardware or software being sold.

**Office automation (OA).** The techniques and means used for the automation of office activities, in particular, the processing and communication of text, images, and voice.

## INFORMATION RESOURCES MANAGEMENT PROCEDURAL DIRECTIVE

**Open system.** A system whose characteristics comply with specified, publicly maintained, readily available standards and that therefore can be connected to other systems that comply with these same standards.

**Operating system.** Software that controls the execution of programs; and that provides services such as resource allocation, scheduling, input/output control, and data management. Usually, operating systems are predominantly software, but partial or complete hardware implementations are possible.

**Outdated equipment.** Any Federal information processing equipment over eight years old, based on the initial commercial installation date of that model of equipment, and that is no longer in current production.

### **P**

**Personal computer.** A stand-alone computer equipped with all the system, utility, and application software, and the input/output devices and other peripherals that an individual needs to perform one or more tasks.

**Physical control.** Use of locks, guards, badges, alarms, barriers, control procedures, or similar measures to limit access to information resources.

### **R**

**Records.** All books, papers, maps, photographs, machine readable materials, or other documentary materials, regardless of physical form or characteristics, made or received by an agency of the United States Government under Federal law or in connection with the transaction of public business and preserved, or appropriate for preservation, by that agency or its legitimate successor, as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of the Government or because of the informational value of data in them.

**Records disposition.** Any activity with respect to disposal of temporary records no longer necessary for the conduct of business by destruction or donation; transfer of records to Federal agency storage facilities or records centers; transfer to the National Archives of the United States of records determined to have sufficient historical or other value to warrant continued preservation; or transfer of records from one Federal agency to any other Federal agency.

**Records management.** Planning, controlling, directing, organizing, training, promoting, and other managerial activities involved with respect to records creation, records maintenance and use, and records disposition in order to achieve adequate and proper documentation of the policies and transactions of the Federal Government and effective and economical management of agency operations.

**Records maintenance and use.** Any activity involving location of records of a Federal agency; storage, retrieval, and handling of records kept at office file locations by or for a Federal agency; processing of mail by a Federal agency; or selection and utilization of equipment and supplies associated with records and copying.

## INFORMATION RESOURCES MANAGEMENT PROCEDURAL DIRECTIVE

**Risk management.** Process of identifying, controlling, eliminating or minimizing uncertain events that may degrade information systems resources. It includes risk analysis, cost/benefit analysis, and the selection, evaluation, and implementation of cost-effective safeguards.

### **S**

**Safeguards.** Protective devices, actions, procedures, techniques or measures prescribed to meet the security requirements specified for an information system. Safeguards include, but are not limited to: hardware and software security features, operational controls, accountability procedures, access and distribution controls, administrative constraints, personal security, and physical control structures areas, or devices.

**Security policy.** Basic information systems security requirements that safeguards all unclassified information as a valuable resource or asset and implemented in every unclassified systems environment without exception.

**Sensitive.** Is synonymous with important or valuable. In general, the more important a system is to the mission of the agency, the more sensitive it is.

**Sensitivity assessment.** Looks at the value of both the information and the system itself. The assessment considers legal implications, organization policy, and the functional needs of the system.

**Software.** A term that applies to computer programs or sets of computer instructions and automated procedures; for example, operating systems, applications programs, programming languages, compilers, security programs, various utility-type programs, etc. The term is used in contrast with hardware.

**Specific make and model specification.** A description of the Government's requirement for FIP resources that is so restrictive that only a particular manufacturer's products will satisfy the Government's needs, regardless of the number of suppliers that may be able to furnish that manufacturer's products.

**Storage media protection.** Proper safeguards and handling of storage media such as diskettes, tape cassettes, fixed hard disks, and removable hard disks in the loss of valuable software or data, or unauthorized disclosure or modification of data.

**System analysis.** A systematic investigation of a real or planned system to determine the functions of the system and how they relate to each other and to any other system.

**System and data access control.** Established safeguards to prevent the unauthorized disclosure, modification, or destruction of word processing and data processing files resident on the system storage devices. Protects against unauthorized access, unique user identifies (user IDs) and passwords are used to identify and authenticate authorized users.

**System description.** Documentation that describes the system design and that defines the organization, essential characteristics, and the hardware and software requirements of the system.

## INFORMATION RESOURCES MANAGEMENT PROCEDURAL DIRECTIVE

**System design.** A process of defining the hardware and software architecture, components, modules, interfaces, and data for a system to satisfy specified requirements.

**System design concept.** An idea expressed in terms of general performance, capabilities, and characteristics of hardware and software oriented either to operate or to be operated as an integrated whole in meeting a mission need.

**System development.** A process that begins with requirements analysis and includes system design, implementation, and documentation.

**System documentation.** The collection of documents that describe the requirements, capabilities, limitations, design, operation, and maintenance of an information processing system.

**System life cycle.** The course of developmental changes through which a system passes from its conception to the termination of its use; for example, the phases and activities associated with the analysis, acquisition, design, development, test, integration, operation, maintenance, and modification of a system. See life cycle management.

**Systems security requirements.** Establishment, implementation, and use of safeguards for Federal Emergency Management (FEMA) application systems, local area networks (LAN), mini and mainframe computer systems and personal computers (PC). The minimum security controls, procedures, and documentation products specified for safeguarding classified and unclassified computer hardware and software systems implemented into the life-cycle process provide reliable security features to protect the confidentiality, integrity, and availability of computer hardware and software resources used in support of FEMA's mission.

**Systems specification.** Specifications which include the delineation of the objective which the system is intended to accomplish, and the data processing requirements underlying that accomplishment.

### **T**

**Telecommunications.** Any transmission, emission, or reception of signs, signals, writing, images and sounds or intelligence of any nature by wire, radio, optical or other electromagnetic systems.

**Telecommunications device for the deaf (TDD).** A machine that uses typed input and output, usually with a visual text display, to enable individuals with hearing or speech impairments to communicate over a telecommunications network.

**Telecommunications facilities.** Equipment used for such modes of transmission as telephone, data, facsimile, video, radio, audio, and such corollary items as switches, wire, cable, access arrangements, and communications security facilities.

**Telecommunications resources.** Telecommunications equipment, facilities, and services.

## INFORMATION RESOURCES MANAGEMENT PROCEDURAL DIRECTIVE

**Telecommunications service priority (TSP).** A regulated service provided by a telecommunications provider, such as an operating telephone company or a carrier, for NSEP telecommunications.

**Telecommunications services.** The transmission, emission, or reception of signals, signs, writing, images, sounds, or intelligence of any nature, by wire, cable, satellite, fiber optics, laser, radio, or any other electronic, electric, electromagnetic, or acoustically coupled means. The term includes the telecommunications facilities necessary to provide such services.

### U

**Used computer equipment.** Mainframe, minicomputer, microcomputer (personal computer), and associated peripheral equipment that has been previously installed. This term includes reconditioned, refurbished or remanufactured equipment.

**User.** An organizational or programmatic entity that receives service from an information technology facility. A user may be either internal or external to the agency organization responsible for the facility, but normally does not report either to the manager or director of the facility or to the same immediate supervisor.

### V

**Vulnerability.** Refers to a weakness in automated system security procedures, administrative controls, internal controls, and so forth, that could be exploited by a threat to gain unauthorized access to information or disrupt critical processing.

### Y

**Year 2000 compliant.** Defined as information technology that accurately processes date/time data (including, but not limited to, calculating, comparing, and sequencing) from, into, and between the twentieth and twenty-first centuries, and the years 1999 and 2000 and leap year calculations. Furthermore, Year 2000 compliant information technology, when used in combination with other information technology, shall accurately process date/time data if the other information technology properly exchanges date/time data with it.

# INFORMATION RESOURCES MANAGEMENT PROCEDURAL DIRECTIVE

## Appendix C-1 Acronyms

### A

ADP	Automatic Data Processing/Automated Data Processing
ADPE	Automatic Data Processing Equipment
AIS	Automated Information Systems
APR	Agency Procurement Review

### C

CIO	Chief Information Officer
COMM	Communications
COMPUSEC	Computer Security
COMSEC	Communications Security
COTS	Commercial-off-the-shelf

### D

DAR	Designated Agency Representative
DEC	Director's Executive Council
DPA	Delegation of Procurement Authority

### E

E-mail	Electronic Mail
--------	-----------------

### F

FAR	Federal Acquisition Regulation
FAX	Facsimile
FED-STD	Federal Standard
FIP	Federal Information Processing
FIPS	Federal Information Processing Standards
FIPS PUBS	Federal Information Processing Standards Publications
FIRMR	Federal Information Resources Management Regulation
FOIA	Freedom of Information Act
FPMR	Federal Property Management Regulations
FSN	FEMA Switched Network
FTS	Federal Telecommunications System

### G

GAO	General Accounting Office
GSA	General Services Administration

# INFORMATION RESOURCES MANAGEMENT PROCEDURAL DIRECTIVE

## I

INFOSEC	Information Systems Security
INTERCOM	Intercommunications
IRB	Information Resources Board
IRM	Information Resources Management
IRPMR	Information Resources Procurement and Management Review
IS	Information Systems
ISP	Information Systems Plan
IT	Information Technology
ITMRA	Information Technology Management Reform Act of 1996

## L

LCM	Life Cycle Management
-----	-----------------------

## M

MIS	Management Information System
MOU	Memorandum of Understanding

## N

NIST	National Institute of Standards and Technology
NSEP	National Security and Emergency Preparedness
NTIS	National Technical Information Service

## O

OA	Office Automation
OMB	Office of Management and Budget

## P

PRA	Paperwork Reduction Act
-----	-------------------------

## T

TDD	Telecommunications Device for the Deaf
TELECOMM	Telecommunications
TSP	Telecommunications Service Priority