Additional Help: 545, 552
File Name: 545sae_071300_cd20
Last Revised: 07/13/2000

CONTINGENCY PLANNING FOR INFORMATION RESOURCES

The overall USAID Contingency Plan for Information Resources is comprised of three distinct components. These components are the Emergency Action Plan (EAP), the Disaster Recovery Plan (DRP) and the Connection Security Plan (CSP). The EAP and DRP jointly assist a USAID site (defined as a building in USAID/W or a mission or other Agency organization overseas) in protecting their ability to process data. The purpose of the EAP is to prevent and/or limit damage to information resources. The purpose of the DRP is to restore secure operations after damage has been contained. The CSP assists a USAID site in protecting the actual data on a system-by-system, connection-by-connection basis. In aggregate, these three components comprise the Agency's Contingency Plan for Information Resources. Specific information follows regarding the EAP and DRP. Specific information regarding the CSP is found in Supplementary Reference, Connection Security Plan**.** Each USAID site should also concurrently review interrelated Supplementary References, Contingency Planning for Information Resources and Connection Security Plan.

EMERGENCY ACTION PLAN

The Emergency Action Plan (EAP) is comprised of three major sections that are completed by each USAID site. The combination of these sections shall assist each USAID site in formulating and documenting their EAP, for the purpose of preventing and/or limiting damage to information resources, heightening computer security awareness and providing a means for continuity of operations.

An EAP is comprised of the following:

The first section is a comprehensive inventory of all information resources and a criticality assessment of those resources.

The second section is identification of potential threats to USAID site operations and existing/proposed countermeasures for each threat.

The third section is the immediate response procedure (IRP) documenting remedial actions to complete after threats have been realized or are identified as imminent.

An EAP is developed and maintained as follows:

The System Manager/Information Technology (IT) Specialist, site ISSO and other personnel, as appropriate, jointly conduct a resource inventory and subsequently determine the criticality of each identified resource,

using the format provided in this attachment.

The System Manager/IT Specialist, site ISSO and other personnel, as appropriate, then identify potential threats to these resources and any existing and/or proposed countermeasures, using the format provided in this attachment. This information is considered sensitive and should be protected accordingly.

The System Manager/IT Specialist, site ISSO and other personnel, as appropriate, formulate the Immediate Response Procedure (IRP) using information provided in this attachment.

The System Manager/IT Specialist, upon completion of their USAID site's EAP, must submit a copy of the EAP to the "ISSO for USAID" for review. If appropriate, the "ISSO for USAID" shall suggest additional recommendations to be incorporated into the EAP. The "ISSO for USAID" shall then update the EAP database maintained at USAID/W and include each EAP in the USAID-wide DRP.

In the event the USAID site subsequently proposes a major procurement or relocation of information resources, the System Manager/IT Specialist and site ISSO must update the EAP to include all proposed changes and send it to the "ISSO for USAID."

Annually, on or before the anniversary of the latest EAP, the System Manager/IT Specialist and site ISSO must review the contents of the EAP for currency and completeness and revise it as necessary. Upon completion of review, the System Manager/IT Specialist must either notify the "ISSO for USAID" that the annual EAP review has been completed with no changes; or, if the EAP was modified must forward a copy to the "ISSO for USAID" for replacement in the USAID-wide DRP and update of the database.

The "ISSO for USAID" shall forward the site specific portion of the DRP to each USAID site for inclusion as an appendix in their EAP. Each USAID site must maintain a copy of their EAP in the central system file. Additional copies of the IRP should be dispersed in appropriate locations (e.g., computer room, ISSO office, etc.).

Section One: Resource Accounting and Criticality Assessment

Resource accounting and criticality assessment identifies all information resources and supporting facilities, then documents the criticality of those resources. The resources identified should include items such as computer hardware and software, peripheral devices, storage media, FAX machines, STUs, modems, encryptors, climate control systems, copiers, shredders, documentation, personnel, etc. Resources also include

services such as telephone, electric, Internet, and other external non-Agency providers. The criticality of these resources should be determined in terms of the length of time the USAID site can function without those resources. For uniformity, a scale of 0 to 5 must be used and is defined as follows:

0 - USAID site is able to function indefinitely without resource
1 - USAID site is able to function up to one month without resource
2 - USAID site is able to function up to two weeks without resource
3 - USAID site is able to function up to one week without resource
4 - USAID site is able to function up to one day without resource
5 - USAID site is able to function up to four hours without resource

A sample format is as follows:

RESOURCE ACCOUNTING AND CRITICALITY ASSESSMENT

Crit.	Quant.	Resource Description	
4	1	486/33 Server:16MB RAM, 1.44MB Flop, 1GB HD, Monitor	
3	1	486/33 Server:16MB RAM, 1.44MB Flop, 500MB HD, Mon	
3	2	FastSCSI 3.5" external 500MB HD	
4	3	32 bit Network Interface Card } Duplicate resources have been	
3	4	32 bit Network Interface Card } separated to note differences	
2	6	32 bit Network Interface Card } in criticality	
1	1	32 bit Network Interface Card (spare)	
4	2	386/25 PC: 1.44MB & 1.2MB Floppy	
3	3	386/25 PC: 1.44MB & 1.2MB Floppy	
2	6	386/25 PC: 1.44MB Floppy	
1	1	386/25 PC: 1.2MB Floppy (spare)	
2	1	CD-ROM	
4	1	525/320MB SCSI External Tape Unit	
4	1	16-Port Non-Managed Concentrator	
4	1	10Base-T Transceiver	
4	1	9600 Modem	
4	1	Racal-Milgo Multiplexer	
4	1	Black KG-84	
4	1	HP LaserJet III	
3	2	HP LaserJet III	
1	1	HP LaserJet III (spare)	
3	1	Murata F-30 FAX	
4	1	Motorola SECTEL 2500	
4	1	Xerox 5052 Copier	
3	1	Cross/Cut 2601 Paper Shredder	
4	2	Vines 5.5	} Software quantities for
4	2	Vines Intelligent Messaging (E-MAIL)	} packages at large

4	2	Vines PC Network Printing
4	2	Vines TCP/IP Routing
4	15	DOS 5.0
4	15	WordPerfect
3	5	Lotus 1-2-3
3	5	Harvard Graphics
1	10aprx.	525MB Tapes
1	100aprx.	1.2MB & 1.44MB Diskettes - both blank & in-use
4	1	Liebert Climate Control System
3	4	Fire Extinguisher (water-based)
5	1	Private Branch Exchange (PBX)
5	1	Telephone Service (Service Provider)
5	1	Electricity
3	2	Maintenance/Service Personnel
4	2	Operations Personnel
1	1	Field Service Manual for Banyan File Server
4	10	Offline Backup Media (tapes, diskettes, etc.)

Section Two: Identification of Threats and Countermeasures

A threat is any circumstance or event with the potential to compromise and/or interrupt an Agency site's daily operations. Threats are perceived as being physical, environmental, support-related or technical in nature. A USAID site is vulnerable when countermeasures have not been implemented to negate and/or mitigate the impact of all identified threats. Threats are realized when one or more vulnerabilities are exploited.

Following is a comprehensive listing of threats, divided into four distinct categories. This list is intended to assist with identification of threats in existence at a USAID site and increase awareness. Each USAID site may have some of these threats, and additional threats not included on this list which are specific to their location.

POTENTIAL THREATS

Environmental

Fire **Flood** **Tsunami** **Earthquake** **Volcanic Eruptions** **Explosion** - nearby gas line, chemical plant, tank farm, munitions depot	**Lightning** **Severe Weather** **Smoke** **Dust** **Insects** **Rodents** **Chemical Fumes** **Sprinkler Activation**	**Water Leakage** - pipe breakage, hole in roof, condensation **Vibration** - nearby railroad track, jet traffic **Electromagnetic Interference** - evidenced by poor radio reception **Electrostatic Discharger**

Support-Related

Power Outage **Electrical Noise/Bad Ground** - evidenced by flickering lights **Unstable Temperatures** **Humidity Extremes** **Improper Maintenance**	**Personnel Unavailability** - inability to contact operations & support personnel **Telephone Failure** - inability to contact site from outside, unable to call out, service completely unavailable

Physical

Unauthorized Facility Access **Improper Transportation** - equipment dropped, submerged, x-rayed in transit **Improper Mounting/Storage** - equipment prone to bumps, kicks, elements **Spillage/Droppage** **Trip Hazards/Falls** **Collision** - fork lift, auto, plane, wheelchair **Theft**	**Sabotage** - malicious hardware and/or software **Vandalism** **Extortion** **Terrorism/Bomb Threat** **Labor Unrest** **War/Civil Unrest** **Inappropriate Fire Suppression** - PKP, water, halon

Technical

As technical threats are specific to systems and not sites, this category is defined and addressed on a system-by-system, connection-by-connection basis in the Connection Security Plan (CSP) (See Supplementary Reference, Connection Security Plan). Technical threats are not included in the EAP.

Each USAID site must select from the threat list all those that pertain to any information resource at their site, countermeasures notwithstanding. After all potential threats have been identified, each USAID site must then evaluate those threats and delineate all existing and/or proposed countermeasures to each threat for each resource. USAID sites must distinguish between existing and proposed countermeasures. In the event proposed countermeasures cannot be implemented in a timely manner, an interim solution must be identified.

A sample format is as follows:

THREATS AND COUNTERMEASURES

Threats	Countermeasures
1. Fire	Sprinkler system throughout both buildings. Water-based fire extinguisher available in both buildings. *** Propose installing fire suppression system in computer room. *** Interim solution - installing carbon dioxide fire extinguisher in

	computer room.
2. Explosion	Both buildings can support each other in operations. *** Propose reciprocal agreement with embassy for automated processing if necessary.
3. Lightning	Lightning rods attached to roof. *** Propose UPS for servers.
4. Smoke	Smoke detectors throughout both buildings.
5. Dust	Cleaning weekly throughout both buildings. Periodic preventive maintenance cleaning for all equipment. Air filters installed in computer room and changed monthly.
6. Insects	Screens on all windows and doors.
7. Water Leakage	Identified shut-off valves. Plastic sheets available near major devices.
8. Power Outage	Generator wired to support both buildings.
9. Bad Ground	*** Propose having building electrician and computer maintenance contractor check and repair all grounds.
10. Personnel Unavailability	Generated listing of operations and support personnel contact numbers. *** Propose wiring two telephone lines independent of PBX.
11. Telephone Failure	Personnel have been instructed to contact embassy. Embassy has agreed to send staff member to site.
12. Unauthorized Physical Access	Locks on all access areas. Alarms activated after COB.
13. Improper Mounting/ Storage	All devices appropriately installed to reduce possibility of bumping or falls. Storage area is just off computer room; access and climate controlled.
14. Collision	All devices placed away from high traffic areas.
15. Theft	Locks on all access areas.
16. Inappropriate Fire Suppression	All PKP fire extinguishers removed from computer room.

Section Three: Immediate Response Procedure

The intent of the Immediate Response Procedure (IRP) is to limit damage, appropriate for the criticality of the resource, in the event a threat against an information resource is realized or is impending. The IRP must document remedial actions in order of execution, specific individuals and/or organizations to contact and, if appropriate, provide for activation of the site specific portion of the DRP. The IRP must be written in clear, understandable English.

The following minimum information must be included and verified on a quarterly basis:

1. Step-by-step instructions detailing remedial actions for existing threats (i.e., fire, water leakage, power outage, etc.);

2. Instruction to review site specific portion of the DRP in preparation of activation;

3. The name, on- and off-duty telephone number and, where applicable, radio frequency/beeper number of the System Manager/Information Technology (IT) Specialist;

4. The name, on- and off-duty telephone number and, where applicable, radio frequency/beeper number of the Program Manager and site ISSO (USAID/W) or Executive Officer/ISSO (USAID mission);

5. The names, on- and off-duty telephone numbers of all operations staff;

6. The names and business-hours/after-hours/emergency telephone numbers of system maintenance personnel. Include corporation name, address and contract-specific information;

7. The telephone number of the Embassy and pre-arranged contact name/office/extension (e.g., Regional Security Officer (RSO));

8. The telephone numbers for local police, fire department and medical services;

9. The name and telephone number of the "ISSO for USAID" and USAID/W technical support representative, for purposes of activating the site specific portion of the DRP.

NOTE: An alternate means of communication should be identified in the event of telephone failure.

DISASTER RECOVERY PLAN

The Disaster Recovery Plan (DRP) is a USAID-wide plan that facilitates restoration of

secure system operations after a threat has been realized and damage has been contained. The intent of the DRP is to lessen the impact of a disaster by recovering quickly. Recovery is accomplished through coordination and effective utilization of all available information resources. This plan envisions a regional and/or global response to disasters through the combined efforts of various USAID sites and USAID/W. This response shall embrace the concept of sharing and/or redirecting spare information resources contained within the same geographical area or in USAID/W. This concept encourages the backup and support of one another without substantial cost considerations.

Upon receipt of each USAID site's EAP, the information contained therein shall be used to provide the foundation of the DRP. The DRP shall be developed and maintained by the "ISSO for USAID." After the DRP is developed using the characteristics of information resources available at sites, each USAID site shall receive from the "ISSO for USAID" their site specific portion of the DRP for inclusion as an appendix in their EAP. As USAID sites submit updated EAPs, the "ISSO for USAID" shall examine these EAPs for changes relative to the DRP, shall update the DRP and then forward the latest site specific portion of the DRP to the USAID site.

SYSTEM CERTIFICATION

(Part I)

I hereby verify the automated information system located in _____, Room _____ meets the security specifications amplified in USAID's ADS Chapter 5**45 and/or 552** and a formal risk analysis has documented potential threats and appropriate countermeasures to negate the identified threats. Further, the prescribed countermeasures are in place and operational.

_____ _____
Signature, "ISSO for USAID" Date

_____
Name (type or print)

(Part II)

I have carefully examined the verification statement and its associated documentation for the automated information system located in _____, Room _____. Based on implementation of all applicable physical, administrative and technical security controls, I authorize this system, as configured and located as of this date, to operate in support of USAID objectives.

As of this date information up to and including the level of _____ may be processed on this system.

This system is subject to recertification and/or revalidation of its security safeguards at any time.

_____ _____

Signature, (Director, M/IRM) Date

_____
Name (type or print)