

Date 04/14/16



## Environmental Management Consolidated Business Center (EMCBC)

### Subject: Cyber Security – Incident Response

Information Management Procedure APPROVED: Signature on File  
OIRM Director

ISSUED BY: Office of Information Resource Management (OIRM)

---

#### 1.0 PURPOSE

The purpose of this procedure is to identify the process to be followed when an Incident or Potential Incident (PIT) is identified by users or administrators. This includes, but is not limited to, incident detection, incident handling activities, training, and incorporating lessons learned into incident response procedures.

#### 2.0 SCOPE

This procedure addresses all unusual events that occur in the Environmental Management Consolidated Business Center (EMCBC) systems and encompasses all EMCBC Accreditation Boundaries.

#### 3.0 APPLICABILITY

This procedure is applicable to all EMCBC operations and all Serviced Sites within the EMCBC Extended Network.

#### 4.0 REQUIREMENTS AND REFERENCES (all documents are the most recent version unless otherwise stated)

- 4.1 DOE O 205.1B, Department of Energy Cyber Security Program
- 4.2 EM Risk Management Approach Implementation Plan (RMAIP)
- 4.3 EMCBC Plan PP-IRM-240-08, Cyber Security – System Security Plan for General Support System
  - 4.3.1 AC-1, Access Control Policy and Procedures
  - 4.3.2 AC-17, Remote Access
  - 4.3.3 AU-1, Audit and Accountability Policy and Procedures
  - 4.3.4 AU-5, Response to Audit Processing Failures
  - 4.3.5 AU-11, Audit Record Retention
  - 4.3.6 AU-12, Audit Generation
  - 4.3.7 CM-1, Configuration Management Policy and Procedures
  - 4.3.8 CM-8, Information System Component Inventory
  - 4.3.9 CP-1, Contingency Planning Policy and Procedures
  - 4.3.10 CP-2, Contingency Plan

- 4.3.11 IR-1, Incident Response Policy and Procedures
- 4.3.12 IR-2, Incident Response Training
- 4.3.13 IR-3, Incident Response Testing and Exercises
- 4.3.14 IR-4, Incident Handling
- 4.3.15 IR-5, Incident Monitoring
- 4.3.16 IR-6, Incident Reporting
- 4.3.17 IR-7, Incident Response Assistance
- 4.3.18 IR-8, Incident Response Plan
- 4.3.19 PE-6, Monitoring Physical Access
- 4.3.20 PL-2, System Security Plan
- 4.3.21 SI-1, System and Information Integrity Policy and Procedures
- 4.3.22 SI-2, Flaw Remediation

## 5.0 DEFINITIONS

- 5.1 Controlled Unclassified Information (CUI) – Unclassified information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 522).

## 6.0 ROLES AND RESPONSIBILITIES

- 6.1 Assistant Director, Office of Information Resource Management (ADIRM): Appoints the Incident Response Team (IRT) leader and the Incident Response Coordinator (IRC); declares an event as an incident and initiates and approves final reports.
- 6.2 Authorizing Official: The Federal official with the authority to formally assume responsibility for operating a system at an acceptable level of risk. This term is synonymous with designated accrediting authority and delegated accrediting authority.
- 6.3 Cognizant Assistant Director: The EMCBC Office Director of the specific department that is responsible for content for a given application. The Cognizant Assistant Director or designee is also the Content Owner of the given application.
- 6.4 Content Owner: The Cognizant Assistant Director or designee responsible for the content within the given application or system.
- 6.5 Content Manager: Individual assigned by the Content Owner to manage the development of applications and to ensure data integrity.
- 6.6 Incident Response Coordinator: Conducts incident response training and the initial evaluation of the PIT. Participates on IRT as requested.
- 6.7 Incident Response Team (IRT) Leader: Leads the evaluations of PITs and recommends declaration of an incident to the ADIRM. Initiates reporting of an incident and conducts incident response training.
- 6.8 Incident Response Team (IRT) Members: Responds to incidents, as required, and attends incident response training.

6.9 Information System Security Manager (ISSM): Manages security during the incident response process.

6.10 Information System Security Officer (ISSO): Ensures security during the incident response process.

## 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 - Network Administrators, IT support personnel and the general user community shall report any unusual activity or potential unauthorized activities that may not be consistent with information technology (IT) operations to the IRC. The general user community may not be aware of who the IRC is, so it is incumbent upon the Information Resource Management (IRM) staff to ensure that any issues are directed to the team. The IRC will evaluate the PIT and elevate it to the ISSM for further evaluation or log the event as a suspicious activity in the Project Management System or its successor.

8.1.1.1 Events that are considered “curious” but do not indicate any malicious activity are logged in the Project Management System at the IRC’s discretion.

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

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 an incident, and the team will recommend to the ADIRM to declare an incident. The ADIRM will appoint an IRT Leader and the issue will be addressed in accordance with Section 8.2 of this procedure.

8.1.2.2 It may be deemed to be a suspicious activity, but not a clear incident. In this case, it will be logged in the Project Management System to document the suspicious activity so that the information will be available for future reference.

8.1.2.3 It 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 in the Project Management System for documentation.

8.1.3 The ADIRM is responsible for reviewing the recommendation of the ISSM and will make the Declaration of an Incident and appoint IRT members as appropriate. The ADIRM will also notify the Authorizing Official (AO) and potentially the Content Owners or Content Managers of the affected system of the declaration of an incident. In the event the ADIRM is not available, the ISSM is authorized to act on behalf of the ADIRM.

## 8.2 Incident Handling

8.2.1 Once an incident has been declared, the IRT shall begin corrective actions. Each action will be logged in the Project Management System 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 were any obvious breaches or serious damage to databases or file systems.

8.2.1.3 The IRT Leader shall then initiate an incident notification of the incident to the Joint Cybersecurity Coordination Center (JC3) and to Environmental Management 72 (EM-72) in accordance with the time frames and guidance from DOE O 205.1B, Department of Energy Cyber Security Program, and Attachment A. The report shall specify the Type and Impact Classification of the incident. EM-72 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 IRT shall conduct analysis and 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 Project Management System.

8.2.1.5 Once the affected system(s) has been restarted, the ADIRM shall initiate review of a 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 A. A final report shall be generated in accordance with the guidance of Attachment B.

8.3 Incident Response Team – The IRT shall consist of a cross section of individuals from IRM, the Office of Technical Support and Asset Management (OTSAM) and the EM Headquarters (HQ) Mission Information Protection Program (MIPP) 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 shall be logged in the Project Management System with each incident.

8.3.1 The IRT consists of:

8.3.1.1 Team Leader – Appointed by the ADIRM

8.3.1.2 EMCBC Security Officer – OTSAM

8.3.1.3 Cognizant Network Administrators or Application Developers

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

8.3.1.5 Member at Large – Appointed by the ADIRM

8.3.2 IRM Training

8.3.2.1 The ADIRM shall ensure that incident awareness and reporting is addressed in user training.

8.3.2.2 The IRC 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 simulated scenarios as applicable. The training date, subject, and participants shall be documented and logged in the Project Management System.

## 9.0 RECORDS MAINTENANCE

9.1 DAA-GRS-2013-0006-0002 – Computer Security Incident Handling, Reporting and Follow-up Records (GRS 3.2)

## 10.0 FORMS USED - None

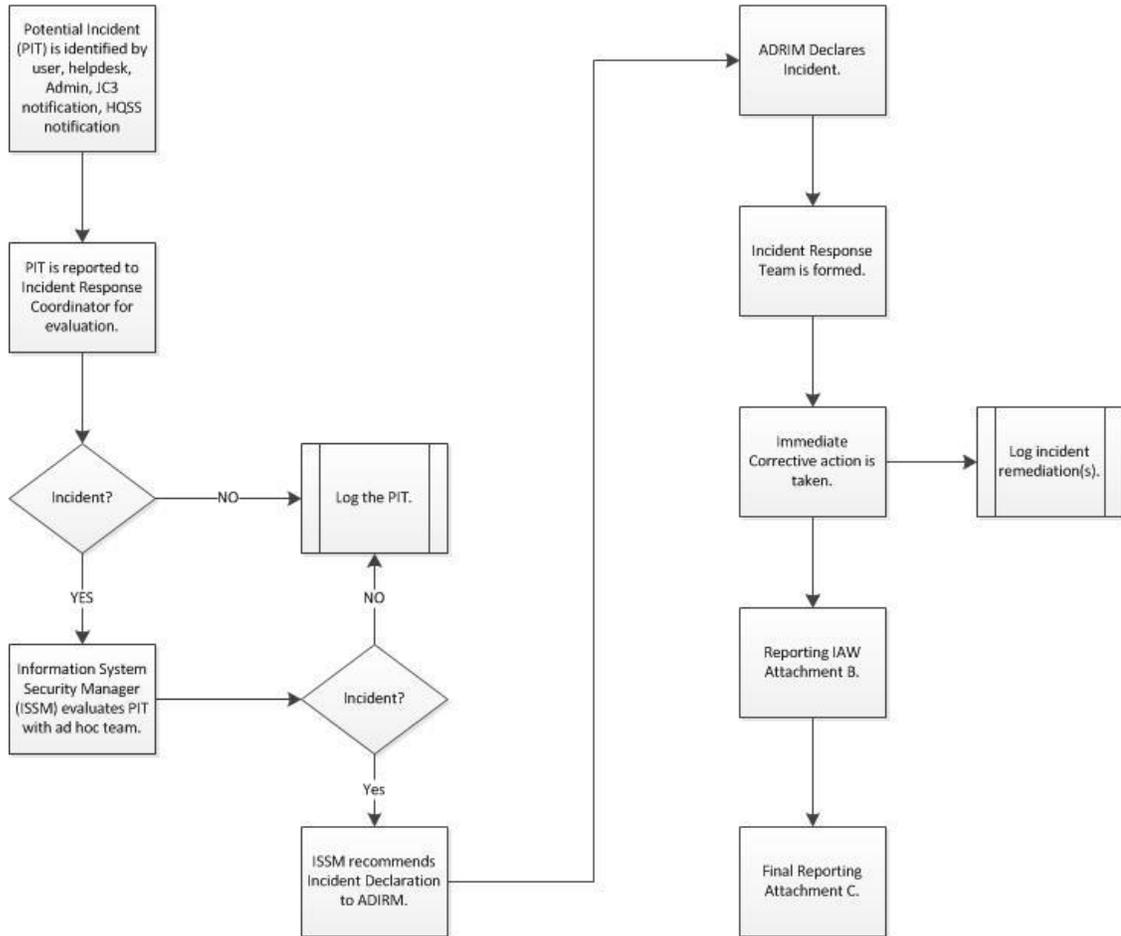
## 11.0 ATTACHMENTS

11.1 Attachment A – Supplemental Instructions for Incident Categorization and Initial Reporting

11.2 Attachment B – Supplemental Guidance for Reporting of Incidents

13.0 FLOWCHART

Incident Response Flow Chart IMP-IRM-8308-04



## Attachment A Supplemental Instructions for Incident Categorization and Initial Reporting

Incidents are to be evaluated by Type and Impact Classification.

### INCIDENT TYPES

- **Malicious Code:** All instances of successful infection or persistent attempts at infection by malicious code, such as viruses, Trojan horses, or worms, must be reported.
- **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 IT resources, including media that contained Sensitive Unclassified Information (SUI) or national security information.
- **PII:** Personally Identifiable Information (PII) is any information collected or maintained by the Department about an individual, including but not limited to, education, financial transactions, medical history and criminal or employment history, and information that can be used to distinguish or trace an individual's identity, such as his/her name, Social Security number, date and place of birth, mother's maiden name, biometric data, and including any other personal information that is linked or linkable to a specific individual.
- **Phishing:** The attempt to acquire sensitive information such as usernames, passwords, and credit card details (and sometimes, indirectly, money), often for malicious reasons, by masquerading as a trustworthy entity in an electronic communication.
- **Attempted Intrusion:** A significant and/or persistent attempted intrusion is an exploit that stands out above the daily activity or noise level, as determined by the system owner, and would result in unauthorized access (compromise) if the system were not protected.
- **Classified Spillage:** Transfer of classified or sensitive information to unaccredited or unauthorized systems, individual's applications, or media. Spillage may result from improper handling of compartments, releasability controls, privacy data, or proprietary information.
- **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 must be reported. Critical services are determined through Business Impact Analyses in the Contingency Planning process.
- **Unauthorized Use:** Any activity that adversely affects an information systems 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.

## IMPACT CLASSIFICATION

Impact Classification characterizes 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. Impact Classification identifies 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—are assessed in the following manner:

### **Functional Impact:**

- **HIGH** - Organization has lost the ability to provide all critical services to all system users.
- **MEDIUM** - Organization has lost the ability to provide a critical service to a subset of system users.
- **LOW** - Organization has experienced a loss of efficiency, but can still provide all critical services to all users with minimal effect on performance.
- **NONE** - Organization has experienced no loss in ability to provide all services users.

### **Information Impact:**

- **CLASSIFIED** -The confidentiality of classified information was compromised.
- **PROPRIETARY** - The confidentiality of unclassified proprietary information, such as protected critical infrastructure information (PCII), intellectual property, or trade secrets was compromised.
- **PRIVACY** - The confidentiality of personally identifiable information (PII) or personal health information (PHI) was compromised.
- **INTEGRITY** - The necessary integrity of information was modified without authorization.

### **Recoverability:**

- **REGULAR** - Time to recovery is predictable with existing resources.
- **SUPPLEMENTED** - Time to recovery is predictable with additional resources.
- **EXTENDED** - Time to recovery is unpredictable; additional resources and outside help are needed.
- **NOT RECOVERABLE** - Recovery from the incident is not possible (e.g., sensitive data infiltrated and posted publicly).
- **NOT APPLICABLE** - Incident does not require recovery.
- **NONE** - No information was exfiltrated, modified, deleted, or otherwise compromised.

## INCIDENT NOTIFICATION

Complete incident notification in a timely manner, and maintain all records. Incident management processes and procedures are included in Contingency Plan testing and integrated with Personally Identifiable Information (PII) incident reporting, Information

Condition (INFOCON) processes and procedures, and each information system Contingency Plan.

- (1) 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.
- (2) 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 notification must be made as soon as possible but no later than one hour from the end of the 24-hour time period.
- (3) Once it is determined that an incident has occurred, the incident must be categorized according to Type and Impact Classification, analyzed for impact to Senior DOE Management operations, and reported to the Joint Cybersecurity Coordination Center (JC3) within one hour.

Email notifications of the incident will be sent, using Encryption software, to the following:

Assistant Director of Information Resource Management (ADIRM)	Ward Best	513-246-0530	ward.best@emcbc.doe.gov
Information System Security Manager (ISSM)	John Muskoff	513-2460226	john.muskoff@emcbc.doe.gov
Information Systems Security Officer (ISSO)	Lisa Rawls	513-246-0059	lisa.rawls@emcbc.doe.gov
Incident Response Coordinator (IRC)	Lisa Rawls	513-246-0059	lisa.rawls@emcbc.doe.gov
Headquarters Security System (HQSS)	Dan Bright	202-586-0718	daniel.bright@em.doe.gov

## Attachment B Supplemental Guidance for Incident Notification

### Incident Reporting Procedures:

Due to the nature of incidents, not all notifications will contain the exact same information. Within the limitation of the scope of the incident, the following information is requested by JC3 through the online incident notification form available at <https://tickets.jc3.doe.gov>. Not all areas are applicable, so they may not need to be completed, but all areas are as follows (required fields are indicated by an asterisk-\*):

#### \*Scenario:

- Reporting Office
  - \*Program Office: EM
  - \*Site name: Environmental Management – Consolidated Business Center
  - \*Reporter First Name: The first name of the individual reporting the incident
  - \*Reporter Last Name: The last name of the individual reporting the incident
  - \*Phone Number: The phone number of the individual reporting the incident
  - \*Email Address: The email address of the individual reporting the incident
  - \*State: The state the incident occurred.
- Incident Detail
  - Internal Tracking Number
  - \*Incident Type
  - Date incident occurred
  - Time Incident occurred
  - Date incident detected
  - Time Incident detected
  - Time zone of incident
  - Impacted User First name
  - Impacted User Last Name
  - Impacted user phone number
  - Impacted user email address
  - Related to existing JC3 ticket: Yes/No
    - Yes requires more information: Details of the existing

(Additional information [e.g., Impact, Recoverability/Mitigation, Technical and Resolution] may be required by the online JC3 form.)

Incidents Requiring Immediate Attention:

For priority handling, contact the JC3 Call Center at 866-941-2472 where an analyst is available 24 hours a day, year-round. Please restrict after-hours calls to emergencies only.

Incidents Involving Classified Computer Systems:

If the incident involves a classified system, call the JC3 Hotline at 866-941-2472 and request a callback on the JC3's STU (Secure Telephone Unit). If you are not near a STU, call the JC3 Hotline with a STU number and a time to return your call. Please note this does not apply to incidents that involve "leaking" of classified material onto an unclassified system.

Incident Report Content:

When reporting cyber-related incidents to JC3, provide detailed information including, but not limited to:

- How the incident occurred
- What occurred
- Impact
- Preventive measures implemented

**EMCBC RECORD OF REVISION**

Document Title: CYBER SECURITY – INCIDENT RESPONSE

If there are changes to the controlled document before the two-year review cycle, the revision number stays the same; one of the following will indicate the change:

**I** Placing a vertical black line in the margin adjacent to sentence or paragraph that was revised, or

**I** Placing the words GENERAL REVISION at the beginning of the text. This statement is used when entire sections of the document are reviewed.

If changes and updates occur at the two-year review cycle, the revision number increases by one.

---

<b>Rev. No.</b>	<b>Description of Changes</b>	<b>Revision on Pages</b>	<b>Date</b>
0	Original Information Management Procedure; supersedes IP-240-04	Entire Document	4/14/16