



Agriculture Security Operations Center (ASOC) Computer Incident Response Team (CIRT)

Standard Operating Procedures for Reporting Security and Personally Identifiable Information Incidents

Reference: SOP-ASOC-001

Revision: 1.10

Date: June 9, 2009

*Prepared for:
USDA Office of the Chief Information Officer
Agriculture Security Operations Center
Computer Incident Response Team*

Document Information

This is a controlled document produced by the United States Department of Agriculture (USDA), Office of the Chief Information Officer (OCIO), the ASOC CIRT. The control and release of this document is the responsibility of the ASOC CIRT office document owner.

General Information	
Document Reference	SOP-ASOC-001
Document Title	Security CIRT Standard Operating Procedure

Primary Author	
Name	Kelvin Fairfax
Contact Number	202-720-2362
Email Address	Kelvin.Fairfax@USDA.gov

Revision History			
Revision	Date	Author	Comments
1.0	03/10/2009	H. Beckstrom	USDA OCIO has reorganized. Cyber Security Incident Response is now the USDA, Agriculture Security Operations Center (ASOC), Computer Incident Response Team (CIRT). This SOP is based on the USDA SOP-SCD-001 version 9.0, December 2008.
1.0	03/10/2009	H. Beckstrom	Revise text. Remove all “Cyber Security, CS, and SCD” from text. Insert where appropriate “ASOC, International Security Operations – cyber.” Added a column “Pre-reorganization Title” to Appendix H. Updated Malware and Category chart Priority Listings. Separated the final incident report from the PII incident report. Clarified Checklist Appendix Headings. Revised Section 5.6, from “PII and Lost and Stolen Equipment Events” to “Incidents Reportable to US-CERT.” Added blocks and shuns graph . Modified Appendix B to have “Sections”
1.0	03/23/2009	K Fairfax	Review text and make recommendations
1.0	03/23/2009	H. Beckstrom	Revise test.
1.0	03/24/2009	J. Donohue	Review text
1.0	03/24/2009	K. Fairfax	Review text
1.0	3/25/2009	H. Beckstrom	Change ASOC-c to ASOC; Update Figure 2; Revise the use of the word “escalate”; verify use of full titles and acronyms; review, research, and respond to SOP change requests from Kelvin, Jim, and Steve. Update Events terminology and definitions of events vs. incidents. Take table references out of the appendix. Standardize format of table and figure headings within the body of the text.
1.0	03/30/2009	J. Donohue	Review Text

Revision History			
Revision	Date	Author	Comments
1.0	3/31/2009	H. Beckstrom	Insert J. Donohue's changes, change USDA CIRT to the ASOC CIRT, Grammatical corrections, Delete duplicate definition of incidents and events, Inserted Instant Messaging, categorized topics.
1.0	4/1/2009	V. Hajela	Modify and create decision Trees for Incident Response and Lost and Stolen Equipment.
1.0	4/1/2009	H. Beckstrom	Incorporate new decision trees, update the tables, change the date, submit to IHDD
1.0	4/1/2009	K. Fairfax	Final Review
1.1	5/5/2009	H. Beckstrom	Add (ASOC) (CIRT) to title page, update keylogger section, user name requirement, lost and stolen equipment AD-112 requirement, define IP and system identification, Update escalation process, add definition of PII
1.1	6/1/2009	B. Banks	Added the Keylogger process. Updated the CIRT Notification and Escalation Process.
1.1	6/1/2009	S. Finch	Updated Forms and reports to include user name and job description for repeat offenders.
1.1	6/8/2009	K. Fairfax	Final Edits
1.1	6/09/2009	B. Banks and H. Beckstrom	Post to internet and notify ISSPM

Distribution List			
Name	Title	Agency/Office	Contact Information
Kelvin Fairfax	Incident Handling Division Director (IHDD)	OCIO – USDA ASOC	Kelvin.Fairfax@USDA.gov
Christopher Lowe	Acting Deputy Assistant Computer Information Officer USDA ASOC	OCIO – USDA ASOC	Christopher.lowe@ocio.usda.gov
Christopher L. Smith	Acting CIO for USDA	OCIO – USDA OCIO	ChristopherL.smith@ocio.usda.gov

Table of Contents

DOCUMENT INFORMATION	II
TABLE OF CONTENTS	IV
LIST OF TABLES	VI
LIST OF FIGURES	VI
1 INTRODUCTION.....	1
1.1 Purpose.....	1
1.2 Background.....	1
1.3 Scope.....	1
1.4 Definitions	2
2 ASOC CIRT	2
2.1 ASOC CIRT Description.....	2
2.2 Incident Management Description	3
2.3 ASOC CIRT Goals.....	3
2.4 ASOC CIRT Responsibilities	4
2.5 ASOC CIRT Incident Management	5
2.6 CIRT Position within USDA	6
3 KNOWLEDGE/EXPECTATIONS OF THE ASOC CIRT	7
4 TRANSITIONING AN EVENT TO AN INCIDENT	8
5 CATALOGING INCIDENTS.....	9
6 CIRT NOTIFICATION AND ESCALATION PROCESS	10
7 REPORTING INCIDENTS.....	11
7.1 Sources Reporting Security Incidents	11
7.2 TSO Staff Reported Security Incidents.....	14
7.3 ISSPM Reported Security Incidents.....	14
7.4 NITC SNCC Reported Incidents	16
7.5 Externally Reported Incidents	18
7.6 US-CERT Reporting Requirements.....	18
8 EVENTS AND INCIDENTS.....	21
8.1 Security Events to Be Reported to the ASOC CIRT	21

8.2 Adverse Events22

8.3 Category 6 Incidents22

8.4 Spam or Phishing Events.....22

8.5 Peer to Peer (P2P)23

8.6 Instant Messaging (IM).....23

8.7 Malicious Code/Malware.....23

8.8 Key Loggers/Keystroke Logging24

9 BLOCKS AND SHUNS..... 24

10 CONTAINMENT AND CLOSURE 26

11 THE ASOC CIRT REPORTS TO MANAGEMENT 26

APPENDIX A. REPORT OF SECURITY INCIDENT TO THE ASOC CIRT..... 27

APPENDIX B. USDA INCIDENT REPORT 29

Cyber Incident Report.....29

Section 1: ISSPM Closing.....29

Section 2: The ASOC-CIRT Incident Notification29

Section 3: Contact Information30

Section 4: USER Information31

Section 5: Incident Checklist from Appendix D (SOP-SCD-001).....31

Section 6: Impact and Scope31

Section 7: Lessons Learned32

Section 8: Supporting Information.....32

APPENDIX C. CIRG/PII INCIDENT PACKET 33

APPENDIX D. INCIDENT RESPONSE CHECKLISTS 39

D.1 Initial Incident Response Checklist39

D.2 Generic Incident Response Checklist for Uncategorized Incidents40

D.3 Multiple Component Incident Response Checklist.....41

D.4 Category 1 – Unauthorized Access Incident Response Checklist.....42

D.5 Category 1.2 – Lost and Stolen Equipment Incident Response Checklist44

D.6 Category 2 – Denial of Service Incident Response Checklist.....44

D.7 Category 3 – Malicious Code Incident Response Checklist47

D.8 Category 4 – Inappropriate Usage Incident Response Checklist49

**D.9 Category 5 – Brute Force Attacks, Port Scans, Social Engineering, Probes,
Attempted Access Incident Response Checklist.....51**

D.10 Category 6 – Under Investigation Incident Response Checklist.....53

D.11 24 Hour Incident Containment Checklist.....54

APPENDIX E. PII/SENSITIVE INFORMATION QUESTIONS CHECKLIST 55

APPENDIX F. INCIDENT SEVERITY RATING..... 57

F.1 Current and Projected Effect Ratings.....57

F.2 Criticality Ratings57

F.3 Severity Formula.....57

F.4 Severity/Effect Score.....58

APPENDIX G. NIST SP 800-61, PRIORITIZATION MATRICES..... 59

G.1 Event Prioritization Matrix.....59

G.2 Technical Issue Prioritization Matrix59

G.3 Criminality Prioritization Matrix.....60

APPENDIX H. ACRONYMS & ABBREVIATIONS 61

APPENDIX I. APPROVAL SIGNATURE 63

List of Tables

Table 1: USDA Agency Incident Categories (Defined by US CERT CONOPS and NIST SP 800-61)..... 16

List of Figures

Figure 1: Incident Response Life Cycle, NIST SP 800-613

Figure 2: CIRT Position within USDA6

Figure 3: Process Flow for PII and SBU Incidents12

Figure 4: Process Flow for Non-PII/SBU Security Incidents13

Figure 5: Lost and Stolen Equipment Decision Tree20

1 Introduction

1.1 Purpose

This Standard Operating Procedure (SOP) documents the incident management procedures for the United States Department of Agriculture (USDA), Agriculture Security Operations Center (ASOC), Computer Incident Response Team (CIRT). The ASOC CIRT processes all USDA computer security events, incidents, and personal identifiable information (PII) compromises. The ASOC CIRT is the central point of contact (POC), liaison, and facilitator; and reports and transmits all USDA incidents and events between external entities such as UC-CERT, other Federal Agencies, and Federal Law enforcement entities.

1.2 Background

As global network connectivity becomes more crucial for conducting everyday operations within the USDA, the need for an effective computer security incident handling capability increases. The Office of Management and Budget (OMB) Circular A-130 “Management of Federal Information Resources,” Appendix III “Security of Federal Automated Information Resources” requires Federal agencies to ensure that there is an incident response capability to help users when a security incident occurs, and to share information concerning common vulnerabilities and threats. The Federal Information Security Management Act (FISMA) of 2002 requires Federal agencies to report all computer security and PII incidents to the United States Computer Emergency Readiness Team (US-CERT). The ASOC CIRT uses the US-CERT concept of operations (CONOPS) guide and the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-61, Computer Security Incident Handling Guide, to categorize incidents and determine the appropriate methodology for responding to each security incident.

On September 20, 2006, OMB issued a memorandum to the Heads of Departments and Agencies titled “Recommendations for Identity Theft Related Data Breach Notification.” One of the recommendations was that agencies establish a core incident response group comprised of senior officials responsible for responding to incidents involving PII. In response, the USDA Chief Information Officer (CIO) created the Core Incident Response Group (CIRG). This group addresses all incidents involving sensitive data, identity theft, and PII data. The ASOC CIRT is responsible for escalating incidents to the CIRG (see the “USDA Incident Notification Plan” dated September 2007 at http://www.ocionet.usda.gov/ocio/security/docs/USDA_Incident_Notification_Plan_FINAL.pdf).

1.3 Scope

This SOP establishes the framework that the ASOC CIRT security analyst uses in determining which events should transition to incidents, be referred to the Office of the Inspector General (OIG), referred to the USDA CIRG, and/or sent to US-CERT. This document also outlines procedures for dealing with different types of events and incidents, escalating incidents to senior officials, and facilitating CIRT interactions with other organizations, both internal and external to the Department. This SOP supplements Departmental Manual (DM) 3505-001, *USDA CIRT Incident Handling Procedures*, dated March 20, 2006.

1.4 Definitions

This SOP uses definitions found in NIST SP 800-61, Revision 1, *Computer Security Incident Handling Guide*:

- **Event:** An *event* is any observable occurrence in a system or network. Events include a user connecting to a file share, a server receiving a request for a Web page, a user sending electronic mail (email), and a firewall blocking a connection attempt.
- **Adverse Event:** *Adverse events* are events with a negative consequence, such as system crashes, network packet floods, unauthorized use of system privileges, unauthorized access to sensitive data, and execution of malicious code that destroys data. This guide addresses only adverse events that are computer security-related and excludes adverse events caused by sources such as natural disasters and power failures.
- **Incident:** A *computer security incident* is a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices. Examples of incidents include:
 - Denial of Service (DOS)
 - Malicious Code
 - Unauthorized Access
 - Inappropriate Usage

2 ASOC CIRT

2.1 ASOC CIRT Description

The ASOC CIRT is the central reporting point for all computer security adverse events, PII incidents, and incidents affecting the Department's network infrastructure. The ASOC CIRT will assist the USDA CIRG, the Department's executive incident response group, in taking the appropriate actions necessary to contain, mitigate, and resolve all incidents involving PII. The ASOC CIRT may assist operational managers and, if appropriate, law enforcement in responding to security events. These actions include:

- Securing resources and/or promoting security and privacy data awareness to avoid future events;
- Working with internet technology (IT) users, security officers, system administrators, and managers to respond to computer security events; and
- Acting as the primary conduit for passing information relating to computer security and PII related events and incidents to US-CERT, and OIG for law enforcement actions both within and outside the USDA.

2.2 Incident Management Description

NIST SP 800-61, Revision 1, *Computer Security Incident Handling Guide*, defines the major phases of the incident response life cycle as:

- Preparation
- Detection and Analysis
- Containment, Eradication, and Recovery
- Post-Incident Activity



01282

Figure 1: Incident Response Life Cycle, NIST SP 800-61

The Preparation Phase includes establishing an incident response capability and issuing preventive measures such as patching, scanning, and user training. The Detection and Analysis Phase includes reviewing known threats and establishing normal baseline activity, network and program profiles, and a knowledge base of signs, symptoms, and indications of incidents. The third phase, Containment, Eradication, and Recovery involves implementing contingency containment strategies designed specifically for the type and occurrence of each incident. This third phase also includes evidence handling, attacker identification, and system restoration. Finally, the Post-Incident Phase involves a lessons learned meeting with stakeholders. During this phase, quantitative statistics are produced such as number of incidents handled and average time lapse in response, etc. Information gathering and analysis take place, and procedures and policies are updated. The ASOC CIRT responsibilities within the NIST SP 800-61 and the Incident Response Life Cycle are outlined in this SOP.

2.3 ASOC CIRT Goals

The goals of the ASOC CIRT are to:

- Protect the USDA network infrastructure by coordinating defense against and in response to cyber attacks.
- Guard against misconfiguration of systems.
- Analyze and reduce cyber threats and vulnerabilities.

2.4 ASOC CIRT Responsibilities

The ASOC CIRT works closely with USDA Agencies and Staff Offices, Information System Security Program Managers (ISSPM), system administrators, network administrators, and customers of the USDA networks in order to respond to computer security incidents involving the USDA networks or USDA assets. In cases where the USDA's critical infrastructure is threatened, the ASOC CIRT will advise the USDA management on the necessary actions to prevent the loss of data or resources. The Incident Handling Division Director (IHDD) of the ASOC is responsible for coordinating incident handling within the USDA and, when necessary, briefing senior officials on critical incidents.

The ASOC CIRT responsibilities are to:

- Disseminate cyber threat warning information to USDA Agencies and Staff Offices;
- Coordinate computer security incident response activities;
- Establish and maintain a comprehensive historical database of events and incidents to assist in identifying common attacks, intrusions, attack methods and trends;
- Serve as liaison, when necessary, to provide security expertise to operational offices;
- Assist in restoring normalcy in the event of service disruption because of a security or PII incident;
- Serve as the central point of contact (POC) for reporting all computer security, identity theft, and PII events within USDA;
- Advise USDA Agency CIRT personnel when adverse events occur; and
- Oversee the handling of all aspects of a security incident until resolution.
- Respond to all events in a timely manner. This includes logging incidents into the ASOC CIRT Tracking Database for threat analysis; investigating to determine the cause of the event; and performing necessary actions in order to contain an event.
- Use US-CERT CONOPS and NIST SP 800-61 guidance to categorize incidents.
- Report incidents to the US-CERT and OIG for USDA agencies and offices.
- Escalate PII and critical incidents to the CIRG.
- Escalate criminal actions and incidents requiring forensics investigations to OIG.
- Report potential and known compromise of information covered by the Privacy Act of 1974 to US-CERT and OIG.
- Make referrals to appropriate entities on reported events that are not computer security related.
- Cooperate with OIG and other law enforcement entities to provide any support needed for criminal investigation/prosecution.
- Stay informed on the latest technologies and exploits through education and communication with other computer incident response groups such as the US-CERT Government Forum of Incident Response and Security Team (GFIRST).

- Work with the USDA OIG Computer Forensics Unit (CFU) to secure evidence on certain types of incidents in compliance with the rules of preservation of evidence.

2.5 ASOC CIRT Incident Management

Incident management affects multiple divisions and occurs across different organizational structures within the USDA. This document contains the operating procedures that the ASOC CIRT follows when processing computer security and PII events. This document also contains a process model that will continue to evolve as USDA refines its incident management process.

The incident type and/or cause will dictate the action required for resolution. CIRT actions may include a referral to another authority (e.g., OIG); a site visit to gather more information, additional coordination with OIG; seizure of a machine; or the reporting of activities to an Internet Service Provider (ISP), US-CERT or other Federal Agencies. NIST SP 800-61, *Computer Security Incident Handling Guide*, contains checklists of initial and generic actions that must take place when responding to an incident. NIST SP 800-61 also provides checklists for specific types of common incidents. Appendix D provides a copy of checklists found in NIST SP 800-61, including:

- Initial Incident Response Checklist;
- Generic Incident Response Checklist for Uncategorized Incidents;
- Denial of Service Incident Response Checklist;
- Malicious Code Incident Response Checklist;
- Unauthorized Access Incident Response Checklist;
- Inappropriate Usage Incident Response Checklist; and
- Multiple-Component Incident Response Checklist.

Multiple component incident and event handling refers to cases where multiple components are affected such as botnets or situations where one responder could be responsible for handling more than one incident simultaneously.

Prioritization guidelines should be used for all incident categories. Prioritization guidelines allow the responder to identify response time requirements and to handle the most urgent need first. Factors to consider include how current each component is and if the attack creates multiple paths to reach targets.

Prioritization guides documented in a Service Level Agreement (SLA) should facilitate faster and more consistent decision-making during the stress of incident response. SLA can be used as performance measures when contracting for incident response services or measuring the effectiveness of a security program. SLA matrices from NIST SP 800-61, based on events, technical issues, and criminality of incidents should be used.

2.6 CIRT Position within USDA

The CIRT hierarchal structure is illustrated below.

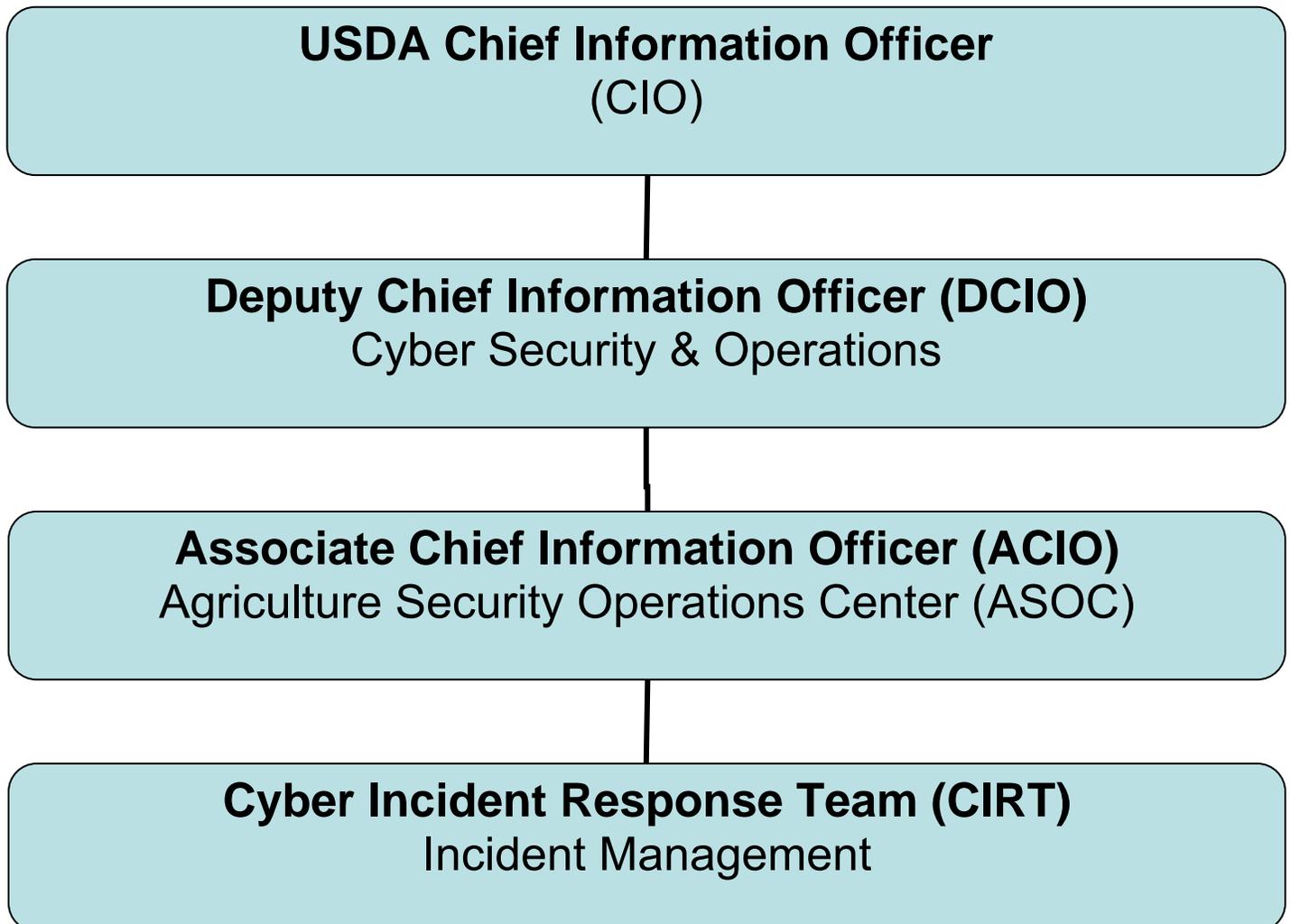


Figure 2: CIRT Position within USDA

3 Knowledge/Expectations of the ASOC CIRT

The ASOC CIRT code of conduct is based on the US-CERT Coordination Center's Elements of a Code of Conduct (Carnegie Mellon University). The following recommendations for CIRT conduct have been widely embraced by the Incident Management community.

1. Focus on strengths.
2. Adapt to the audience.
3. Speak for yourself.
4. Do not speak for others.
5. Make complete statements.
6. Make concise statements.
7. Avoid the use of jargon.
8. Be sensitive and diplomatic.
9. Avoid arrogance.
10. Avoid being familiar.
11. State the facts.
12. Be truthful.
13. Retain control.
14. Avoid shock tactics.
15. Maintain confidences.
16. Make no promises.
17. Teach.
18. Stress the positive.
19. Apply quality control.
20. Use constructive criticism.

4 Transitioning an Event to an Incident

Generally speaking, an incident poses a higher threat to the USDA network than an event, and therefore has a higher priority. An event may be escalated if it is determined to be a potential threat, not necessarily a proven threat, to the USDA networks. Once elevated, further analysis will determine if the threat can result in DOS, introduction of malicious code, unauthorized access, or inappropriate or unauthorized use of USDA assets. The severity of the threat is a key factor in escalating an event to incident status.

The USDA definition of events and incidents is based on NIST SP800-61, *Computer Security Incident Handling Guide*, and can be found in this SOP Section 1.4, *Definitions*.

The ASOC CIRT is the final decision authority when determining if an adverse event meets the incident status threshold. ISSPMS will follow this SOP, currently issued updates, and OCIO and agency OCIO guidance to determine when events meet the adverse event status. All adverse events will be reported to the ASOC CIRT for further determination and network security analysis.

Upon receipt of an adverse event report, the ASOC CIRT analyst will verify that the activity reported is within the scope of the ASOC CIRT adverse event guidelines. Adverse events reported to the ASOC CIRT are tracked in Cyber Security Incident Response Management (CSIRM) system database, Public Folders and on the Share drive. The ASOC CIRT analyst will utilize all available resources to determine the cause of the adverse event and coordinate any response necessary. At any point during the analysis, the event may transition to an incident.

Internal procedural warnings and monitoring of adverse events may transition to incidents, such as routine reporting from USDA enterprise assets and computer defenses; to include but not limited to: traffic log reviews, scanning, and penetration testing. SPAM and spear phishing caught at the firewall may be transitioned on a case by case basis depending on the threat and criticality of the event. Below are a few examples of events stemming from internal procedural warnings and monitoring of adverse activities that could be escalated to incidents.

- a. : Spam and Spear Phishing
 - i. Specifically target a critical asset or essential person/duty position such as, finance center machines or the Secretary of Agriculture
 - ii. Create enough traffic to threaten a DOS
 - iii. Involve USDA with incidents of other federal agencies or civilian entities

- b. Enterprise Monitoring Thresholds:
 - i. The *Alarms by Day Summary* threshold for constituting an incident is any hits over 100 for the source or destination internet protocol (IP) based on daily reports submitted to the ASOC CIRT.
 - ii. The *Shunning Events by Day Summary* threshold for constituting an incident is any hits over 100 for the source or destination internet protocol (IP) based on daily reports submitted to the ASOC CIRT.
 - iii. The “single entity” known malicious site offenders threshold for constituting an incident is any warnings over 75 on a daily basis.

- iv. The peer 2 peer (P2P) threshold that constitutes an incident is any hits of a single IP over 75 on a daily basis.
- v. Instant Messaging threshold that constitutes an incident is any hits of a single IP over 75 on a daily basis.

Other examples of adverse events that would transition to incident status include but are not limited to events involving:

- Privacy Act or sensitive data;
- Unauthorized access to network;
- Web site defacement;
- Unauthorized software that poses a threat to network security (backdoors);
- Fraud;
- Misuse of government computer resources;
- Access of unauthorized or illegal web sites;
- Emails of a threatening or malicious nature;
- Social engineering; and
- Any violation of local, state, or federal law.

Events will be considered an incident after it has been analyzed by the ASOC CIRT. Other incident indicators include but are not limited to the following actions:

- An official incident ticket is opened by the ASOC CIRT analyst and directed to the responsible agent or agency ISSPM of the cyber assets involved in the adverse event. The recipient of the memo may be internal or external to the USDA, and the notification may be sent in the form of an email.
- An event is referred to any entity outside of USDA.
- An event is referred from an outside agency, such as US-CERT or law enforcement agencies.
- Actual penetration of systems or resources or a DOS attack has occurred.

5 Cataloging Incidents

Whenever an adverse event transitions to an incident, the ASOC CIRT Duty Officer initiates and maintains a chronological log of activities. This log is an official record of activity, and serves as the basis for all reports to management on the handling of an incident. The incident logs are stored in the CSIRM database, the share drive and in the public folders. Incidents are saved to the ASOC CIRT shared directory in a folder with the following naming convention USDAYFYNNNN-XXX (e.g., USDA08090001-FS) Description (e.g., Trojan)

- YY – Calendar year (e.g., 08)
- FY – Fiscal year (e.g., 09)

- NNNN – Sequential Number (e.g., 0001)
- XXX – Responsible Agency (e.g., FS for “Forest Service,” AMS for “Agricultural Marketing Service,” etc.)
- A brief description of the incident, usually the type of incident (e.g. Trojan, Lost Equipment- No PII) note: If the incident is PII this section of the name must include the letters: “PII”.

Management may request additional information when titling incidents for tracking and analysis purposes. When additional information is added it will be added as a final segment to the original title

The log should contain a running record of all telephone conversations (summary), contacts made and pertinent information. All conversations, emails or other communications concerning the incident must be documented. If warranted, these logs may be called upon for legal review so accuracy and thoroughness are imperative.

The ASOC CIRT team is responsible for providing timely status reports of incidents until resolution. These reports may include referrals to another internal/external agency for action.

6 CIRT Notification and Escalation Process

The ASOC CIRT notification and escalation process is:

- The ASOC CIRT notifies the USDA-ASOC Incident Handling Division Director (IHDD), ACIO, Deputy CIO, OIG, and the affected Agency CIO and ISSPM of all high priority and/or PII incidents.
- If the incident involves PII, the Agency CIO must be notified immediately, and the Agency ISSPM must complete the Initial Incident Report within one hour after the incident occurred. The completed report will be sent to cyber.incidents@usda.gov.
- All incidents except Lost and Stolen Equipment, Category 6 “Under Investigation,” and Machine(s) involved with malicious code incidents will be taken off line and verification of containment will be sent to USDA-CIRT within 24 working hours.
- The affected Agency ISSPM will provide the ASOC CIRT analyst with daily status updates until the incident has been closed.
- The ASOC CIRT analyst will provide the ACIO-ASOC, IHDD, and DCIO-ASOC with the most current incident status.
- Agency ISSPM will report to the ASOC CIRT as defined in section 5.3.
- **24 HOUR:** Failure to submit a 24 Hour Incident Containment Checklist will result in internet access being blocked at USDA gateway.
- If an incident is not closed after 25 days, the ASOC CIRT will escalate to the USDA DCIO-ASOC who will contact the Agency CIO and the USDA CIO.
- If an incident is not closed after 30 days, the agency ISSPM will be required to open a Plan of Action and Milestone (POA&M) task in the Cyber Security Assessment and Management (CSAM) Database System.

7 Reporting Incidents

Figures 3 and 4 illustrate the USDA incident handling process, and define the general processes that must be used for incident management, including incident management of PII and Sensitive But Unclassified (SBU) data. All incidents are reported to the OIG. The diagrams do not show all methodologies that may be used. (See USDA DM 3505-001 for more policy information.)

7.1 Sources Reporting Security Incidents

Computer security incidents are reported to the ASOC CIRT by many different sources and groups. Some of the common sources are:

- USDA Telecommunications Services and Operations (TSO) Staff
- Universal Telecommunications Network (UTN)
- USDA email abuse hotline abuse@usda.gov
- USDA email administrators
- USDA Gateway
- 24 hour USDA Security Incidents Hotline at 1-888-926-2373 or 1-877-PII-2YOU , 1-866-905-6890, or 1-866-905-6890.
- USDA employees, contractors, partners, and customers who utilize USDA information technology (IT) resources; and
- US-CERT, other Federal Agencies or Law Enforcement organizations.

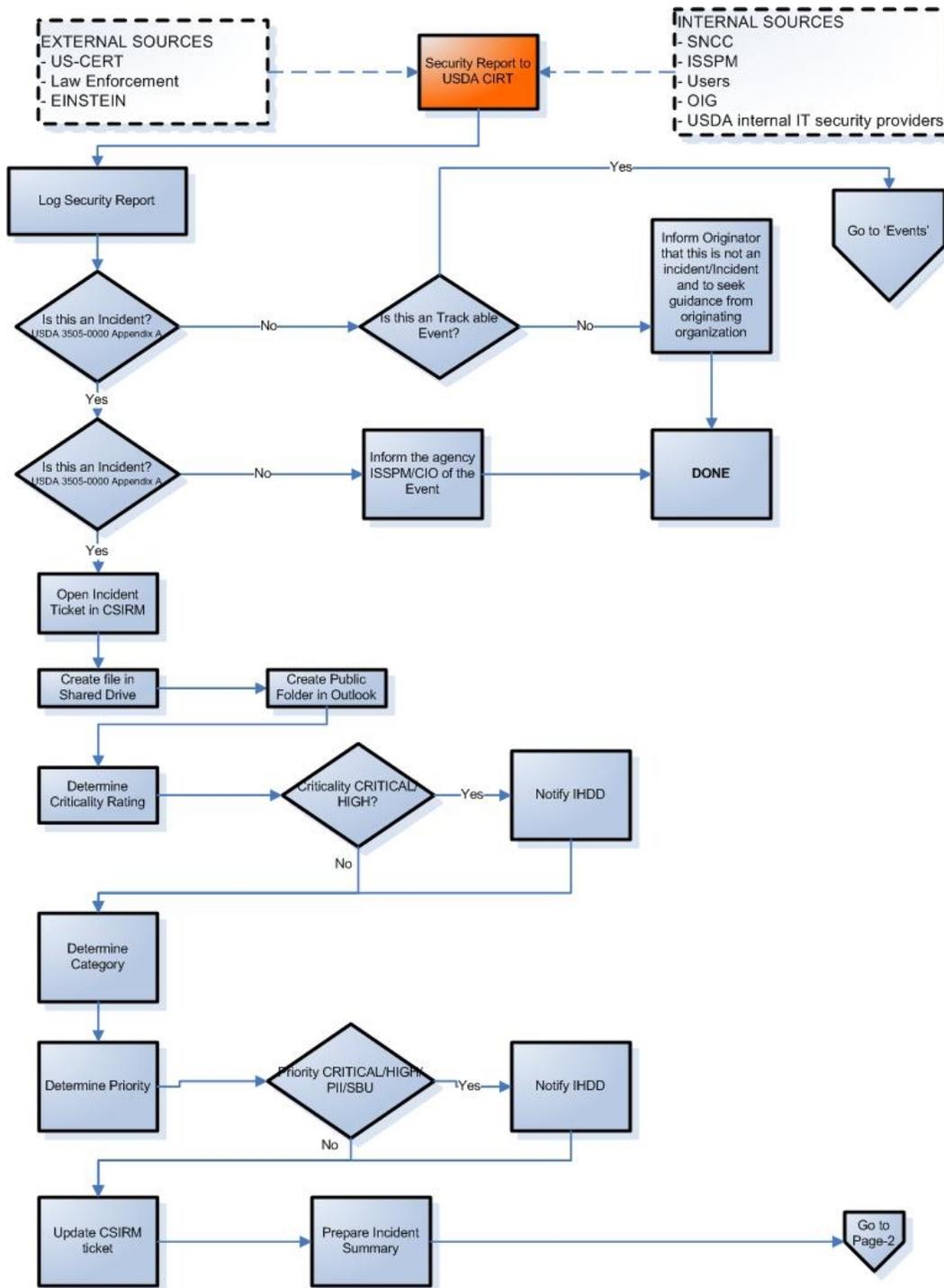


Figure 3: Process Flow for PII and SBU Incidents

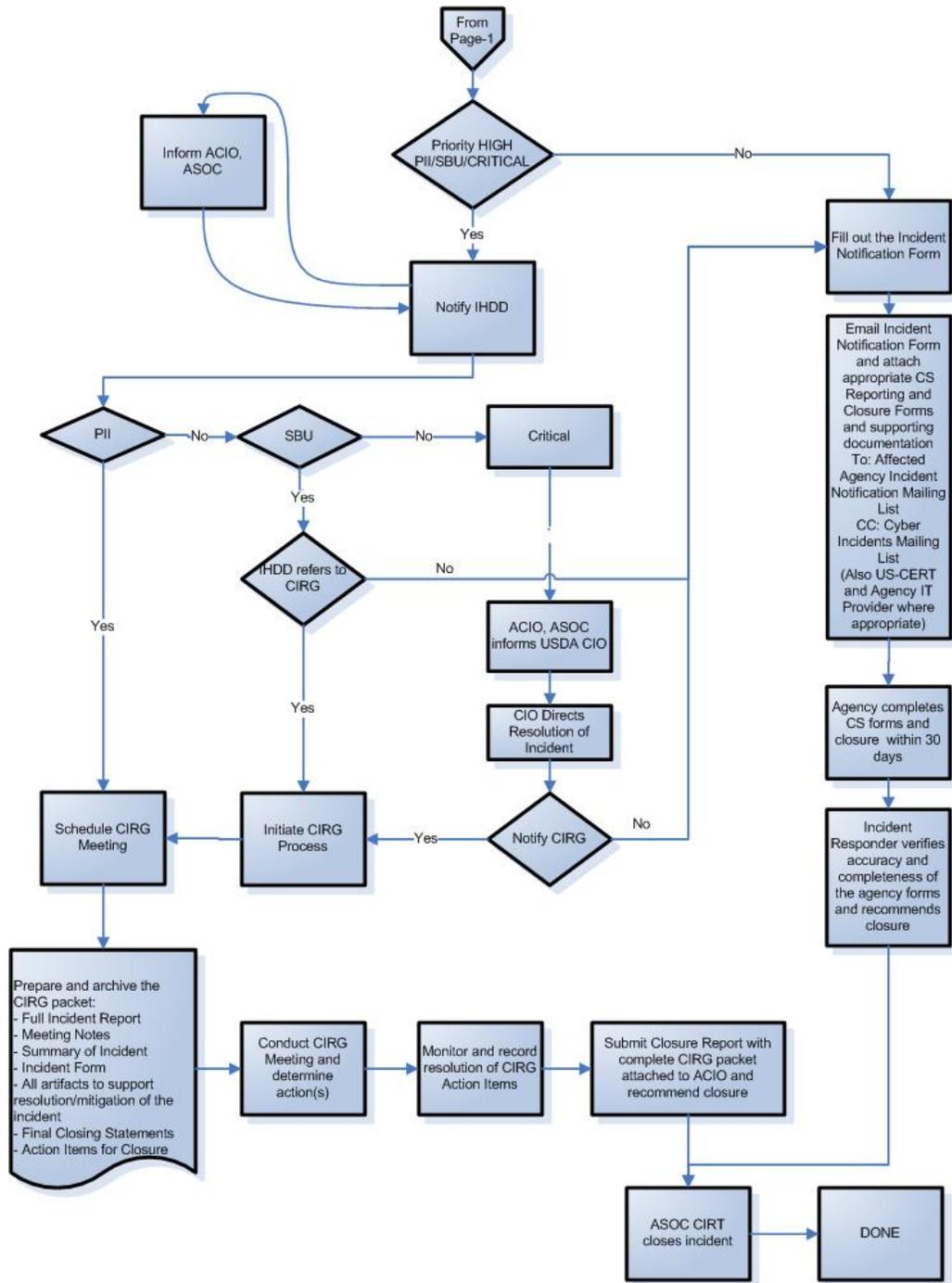


Figure 4: Process Flow for Non-PII/SBU Security Incidents

7.2 TSO Staff Reported Security Incidents

All cyber security events received by TSO to the 24x7 telephone number (866-USDA-WAN), or to the abuse@USDA.gov, want@mail.netman.usda.gov, or duty.officer@usda.gov email addresses are:

- Logged using TSO established procedures;
- Reported immediately to the CIRT Duty Officer at cyber.incidents@usda.gov and/or 1-866-905-6890;

The TSO staff will wait no more than 30 minutes (10 minutes in the most disruptive or critical cases) before communicating the notification to the next person in the CIRT notification chain if the first person cannot be reached. If the TSO duty officer is unable to contact anyone on the ASOC contact list, the duty officer will communicate the event to TSO management.

For TSO UTN incidents, the ASOC CIRT Duty Officer will:

- Open an incident in the CSIRM database and assign a USDA incident number;
- Notify the affected Agency ISSPM, USDA OIG, OCIO, the ASOC staff, CIRT members, and US-CERT (when applicable);
- Monitor the incident until it is closed;
- Close the incident in the CSIRM database and, if applicable, with US-CERT.

Post incident, the TSO UTN team will extract, gather, and compile relevant log data, etc., and submit it as an attachment to their initial the ASOC CIRT report, which will be forwarded to cyber.incidents@usda.gov. TSO will also follow through with additional data gathering or more restrictive actions as deemed necessary by TSO management in cooperation with the ASOC CIRT.

7.3 ISSPM Reported Security Incidents

A USDA Agency ISSPM who suspects or confirms an adverse event will immediately report the event to the ASOC CIRT using the following process:

- Log the event using the agency's established procedures.
- Using Table 1 (below), timely report all security incidents. (**Note:** Report all PII incidents within one hour, whether suspected or confirmed, through the ASOC CIRT.)
- Send an email to cyber.incidents@usda.gov. Complete and attach the USDA Incident Report (Appendix B). If the incident involves any data device, call the USDA Security Incidents Hotline at 1-888-926-2373 or 1-877-PII-2YOU, 1-866-905-6890, or 1-866-905-6890.

Upon receiving an incident report from an agency ISSPM, the ASOC CIRT Duty Officer will:

- Open an incident in the CSIRM database and assign a USDA incident number.
- Notify OIG and, if applicable, US-CERT.
- File all documentation in the ASOC CIRT local area network (LAN) folder.

- Monitor the incident until it can be closed.
- Ensure the Agency ISSPM has completed the USDA Incident Report and the Follow-up Report to Lost/Stolen Equipment with No PII Involved report, if applicable.
- Close the tickets with the ISSPM, USDA CSIRM database, and US-CERT, if applicable.

Category	Example	Description	Priority	Agency Reporting Timeframe to the ASOC	ASOC Reporting Timeframe to US-CERT
CAT 1	1.1 Unauthorized Access 1.2 Equipment Loss 1.3 Network Intrusion 1.4 Non-Privileged Account or System Access 1.5 Privileged Account or System Access	An individual gains logical or physical access without permission to a federal agency network, system, application, data, or other resource (i.e., lost or stolen electronic-based resources with PII data, and portable electronic devices PDA, USB devices, etc.). HSPD-12 /LincPass badges	High	Upon detection	USDA must report this to US-CERT within one hour of discovery/detection. All incidents involving PII must be reported to US-CERT within one hour
CAT 2	Denial of Service (DOS)	An attack that successfully prevents or impairs the normal authorized functionality of networks, systems or applications by exhausting resources. This activity includes being the victim of, or participating in, a DOS attack.	High	Upon detection	USDA must report this to US-CERT within two hours of discovery/detection if the successful attack is still ongoing and the agency is unable to successfully mitigate the activity.
CAT 3	3.1 Malicious Code	Successful installation of malicious software (i.e., virus, worm, spyware, bots, Trojan horse, or other code-based malicious entity) that infects or affects an operating system or application.	High	Upon detection	USDA must report this to US-CERT within one hour of discovery/detection if it is widespread across USDA.
CAT 4	4.1 Improper Usage	Any violation of USDA policy (i.e., peer to peer activity, viewing inappropriate content on the Internet, improper electronic transfer of PII).	Medium To High	Within two days	USDA must report this to US-CERT weekly. All incidents involving PII must be reported to US-CERT within one hour.

Category	Example	Description	Priority	Agency Reporting Timeframe to the ASOC	ASOC Reporting Timeframe to US-CERT
CAT 5	5.1 Brute Force Attack 5.2 Port Scans 5.3 Social Engineering 5.4 Social Engineering Phishing 5.5 Probes 5.6 Attempted Access	Internet activity that seeks to access or identify federal agency computers, open ports, protocols, services, or any combination thereof for later exploitation. This activity does not directly result in a compromise or denial of service.	Low to High	Within two days unless PII is involved, then upon detection	USDA must report this to US-CERT monthly unless PII data is involved. PII data compromises must be reported within one hour.
CAT 6	6.1 Investigation 6.2 Paper-Based PII	Unconfirmed incidents that may be potentially malicious or anomalous activity deemed by the reporting entity to warrant further review, (i.e., paper-based PII, security violations that threaten Confidentiality, Integrity, and/or Availability, Investigation/Non Cyber incidents (e.g., piece of paper containing PII was left at bus stop))	Low to High 6.2-All Paper based PII is High	Not applicable, and not reported	Potential incidents are not reported to US-CERT. All incidents involving PII must be reported to US-CERT within one hour

Table 1: USDA Agency Incident Categories (Defined by US CERT CONOPS and NIST SP 800-61)

Incident reports to US-CERT should have a severity rating that reflects the incident’s effect on the agency, the Federal government, and the national critical infrastructure. The severity rating enables US-CERT to effectively respond to incidents that are threatening or affecting the critical infrastructure.

Use the following formula based on the tables in Appendix F to determine the overall severity rating of an incident.

Overall Severity/Effect Score = Round ((Current Effect Rating * 2.5) + (Projected Effect Rating * 2.5) + (System Criticality Rating * 5))

Note: “Round” in the above equation means to round to the nearest 100th.

Incident criticality is also determined by using matrices based on events, technical assets, and criminality. See Appendix F and NIST SP 800-61 for additional guidance.

7.4 NITC SNCC Reported Incidents

The National Information Technology center (NITC) System Network Control Center (SNCC) reporting process consists of the following:

- Customer calls NITC SNCC on the toll free hotline to report lost or stolen equipment.
- SNCC answers the call and assigns a SNCC tracking number.
- SNCC asks the customer if the lost or stolen equipment contains PII or Sensitive data.
- **If the equipment contains PII or Sensitive Data** – SNCC personnel will contact the CIRT Duty Officer and initiate a teleconference with the customer to identify the scope, sensitivity, and containment of the incident. The CIRT Duty Officer will ask the questions in Appendix E, PII/Sensitive Information Questions Checklist, as a minimum.
- The CIRT Duty Officer notifies US-CERT, IHDD, ACIO-ASOC, DCIO- ASOC, CIO, OIG, and the affected Agency CIO and ISSPM (who will be responsible for notifying the Agency Privacy Officer) about the PII data and how many instances of the data were compromised.
 - If the data **was not** encrypted and the data loss was significant, the CIRT Duty Officer will inform the IHDD, who will inform the Agency and USDA CIO to alert the USDA CIRG.
 - If the data **was** encrypted, the CIRT Duty Officer will continue processing this as a high priority incident, communicating with the affected Agency ISSPM.
- **If the equipment does not contain PII** – SNCC personnel will email the CIRT Duty Officer with the completed stolen equipment report.
 - A USDA Incident Tracking number will be assigned to the incident, and the ASOC CIRT will send the incident number and a follow-up report (Appendix B) to the Agency ISSPM.
 - The Agency ISSPM will complete the checklist and send it back to the ASOC CIRT at cyber.incidents@usda.gov.
 - Equipment like global positioning systems (GPS), cell phones, and monitors where PII data is not stored will **NOT** be reported to US-CERT.
 - If the lost or stolen equipment does not include PII, the loss will be handled according to the affected agency's policies and procedures and the CIRT Duty Officer will email the SNCC report to the Agency ISSPM and the customer who telephoned the SNCC initially.

7.5 Externally Reported Incidents

On occasion the USDA receives direct notification from outside sources on events that involve USDA TCP/IP addresses. Notification may come from several different sources including:

- US-CERT
- US-CERT – Einstein
- US-CERT – Joint Agency Cyber Knowledge Exchange (JACKE)
- Other Federal Agencies
- Law Enforcement Agencies
- Private Companies
- News Media
- Internet Service Providers

In these instances the ASOC CIRT Duty Officer will:

- Open an incident in the CSIRM database and assign a USDA incident number;
- Contact US-CERT, OIG and Agency CIO when incidents involve PII;
- Research the event;
- Respond to the source that reported the event or finding;
- Monitor the incident until it can be closed;
- Complete a Final Incident Report with required attachments in the CSIRM database;
- Provide the Final Incident Report with required attachments to US-CERT and OIG; and
- Close the tickets with US-CERT, OIG, and in the USDA CSIRM database.

7.6 US-CERT Reporting Requirements

FISMA requires all agencies to report security incidents to a Federal incident response center (US-CERT). OMB Memorandum M-06-19, *Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments*, and M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*, require Federal Agencies to report all security incidents that involve PII, suspected and confirmed, including paper based events, and lost and stolen equipment to US-CERT within one hour of notification of the incident. When reporting PII or Sensitive incidents to the ASOC CIRT, agencies must identify the scope, sensitivity, and containment of the incident and include, in the closing report, the completed PII/Sensitive Information Questions Checklist found in Appendix E.

PII is defined as any information, which can be used to distinguish or trace an individual's identity such as a name, social security number, date and place of birth, mother's maiden name, biometric records, etc., including any other personal information that is linked or linkable to an individual.

Other working examples of PII can be found at <http://www.ocio.net.usda.gov/ocio/security/pii.html>.

PII, lost and stolen IT equipment and incidents involving malicious code must be reported within one hour of detection to USDA-CIRT. Then USDA-CIRT will report the incident within one hour of notification to US-CERT. Not all incidents involving PII will be reviewed by the Core Incident Response Group (CIRG). The USDA-CIRT PII analyst will notify agencies if their PII incident is going to be reviewed by the CIRG during their weekly sessions. Lost or stolen HSPD-12/LincPass Badges will be reported as lost and stolen equipment – PII.

USDA-CIRT must report incidents to US-CERT when:

- An individual gains logical or physical access without permission to a federal agency network system, application, data, or other resource;
- There is a suspected or confirmed breach of PII regardless of the manner in which it might have occurred; and
- There is loss of government issued IT equipment or media that includes, but is not limited to, laptops, desktop computers, personal data assistants, cellular telephones, global positioning systems, magnetic tapes, thumb drives or any removable storage media devices.

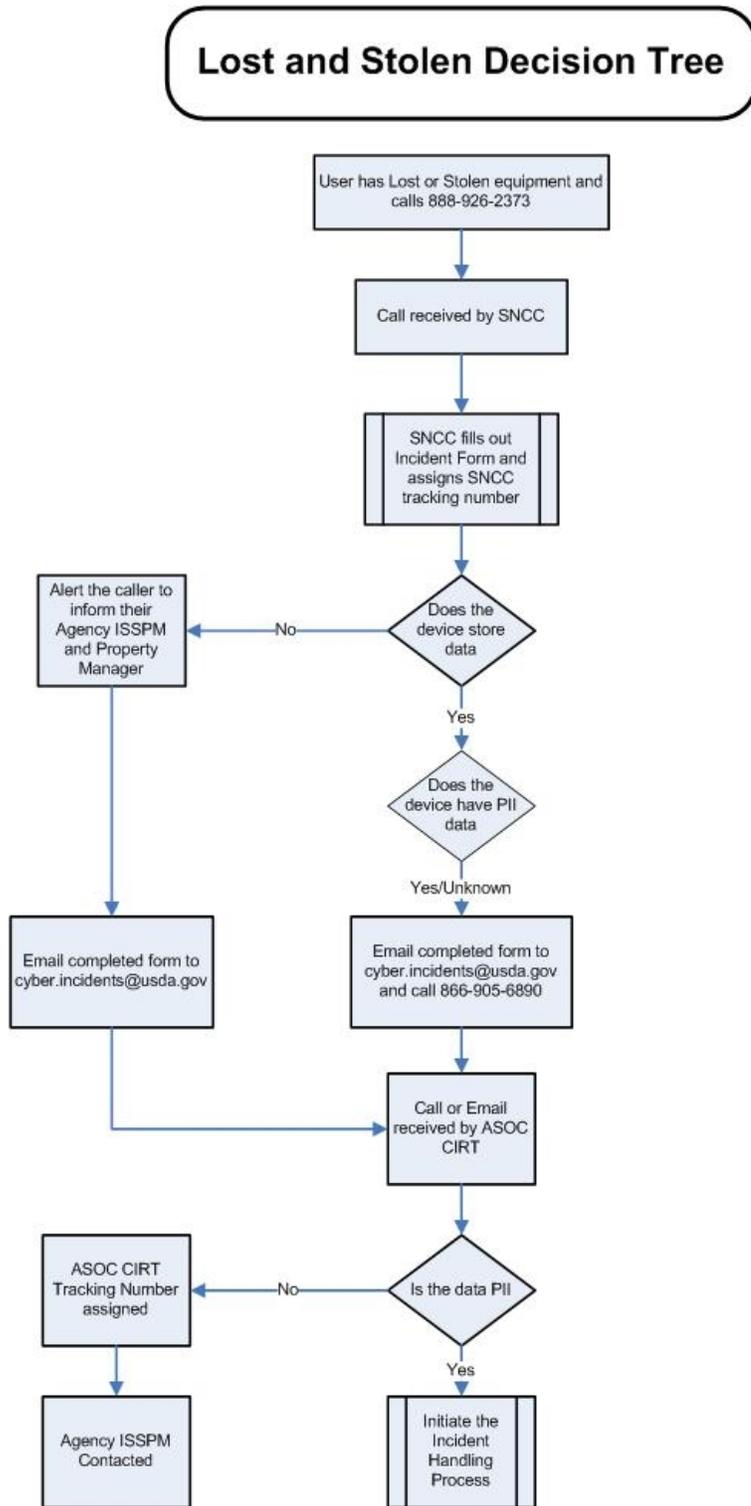


Figure 5: Lost and Stolen Equipment Decision Tree

8 Events and Incidents

8.1 Security Events to Be Reported to the ASOC CIRT

An event is any abnormal occurrence or activity on the USDA network. Once reported to the ASOC CIRT, an analysis will be made to determine the effect on the USDA network. If the reported activity is not a security related event, the ASOC CIRT will not accept the report as an event and will instruct the reporter on how to proceed. If the event is determined to be out of the jurisdiction of the ASOC CIRT, it will be referred to the appropriate office or entity.

Although the following list is not comprehensive, these are events that must be reported to the ASOC CIRT (see USDA DM 3505):

- Unauthorized access attempts to any network resources;
- Excessive logon attempts;
- Unauthorized access attempts after hours;
- Unauthorized access or permissions to file directories, share data, and folders;
- Unauthorized access to system applications and operating systems;
- Unusual logon screens or procedures;
- Passwords displayed in plain text;
- Emails that are threatening or malicious in nature;
- Suspicious attachments to emails;
- Contact by unfamiliar persons attempting to solicit user or account information;
- Unauthorized installation of any software or hardware;
- Any system applications, including locally developed ones, not authorized by USDA;
- Use of unauthorized encryption software;
- Use of unauthorized modems;
- Use of unauthorized networking devices;
- Unexplained system issues that cannot be resolved operationally;
- Unexplained system crashes;
- Inaccessible or altered system resources or data;
- Unexplained alteration of data;
- Altered web site content/defaced web sites;
- All suspicious events on systems that have PII;
- All lost or stolen equipment that is used for data storage or data transmissions (see Section 5.4); and
- The loss of paper based PII/Privacy Act information.

Table 1 describes the reporting requirements and categorization of security events for USDA as defined by NIST SP 800-61, and the US-CERT Concept of Operations.

8.2 Adverse Events

Adverse events such as suspicious Spam or Phishing that are not considered an incident reportable to US-CERT **will be assessed by the ASOC CIRT and may be** recorded as a Category 6 incident in CSIRM, the share drive and public folders. If the adverse event transitions to an incident it will maintain the same cataloging number with the new category rating.

8.3 Category 6 Incidents

Category 6 incidents are events and incidents under investigation that do not fall within the other five incident categories established in the US-CERT CONOPS. These types of incidents include, but are not limited to:

- **Investigations** – Whether or not the incident information available to the ASOC CIRT is complete or of limited content. Externally investigated incidents are managed and closed upon request of the IHDD.
- **Paper based PII** – PII must be reported as “HIGH” priority to US-CERT within 1 hour

8.4 Spam or Phishing Events

The USDA process for reporting Spam and Phishing is:

- If the attack gets through USDA first line of defenses, it is reportable under this Incident Reporting SOP.
- If USDA Information Technology defenses successfully stop the attack, then it is generally not reportable except in cases where:
 - The saturation is large enough to have an impact on usage; in which case, it can be reported as attempted DOS (lasting two hours).
 - The targets are of a sensitive nature such as VIP, overseas travelers, SBU, sensitive facilities, etc.
 - There are suspicious sources such as IP addresses that US-CERT has asked USDA to block, malicious IP sources with a USDA history, or High-Side sources.

When reporting Spam or Phishing that is generally not reportable, include an explanation of why the agency is concerned about the Spam or Phishing in the report to draw the attention of US-CERT analysts.

USDA-CIRT will transmit submissions of agency spam, spear phishing, and malware to US-CERT. When US-CERT informs USDA-CIRT of their findings and actions taken, USDA-CIRT will inform the agency of the US-CERT findings and maintain a record for reference and analysis.

- SPEAR PHISHING captures should include the source IP and full header information, if possible, and can be sent to http://www.us-cert.gov/nav/report_phishing.html.

- MALWARE/VIRUS captures should include the source IP and full header information, if possible, and can be sent to virus-submit@us-cert.gov.

8.5 Peer to Peer (P2P)

Workstations with Peer to Peer (P2P) software are to be taken offline immediately upon detection. The P2P transfers are to be shunned. P2P incidents will be processed and the “Inappropriate Usage” incident containment checklist will be completed and returned to cyber.incidents@usda.gov .

P2P software will be removed from the machine before it is reconnected to the USDA network. The ASOC CIRT authorizes the machine to be placed back online and remove blocks and shuns after the agency ISSPM submits the incident closing documentation and verifies the machine is no longer a threat to the USDA network.

8.6 Instant Messaging (IM)

Commercial Instant Messaging (IM) software, that is not licensed to and distributed by USDA, is not authorized for use on USDA systems. Exceptions are made on an individual basis when approved IM software is not available and IM service is needed to accomplish mission essential tasks such as exceptions being authorized to facilitate communications with hearing impaired individuals.

Instances of unauthorized IM will be mitigated using the same procedure as described in P2P of this SOP, Section 8.5 above.

8.7 Malicious Code/Malware

Machines identified with malware activity are to be taken off line within 24 working hours of notification. The 24 Hour Incident Containment Checklist (Appendix D, section D.11) will be completed and returned to cyber.incidents@usda.gov within 24 working hours of notification. (Weekends and legal holidays are now excluded from the timeline.) The completed Malicious Code Incident Response Checklist (Appendix D, section D.7) will be completed and returned to cyber.incidents@usda.gov as an enclosure with the incident closing report. After the agency provides a signed containment and closing report that describes the actions taken, the ASOC CIRT will validate that the actions described in the agency’s containment and closure documents meet USDA policy objectives and are in compliance with Federal Desktop Computer Configuration (FDCC) and NIST SP800-53 configuration and controls.

Upon request from the ASOC CIRT, agencies will send malicious code identified through forensic analysis or deemed non detectable by updated anti-virus programs to the ASOC CIRT at cyber.incidents@USDA.gov. The Malicious code will be transmitted in .zip or .rar format, renamed using an .usc extension, and password protected with the password “infected.” USDA components having technical difficulties or questions about the submission process should contact the ASOC CIRT directly for further guidance.

8.8 Key Loggers/Keystroke Logging

Key logging is one of the first spyware techniques used to capture sensitive data from a system. When a USDA user ID has been compromised an incident will be created for the User ID and the Device. All user ID and passwords for USDA systems that are associated with the user will be changed and the user machine reimaged before the user's access will be restored. To assist ISSPM with resolving key logger incidents a zip file containing technical information will be created with a password. The zip file and the password will be sent separately to the owner/Agency of the device. Below is a brief description of basic key loggers.

Both hardware and software key loggers exist. Hardware based key loggers do not depend on software and require physical or root-level access to be installed. Hardware devices usually exist between the keyboard and the computer or they are firmware based and exist in the BIOS with code written specifically for the type of hardware it will be using.

Software based key loggers work on the computer's operating system. There are four main types of software key loggers.

- Hypervisor-based (virtual machine monitor) key loggers reside in the form of malware and run underneath the operating system by trapping a virtual instance of the operating system. Virtual machines are often difficult to detect using conventional scanning tools. Hypervisor key loggers can also allow others to obtain complete control of the system.
- Kernel-based key loggers reside at the kernel level and are often implemented as root kits that allow them to gain unauthorized access to hardware. Kernel-based key loggers can act as keyboard drivers and gain access to information flowing between the keyboard and the operating system.
- Hook-based key loggers use hooking techniques to alter or augment operating system or application behavior. Hooks can fake the output of application programming interface (API) calls to remain undetected and can intercept function calls to change the outcome of the function. Hook-based key loggers use the operating systems application functionality to record each stroke of the keyboard.
- Passive Methods use the operating system's API to poll keyboard state, subscribe to keyboard events or to poll the BIOS for pre-boot authentication personal identification numbers (PIN). Passive key loggers can turn themselves on and off to target specific information such as, instant messaging clients, email applications, web browsers such as the form grabber that targets the submit event function to grab the data before it is protected by https.

9 Blocks and Shuns

The CIRT Duty Officer will occasionally need to block or shun IP addresses that have been reported as being involved with malicious activity. Malicious activity is any unauthorized attempt to alter, harm, or gain unauthorized access to USDA systems. Examples of malicious activities

include, but are not limited to, Secure Socket Shell (SSH) scanning, structured query language (SQL) injections, P2P, beaconing, etc.

The ASOC CIRT will immediately request a block for all reported external malicious IP addresses. Internal IP addresses will be managed on an independent basis but should be shunned before blocking as a general rule.

The ASOC CIRT Duty Officer will call the UTN Duty Officer and request to shun or block a malicious IP upon being notified of this activity. The determination of whether to place a block or shun will be based on the severity and priority rating of the incident as well as the constraints of the process. To determine the severity of the incident, refer to Appendix F; and to determine the priority of the incident, refer to Appendix G.

Blocks and shuns are constrained by their defined criteria. Blocks are implemented at the firewall level, and are generally implemented at 1 A.M. on Tuesday and Thursday mornings. Blocks are implemented as a shun immediately, and are automatically converted to a block during the next bi-weekly rotation. If the IP to be blocked is external to USDA or if there is an emergent need, a block will be implemented as a shun and then converted to a block at 1AM the next morning. Blocks are low maintenance, but slow to implement and slow to remove, making them more permanent in nature than a shun.

Shuns are implemented at the Intrusion Detection System (IDS) level. They are more high maintenance, but near instantaneous to implement and remove. If the shun is implemented by the IDS, it will remain effective for 30 minutes and then be automatically removed. If the shun is implemented manually, it can remain in effect indefinitely. Shuns tend to be flushed from the IDS when IDS signature updates are installed, and must be re-entered manually; therefore, if the shun is anticipated to be in effect more than 72 hours, a block should be requested.

The ASOC CIRT Duty Officer may also request UTN to implement a shun with the following stipulation: "Please implement the shun immediately and if the ASOC does not lift the shun within 72 hours, please convert it to a block."

IP addresses often need to be blocked because of traffic or connectivity to malicious websites. These communications are recorded in IP traffic logs. The UTN Duty Officer can provide log traffic to the ASOC through packet captures, which will help identify the scope and sensitivity of an incident.

Log information or packet captures are needed to ensure that agencies can locate the host or workstations being used to execute malicious activity. The ASOC CIRT Duty Officer must provide the UTN Duty Officer with the malicious IP, the associated host name of the USDA system, and the time frame and size of the file (i.e., 30 minutes and 20MB, etc.). Packet captures can be requested to monitor USDA IP activity or to monitor which USDA assets are communicating with or being targeted by a malicious external IP.

Packet captures take about 15-20 minutes to set up before they are initiated; therefore, depending on the sensitivity of the incident, the CIRT Duty Officer may need to implement the shun or block immediately and then request a historical search of the log files. Firewall logs can be searched for up to one week, but the information recorded is limited and may not satisfy the needed criteria.

Domain Name Server (DNS) logs are searchable for 3-4 days. IDS systems are only searchable for up to 48 hours, but generally provide the type of detail needed to satisfy incident response criteria.

10 Containment and Closure

USDA-CIRT will remove agency IP blocks and shuns and close incidents as appropriate after the agency ISSPM verifies containment and closure of the incident in compliance with USDA policy, FDCC, and NIST SP800-53 controls. All incidents, except Category 6, *Investigation and Paper Based PII*, and Category 1.2, *Lost and Stolen Equipment*, will require completion of the 24 Hour Containment Checklist found in Appendix D.11. Examples of containment and closure processes include, but are not limited to:

- Containment:
 - a. All user credentials reset
 - b. System(s) off-line within 24 hours—undergoing, or held for further review and analysis
- Closure:
 - a. System wipe/restoration process is validated as compliant with policy and standards such as, USDA policy, FDCC, and NIST SP800-53 controls.
 - b. All user-accessible data (both local and network drive(s)) have been scanned before being restored.
 - c. Data review process is validated as compliant with policy and standards
 - d. POA&M is created and assigned to system owner

The Agency ISSPM will ensure the machine meets USDA and FDCC security standards. The ASOC CIRT will remove blocks and authorize the machine to be placed back online after the agency ISSPM submits the incident closing documentation and verifies the machine is no longer a threat to the USDA network.

11 The ASOC CIRT Reports to Management

The ASOC CIRT management reporting process is:

- At the end of each business day, the ASOC CIRT analyst will generate an “End of Day” report of all open incidents. The report is produced using the CSIRM database. The daily report is emailed to OCIO senior level management.
- The ASOC CIRT provides a status report on all incidents opened within the reporting week as required for the ASOC Weekly Activity Report (WAR).
- The ASOC CIRT provides an “Escalation Report” to management of open incidents that have aged past the due dates listed in the *Notification and Escalation Process*. The escalation report is produced on a weekly basis or more often as requested by management.



Appendix A. Report of Security Incident to the ASOC CIRT

Ask the caller for complete details when completing this form, and determine the type of incident being reported. Check the box that applies. (Check both boxes if the report will be both PII and equipment lost/stolen.)

Incident involves PII, Privacy or Sensitive Data

Incident involves Lost/Stolen Equipment

If this is an incident that involves PII, obtain specific details about what type of PII and how the incident was discovered. Be sure to answer all of the questions to capture as many details as possible.

SNCC Information	
SNCC tracking number:	
Date and time incident was received by the SNCC:	
Name of SNCC reporting person:	

User / Person Reporting Incident to SNCC	
Name:	
Email Address:	
Work Phone Number:	
Cell Phone Number:	
Agency for which the person works:	



USDA Incident Report

Incident Information	
Date and time, including the Time Zone, of incident:	
Type and number of equipment items lost (include phone number of lost data device (i.e., Blackberry number)):	
Was the device encrypted?	
Address where the incident occurred:	
Did the incident involve PII, proprietary, financial, sensitive or Privacy Act data?	
What was the PII, proprietary, financial, sensitive, or Privacy Act data?	
What type of work does the person reporting the incident do (e.g., management, inspector, loan officer, payroll, scientist, etc.)?	
Overall Severity/Effect Score (see Appendix F for instructions on determining score):	

The ASOC CIRT Notification	
How did SNCC notify the ASOC CIRT?	
Date and time, including the Time Zone, the ASOC CIRT was notified:	

Incident Detailed Notes
<p>Use this section to provide additional notes and important information about the incident being reported.</p> <p>Some questions to keep in mind are:</p> <ul style="list-style-type: none"> ▪ Who was involved (i.e., employee name(s))? ▪ What actually happened? ▪ What are the details about the event? <p>If this was not an equipment loss, what type of incident occurred? (Add notes below to describe the incident.)</p>



Appendix B. USDA Incident Report



Cyber Incident Report USDA0909NNN-AAAA

Section 1: ISSPM Closing

Closing Information		
Agency Incident Number	Name of Person submitting the incident for closing	Date

Section 2: The ASOC-CIRT Incident Notification

Incident Notification	
USDA Incident Number:	
Incident Category Type:	
Incident Description:	
Incident Date/Time Reported:	
Incident Date/Time Occurred:	
USDA IP, Port, Protocol:	
Distant IP, Port, Protocol:	
System/Equipment:	
Location:	
NITC SNCC Number	
US-CERT Number	
How was the incident identified?	
Impact to agency?	
Additional Information provided to USDA-CIRT	
Required Action:	
Complete the Incident Containment Checklist and return to the ASOC-CIRT within 24 hours. Complete final incident report and return to the ASOC-CIRT.	



USDA Incident Report

Provide the User Name, and User Information in the final report.

Please send all updates, information or reports about this incident to Cyber.incidents@ocio.usda.gov

To report an incident or inquire about an incident or event: call 1-866-905-6890 or email Cyber.incidents@ocio.usda.gov 24 hours a day.

Section 3: Contact Information

ISSPM Contact	
ISSPM POC:	
Title:	
E-Mail:	
Office Telephone:	
Cell Phone:	
Technical Contacts	
Technical POC:	
Title:	
E-Mail:	
Office Telephone:	
Cell Phone:	
Other Contact:	
Title:	
E-Mail:	
Office Telephone:	
Cell Phone:	



Section 4: USER Information

Provide the following information for each user involved with this incident.

User Information	
Name:	
Position Title:	
Summary of Duties:	
Does this user have Administrator rights? If So Why?	
E-Mail:	
User-ID:	
Office Telephone:	
Cell Phone:	
Location:	

Section 5: Incident Checklist from Appendix D (SOP-SCD-001)

Complete all checklists. If a block does not apply or the information is not known, complete with N/A.

Section 6: Impact and Scope

Impact	
Determine the Information Security Categorization (FIPS 199/Risk Level)	Low Medium High
Determine the Incident Severity Rating. (See appendix H, SOP-SCD-001)	
Determine the impact this incident has had or will have on your agency.	
Determine whether the activity is criminal in nature.	
Forecast how severely the organization's reputation may be damaged.	
Report the incident to the appropriate internal personnel and external organizations, copy the notification here.	
Identify all other affected/	



USDA Incident Report

compromised systems or machines in agency	
What corrective action was taken to contain affects to compromised machines	

Section 7: Lessons Learned

Lessons Learned	
Could this incident be prevented? How?	
What additional information was required to investigate/ resolve this incident?	
Where was this information available?	

Section 8: Supporting Information

Copy all information used to establish, investigate and close this incident here.

Appendix C. CIRG/PII Incident Packet



COVER SHEET
USDA0809NNNN-XXXX

Core Incident Response Group (CIRG)
Supporting Documentation for Closure

Total pages for this incident – NN



USDA Incident Report

FINAL CLOSURE OF INCIDENT FORM

Official Approving Closure of Incident

Signature(s) Approval Date

Table with 3 columns: The ASOC CIRT Employee closing incident, Date closed with US-CERT, Date closed with USDA.

Section 1: Executive Summary:

Brief Description of Incident:

Actions Taken to Mitigate:

Outstanding Actions:

(INSERT THE NITC-SNCC REPORT HERE AFTER OUTSTANDING ACTIONS)



USDA Incident Report

Section 2: The ASOC CIRT Initial Contact Information

USDA Incident Number:	Date & Time Reported to the ASOC CIRT: YYYY/MM/DD HR:MN AM/PM	Name of the ASOC CIRT taking the report:
US-CERT Number:	Date & Time Reported to US-CERT: YYYY/MM/DD HR:MN AM/PM	
Date & Time SNCC Hotline was notified: YYYY/MM/DD HR:MN AM/PM		Date & Time the incident occurred: YYYY/MM/DD HR/MN AM/PM

INCIDENT CONTACT INFORMATION

Name of person making the report:	
Type of Employee: (Federal, Contractor, etc.)	USDA Agency:
Office Phone Number:	Cell Phone Number:
Email:	Other Contact Info:

IMPACT AND SCOPE

Type of Media or Exposure (i.e. laptop, desktop, PDA, flash drive, website posting, paper based, etc.):	
Property Description:	
Item:	Approximate Value:
Make:	
Personally Identifiable Information (PII) Involved:	
Type of PII:	
Information Security Categorization (FIPS199 / Risk Level – Low, Med, High):	
Potential Affected Population Size [1-99, 100-999, 1000-9999, 10,000 or more]:	
Location of Incident:	
Potential Affected Geographic Area:	
Was the data encrypted? [Yes or No]	
Summary [chronological timeline of the incident and the details surrounding the incident]:	



USDA Incident Report

CONTAINMENT INFORMATION

Describe steps taken to contain the incident.

Section 3: Notification & Communications Plan

Core Incident Response Group Meeting Date:	
Attendees:	

Individuals Notified of the Security Incident	Yes / No	If Yes, who was notified?
Affected USDA Agency ISSPM and/or Agency CIRT:		
Affected USDA Agency CIO:		
USDA ACIO ASOC:		Christopher Lowe
USDA Deputy CIO:		Christopher Lowe
USDA CIO:		Christopher Smith
USDA OIG:		Craig Goscha / Lance Moore
USDA OSEC:		
USDA Physical Security Dept (i.e. GAS, FPO, Bldg Sec):		
Any organization outside of USDA (i.e. local, state or federal law enforcement agency):		
Affected:		
Congress:		
Media / Public:		
Provide Benefits?		
Credit Monitoring?		
Data Breach Analysis:		

Section 4: Meeting Minutes

Incident #:															
Date:															
Location:															
Attendees:	<table border="1"><tr><td>CFO/CIO:</td><td></td></tr><tr><td>ASA (agency)</td><td></td></tr><tr><td>Senior Advisor to Secretary:</td><td></td></tr><tr><td>Deputy CIO:</td><td></td></tr><tr><td>Agency Rep:</td><td></td></tr><tr><td>Agency Rep:</td><td></td></tr><tr><td>Guests:</td><td></td></tr></table>	CFO/CIO:		ASA (agency)		Senior Advisor to Secretary:		Deputy CIO:		Agency Rep:		Agency Rep:		Guests:	
CFO/CIO:															
ASA (agency)															
Senior Advisor to Secretary:															
Deputy CIO:															
Agency Rep:															
Agency Rep:															
Guests:															

I. Call to Order

II. Introductions

III. Presentations

A.

B. Action Items (Follow-Up)

IV. Approval of Minutes

Minutes approved by CIRG with corresponding signature(s) and date.

Signature(s)

Approval Date

V. Adjournment

Meeting notes prepared by:

Appendix D. Incident Response Checklists

Checklists in accordance with NIST SP 800-1, , are provided in this Appendix to assist personnel in handling incidents. Submit checklist(s) used with documentation. Comments may be included in the “Completed” column along with “Yes” or “No” notations.

D.1 Initial Incident Response Checklist

No.	Action	Completed
Detection and Analysis		
1.	Determine whether an incident has occurred.	
1.1	Analyze the precursors and indications.	
1.2	Look for correlating information.	
1.3	Perform research (e.g., search engines, knowledge base).	
1.4	As soon as the handler believes an incident has occurred, begin documenting the investigation and gathering evidence.	
2.	Classify the incident using the categories presented in Table 1 (e.g., denial of service, malicious code, unauthorized access, improper usage, etc.).	
3.	Follow the appropriate incident category checklist. If the incident does not fit into any of the categories, follow the generic checklist.	

Verification Information	
Checklist Used By:	
Date:	
Signature:	

D.2 Generic Incident Response Checklist for Uncategorized Incidents

No.	Action	Completed
Detection and Analysis		
1.	Prioritize handling the incident based on the business impact.	
1.1	Identify which resources have been affected and forecast which resources will be affected.	
1.2	Estimate the current and potential technical effect of the incident (Appendix F).	
1.3	Find the appropriate cell(s) in the prioritization matrix (Appendix G) based on the technical effect and affected resources.	
2.	Report the incident to the appropriate internal personnel and external organizations.	
Containment, Eradication, and Recovery		
3.	Acquire, preserve, secure, and document evidence.	
4.	Contain the incident.	
5.	Eradicate the incident.	
5.1	Identify and mitigate all vulnerabilities that were exploited.	
5.2	Remove malicious code, inappropriate materials, and other components.	
6.	Recover from the incident.	
6.1	Return affected systems to an operationally ready state.	

Verification Information	
Checklist Used By:	
Date:	
Signature:	

D.3 Multiple Component Incident Response Checklist

No.	Action	Completed
Detection and Analysis		
1.	Prioritize handling the incident based on its business impact.	
1.1	Follow the Step 1 instructions for each applicable incident category.	
1.2	Determine the proper course of action for each incident component.	
2.	Report the incident to the appropriate internal personnel and external organizations.	
Containment, Eradication, and Recovery		
3.	Follow the Containment, Eradication, and Recovery steps for each component, based on the results of Step 1.	
Post-Incident Activity		
4.	Create a follow-up report.	
5.	Hold a 'lessons learned' meeting.	

Verification Information	
Checklist Used By:	
Date:	
Signature:	

D.4 Category 1 – Unauthorized Access Incident Response Checklist

Category 1 Unauthorized Access Incident Response Checklist	
Computer/Host Information	
Provide information about all host(s) involved in the incident. Please copy this form for each additional Host.	
Item	Description
USDA Host Name:	
USDA Host IP Address(es):	
USDA PORTS Used:	
Distant Host IP Address(es):	
Distant PORTS Used:	
What are the Make and Model of the Hardware?	
What Operating System and Version is installed?	
What USDA Application/System is used?	
What is the use of this device?	
What Anti-virus software and Version is installed?	
What Firewall and version is installed?	
Was the computer password protected?	
What encryption software and version is installed?	
Does the assigned user have “Administration” rights? If so, why?	

Mitigation		
Tasks	Action to Complete	Date Completed
Locate the USDA computer suspected/ identified as accessed		
Remove the identified computer from the network		
Confirm the unauthorized access.		
Scan the computer with the installed virus protection software.		
Determine the results of the unauthorized access/ files/ information accessed.		
Has the computer name been changed?		
Were new users added to the computer?		
Were any files password protected?		
Are there any workgroup changes on the computer?		
Has the IP configuration been changed?		
Have any printers been added to the computer? Has the default printer been changed?		
Check "My Recent Documents." What documents have been accessed? Have any zip files been created?		
If contamination can not be removed, re-image the machine.		

D.5 Category 1.2 – Lost and Stolen Equipment Incident Response Checklist

Category 1.2 Loss/ Stolen Equipment	
Supervisor Information	
Item	Description
Name:	
Email Address:	
Work Phone Number:	
Cell Phone Number:	
Work Location:	
Verification that PII was not compromised.	Signature:
Equipment Information	
Item	Description
Date and time of Incident including the Time Zone of incident:	
Type and number of equipment items lost (include phone number of lost data device (i.e., Blackberry number):	
Property description:	
Approximate value:	
Make:	
Model & Serial Number:	
Address where the Incident occurred:	
What encryption software and version is installed?	
Was the device password protected?	
What is the use of the equipment?	
If the equipment was a Blackberry or other device that allows for remote wiping of the data, please confirm that the device was flagged for wiping.	
Was the equipment in an unsecured location?	

D.6 Category 2 – Denial of Service Incident Response Checklist

Category 2 Denial of Service Incident Response Checklist
Computer/Host Information
Provide information about all host(s) involved in the incident. Please copy this form for each additional Host.

Item	Description
System Name:	
USDA Host Name:	
USDA Host IP Address(es):	
USDA PORTS Used:	
What Operating System and Version is installed?	
What application systems are installed? Version? (ie: SQL 2005)	
When was the last vulnerability scan run?	
What Operating System and Version is installed?	
What is the Make and Model of the Hardware?	
C & A Data?	
What USDA Application/System is used?	
What is the use of this device?	
What Anti-virus software and Version is installed?	
What Firewall and version is installed?	
Was the computer password protected?	
What encryption software and version is installed?	
Does the assigned user have "Administration" rights? If so, why?	

Mitigation		
Task	Action to Complete	Date Completed
Investigate the success of the denial of access attempts.		
If not contained or discontinued, filter the attack based on analysis of the source.		
If not contained, block the IP/ Ports, if required.		
Move the USDA machine to a new IP, and monitor for activity.		
Review the effectiveness of the corrective action. Continue to monitor to identify renewed attempts of DOS.		

D.7 Category 3 – Malicious Code Incident Response Checklist

Category 3 Malicious Code – Spyware/Malware- Virus/Worm/Trojan Incident Response Checklist	
Computer/Host Information	
Provide information about all host(s) involved in the incident. Please copy this form for each additional Host.	
Item	Description
System Name:	
USDA Host Name:	
USDA Host IP Address(es):	
USDA PORTS Used:	
What Operating System and Version is installed?	
What application systems are installed? Version? (ie: SQL 2005)	
When was the last vulnerability scan run?	
What is the Make and Model of the Hardware?	
C & A Data?	
What Anti-virus software and Version is installed?	
What Firewall and version is installed?	
Was the computer password protected?	
What encryption software and version is installed?	
Who is the System Administrator?	
Email?	
Phone?	
Where is the server/ computer located?	

Mitigation		
<i>This action must be completed and returned to the ASOC CIRT</i>		
Task	Action Taken by the Agency	Date/Time Completed
Locate the USDA computer suspected/ identified as contaminated.		
Remove the identified computer from the network.		
Mitigate network vulnerabilities that were/ could have been exploited by the malicious code.		
Reimage the machine		

D.8 Category 4 – Inappropriate Usage Incident Response Checklist

Category 4 Inappropriate Usage Incident Response Checklist	
Computer/Host Information	
Provide information about all host(s) involved in the incident. Please copy this form for each additional Host.	
Item	Description
USDA Host Name:	
USDA Host IP Address(es):	
USDA PORTS Used:	
What Operating System and Version is installed?	
What application systems are installed? Version? (ie: SQL 2005)	
When was the last vulnerability scan run?	
What is the Make and Model of the Hardware?	
C & A Data?	
What Anti-virus software and Version is installed?	
What Firewall and version is installed?	
Was the computer password protected?	
What encryption software and version is installed?	
Who is the System Administrator?	
Email?	
Phone?	
Where is the server/ computer located?	

Mitigation		
<i>This action must be completed and returned to the ASOC CIRT Incidents</i>		
Task	Action to Complete	Date Completed
Locate the USDA computer suspected / identified as contaminated.		
Remove the identified computer from the network.		
Determine if the activity appears to be criminal in nature.		
Mitigate network vulnerabilities that were/ could have been exploited by inappropriate usage.		
Run Virus detection/removal software. Evaluate for presence of P2P client software and remove if present.		
If Malicious code is found, attempt to capture the code for forensic analysis.		
Report the activity to the appropriate supervisory personnel. If a policy violation has been committed, issue a letter to the employee involved outlining disciplinary action for future violations. Provide a signed copy of the letter with the completed incident report.		
Review the effectiveness of the corrective action to determine if the computer is safe to replace on the network.		

D.9 Category 5 – Brute Force Attacks, Port Scans, Social Engineering, Probes, Attempted Access Incident Response Checklist

Category 5	
Brute Force Attacks, Port Scans, Social Engineering, Probes, Attempted Access Incident Response Checklist	
Computer/Host Information	
Provide information about all host(s) involved in the incident. Please copy this form for each additional Host.	
Item	Description
USDA Host Name:	
USDA Host IP Address(es):	
USDA PORTS Used:	
What Operating System and Version is installed?	
What application systems are installed? Version? (ie: SQL 2005)	
When was the last vulnerability scan run?	
What is the Make and Model of the Hardware?	
C & A Data?	
What Anti-virus software and Version is installed?	
What Firewall and version is installed?	
Was the computer password protected?	
What encryption software and version is installed?	
Who is the System Administrator?	
Email?	
Phone?	
Where is the server/ computer located?	

Mitigation		
Task	Action to Complete	Date Completed
Locate the USDA computer suspected / identified as contaminated.		
Remove the identified computer from the network. If it's an email server, block access and search for spam or malicious named emails.		
Mitigate network vulnerabilities that were / could have been exploited by the malicious code.		
Block the IP/ Ports of the malicious site (if required).		
Run Virus detection/removal software and/or re-image the machine depending on the identification of the malicious code.		
If Malicious code is found, attempt to capture the code for forensic analysis.		
If malicious code can not be removed, re-image the machine.		
Review the effectiveness of the corrective action to determine if the computer is safe to replace on the network.		

D.10 Category 6 – Under Investigation Incident Response Checklist

Category 6 Under Investigation Incident Response Checklist		
Complete applicable tasks. If the investigation reveals the loss or potential loss of computer based information or resources, notify cyber.incidents@usda.gov . The incident may be reclassified with a new US-CERT category and investigation / mitigation requirements.		
Task	Action to Complete	Date Completed
Investigate to determine the type of USDA property and/or materials involved.		
Acquire, preserve, secure and document evidence.		
If computer based resources are involved, remove the computer from the network and notify cyber.incidents@usda.gov for reclassification.		

D.11 24 Hour Incident Containment Checklist

24 Hour Incident Containment Checklist

Provide information about all host(s) involved in the incident. Please copy this form for each additional Host. Must be completed and returned to the ASOC CIRT within 24 hours.

Computer/Host Information		
Item	Description	
User Name		
User Phone		
User Organization		
Does the assigned user have "Administration" rights? If so Why?		
USDA Host name:		
USDA Host IP Addresses:		
USDA PORTS Used:		
Distant Host IP Addresses:		
Distant PORTS Used:		
Make and Model of the Hardware?		
What Operating System and Version is installed?		
What USDA Application/System is used?		
What is the use of this device?		
What Anti-virus software and Version is installed?		
What Firewall and version is installed?		
Was the computer password protected?		
Encryption software and version?		
Containment		
Task	Date Completed	Name of person taking action.
Locate the USDA computer suspected/ identified as contaminated.		
Remove the identified computer from the network.		
Mitigate network vulnerabilities that were/ could have been exploited by the malicious code.		

Appendix E. PII/Sensitive Information Questions Checklist

Scope	Comment
What is the type(s) of PII or Sensitive data compromised?	
How many instances of PII or Sensitive data have been lost (e.g., number of employee performance records, customer loan applications, inspection results, etc.)?	
How many people/entities are involved?	
How many and what type of equipment was involved?	
Was other equipment lost (e.g., removable hard drives, USB drives, printers, security badges, LincPass Cards, etc.)?	
Were PII or sensitive paper based documents lost with the equipment (e.g., copies of reports, lists of passwords, etc.)?	
Did the equipment have wireless capability?	
What data is or could be compromised?	
How is the data stored (e.g., limited compatibility software, hard drive, USB drive, CD, shared files on server, etc.)?	
When was the data last uploaded to a server or backed up?	
Does the lost PII data compromise or point to other PII (e.g., email attachments, URL links, etc.)?	
What other PII or Sensitive data did the user have access to, and were those accesses or passwords compromised?	

Sensitivity	Comment
What is the sensitivity of the data?	
What type of work does the person do?	
Does this person's duty require access to PII or sensitive data at any time?	
Does this person access customer data in the course of their duty?	
What type of customer data does this person access?	
How often is customer data accessed?	
Have USDA personnel or financial data been compromised?	
Could the data pose a possible threat, embarrassment, or privacy compromise to an individual, the USDA, or the US Government?	

Containment	Comment
What containment measures have been taken?	
Was a police report filed?	
Have individuals/entities been notified?	
Was the data and equipment encrypted?	
Was the data and equipment password protected?	
Have passwords and access been changed?	
Have wipe commands and disconnect orders been issued?	
Have scans, patches and re-imaging processes been conducted?	
Have packet captures been forwarded to US-CERT?	
When was the last data synchronized with the central server?	

Verification Information	
Checklist Used By:	
Date:	
Signature:	

Appendix F. Incident Severity Rating

F.1 Current and Projected Effect Ratings

This Appendix is based on NIST SP 800-61, .

Value	Rating	Definition
0.00	None	No effect on a single agency, multiple agencies, or critical infrastructure
0.10	Minimal	Negligible effect on a single agency
0.25	Low	Moderate effect on a single agency
0.50	Medium	Severe effect on a single agency or negligible effect on multiple agencies or critical infrastructure
0.75	High	Moderate effect on multiple agencies or critical infrastructure
1.00	Critical	Severe effect on multiple agencies or critical infrastructure

To assign a severity rating for an incident, organizations should first determine the effect ratings for the incident based on the above table. Two ratings need to be determined for each incident: the current effect and the projected (potential) effect.

F.2 Criticality Ratings

Value	Rating	Definition
0.10	Minimal	Non-critical system (e.g., employee workstations, systems, or infrastructure)
0.25	Low	System or systems that support a single agency's mission (e.g., DNS servers, domain controllers), but are not mission critical
0.50	Medium	System or systems that are mission critical (e.g., payroll system) to a single agency
0.75	High	System or systems that support multiple agencies or sectors of the critical infrastructure (e.g., root DNS servers)
1.00	Critical	System or systems that are mission critical to multiple agencies or critical infrastructure

After setting the effect ratings, organizations should use the above table for assigning a *criticality rating* to the systems involved in the incident.

F.3 Severity Formula

To determine the overall severity rating for an incident, organizations should use the following formula:

Overall Severity/Effect Score = Round ((Current Effect Rating * 2.5) + (Projected Effect Rating * 2.5) + (System Criticality Rating * 5))

Note: "Round" in the above equation means to round to the nearest 100th.

F.4 Severity/Effect Score

Using the resulting overall severity/effect score, organizations can apply the respective overall rating to the incident, as shown in the table below.

Score	Rating
00.00 – 00.99	None
01.00 – 02.49	Minimal
02.50 – 03.74	Low
03.75 – 04.99	Medium
05.00 – 07.49	High
07.50 – 10.00	Critical

Appendix G. NIST SP 800-61, Prioritization Matrices

G.1 Event Prioritization Matrix

Symptom	Denial of Service	Malicious Code	Unauthorized Access	Inappropriate Usage
Files, critical, access attempts	Low	Medium	High	Low
Files, inappropriate content	Low	Medium	Low	High
Host crashes	Medium	Medium	Medium	Low
Port scans, incoming, unusual	High	Low	Medium	Low
Port scans, outgoing, unusual	Low	High	Medium	Low
Utilization, bandwidth, high	High	Medium	Low	Medium
Utilization, email, high	Medium	High	Medium	Medium

G.2 Technical Issue Prioritization Matrix

Criticality of Resources Currently Impacted or Likely To Be Impacted by the Incident			
Current Impact or Likely Future Impact of the Incident	High (e.g., Internet Connectivity, Public Web Servers, Firewalls, Customer Data)	Medium (e.g., System Administrator Workstations, File and Print Servers, XYZ Application Data)	Low (e.g., User Workstations)
Root-level access	15 minutes	30 minutes	1 hour
Unauthorized data modification	15 minutes	30 minutes	2 hours
Unauthorized access to sensitive data	15 minutes	1 hour	1 hour
Unauthorized user-level access	30 minutes	2 hours	4 hours
Services unavailable	30 minutes	2 hours	4 hours
Annoyance	30 minutes	Local IT staff	Local IT staff

G.3 Criminality Prioritization Matrix

Nature of Incident		
Current Impact or Likely Future Impact of the Incident	Criminal Activity	Non-criminal Activity
Major damage to the organization's reputation	<ul style="list-style-type: none"> ▪ Within 15 minutes, initial response begins ▪ Within 1 hour, team contacts public affairs, human resources, legal department, and law enforcement 	<ul style="list-style-type: none"> ▪ Within 1 hour, initial response begins ▪ Within 2 hours, team contacts public affairs and human resources
Minor damage to the organization's reputation	<ul style="list-style-type: none"> ▪ Within 2 hours, initial response begins ▪ Within 4 hours, team contacts human resources, legal department, and law enforcement 	<ul style="list-style-type: none"> ▪ Within 4 hours, initial response begins ▪ Within 8 hours, team contacts human resources
No damage to the organization's reputation	<ul style="list-style-type: none"> ▪ Within 4 hours, initial response begins ▪ Within 8 hours, team contacts human resources, legal department, and law enforcement 	<ul style="list-style-type: none"> ▪ Within 1 day, initial response begins ▪ Within 2 days, team contacts human resources

Appendix H. Acronyms & Abbreviations

Acronyms/abbreviations used in this document are listed below in alphabetical order.

Acronym/Abbreviation	Description
ACIO	Associate Chief Information Officer
ASOC	The “Agriculture Security Operation Center” for “Computer Incident Response Team” = ASOC CIRT
CFU	Computer Forensics Unit
CIO	Chief Information Officer
CIRG	Core Incident Response Group
CIRT	Computer Incident Response Team
CONOPS	Concept of Operations
CSAM	ASOC CIRT Assessment and Management
CSIRM	ASOC CIRT Incident Response Management
DCIO	Deputy Chief Information Officer
DHS	Department of Homeland Security
DM	Department Manual
DNS	Domain Name System
DOS	Denial of Service
FDCC	Federal Desktop Computer Configuration
FISMA	Federal Information Security Management Act of 2002
FS	Forest Service
GFIRST	Government Forum of Incident Response and Security Team
GPS	Global Positioning System
HD	Hard Drive
IDS	Intrusion Detection System
IHDD	Incident Handling Division Director
IP	Internet Protocol
ISP	Internet Service Provider
ISSPM	Information Systems Security Program Manager
IT	Information Technology
JACKE	Joint Agency Cyber Knowledge Exchange
LAN	Local Area Network
NIST	National Institute of Standards and Technology
OCIO	Office of the Chief Information Officer
OIG	Office of Inspector General
OMB	Office of Management and Budget
P2P	Peer-to-Peer
PII	Personal Identifiable Information
POA&M	Plan of Action and Milestone
POC	Point of Contact
SBU	Sensitive But Unclassified

SCD	Security Compliance Division
Acronym/Abbreviation	Description
SLA	Service Level Agreement
SNCC	System Network Control Center
SOP	Standard Operating Procedure
SP	Special Publication
SQL	Structured Query Language
SSH	Secure Socket Shell
TCP/IP	Transmission Control Protocol/Internet Protocol
TSO	Telecommunications Services and Operations Staff
US-CERT	United States Computer Emergency Readiness Team
USDA	United States Department of Agriculture
UTN	Universal Telecommunications Network
WAN	Wide Area Network
WAR	Weekly Activity Report

Appendix I. Approval Signature

The following approval, date and revision reflect the most current the ASOC CIRT SOP.

Approval	
Signature:	
Name:	Christopher Lowe
Title:	Acting Associate CIO for the ASOC CIRT
Date:	1 April 2009
Revision:	9