



**Environmental Management Consolidated Business Center (EMCBC)**

**Subject: Cyber Security – Incident Response**

Implementing Procedure

APPROVED: (Signature on File)

EMCBC Director

ISSUED BY: OFFICE OF INFORMATION RESOURCE MANAGEMENT

---

1.0 PURPOSE

The purpose of this procedure is to identify the procedures to be followed when an Incident or Potential Incident is identified by users or administrators.

2.0 SCOPE

This procedure addresses all unusual events that occur in EMCBC systems and encompasses all EMCBC Accreditation Boundaries.

3.0 APPLICABILITY

This procedure is applicable to all EMCBC operations and all Serviced sites with the EMCBC Extended Network.

4.0 REQUIREMENTS and REFERENCES

Cyber Security Plan Sections

- IR-1 Incident Response Policy and Procedures
- IR-2 Incident Response Training
- IR-3 Incident Response Testing
- IR-4 Incident Handling
- IR-5 Incident Monitoring
- IR-6 Incident Reporting
- IR-7 Incident Response Assistance

TMR-9, October 10, 2007 Cyber Security Technical and Management Requirements- Incident Management

5.0 DEFINITIONS

- 5.1 ADIRM – Assistant Director for Information Management
- 5.2 IRT – Incident Response Team
- 5.3 PIT – Potential Incident
- 5.4 IRC – Incident Response Coordinator

## 6.0 RESPONSIBILITIES

### 6.1 Assistant Director, Information Resource Management

- 6.1.1 Appoint Incident Response Team Leaders
- 6.1.2 Appoint the Incident Response Coordinator
- 6.1.3 Declare Incidents
- 6.1.4 Initiate and approve final reports

### 6.2 Incident Response Coordinator

- 6.2.1 Conduct Incident Response Training
- 6.2.2 Conduct initial evaluation of Potential Incidents (PITs)
- 6.2.3 Participate on IRTs as requested.

### 6.3 Incident Response Team Leader

- 6.3.1 Lead the evaluations of Potential Incidents
- 6.3.2 Recommend Declaration of an Incident to the ADIRM
- 6.3.3 Initiate Reporting of an Incident
- 6.3.4 Conduct Training

### 6.4 IRT Team members

- 6.4.1 Respond to Incidents as required
- 6.4.2 Attend Incident Training

## 7.0 GENERAL INFORMATION

The intent of this procedure is to provide the methods to respond quickly and effectively to incidents. The process provides for response to obvious “earthquake” type events, as well as incidents that may only reveal themselves through a series of small irrelevant events.

## 8.0 PROCEDURE

### 8.1 Incident Declaration

8.1.1 Potential Incidents (PIT) - Network Administrators, Help Desk personnel and the general user community shall report any unusual activity that may not be consistent with IT operations to the Incident Response Coordinator (IRC). The general user community may not be aware of who the IRC is, so it is incumbent on IRM staff to ensure that any issues are directed to the team. The IRC will evaluate the PIT and elevate it to the ISSM (Information System Security Manager) for further evaluation or log the event as a suspicious activity in the IM Maintenance Log.

8.1.1.1 Events that are considered “curious” but do not indicate any malicious activity are logged by the IRC at his discretion.

8.1.1.2 In addition to the IRC, any member of the IRM organization may record unusual activity in the log.

- 8.1.2 Once a PIT is identified, the ISSM will call key IRM staff together into an ad hoc team to examine the type and nature of the PIT and will evaluate if indeed there is an incident. The PIT may be evaluated by the team in three ways.
  - 8.1.2.1 It may be declared as an Incident and the team will recommend to the ADIRM to declare an Incident. In which case the ADIRM will appoint an Incident Response Team Leader and the issue will be address in accordance with section 8.2 of this procedure.
  - 8.1.2.2 It may be deemed to be suspicious activity, but not a clear incident. In which case, it will be logged in the Maintenance Log to document the suspicious activity so that the information will be available for future reference.
  - 8.1.2.3 Or the PIT may be considered a non incident. Usually the anomaly is related to user error or some other type of system glitch. All non-event PITs will be Logged.
- 8.1.3 The ADIRM is responsible for reviewing the recommendation of the ISSM and will make the Declaration of an Incident and appoint team members as appropriate. The ADIRM will also notify the DAA and potentially affected Content Owners or Content Mangers of the declaration of an incident.

## 8.2 Incident Handling

- 8.2.1 Once an Incident has been declared the IRT shall begin corrective actions. Each action will be logged for inclusion in interim or final reports.
  - 8.2.1.1 The first action shall be to determine the nature of the incident and to isolate the system or systems affected. This shall be done as agreed to by the team.
  - 8.2.1.2 Once the affected system or systems have been isolated or shut down, the team shall conduct a quick damage assessment to systems and system security to determine if there where any obvious breaches or serious damage to databases or file systems.
  - 8.2.1.3 The Team Leader shall then initiate reporting of the incident to Computer Incident Advisory Capability (CIAC) and to EM Cyber Security in accordance with the time frames and guidance from TMR-9 in Attachment (B). The report shall specify the Level and Categorization of the Incident. EM shall provide further direction on reporting.
  - 8.2.1.4 The IRT shall then initiate recovery operations to return the system or systems to operations. The Team shall conduct an

analysis and conduct testing as appropriate to ensure that the incident has been dealt with effectively. The ADIRM shall authorize restart. All testing and analysis shall be logged in the Maintenance Log.

8.2.1.5 Once the affected systems have been restarted the ADIRM shall initiate review of possible long term solution to the problem as necessary and shall develop a final report that describes the incident, immediate actions taken, long term actions necessary for preventive actions, and address any lessons learned.

8.2.1.6 Interim reports shall be generated to fulfill the reporting requirements of Attachment (B). A final report shall be generated in accordance with the guidance of Attachment (C).

8.3 Incident Response Team – The IRT shall be made up of a cross section of individuals from IRM, Logistics and the EM HQ MIPP (Mission Information Protection Program) team. The IRT may vary from incident to incident, depending on the nature of the incident, the systems affected and on the availability of staff due to vacation, sickness, or travel. Appointments to the IRT Team shall be logged with each incident.

8.3.1 The IRT is made up of:

8.3.1.1 Team Leader – Appointed by the ADIRM

8.3.1.2 EMCBC Security Officer – Office of Technical Support and Asset Management

8.3.1.3 Cognizant Network Administrators or Application Developers

8.3.1.4 Representative from the EM MIPP team – Appointed by EM HQ.

8.3.1.5 Member at large – Appointed by the ADIRM.

8.3.2 Training

8.3.2.1 The ADIRM shall ensure that Incident Awareness and Reporting is addressed in User Training.

8.3.2.2 The Incident Response Coordinator shall conduct annual training in incident response. The following methods may be used for training: small group discussion of known incidents, simulated response to penetration testing, critiques of real incidents, and may use simulated scenarios as applicable. The training date, subject, and participants shall be documented and Logged.

## 9.0 RECORDS MAINTENANCE

9.1 Records generated as a result of implementing this document are identified as follows and are maintained in accordance with the Office of Information Resource Management:

- 9.1.1 ADM 01-29.2-A3 – Administrative Training Records – Cyber Security Incident Response Training
- 9.1.2 GRS 24-05 – Cyber Security Configuration Records
- 9.1.3 GRS 24-07 – Computer Security Incident Handling, Reporting and Follow-up Records
- 9.1.4 GRS 24-08-C - Information Technology Operation and Management Records – IT Operations Records

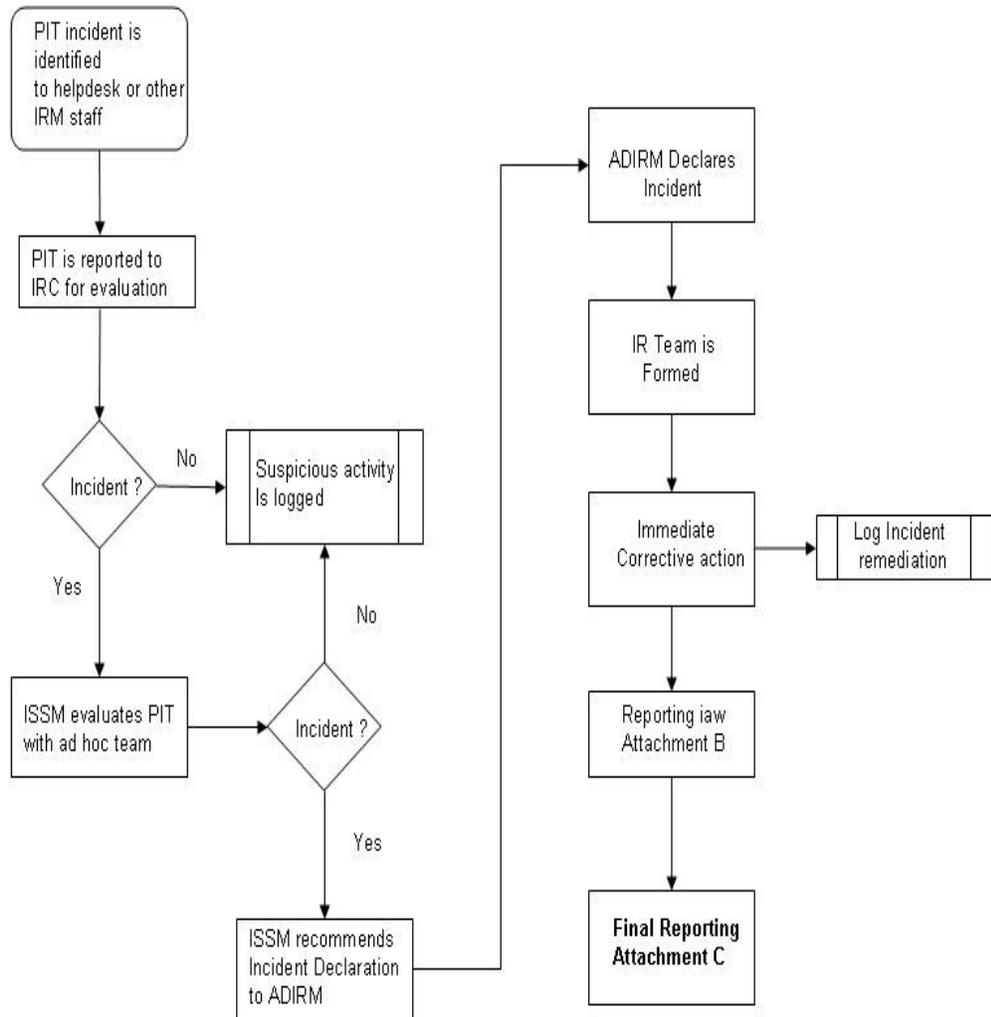
10.0 FORMS USED - None

11.0 ATTACHMENTS

- 11.1 Attachment A - Sample IM Maintenance Log Sheet
- 11.2 Attachment B – Supplemental Instructions for Incident Categorization and Initial Reporting
- 11.3 Attachment C – Supplemental Guidance for Reporting of Incidents

12.0 FLOWCHART

### Incident Response Flow Chart IP-240-04



Attachment A

**EMCBC MAINTENANCE LOG**

**Add New**

Control Point	System Name	Action	Date	Co Ch:
Logs	PIT	Unusual Traffic Alert - Dan Bright reported seeing	2006-11-03	No
Logs	COOP	HVAC Break down - Based on the break down of HVAC	2006-10-27	No
Logs	CBCFS1	Gave Betsy Volk special permissions to the sb07 to	2006-10-27	No
Network	CBCSQL	Changed the IP address that is allowed to authenti	2006-10-18	Yes
Audit	Active	Reviewed active dir accounts 10/2006 disabled G G	2006-10-17	No
Audit	Desktop	Verified that the vml exploitation would not affec	2006-10-05	No
Network	CBCCORE1 & CBCCORE2	Change route to include a route to HQ DNS.	2006-07-17	Yes
Server	CBCINTRANET	Changed in PHP.ini SMTP=localhost to SMTP=cbcech1	2006-06-29	Yes
Server	CBCMG1	Upgrade Spherical to 4.0.2.13 and install patch s	2006-06-19	Yes
Server	CBCSQL	Admin ToolPack from Microsoft downloaded and instal	2006-06-16	Yes
Logs	CBCSQL	1st SMS Package Released and Successfully Pushed t	2006-06-14	No
Server	CBCSQL	SMS Toolkit for SP2	2006-06-14	No
Server	CBCSQL	SMS to D.: instant update of SP2	2006-06-14	No
Server	CBCBES	Uninstalled SMS 2003 SP1 and SP2	2006-06-14	No
Server	CBCBES	COM + Reinstalled (Corrupted) --- IIS Services	2006-06-14	No
Server	CBCINTRANET	Completed Add. Update on local --> Transfer to CBC	2006-06-08	No

**Attachment B****Supplemental Instructions for Incident Categorization and Initial Reporting**

Incidents are to be evaluated by type and category. This overall categorization will determine the reporting requirements of the incident in accordance with the table at the end of this attachment.

**Incident Types:**

**Type 1** Incidents are successful incidents that potentially create serious breaches of DOE cyber security or have the potential to generate negative media interest. The following are defined as Type 1 Incidents, and shall be reported.

(a) **System Compromise/Intrusion** - All unintentional or intentional instances of system compromise or intrusion by unauthorized persons, including user-level compromises, root (administrator) compromises, and instances in which users exceed privilege levels.

(b) **Loss, Theft, or Missing** - All instances of the loss of, theft of, or missing laptop computers; and all instances of the loss of, theft of, or missing information technology resources, including media that contained Sensitive Unclassified Information (SUI) or national security information.

(c) **Web Site Defacement** - All instances of a defaced Web site.

(d) **Malicious Code** - All instances of successful infection or persistent attempts at infection by malicious code, such as viruses, Trojan horses, or worms.

(e) **Denial of Service** - Intentional or unintentional denial of service (successful or persistent attempts) that affects or threatens to affect a critical service or denies access to all or one or more large portions of a network. Critical services are determined through Business Impact Analyses in the Contingency Planning process.

(f) **Critical Infrastructure Protection (CIP)** - Any activity that adversely affects an asset identified as critical infrastructure. CIP assets are identified through the Contingency Planning process. At this time EMCBC does not have any assets identified as critical infrastructure

(g) **Unauthorized Use** - Any activity that adversely affects an information system's normal, baseline performance and/or is not recognized as being related to Senior DOE Management mission is to be reported. Unauthorized use includes, but is not limited to, port scanning that excessively degrades performance; IP (Internet protocol) spoofing; network reconnaissance; monitoring; hacking into DOE servers and other non-DOE servers; running traffic-generating applications that generate unnecessary network broadcast storms or drive large amounts of traffic to DOE computers; or using illegal (or misusing copyrighted) software images, applications, data, and music. Unauthorized use can involve using DOE systems to break the law.

(h) Information Compromise - Any unauthorized disclosure of information that is released from control to entities that do not require the information to accomplish an official Government function such as may occur due to inadequate clearing, purging, or destruction of media and related equipment or transmitting information to an unauthorized entity or transmitting information over a network not authorized for the information (e.g., classified on an unclassified network, SUI over the Internet, etc).

Type 2 Incidents are attempted incidents that pose potential long-term threats to DOE cyber security interests or that may degrade the overall effectiveness of the Department's cyber security posture. The following are the currently defined Type 2 incidents.

(a) Attempted Intrusion - A significant and/or persistent attempted intrusion is an exploit that stands out above the daily activity or noise level and would result in unauthorized access (compromise) if the system were not protected.

(b) Reconnaissance Activity - Persistent surveillance and resource mapping probes and scans are those that stand out above the daily activity or noise level and represent activity that is designed to collect information about vulnerabilities in a network and to map network resources and available services. The Senior DOE Management PCSP (Program Cyber Security Plan) must document the parameters for collecting and reporting data on surveillance probes and scans.

Incident Categories: Incident Categories characterize the potential impact of incidents that compromise DOE information and information systems. Such incidents may impact national security, DOE operations, assets, individuals, mission, or reputation. Incident categories identify the level of sensitivity and criticality of information and information systems by assessing the impact of the loss of confidentiality, integrity, and availability. Each of the security objectives—confidentiality, integrity, and availability—is assessed in the following manner.

- (1) Low Incident Category - Loss of system confidentiality, integrity, or availability could be expected to cause little or no damage to national security or have a limited adverse effect on DOE operations, assets, or individuals, including loss of secondary mission capability, requiring minor corrective actions or repairs.
- (2) Moderate Incident Category - Loss of system confidentiality, integrity, or availability could be expected to cause serious damage to national security or have a serious adverse effect on DOE operations, assets, or individuals, including significant degradation, non-life threatening bodily harm, loss of privacy, or major damage, requiring extensive corrective actions or repairs.
- (3) High Incident Category - Loss of system confidentiality, integrity, or availability could be expected to cause serious effect to national security or have a severe or catastrophic adverse effect on DOE operations, assets, or individuals. The incident could pose a threat to human life, cause the loss of mission capability, or result in the loss of major assets.

(4) Very High Incident Category - Loss of system confidentiality, integrity, or availability could be expected to cause grave damage to national security.

Complete incident reports in a timely manner, and maintain all records. Incident management processes and procedures are included in Contingency Plan testing and integrated with PII incident reporting, Information Condition (INFOCON) processes and procedures, and each information system Contingency Plan.

- a. When a cyber-security incident has occurred or is suspected to have occurred (potential incident), the affected site will immediately examine and document the pertinent facts and circumstances surrounding the event.
- b. The initial investigation of an event is completed within 24 hours. If the initial investigation of a potential incident cannot be completed within 24 hours, an initial report must be made as soon as possible but no later than 2 hours from the end of the 24-hour time period.
- c. Once it is determined that an incident has occurred, the incident must be categorized according to Incident Type and Incident Category, analyzed for impact to Senior DOE Management operations, and reported to Computer Incident Advisory Capability (CIAC) within the time frames indicated in Table 1. All reporting timeframes begin at discovery of the potential incident

**Table 1 - Required Time Frame for Reporting Cyber Security Incidents to the Computer Incident Advisory Capability**

Incident Category					
Incident Type	Low	Moderate	High		Very High
Type 1	Within 4 hours	Within 2 hours	Within 1 hour	PII within 45 minutes	Within 1 hour
Type 2	Within 1 week	Within 48 hours	Within 24 hours		Within 8 hours

## Attachment C

**Supplemental Guidance for Reporting of Incidents**

Due to the nature of incidents not all reports will contain the exact same categories. Within the limitation of the scope of the incident the following list of categories is provided as consideration for generation of incident report. Where areas are not applicable to the report they need not be included, but all areas are as follows:

- a. Name of organization;
- b. Contact information for the incident;
- c. Physical location of affected computer/network;
- d. Date incident occurred;
- e. Time incident occurred;
- f. Which critical infrastructure was affected, if any;
- g. Type of incident (e.g., intrusion, denial of service, Web site defacement);
- h. Internet protocol (IP) address and domain name of affected system(s);
- i. IP address and domain name of apparent attacker(s);
- j. Operating system of affected host(s);
- k. Functions of affected host(s);
- l. Number of hosts affected;
- m. Suspected method of intrusion/attack;
- n. Suspected perpetrators and/or possible motivations;
- o. Evidence of spoofing;
- p. Application software affected;
- q. What security infrastructure was in place;
- r. Whether the intrusion resulted in loss of sensitive information;
- s. Whether the intrusion damaged the system(s);
- t. What actions have been taken;

- u. With whom the information can be shared (e.g., National Infrastructure Protection Center, National Security Incident Response Center);
- v. Whether any other agency has been informed, and if so, what its contact information is;
- w. Last time the system(s) was modified or up; and
- y. Assessment of the impact of the incident.

All written final reports will be signed by the Incident Response Team Leader, the Designated Approving Authority (DAA) Representative and the (DAA).

**EMCBC RECORD OF REVISION****DOCUMENT - Cyber Security – Incident Response**

If there are changes to the controlled document, the revision number increases by one. Indicate changes by one of the following:

- 1 Placing a vertical black line in the margin adjacent to sentence or paragraph that was revised.
- 1 Placing the words GENERAL REVISION at the beginning of the text.

---

<b>Rev. No.</b>	<b>Description of Changes</b>	<b>Revision on Pages</b>	<b>Date</b>
1	Original Procedure	Entire Document	1/29/07
2	Added reference	1	6/16/08
2	Added 1 definition	1	6/16/08
2	Add Incident Response Coordinator Role. Added sections 8.1.1.1 and 8.1.1.2 to clarify logging responsibilities	2	6/16/08
2	Broke out sections 8.1.2.1 – 8.1.2.3 for clarity. Assigned ISSM responsibility of assembling team	3	6/16/08
2	Added sentence to 8.2.1 to require logging actions, changed “will” to “shall” in section 8.2	3	6/16/08
2	Added references to Attachment B and C and added as these attachments	3,4,5,6,7,8, 9,	6/16/08
Periodic Rev.	Accomplished with no changes.	All	6/10/10