

Ames Laboratory		Plan	48400.005
Office	Information Systems	Revision	1
Title	Cyber Incident Response Plan	Effective Date	12/1/2012
Page	2 of 12	Review Date	12/1/2015

1.0 Revision/Review Log

This document will be reviewed once every 2 years as a minimum.

<u>Revision Number</u>	<u>Effective Date</u>	<u>Contact Person</u>	<u>Pages Affected</u>	<u>Description of Revision</u>
0	10/1/2009	William Sears	All	Initial Version
1	8/1/2011	William Sears	All	Staff revision and evidence retention added
2	12/1/2012	William Sears	All	Staff revision and added Section 5.

2.0 Purpose and Scope

This Ames Laboratory Cyber-Incident Response Plan describes the policies and processes used to perform cyber-incident response and apply DOE M 205.1-8 as its foundation. The purpose of this plan is to establish a protocol for the Ames Laboratory Cyber Incident Response Team to follow when responding to a cyber based incident.

3.0 Responsibility

ACSM: Assistant Cyber Security Manager
Named Specifically by Program

ALCIRT: Ames Laboratory Cyber Incident Response Team

Diane Denadel
Nathan Humeston
William Sears
Chris Strasburg
Aaron Mills
Klarida Cubacub

CSM: Cyber Security Manager
William Sears

CSA: Cyber Security Analysts
Chris Strasburg
Aaron Mills
Klarida Cubacub

CST: Cyber Security Team
Diane Denadel
William Sears

Ames Laboratory		Plan	48400.005
Office	Information Systems	Revision	1
Title	Cyber Incident Response Plan	Effective Date	12/1/2012
Page	3 of 12	Review Date	12/1/2015

Chris Strasburg
Aaron Mills
Klarida Cubacub

AO: Approving Official
Cynthia Baebler

ESH&A: Environment, Safety, Health, and Assurance (Key Contacts)
Jeff Bartine
Shawn Nelson

4.0 Performance

Definitions:

- Incident Types
 - Type 1 incidents are successful incidents that potentially create serious breaches of DOE (Department of Energy) cyber security. The following are defined as Type 1 incidents:
 - **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. Ames requires that drives of affected systems be acquired, imaged, and stored for a period of 1 year.
 - **Loss, Theft, or Missing.** All instances of the loss of, theft of, or missing information technology resources, including media that contains SUI (Sensitive Unclassified Information), PII (Personally Identifiable Information) or national security information.
 - **Web Site Defacement.** All instances of a defaced Web site. Ames requires that drives of affected systems be acquired, imaged, and restored to pre-defacement state.
 - **Malicious Code.** All instances of successful infection or persistent attempts at infection by malicious code, such as viruses, Trojan horses, or worms. Ames requires that drives of affected systems be acquired, imaged, and wiped, then returned back to the system administrator.
 - **Denial of Service (DoS).** 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. No system evidence is acquired.
 - **Critical Infrastructure Protection (CIP).** Any unplanned activity that adversely affects an asset identified as critical infrastructure. Ames requires that drives of affected systems be acquired, imaged, and stored for a period of 1 year.
 - **Unauthorized Use.** Any activity that adversely affects an information system's normal, baseline performance and/or is not recognized as being

- **High Incident Category.** Loss of system confidentiality, integrity, or availability could be expected to cause catastrophic effect to national security or have a severe or catastrophic adverse effect on DOE operations, assets, or individuals or on assets and information under DOE purview. The incident could pose a threat to human life, cause the loss of mission capability, or result in the loss of major assets. All drives from affected system will be kept for 1 year.
 - **Very High Incident Category.** Loss of system confidentiality, integrity, or availability could be expected to cause grave damage to national security. All drives from affected system will be kept for 1 year.
 - Incidents involving PII are categorized either moderate or high depending on the severity of the breach. All drives from affected system will be kept for 1 year.
- **Data/Image Retention**

INCIDENT TYPE	INCIDENT CATEGORY			
	LOW	MODERATE	HIGH	VERY HIGH
Type 1	Up to 1 year	At least 1 year		
Type 2	No Retention			

Reporting:

- Records for incidents and potential incidents are maintained and archived.
 - **DOE-CIRC (Department of Energy Cyber Incident Response Center) Reports**
 - Non-urgent incidents. Send e-mail describing the cyber security incident to doecirc@doecirc.energy.gov. Alternatively, call the hotline at 866-941-2472, or fax information to 702-932-0189.
 - Incidents requiring immediate attention. If the cyber security incident requires priority handling, use the phrase "URGENT" in the e-mail subject line and an analyst will contact you. You can also call the hotline at 866-941-2472, where an analyst will man the phone 24x7x365. Please restrict the non-business hours use of the incident hotline to only emergency situations.
 - Sensitive Information. Information about unclassified cyber security incidents of a sensitive nature should be sent protected with encrypted e-mail. To facilitate this process, supply CIRC with your public encryption key, either Entrust or PGP. Contact CIRC for guidance on how to transmit information securely if encrypted means are not available.
 - Automated scan detection and reporting. Some sites are utilizing automated methods for both detecting and reporting scans and probes.

This provides CIRC with valuable data without undue burden on the site. If you are interested in using an automated tool, send e-mail to doecirc@doecirc.energy.gov;

- Incidents involving classified computer systems. If the cyber security incident involves a classified system, call the CIRC Hotline 866-941-2472 and request a callback on the CIRC's STU (Secure Telephone Unit). If you are not near a STU, call the CIRC Hotline with a STU number and a time to return your call. Please note these are not incidents that involve the "leaking" of classified material onto an unclassified system.

○ **Negative Reporting**

- To indicate there have been no incidents for a given month at your site, please send an e-mail to doecirce@doecirc.energy.gov. The e-mail should contain the following:
 - In the Subject line, please type: "CIRC NEGATIVE REPORT"
 - In the body of the message, please type the following (including the sentence "No incidents to report"):
 - Your Name = *your name* (Example: John Doe)
 - Job Title(s) - Optional = *your title(s)* (Example: ISSM, Network Security Lead)
 - Site = AMES
 - Reporting Month = *the 3-letter abbreviation for the month you are reporting* (Example: MAR)

○ **Reporting Schedule**

INCIDENT TYPE	INCIDENT CATEGORY				
	LOW	MODERATE	HIGH		VERY HIGH
Suspected/Potential Type 1	4 hours	2 Hours	1 Hour	PII - 45 Minutes	1 Hour
Type 2/Confirmed Type 1	1 Week	48 hours	48 Hours		8 Hours

4.1 Contacts with other Entities

Ames Laboratory		Plan	48400.005
Office	Information Systems	Revision	1
Title	Cyber Incident Response Plan	Effective Date	12/1/2012
Page	7 of 12	Review Date	12/1/2015

All contact with the media is handled through Public Affairs as directed by the COO. All contact attempts made by the media are to be referred to Public Affairs.

All contact made with Ames Laboratory Entities other than Information Systems will be directed through the COO. Specifically, this includes personnel issues with Human Resources and media relations with Public Affairs.

5.0 Significant Cyber Security Incident

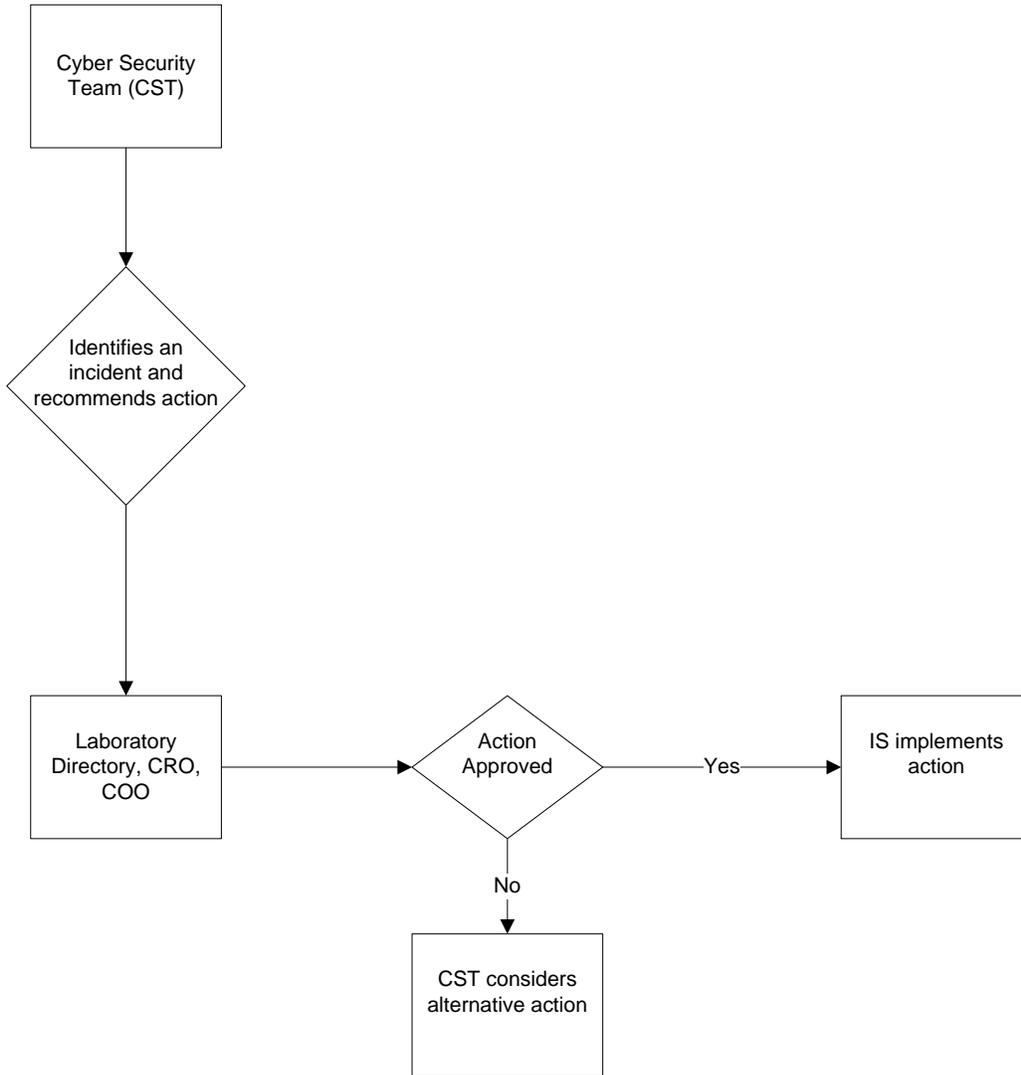
A significant cyber security event is a set of conditions that require increased coordination by the Cyber Security Team (CST) to reduce threat, vulnerability and potential consequences of observed activity. A significant incident will be reported following the guidance in this document.

5.1 Scenarios That May Require Escalation.

A significant incident could include, and is not limited to, the following events:

- Essential infrastructure compromised including:
 - DNS or DHCP.
 - Core networking components.
 - Central authentication systems.
 - Central IT management systems.
 - Cyber Security systems.
 - Key business systems.
- Lack of understanding of the attack and scope.
- Ten computers compromised/possible compromised.
- Widespread or targeted exfiltration.
- Potential to preemptively avoid damage.
- Successful large Advanced Persistent Threat.
 - Increased by simultaneous attacks against multiple DOE sites.
- Significant Public Relations risk (outbound DOS or web defacement).

5.2 Escalation Process.



6.0 Additional Information



U.S. Department of Energy
 Office of the Chief Information Officer
 Office of Cyber Security
 DOE-JC3 Cyber Security Incident Report

Contact Information	
Site Name:	For Call Center use only: DOE-JC3 Ticket #: OTHER Ticket #: US-CERT Ticket #:
Contact name:	Program Office Name (NNSA, SC, EM, etc.):
Phone #:	Email address:
Incident Information	
Date incident occurred:	Date incident discovered:
Time incident occurred:	Time incident discovered:
Type 1 Incident: System Compromise/Intrusion <input type="checkbox"/> Root Compromise <input type="checkbox"/> User Compromise Loss, Theft, or Missing <input type="checkbox"/> Desktop <input type="checkbox"/> Laptop <input type="checkbox"/> Media <input type="checkbox"/> Other (please specify) Malicious Code <input type="checkbox"/> Trojan <input type="checkbox"/> Virus <input type="checkbox"/> Worm <input type="checkbox"/> Other (please specify)	Type 2 Incident: <input type="checkbox"/> Web Site Defacement <input type="checkbox"/> Denial of Service <input type="checkbox"/> Critical Infrastructure Protection <input type="checkbox"/> Unauthorized Use <input type="checkbox"/> Information Compromise <input type="checkbox"/> Attempted Intrusion <input type="checkbox"/> Reconnaissance Activity
IMI Category: <input type="checkbox"/> IMI1- <input type="checkbox"/> IMI2- <input type="checkbox"/> IMI3- <input type="checkbox"/> IMI4-	
Information sensitivity: <input type="checkbox"/> OOU <input type="checkbox"/> PII <input type="checkbox"/> SUI <input type="checkbox"/> UCNI <input type="checkbox"/> Other (please specify)	Security Category: <input type="checkbox"/> Low Security Category: <i>limited</i> adverse affect <input type="checkbox"/> Moderate Security Category: <i>serious</i> adverse affect <input type="checkbox"/> High Security Category: <i>severe</i> or <i>catastrophic</i> adverse affect
# Machines affected:	Which critical infrastructure was affected, if any?
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	For PII Incidents: Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	Operating system(s) of affected machine(s):
Description of incident:	
Method of detection:	
IP address(es) of attackers:	Destination Port(s) and Protocol(s):
Domain name(s) of attacker(s):	Country(ies) of attacker(s):
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	Evidence of spoofing:
Impact and Actions Taken	
Assessment of the impact of the incident:	

Ames Laboratory
Office Information Systems
Title Cyber Incident Response Plan
Page 10 of 12

Plan 48400.005
Revision 1
Effective Date 12/1/2012
Review Date 12/1/2015

What actions have been taken:	
Other Information	
Who has been notified?	
<input type="checkbox"/> OIG <input type="checkbox"/> FBI <input type="checkbox"/> CI <input type="checkbox"/> Other Agencies (please specify)	
Report Information (Call Center Use Only)	
Report Date:	Report Time:

DOE-JC3 08.001

7.0 Cyber Incident Response Checklist

Ames Laboratory Cyber Incident Checklist Form# 48400.020

Incident Data

Name of Affected System: _____

Name(s) of Affected User(s) (If possible): _____

Name Of Affected ACSM/GroupAdmin _____

Name(s) of Cyber Security Staff: _____

Type 1 Incidents

If notified by user or ACSM:

Inform the user:

- System hard drive will be acquired.
- ACSM and Program Director will be notified.
- Cost and Installation of a new hard drive is the responsibility of the program.
- Hard Drive will remain with IS for 1 year.

All incident notifications:

Email and Call the ACSM and Email the Program Director and ESH&A of the possible incident.

- The ACSM (if possible) needs to notify the user that use of their computer needs to cease immediately.
- The ACSM will accompany a person from cyber security to acquire the system's hard drive.
- The ACSM will be responsible for requisitioning a new hard drive for the affected system.

Acquisition Procedure:

The ACSM and Cyber Security staff will go to the location of the affected system.

The ACSM and Cyber Security staff will explain to the affected user (if possible) about the incident and actions that will need to be taken.

- Inform the user that data can be recovered from the drive after the initial investigation is complete (Usually within 24 hours).

- The ACSM or Cyber Security staff will pull the network cable from the system while leaving it on.
- At the discretion of Cyber Security staff, the system will be searched for malware on the spot and/or the system's power will be pulled.
- Cyber Security staff will remove the hard drive for forensic analysis.
- Inform the ACSM that there will be a 24 hour investigative period and that only the ACSM may have limited contact with Cyber Security staff during that time.

Investigation Procedure:

- Load the confiscated [drives][VM images] (one drive if it is mirrored) into forensic software using a FASTBLOC/DRIVELOCK device to prevent writing to the disk.
- Check IDS, Netflow, and Remote Logs for additional evidence.
- Report on any findings on the CRIC Incident Response form and send it to JC3, ACSM, ALCIRT, Program Director, Authorizing Official, ESH&A, and COO.
- Update the internal web page with the incident report.
- If nothing is found, inform the ACSM, Program Director, and ESH&A.
 - Return Hard Drive to ACSM.

Type 2 Incidents

- Inform ACSMs, Group Admins, and ESH&A of the possible incident.
- Check IDS, Netflow, and remote system logs for further information.
- Report on any findings on CIRC Incident Response form and send it to JC3, ACSM, Program Director, Authorizing Official, ESH&A, and COO.
- Update the internal web page with the incident report.
- If nothing is found, inform the ACSM, Program Director, and ESH&A.

Checklist completed by (Print): _____

Checklist completed by (Sign): _____

Checklist Completed (Date): _____