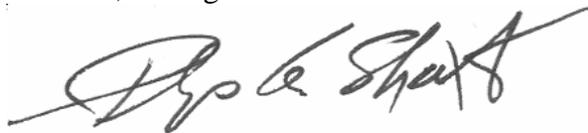


For: FSA Employees and Contractors

FSA Information Security Incident Response Policy and Procedures

Approved by: Deputy Administrator, Management



1 Overview

A Background

The Federal Information Security Management Act of 2002 (FISMA) requires Federal agencies to provide a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support Federal operations and assets.

In support of FISMA; OMB, through Circular A-130 “Management of Federal Information Systems”; supplemented by Appendix III titled, “Security of Federal Automated Information Resources,” commissioned the National Institute of Standards and Technology (NIST) with publishing standard information security controls for Federal information systems. NIST Special Publication (SP) 800-53, “Recommended Security Controls for Federal Information Systems”, catalogs security controls including controls about incident response.

FSA incident response policy and procedures are program-level security controls that are implemented, managed, and executed by FSA Information Security Office (ISO) and are inherited by all FSA information systems.

This notice applies to **all** FSA personnel including the following:

- COC advisors
- COC alternates
- contractors
- full- and part-time employees
- permanent and temporary employees
- STC and COC members.

Disposal Date April 1, 2010	Distribution All FSA employees and contractors; State Offices relay to County Offices
---	---

1 Overview (Continued)

B Purpose

This notice:

- defines the following:
 - information security incident
 - FSA information security incident response policy and procedures
- identifies the following:
 - sources of authority and references
 - roles and responsibilities
- specifies compliance requirements
- provides:
 - support resources
 - definitions (Exhibit 1)
 - incident categories (Exhibit 2)
 - examples of common information security incidents (Exhibit 3).

Notice IRM-417

1 Overview (Continued)

C Contacts

If there are questions about this notice:

- County Offices shall always contact the State Offices
- State Offices shall contact Brian Davies, ITSD, ISO, Information Systems Security Program Manager (ISSPM) and FSA-Incident Response Team (FSA-IRT) coordinator by either of the following:
 - e-mail to **brian.davies@wdc.usda.gov**
 - telephone at 202-720-2419.

State Offices shall contact any of the following FSA-IRT members to assist with information security incidents.

Contacts	
Jeff Wagner, ITSD, ISO, Information System Security Officer (ISSO) by any of the following: <ul style="list-style-type: none">• e-mail to jeff.wagner@kcc.usda.gov• telephone at 816-926-6747• mobile phone at 816-809-6806.	Roger Scaife, ITSD, ISO, ISSO by any of the following: <ul style="list-style-type: none">• e-mail to roger.scaife@wdc.usda.gov• telephone at 202-720-9152• mobile phone at 202-834-3979.
Brian Davies, ITSD, ISO, ISSPM by any of the following: <ul style="list-style-type: none">• e-mail to brian.davies@wdc.usda.gov• telephone at 202-720-2419• mobile phone at 202-391-5571.	Michael Serrone, Chief, ITSD, ISO by any of the following: <ul style="list-style-type: none">• e-mail to michael.serrone@kcc.usda.gov• telephone at 816-926-6567• mobile phone at 816-719-8734.

D Authority and References

Sources of authority and references include the following:

- 6-IRM
- Agriculture Security Operations Center, Computer Incident Response Team (CIRT) Standard Operating Procedures for Reporting Security and Personally Identifiable Information Incidents; Reference: SOP-ASOC-001
- DM 3505-001, USDA Cyber Security Incident Handling Procedures, Chapter 1, Part 1
- E-Government Act of 2002, Pub. L. 107-347, 44 U.S.C. 3531 et seq., Title III, FISMA

1 Overview (Continued)

D Authority and References (Continued)

- NIST SP 800-53 Rev 3, Recommended Security Controls for Federal Information Systems
- NIST SP 800-61 Rev. 1, Computer Security Incident Handling Guide
- NIST SP 800-84, Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities
- OCIO, ITS Security Policy Manual
- OMB Circular A-130, Management of Federal Information Resources, Appendix III, Security of Federal Automated Information Resources
- USDA Incident Notification Plan, September 2007.

2 Roles and Responsibilities

A ISO Roles and Responsibilities

ISO coordinates, manages, implements, executes, and monitors FSA's incident response program.

ISO shall:

- develop, distribute, and periodically review and update incident response policy and procedures
- develop, distribute, and track incident response training of FSA personnel
- test and/or exercise FSA's incident response capability
- implement, manage, and execute FSA's incident capabilities of:
 - handling
 - tracking
 - reporting
- provide incident response support resources.

2 Roles and Responsibilities (Continued)

B Management Officials, Supervisors, Contracting Officer Technical Representatives (COTR's), and Security Liaison Representatives (SLR's)

Management officials, supervisors, contracting officer representatives/COTR's, and SLR's shall assist ISO in implementing, executing, and monitoring FSA's incident response program.

Management and representatives have the responsibility to:

- ensure that policy and procedures are distributed to subordinates
- ensure that applicable FSA personnel complete incident response training
- participate in tests and/or exercises of FSA's incident response capability
- ensure incidents are reported according to policy and procedure
- notify subordinates of incident response support resources.

C All Personnel Roles and Responsibilities

FSA personnel, including COC advisors, COC alternates, contractors, STC and COC members, permanent and temporary, and full- and part-time employees shall:

- execute FSA's incident response program
- be aware of FSA policy, procedures, roles, and responsibilities
- report incidents according to FSA procedures
- prevent incidents by following information security policy and procedures.

3 Incident Response

A Policy

FSA shall:

- develop, distribute, and periodically review/update a formal, documented, incident response **policy** that addresses:
 - purpose
 - scope
 - roles and responsibilities
 - management commitment
 - coordination among organizational entities
 - specific compliance requirements

3 Incident Response (Continued)

A Policy (Continued)

- ensure that the incident response policy is:
 - consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance
 - included as part of the general information security policy for the organization
 - develop, distribute, and periodically review/update formal, documented, incident response **procedures** to facilitate implementing the incident response policy and associated incident response controls
 - ensure that incident response procedures are consistent with the following:
 - applicable laws
 - directives
 - Executive Orders
 - guidance
 - policies
 - regulations
 - standards
- Note:** Incident response procedures can be developed for the security program in general, and a particular information system, when required.
- train FSA personnel in their incident response roles and responsibilities
 - annually:
 - require and provide refresher training
 - test and/or exercise incident response capabilities for FSA to determine effectiveness and document results
 - implement an incident handling capability for security incidents to include:
 - preparation
 - detection and analysis
 - containment
 - eradication
 - recovery

3 Incident Response (Continued)

A Policy (Continued)

- incorporate lessons learned from ongoing incident handling activities into incident response procedures and implement procedures accordingly
- track and document information system security incidents on an ongoing basis by employing automated mechanisms to support incident handling and reporting processes
- promptly report incident information to appropriate authorities including:
 - types of incident information reported
 - content and timeliness of reports
 - a list of designated reporting authorities or organizations that are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance
- ensure that weaknesses and vulnerabilities in the information system are reported to appropriate organizational officials in a timely manner to prevent security incidents
- provide an incident response support resource that offers advice and assistance to users for reporting, handling, and recovering from security incidents including automated mechanisms to increase the availability of incident response-related information and support.

B Incident Reporting Procedures

Incident reporting procedures are established according to Department policy, procedure, standards, and guidance. FSA is serviced by OCIO-ITS; therefore, reporting procedures are also established according to OCIO-ITS Joint Agency procedures.

OCIO Cyber Security shall report incidents to the United States Computer Emergency Readiness Team (US-CERT) within a specified timeframe designated in the US-CERT Concept of Operations for Federal Cyber Security Incident Handling

Notice IRM-417

3 Incident Response (Continued)

B Incident Reporting Procedures (Continued)

If an incident is suspected or detected, the reporting source shall immediately notify FSA-IRT by either of the following:

- Information Security Operations Support (ISOS) staff may be contacted between the hours of 6 a.m. and 6 p.m. c.t. by telephone at 800-255-2434, Option 2, then Option 8
- calling a member of FSA-IRT directly (subparagraph 1 C).

Important: If the reporting source is unable to contact FSA-IRT, call USDA at either of the following:

- 888-926-2373
- 877-PII-2-YOU (877-744-2968).

C Incident Handling Procedures

The following table provides major steps to be performed when handling an incident. Actual steps performed may vary based on the type of incident being handled and nature of individual incidents. Used as a checklist, the following does **not** dictate the exact sequence of steps that should always be followed.

Note: Checklist items may be accomplished by USDA agencies or external organizations other than FSA and may be accomplished formally or informally. ISO maintains updated internal incident handling standard operating procedures.

Step	Action
1	Incident preparation and detection as follows: <ul style="list-style-type: none">• determine whether an incident has occurred• analyze precursors and indications• look for correlating information• perform research• once handler believes an incident has occurred, begin documenting investigation and gather evidence.

3 Incident Response (Continued)

C Incident Handling Procedures (Continued)

Step	Action
2	Incident analysis as follows: <ul style="list-style-type: none"> • classify incident using categories provided by the Department (Exhibit 2) • identify which resources have been affected and forecast which resources will be affected • estimate current and potential technical effect of incident • prioritize handling incident based on business impact • report incident to appropriate internal personnel and external organizations.
3	Incident containment, eradication, and recovery as follows: <ul style="list-style-type: none"> • acquire, preserve, secure, and document evidence • contain incident • eradicate incident • identify and mitigate all vulnerabilities that were exploited • remove malicious code, inappropriate materials, and other components • recover from incident • return affected systems to an operationally ready state • confirm affected systems are functioning normally • if necessary, implement additional monitoring to look for future related activity • create a followup report • communicate lessons learned.
4	Enter incidents into automated database for handling.

D Incident Monitoring and Tracking Procedures

ISO maintains internal standard operating procedures about monitoring and tracking incidents.

All incidents assigned to FSA that receive an incident number from USDA CIRT or US-CERT are monitored and tracked. For any incident without an incident number or not otherwise assigned, ISO chief will make a determination of whether or not an incident will be monitored and tracked.

An access-restricted database has been implemented for the automated monitoring and tracking of FSA incidents. Access is restricted to FSA-IRT members and support staff.

3 Incident Response (Continued)

E Incident Response Testing Procedures

ISO maintains internal standard operating procedures about testing incident response capabilities according to NIST SP 800-84, "Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities."

FSA tests and/or exercises the incident response capability for FSA annually to determine the incident response effectiveness and documents the results.

ISO maintains internal standard operating procedures about training FSA-IRT members.

According to their incident response roles and responsibilities, FSA-IRT members receive specialized training in the following:

- incident response
- reporting
- handling
- monitoring and tracking
- detection
- preparation
- analysis
- containment
- eradication
- recovery
- computer emergency response
- computer forensics
- intrusion detection
- responding to various threat vectors.

FSA-IRT members are **required** to accomplish a minimum of 1 hour of incident response training annually. Training documentation is maintained by ISO chief and individual FSA-IRT members.

4 Compliance and Support Resources

A Compliance

Complying with policy is important to the security of FSA. Failure to comply with any FSA policy may result in administrative action ranging from counseling to removal from FSA, as well as any criminal penalties or financial liability, depending on the noncompliance severity.

4 Compliance and Support Resources (Continued)

B ISO Support Staff

ISOS staff will record initial contact information and file an incident report with FSA-IRT according to standard operating procedures.

Depending on the incident category and severity, ISOS staff may provide handling and mitigation options according to standard operating procedures maintained by ISO.

C Automated Incident Reporting System

Incident reports may be filed by sending an e-mail to fsa.incidents@wdc.usda.gov.

D Computer Forensics Services

ISO provides computer forensics services. All requests **must** be submitted by a second-line supervisor or HRD Employee and Labor Relations staff member directly to ISO chief or FSA ISSPM. All computer forensics service requests will be approved by ISO chief.

Definitions of Terms Used With Incident Responses

Adverse Events

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.

Computer Forensics

Computer forensics is the practice of gathering, retaining, and analyzing computer-related data for investigative purposes in a manner that maintains the integrity of the data.

Computer Security Incident

See Incident.

Computer Security Incident Response Team (CSIRT)

CSIRT is a capability set up for assisting in responding to computer security-related incidents.

Note: Also referred to as any of the following:

- Computer Incident Response Team (CIRT)
- Computer Incident Response Center (CIRC)
- Computer Incident Response Capability (CIRC).

Declaration

A declaration is an assignment of a USDA incident number and FSA beginning its incident handling process. An incident is declared by FSA, another USDA agency, staff office, or IRT that is recognized and documented as being responsible for incident handling.

Denial of Service (DoS)

DoS is an attack that prevents or impairs the authorized use of networks, systems, or applications by exhausting resources.

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 e-mail, and a firewall blocking a connection attempt.

Definitions of Terms Used With Incident Responses (Continued)**Forensics**

See Computer Forensics.

Incident

An incident is any violation or imminent threat of violation of computer security policies, acceptable use, or standard computer security practices. It is also any adverse event whereby some aspect of a computer system is compromised, such as loss of data confidentiality, disruption of data integrity, disruption, or denial of service (loss of availability).

Incident Handling

Incident handling involves the comprehensive management process of receiving incident indications and warnings, identifying the actual incident type, verifying the victim or perpetrator's responsible agency, alerting the agency, reporting, responding to, mitigating, and closing a USDA Cyber Security (USDA CS) incident.

Incident Response

Incident response involves the comprehensive program of incident detection, reporting, preparation, analysis, monitoring, tracking, handling, containment, eradication, recovery, documenting lessons learned, training, and testing.

Malicious Code (malware)

Malware is a virus, worm, Trojan horse, or other code-based malicious entity that successfully infects a host.

Notification

Notification is the formal transmission of declared incident information to the documented incident handling or management personnel in the USDA organization that is experiencing a CS incident.

Oversight

Oversight is the process of ongoing review and follow-up of incident status by the USDA incident handling organizations, staff, or assignees to maintain accurate USDA incident records on the number of incidents declared open, closed, or cancelled. USDA-wide incident oversight is required for record keeping and review of close-out reports, as well as compliance with FISMA.

Definitions of Terms Used With Incident Responses (Continued)**Preparation**

Preparation means establishing an incident response capability so that the organization is ready to respond to incidents and preventing incidents by ensuring that systems, networks, and applications are sufficiently secure.

Prevention

Prevention is the review of alerts, warnings and suspected events from various sources; the continuous system monitoring and review of risk assessments for systems.

Reporting

Reporting is the formal notification of a suspected incident to a Department or FSA official.

Social Engineering

Social engineering is an attempt to trick someone into revealing information (for example, a password) that can be used to gain unauthorized access to or attack systems or networks.

Tracking

Tracking is the process and requirement of maintaining comprehensive records of all incidents from the time of declaration through closure, and providing historical reports to USDA OCIO and OIG.

Threat

A threat is the potential source of an adverse event.

Trojan Horse

A Trojan horse is a non-self-replicating program that seems to have a useful purpose, but in reality has a different, malicious purpose.

Unauthorized Access

Unauthorized access is when a person gains logical or physical access without permission to a network, system, application, data, or other IT resource.

Definitions of Terms Used With Incident Responses (Continued)**Victim**

Victim is a machine that is attacked.

Virus

A virus is a self-replicating program that runs and spreads by modifying other programs or files.

Virus Hoax

A virus hoax is an urgent warning message about a nonexistent virus.

Vulnerability

Vulnerability is a weakness in a system, application, or network that is subject to exploitation or misuse.

Worm

A worm is a self-replicating, self-propagating, self-contained program that uses networking mechanisms to spread itself.

Incident Categories

The following table contains USDA Agency Incident Categories (Defined by US CERT Concept of Operations (CONOPS), NIST SP 800-61, and USDA SOP-ASOC-001).

Category	Example	Description	Priority	FSA Reporting Timeframe to CS
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, other resource (that is, lost or stolen electronic-based resources with PII data, and portable electronic devices PDA, USB devices, etc.), or HSPD-12/LincPass badges.	High	When Detected
2	2.1 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	When Detected
3	3.1 Malicious Code	Successful installation of malicious software (such as, virus, worm, spyware, bots, Trojan horse, or other code-based malicious entity) that infects or affects an operating system or application.	High	When Detected
4	4.1 Improper Usage	Any violation of USDA policy (that is, peer to peer (P2P) activity, viewing inappropriate content on the Internet, or improper electronic transfer of PII).	Medium To High	Within 2 workdays.

Examples of Common Information Security Incidents

The following is a list of common information security incidents:

- Government credit card is lost or stolen
- Government-issued laptop, cell phone, or Blackberry is lost or stolen
- official Government business documents sent through mail or courier do not arrive at intended destination
- official Government business documents sent through mail or courier do not arrive intact at intended destination
- on-screen message that workstation or laptop is infected with a virus
- taking unauthorized action to prohibit or inhibit access to automated information systems
- telephone calls, e-mails, or FAXes requesting unauthorized PII disclosure, sensitive, but unclassified information, sensitive security information, or other access-restricted information
- unauthorized exploration of networked information resources
- unauthorized use of Government information systems.
- unsolicited e-mails that target a specific individual that are frequently characterized by, but not limited to, unique pre-existing knowledge of the individual, such as title or position, unpublished phone number or address, or account numbers
- using P2P applications, such as Morpheus, LimeWire, etc.