USDA COMPUTER INCIDENT RESPONSE PROCEDURES MANUAL
TABLE OF CONTENTS
DM 3505-000

U.S. DEPARTMENT OF AGRICULTURE
WASHINGTON, D.C. 20250

# DEPARTMENTAL MANUAL	**Number:** 3505-000
SUBJECT: USDA Cyber Security Incident Handling Procedures	**DATE:** March 20, 2006 **OPI:** OCIO, Cyber Security

CHAPTER 1
GENERAL INFORMATION

1 PURPOSE

This Departmental Manual establishes policy and procedures for handling Cyber Security (CS) incidents that may compromise the availability, integrity, and confidentiality of Department of Agriculture (USDA) information technology (IT) and telecommunications resources. The purpose of an incident handling policy is to:

a Document, authorize and establish continuing incident handling management standards, disciplines and processes with in the USDA that are acceptable as best practices within law enforcement and the federal CS community;

b Facilitate cooperation and information exchange among all USDA personnel who are responsible for detecting, identifying, declaring and reporting CS incidents; and

c Comply with Federal laws, National Institute of Standards and Technology (NIST) guidance and USDA Office of Inspector General (OIG) recommendations.

2 SPECIAL INSTRUCTIONS/CANCELLATION

This Departmental Manual chapter replaces: DM 3505-000 (10/25/01) and DM 3505-001 (7/15/04). This chapter will be in effect until superseded.

3 SCOPE

This manual applies to all USDA agencies, programs, teams, organizations, appointees, employees, contractors and other entities responsible for USDA systems and data.

4 ABBREVIATIONS

ACIO CS	Associate CIO for Cyber Security
CIO	Chief Information Officer
CS	Cyber Security
DNS	Domain Name Server
DoS	Denial of Service
FBI	Federal Bureau of Investigation
FTP	File Transfer Protocol
I/D	Intrusion Detection
IDS	Intrusion Detection System
IP	Internet Protocol
IRT	Incident response team
ISP	Internet Service Provider
ISSO	Information Systems Security Officer
ISSP	Information Systems Security Program
ISSPM	Information Systems Security Program Manager
IT	Information Technology
OCIO	Office of the Chief Information Officer
OIG	Office of the Inspector General
POC	Point of Contact
OMB	Office of Management & Budget
SA	System Administrator
SOC	Security Operations Center
TSO	Telecommunications Service Organization
US-CERT	United States Computer Emergency Response Team
USDA	United States Department of Agriculture

5 DEFINITIONS

Adverse event – An event that indicates or produces an actual or potential negative consequence to USDA IT systems. Included are: attempted or actual system crashes, network packet floods, unauthorized use or disclosure, defacement of a webpage, and execution of malicious code. [USDA rates LOW and MEDIUM Intrusion Detection reports as undesirable events. HIGH Intrusion Detection reports are considered CS incidents.] Documented and verified adverse events are incidents.

Adware – Any software application, which displays advertising banners while running a program. Adware includes additional code that delivers the ads, which can be viewed through pop-up windows or through a bar that appears on the computer screen. It usually includes code that tracks a user's personal information and passes it on to third parties without the user's authorization or knowledge.

Botnet – A network of compromised machines that can be remotely controlled by an attacker. Due to their immense size (tens of thousands of systems that can be linked together), they pose a severe threat to the Government's IT infrastructure.

Breach - Any illegal penetration or unauthorized access to a computer system that causes damage or has the potential to cause damage.

Chain of Custody - Protection of evidence by each responsible party to ensure against loss, breakage, alteration or unauthorized handling. Protection also includes properly securing, identifying, and dating evidence.

Compromise –The unauthorized disclosure, modification, substitution, or use of sensitive information or the successful action to invade system by getting around its security. A computer has been compromised, for example, when a Trojan Horse has been installed.

Compromise of Integrity –Any unauthorized modification of information or data.

Cyber/Computer Security Incident – A violation or imminent threat of violation of computer security policies, acceptable uses or standard computer security policies. It is also any adverse event whereby some aspect of a computer system is compromised as: loss of data confidentiality; disruption of data integrity; disruption of availability, also known as a denial of service.

Damage –The unauthorized deliberate or accidental physical or logical modification, destruction or removal of information or data from an IT system.

Denial of Service (DoS) – An inability to use system resources due to unavailability; for example, when an attacker has disabled a system, a network worm has saturated network bandwidth, an IP address has been flooded with external messages or the system manager and all other users become locked out of a system.

Event – Any observable or measurable occurrence in a system or network. Events may include, but are not limited to, a user connecting to a file share, a server receiving a request for a Web page, a user sending electronic mail, and firewall blocking a connection attempt.

Finding – An event or occurrence that may cause a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard computer security practices. Findings require agencies or OCIO CS analysis prior to becoming an incident.

Firewall – A system that controls network traffic between two networks to minimize unauthorized traffic or access. Firewalls can protect networks and systems from exploitation of inherent vulnerabilities. Firewalls are frequently used to prevent unauthorized Internet users from accessing private networks connected to the Internet.

Harm – To cause damage, injure or impair IT systems using electronic methods, which can include intangible things such as identity theft.

Incident Closure or Closeout – The last phase of incident handling lifecycle during which the agency ISSPM submits the incident report to ACIO CS for review and comment. Closeout is not final until peer review has been completed and all questions regarding the incident are answered satisfactorily.

Incident (Cyber Security) – A 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. The types of incidents are been classified into LOW, MEDIUM or HIGH levels depending on the severity.

Incident Declaration – The phase of the incident handling lifecycle during which a USDA incident number is assigned and the responsible USDA organization begins its incident handling process. An incident is declared by a USDA agency, staff office, or incident response team (IRT) that is recognized and documented as being responsible for incident handling.

Incident Handling - The comprehensive management process of receiving incident indications and warnings from Intrusion Detection Systems (IDS), United States Computer Emergency Response Team (US-CERT), law enforcement or Internet Service Providers (ISP) that an incident has occurred. It includes identifying the actual incident type, verifying the victim or perpetrator's responsible agency, alerting the agency. It also requires reporting, responding to, mitigating and closing a USDA CS incident.

Incident Notification – This phase of the incident handling lifecycle involves 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.

Incident Oversight – 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.

Incident Preparation – This phase of the incident handling lifecycle involves preparing reports and providing continuous status on the incident.

Incident Prevention – This phase of the incident handling lifecycle involves the review of alerts, warnings and suspected events from various sources. In addition, it involves continuous system monitoring and review of risk assessments for systems with high CS incident rates.

Incident Reporting - This phase involves a formal acknowledgement by the USDA incident handler that a CS incident has occurred and that notification of all personnel responsible for responding to, acting upon, or resolving an incident have been notified. The incident reporting process includes notification of the ACIO CS, USDA Office of the Inspector General (OIG) and US-CERT.

Incident Response – The process of acting upon known identified incidents. The process includes analysis of how the incident occurred actions to contain the incident, eradicate the cause of the incident, repair the damage, and recover from the incident. This phase includes collection and preparation of a lessons learned report and assistance in the development of an incident report.

Incident Tracking – The process and requirement for USDA and its agencies to maintain comprehensive records of all incidents from the time of declaration through closure. USDA and its agencies are required to track incidents and report the status of those incidents periodically to OCIO and OIG.

Intrusion – An unauthorized, inappropriate or illegal activity by insiders or outsiders that can be considered a penetration of a system.

Intruder - A person who is the perpetrator of a computer security incident. Intruders are often referred to as “hackers” or “crackers.” Hackers are highly technical experts who penetrated computer systems; the term crackers refers to the experts with the ability to “crack” computer systems and security barriers. Most of the time “cracker” is used to refer to more notorious intruders and computer criminals. An intruder is a vandal who may be operating from within USDA or attacking from the outside of Department.

Level of Consequence - The impact an incident has on an organization. Impact includes: loss of data; the cost to a USDA agency or mission area; negative consequences to the organization (e.g. damage to reputation); and the magnitude of damage that must be corrected.

Malicious Code – Also known as “Malware” (malicious software), is a computer code or program designed to deny, destroy, modify, or impede a system’s configuration, programs, data files, or routines. Malicious code comes in several forms, including viruses and worms.

Misuse - Unauthorized use of an account, computer or network by an intruder or malicious user (or insider).

Need-to-Know - The necessity for access to, knowledge of, or possession of classified or other sensitive information in order to carry out officially sanctioned duties. Responsibility for determining whether a person’s duties require possession or access to this information rests upon the individual having current possession (or ownership) of the information involved, and not upon the prospective recipient. This principle is applicable whether the prospective recipient is an individual, a contractor, another Federal agency or a foreign government.

Pharming – An exploit of the Domain Name Server (DNS) that tries to or actually transforms the legitimate host name into another IP address. The "pharmer" sets up a website looking similar to a legitimate site and harvests personal information from unsuspecting users. Also known as "DNS cache poisoning."

Phishing – An exploit that imitates legitimate companies' e-mails to entice people to reveal sensitive or private information, or creates a replica of an existing web page to fool a user into submitting personal, financial or password data.

Rootkit – A set of tools used by an attacker after gaining root-level access to a host to conceal the attacker's activities on the host and permit the attacker to maintain root-level access to the host through covert means.

Spyware - Any technology that aids in gathering information about a person or organization without their knowledge. Sometimes this software is called a "spybot" or "tracking software." Spyware is put in someone's computer to secretly gather information about the user, agency or company and relay it to advertisers, foreign governments, and other interested parties. Spyware can be installed as part of a virus, worm, or result from installation of a program. Spyware is often installed without the user's consent as a drive-by download, by clicking on some option of a deceptive pop-up or webpage, adware or e-mail attachment.

Threat –A circumstance, condition, or event with the potential to cause harm to personnel and/or network resources in the form of destruction, disclosure, modification of data, DoS, and/or fraud, waste and abuse. The most common security threats are to network systems. Network security threats include impersonation, eavesdropping, DoS, packet replay/modification.

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

USDA Organization – Any USDA agency, staff office, state and county offices, mission area, project or working group responsible for purchasing, installing and managing IT resources.

Virus – A small piece of malicious code that attaches itself to another program. It does not run on its own, but executes when the host program is run.

Worm – A type of malicious code that acts as an independent program, and can usually replicate itself without human interaction from one system to another.

CHAPTER 1 - PART 1
INCIDENT RESPONSE PROCEDURES

1 BACKGROUND

Networks and information technology (IT) resources are continually vulnerable to illegal/malicious activity or exploitation by internal and external sources. Cyber Security(CS) incident handling is an important and required component of USDA's CS program. CS related threats can exploit vulnerabilities in new or rapidly changing IT. The most common security threats are those that travel through and to networked systems. While it is impossible to eliminate all CS incidents, proactive incident prevention is a critical element of a mature incident management capability.

Preventative procedures such as patch management, firewalls, risk and vulnerability assessments and mitigation can reduce incidents. Not all incidents can be prevented. A flexible and adaptable incident response capability is a necessary part of managing network security threats. Damage to IT systems from a CS incident can occur in a short period. It is essential that all USDA organizations (agencies, staff offices, projects, mission areas, and contractor managed locations) have procedures in place that can be activated immediately. The inability of any USDA organization to recognize and promptly report incidents impacts and potentially compromises the information systems security program (ISSP) efforts of other USDA organizations and their customers.

The Federal Information Security Management Act (FISMA) of 2002 requires Federal agencies to establish incident response and handling capabilities. The law also requires USDA to report incidents to United States Computer Emergency Response Team (US-CERT) (formerly FedCIRC) in the Department of Homeland Security (DHS). Each Federal agency is required to designate a primary and secondary Point of Contact (POC) with US-CERT. The USDA US-CERT POC is located in OCIO CS. Each USDA agency, mission area and staff office is required to communicate with US-CERT through OCIO CS.

The need for an incident handling capability within USDA organizations that crosses agency boundaries has never been greater. This need will continue as long as those who exploit IT exist. Standard reporting and uniform operating procedures permit USDA and US-CERT to be better positioned for assessing risks, addressing vulnerabilities, reducing overall costs and meeting the security challenges of USDA's information infrastructure.

2 POLICY

This chapter establishes the minimum policy and procedures for CS incident handling in USDA. A Department-wide incident handling and tracking capability will be supported and maintained by OCIO CS. Each agency is expected to establish, support and maintain their own internal policies, procedures or team to support prompt, effective and efficient resolution of CS incidents in accordance with the process outlined below. USDA organizations must acknowledge and respond to all CS incidents in accordance with the timeframes in the procedures below. A critical component of successful incident handling is a comprehensive knowledge and inventory of all Internet Protocol (IP) addresses that were delegated to agencies by Telecommunications Service Organization (TSO). Each USDA organization is also expected to control, allocate and maintain accurate electronic records of all assigned IP addresses as required by DR 3300 and assist with notification of emergency personnel. OCIO CS has documented its responsibilities and role to be the POC to US-CERT. OCIO CS will be responsible for notifying OIG and US-CERT of USDA incidents and their closure. US-CERT will acknowledge closure of incidents assigned their tracking number. All USDA organizations will ensure that all incident procedures are followed and that incident reporting is accomplished by the ISSPM through OCIO CS for all OCIO CS assigned incidents, even if they have their own incident response team (IRT). ISSPMs shall be responsible for certifying the accuracy of incident reports.

Policy Exception Requirements – There are no exceptions to the requirement that all agencies report incidents. However, USDA organizations that cannot comply with this policy are required to document shortcomings as formal policy exceptions. The CIO of the agency/staff office/mission area will submit all policy exception requests directly to the ACIO CS. Exceptions to policy will be considered only in terms of implementation timeframes; exceptions will not be granted to the requirement to conform to this policy. USDA organizations cannot wait until CS incidents occur or cannot be closed to request an exception to policy requirements. Exceptions that are approved will be interim in nature and will require that each agency report this Granted Policy Exception

(GPE) as a Plan of Action & Milestones (POA&M) in their FISMA reporting, with a GPE notation, until full compliance is achieved. Interim exceptions expire with each fiscal year. Compliance exceptions that require longer durations must be submitted to the USDA CIO for approval and contain a convincing case for the extension with an updated timeline for completion. Any approved extensions must continue to be documented in the agency's annual FISMA report and quarterly POA&Ms. OCIO CS will monitor all approved exceptions.

3 PROCEDURES

An incident is the act of violating an explicit or implied security policy. The types of activity that are widely recognized as being CS incidents are violations categorized as, but are not limited to, attempts (either failed or successful) to gain unauthorized access to a system or its data, unwanted disruption or denial of service, the unauthorized use of a system for the processing or storage of data, or changes to system hardware, firmware or software characteristics without the owner's knowledge, instructions, and approval. The level of consequence of an incident refers to the relative impact it has on an organization. The types of impact include: loss of data; the loss or theft of information, IT resources, revenue or confidence in a USDA agency or mission area by the general public or customers; or a high level of damage that must be corrected prior to system restoration.

a In USDA, CS incidents shall be declared for the following reasons:

(1) Analysis of intrusion detection system (IDS) reports that are rated as High: Internal, or High: External, and show system compromises in the logs;

(2) Notification by US-CERT of a USDA IP or e-mail address being the cause or victim of malicious or questionable activity;

(3) Alert, notification, or warning from other U. S. Government agencies that USDA IP address(s) is the target or originator of malicious activity;

(4) Notification by the USDA OIG of a complaint that requires CS investigation or technical support;

(5) Complaints by an Internet Service Provider (ISP) that detail specific, prohibited activities by a USDA host, IP address or e-mail address;

(6) Complaints by organizations and companies that exist to ensure copyright protection. These include the Business Software Alliance (BSA), Software & Information Industry Association (SIIA), Recording Industry Association of America (RIAA), The Motion Picture Association of America (MPAA), and companies that monitor the Internet on behalf of movie, video, and music copyright holders;

(7) Floods of viruses, worms and Trojan Horses for which anti-malicious code/anti-virus software is not available. In attacks such as Code Red, Nimda, Slammer, and Blaster One, one USDA incident number will be assigned for the entire process;

(8) Complaints from the public, or other employees that include specific examples or references of inappropriate or illegal use by USDA employees, cooperators, partners or contractors utilizing USDA IT; and

(9) A self-discovery by a USDA organization that meets the definition of an incident (i.e., virus discoveries, criminal actions, etc.)

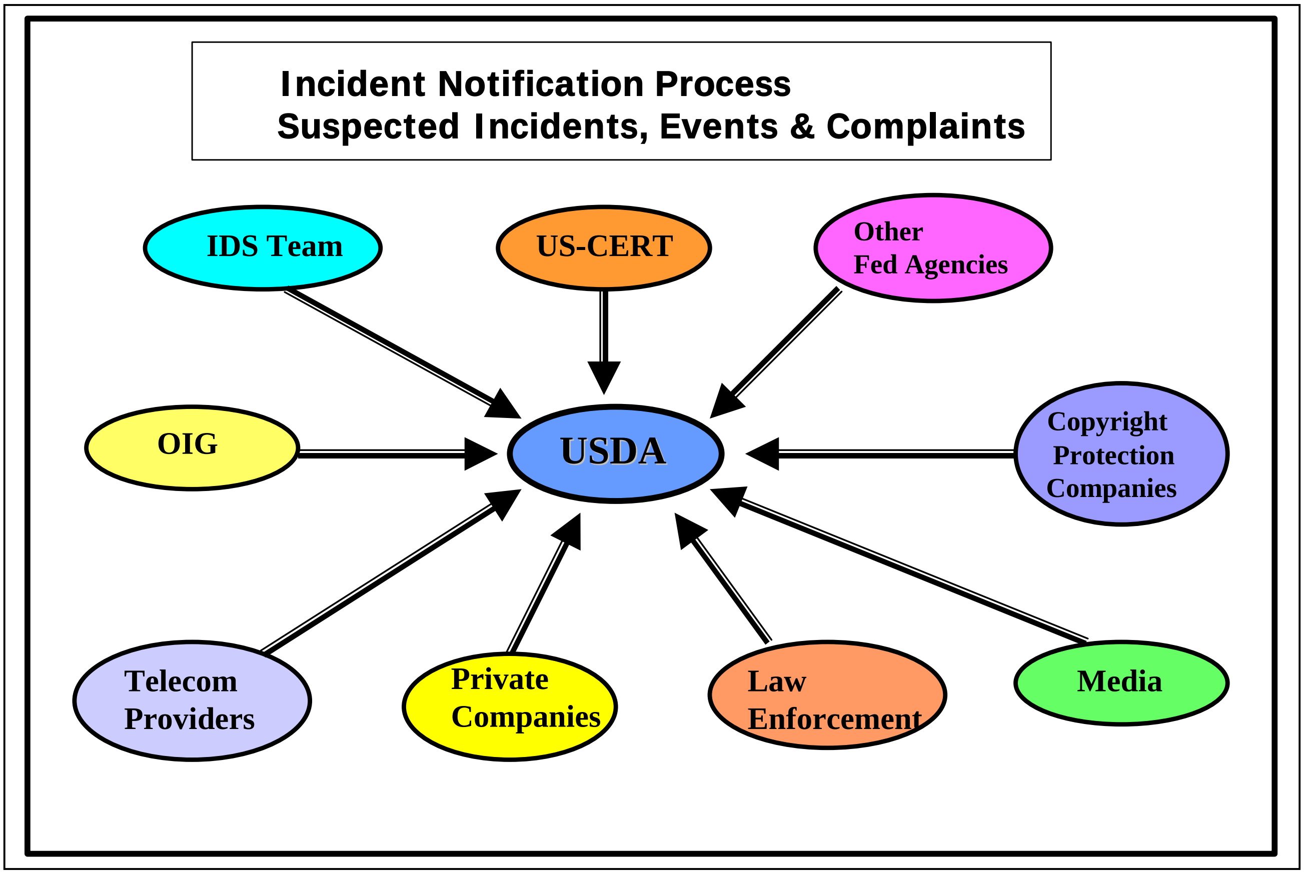

Incident Notification Process
Suspected Incidents, Events & Complaints
IDS Team
US-CERT
Other Fed Agencies
OIG
USDA
Copyright Protection Companies
Telecom Providers
Private Companies
Law Enforcement
Media

Figure 1

b CS incidents are to be declared when they are serious and considered major in nature. They are declared based on the assessment of the gravity of the situation, sensitivity of information threatened or compromised and the potential for harm to USDA.

Outlined below are criteria for the CS incidents (High Level Events) or medium and low level events:

(1) Cyber Security (CS) incidents are High Level Events or US-CERT Priority Level 1 and 2 disruptions that are the most serious and considered 'major' in nature. Because of the gravity of the situation and the high potential for harm to USDA, these incidents should be handled immediately. USDA CS incidents include events, activities, and violations such as: possible life threatening activity, compromise of critical systems or

information, root compromise, child pornography, pornographic trafficking, music/unauthorized software trafficking, any violation of law or agency specific policies or statute. Any activities that are not normally reported to US-CERT but are reported to OIG, Human Resources or law enforcement are defined as CS incidents and will be assigned an incident tracking number (ITN). These incidents will be handled using an accelerated and principals only/limited distribution CS incident response. If criminal proceedings are initiated, the USDA incident handler may not have a need-to-know further details.

Agency ISSPMs who have suspected or confirmed incidents in this category are to immediately report the severity and coordinate the incident response with the ACIO for CS or designate. If the incident remains open for more than 15 days, ACIO CS will send the agency CIO a one-time notification of open incident(s). Each USDA organization’s CIO will respond with corrective actions; a POA&M will also be initiated until incident(s) are closed.

CS incidents include:

- Suspected computer or network break-In (of a USDA computer or by USDA computer);
- USDA website defacements or compromises, including failure to take the website offline or deregister the URL when the website is no longer used or supported by USDA;
- Successful DoS attacks by USDA computers or against USDA computers;
- Computer Virus/Worms/Trojan Horses for which anti-virus software updates are not available or their deployment will be delayed (depending on impact to Agency/Department);
- Detection of malware, including viruses, worms, Trojan Horses or spyware, caused by employees who have declined to bring laptops into the office for upgrades;
- Connection of non-Government computers and servers to the USDA network without authorization or in violation of security policies;

- Unauthorized use of a system for processing or storing non-USDA or prohibited data or information on USDA IT resources, including the establishment and operation of a private or personal business;
- Changes to system hardware, firmware or software without the system owner's authorization;
- Property destruction related to a CS incident (exceeding $100,000);
- Personal theft related to a CS incident (exceeding $100,000);
- Electronic file transfer (EFT) exploitation/manipulation or engaging in Phishing or Pharming;
- Installation, use or sharing of Peer-To-Peer Software;
- Activity including unauthorized or illegal serving out, downloading or sale of copyright material;
- Child pornography;
- Pornography;
- On-Line gambling;
- Attempts to circumvent access to any USDA blocked Web Sites such as pornography, gambling and hate crimes;
- Download, use or sharing of copyright protection music or unauthorized software;
- Misuse of Government property, facilities or services including accepting payment or services to provide access to or use of USDA IT resources in excess of one's authority, such as forwarding spam, engaging in unofficial/unauthorized chat, non-USDA e-mail and instant messaging services; and
- Any violation of law.

Other types of incidents are categorized as adverse CS events and shall not be declared CS incidents unless there is a confirmed compromise of sensitive information, a threat to USDA IT resources or subsequent escalation to a CS Incident.

(2) Medium level Cyber Security (CS) events are potentially serious and should be handled the same day the event

occurs or notification of the event is made to USDA organization (normally in two to four hours of the event). These events can be reported to the agency ISSPM by OCIO CS (when detected in USDA/OCIO), the helpdesk, system administrator (SA) or incident handler(s) or incident response team (CSIRT).

These include:

- Adverse action resulting in employee termination in which the Government computer is neither the tool or target of the action;
- US-CERT priority level 3 activity;
- IDS reports that define activity as medium;
- Unauthorized use of a system for processing or storing USDA data;
- Property destruction related to a CS incident (less than $100,000);
- Personal theft related to a CS incident (less than $100,000);
- Misuse of Government property, facilities and services;
- Unconfirmed computer virus/worms (depending on impact to Agency/Department and if the infection is the result of a security policy violation); and
- Undocumented or unapproved vulnerability scans.

(3) <u>Low level Cyber Security (CS) events</u> are the least severe and should be investigated within three working days after the event occurs. These events can be reported to the agency ISSPM by OCIO CS (when detected in USDA), the helpdesk, SA or incident handler or incident response team (IRT).

Low level CS events include:

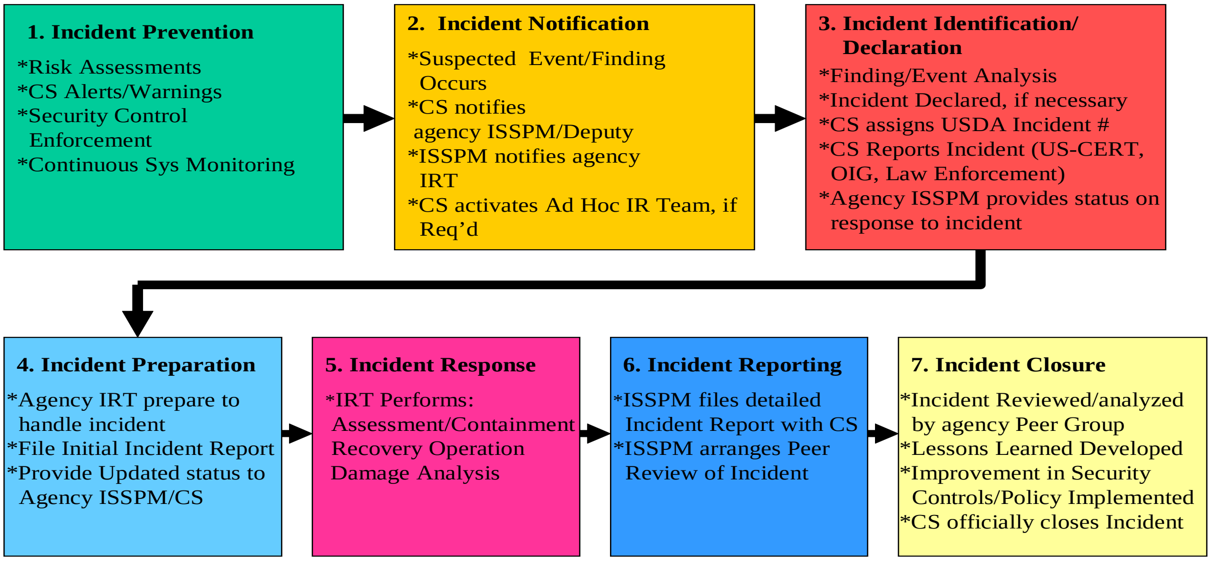
- Loss or compromise of a personal password;
- Suspected sharing of USDA accounts;
- Minor misuse of Government property, facilities and services;
- US-CERT Priority Level 4 Incident Reporting Guideline events;

- Unsuccessful scans/probes (internal & external); and
- Computer virus/worms (depending on impact to Agency/Department).

Agencies and staff offices shall not be required to report actions taken to mitigate adverse events unless requested or instructed to by ACIO CS.

c Incident Handling Phases – The incident handling process is comprised of seven phases that compose an effective response to the overall incident. These phases are designed to ensure that no portion of the process is overlooked and consistency in incident handling is maintained. The steps in each phase are listed below:

Incident Handling Phases



1. Incident Prevention
*Risk Assessments
*CS Alerts/Warnings
*Security Control Enforcement
*Continuous Sys Monitoring

2. Incident Notification
*Suspected Event/Finding Occurs
*CS notifies agency ISSPM/Deputy
*ISSPM notifies agency IRT
*CS activates Ad Hoc IR Team, if Req'd

3. Incident Identification/ Declaration
*Finding/Event Analysis
*Incident Declared, if necessary
*CS assigns USDA Incident #
*CS Reports Incident (US-CERT, OIG, Law Enforcement)
*Agency ISSPM provides status on response to incident

4. Incident Preparation
*Agency IRT prepare to handle incident
*File Initial Incident Report
*Provide Updated status to Agency ISSPM/CS

5. Incident Response
*IRT Performs: Assessment/Containment Recovery Operation Damage Analysis

6. Incident Reporting
*ISSPM files detailed Incident Report with CS
*ISSPM arranges Peer Review of Incident

7. Incident Closure
*Incident Reviewed/analyzed by agency Peer Group
*Lessons Learned Developed
*Improvement in Security Controls/Policy Implemented
*CS officially closes Incident

Figure 2

(1) Incident Prevention – NIST Special Publication 800-61 reminds Federal agencies that keeping the number of incidents low is important to protect their business

processes, mission and reputation. If security controls are insufficient or security policies are not enforced large numbers of incidents can occur with overwhelming consequences for the agency and USDA as an organization. In addition, to prevent incidents each agency and staff office must conduct and keep current risk assessments of systems and applications. These assessments should determine what risks, if any, the combinations of threats and vulnerabilities pose to those systems.

Incident Indications, Alerts & Warnings – OCIO CS will analyze suspected events, complaints and findings from a variety of sources and notify agencies of these occurrences. These sources include: the IDS, US-CERT, other Federal agencies, Federal Trade Commission, OIG, ISP, internal audit or assessment, and private copyright protection organizations. ACIO CS does not automatically declare those communications to be incidents. When OCIO CS and/ or TSO cannot adequately or promptly determine the accuracy of the indications, alerts and warnings by providing their own findings they will defer to the USDA organization to make a finding. When USDA organizations do not respond with a finding within 48 hours, ACIO CS will declare these to be a CS Incident.

(2) Incident Notification - Incident notification is a multi-stage process. Suspected events, complaints and incidents can occur anytime during a 24-hour period. For this reason, USDA has established an Incident Handling Program Manager in OCIO CS. The Incident Handling Program Manager will ensure that USDA organizational personnel are provided with notification of suspected intrusions and receive and document the suspected incident regardless of the source. Each USDA organization will ensure that OCIO CS has a current electronic list of Agency incident contacts in order to ensure that USDA organizations can be reached promptly to resolve incidents effectively. This list will include the agency ISSPM, Deputy ISSPM and the CIO. The ISSPM will be the individual who is responsible for the overall management and resolution of all suspected incidents in agencies and staff offices.

Each USDA organization will establish internal IRT to handle incident data, determine the impact of the incident and act appropriately to limit the damage to the organization and restore normal services. In OCIO, there is a coordinating team Led by OCIO CS staff who will act as the Incident Handling Program Manager. This coordinating team can elect to activate the "Ad Hoc IRT" from all areas of USDA, as required, to assist USDA organizations in responding to major incidents that threaten department resources. Outside resources often provide objectivity and can be helpful to the internal team under pressure to resolve the crisis. The primary role of the coordinating team is to provide guidance and advice to the agency internal IRT without having authority over the team. The agency ISSPM or Deputy ISSPM will notify the agency IRT when a suspected incident is reported by OCIO CS for response and action. Agencies can respond to these incidents using a team already established for this purpose or assign individuals based on the action needed in an ad hoc fashion. However, the designated team should be part of a centralized response by the agency to ensure that the process is consistent across the organization and information is shared at all layers rapidly and effectively.

(3) Incident Identification/Declaration – ACIO CS does not automatically declare findings to be incidents. However, USDA organizations must respond in 48 hours or ACIO CS will declare an incident. ACIO CS will need a finding or status report to prevent their declaration. When ACIO CS declares an incident, a USDA Incident Tracking Number (ITN) is assigned by which the department tracks and responds to requests for information concerning the incident. Agency internal IRTs may also assign their own internal number for tracking purposes. However, all reports must reference the USDA and US-CERT tracking number for reporting purposes. ACIO CS is still the departmental POC for all incidents and is responsible for providing notifications, status reports and close out recommendations to US-CERT, OIG and other oversight authorities. In addition, ACIO CS acts as the POC for notification of the CIO,

responds to requests for status and to Secretarial inquires. OCIO, in coordination with the Office of Communication (OC), is responsible for all dealings with the media and public. USDA agencies are to direct inquiries from these sources to OCIO for response and resolution.

During this phase an incident or incidents may be cancelled. Cancellation occurs when investigations determine that no incident occurred, the IDS provided a "false positive", or information related to the incident was incorrect. A cancelled incident is the same as a closed incident.

(4) Incident Preparation – Each USDA organization will develop their own incident handling procedures and notification trees. Documentation and forms should be available at the outset of each formal incident or event that shall be updated at each stage of the incident and shall be finalized at incident/event conclusion. The USDA CIO, through ACIO CS, will be kept abreast of the status of ongoing major incidents at regular intervals (as events change or progress is made) by the agency until resolution of the incident.

(5) Incident Response – This phase includes the analysis of how the incident happened, how to handle the situation so that it is resolved quickly and to ensure that it does not reoccur. Each USDA organization will develop internal response procedures that support the actions that must be taken in responding to incidents. At a minimum, the internal procedures will include a reporting chain and require the involvement of organizational personnel and OCIO CS. These procedures will also require the preservation of evidence, assessment, containment and recover actions, damage determination, report documentation, lessons learned and the identification of corrective actions required by the agency security program managers and CIO.

There are three definitive sub-phases of this process: assessment and containment, recovery operations, and damage analysis.

Assessment and containment – This process begins as soon as suspicious activity is detected and personnel are designated to take immediate action to resolve the incident. The IRT(s) must be empowered to take containment actions up to and including the immediate shut down of the system to prevent further intrusion or damage to the agency system or other department networks or resources. The Department CIO also has the authority to issue a “Cease and Desist” order to bring a system down should the circumstances dictate or the agency not respond in a expeditious manner to the incident (normally 12 hours). Additionally, the department may issue a port or IP address block internally or externally. This block will remain in place until the incident is officially closed by OCIO. Reporting through the agency ISSPM to OCIO CS will occur simultaneously when accurate information is available, particularly in cases where the preliminary assessment indicates that significant damage to USDA resources may have occurred. Unavailability of any official in the organizational reporting chain is not to delay the continuation of the incident notification or response process.

Recovery operations - Each USDA organization should prioritize those actions that support the smooth recovery of a compromised system(s). In no case should a compromised system, web page or application be returned to normal operation without the approval of ACIO CS. The ISSPM will request that OCIO CS permit the system(s), web page, or application to resume normal operation. OCIO CS reserves the right to further scan the system to ensure that appropriate security is in place to protect the Department. The agency may resume normal operation of the restored system, upon ACIO CS approval and the completion of the IT incident report. The ACIO CS will have 1 working day to respond with the approval or disapproval to return the system to normal operation. If a system is mission critical, the USDA organization can coordinate directly with the ACIO CS for a more immediate system restoration, on a case-by-case basis. If the USDA organization does not receive a response within that time, they can return the system to normal operation provided that they feel adequate security protection is in place to prevent future incidents.

Damage analysis - An analysis of all CS incidents is to be initiated immediately after assessment, containment and recovery actions are completed by each agency ISSPM. The ISSPM will determine if the incident is confined to one agency or multiple agencies and if there is impact to organizations outside USDA. The impact to each system will be analyzed to determine if the control of the system has been compromised. All compromised systems will be disconnected from external communications as soon as possible, but not later than 12 hours from discovery of the incident. Control of a system is lost when the intruder obtains control of the root or system accounts with administrative privileges. A determination is to be made if log files have been erased or compromised.

The ISSPM will initiate the process of estimating the overall economic impact of the incident to the USDA organization and Department in coordination with the system owner/business manager. At a minimum, the estimate will be quantified in terms of loss of system(s) availability, loss of response capability to customers, cost of equipment/software to repair, and hours of personnel associated with the repair or restoration of the system(s). The damage assessment report will be reviewed and concurred on by the system owner/business manager prior to inclusion in the CS Incident report. This information will then be updated in the CS Incident report.

(6) Incident Reporting – involves formal documentation that a CS Incident occurred using the departmental formal reporting process established in this policy. All USDA completed incident report documentation is to be reported to OCIO CS. OCIO CS is responsible for incident reporting to the OIG, US-CERT, and law enforcement for any violation of law. CS incidents are to be tracked and closed in accordance with the requirements of this policy. However, CS incidents that

involve violations of the law or investigation will be separately tracked as resolution may not occur for a protracted period of time.

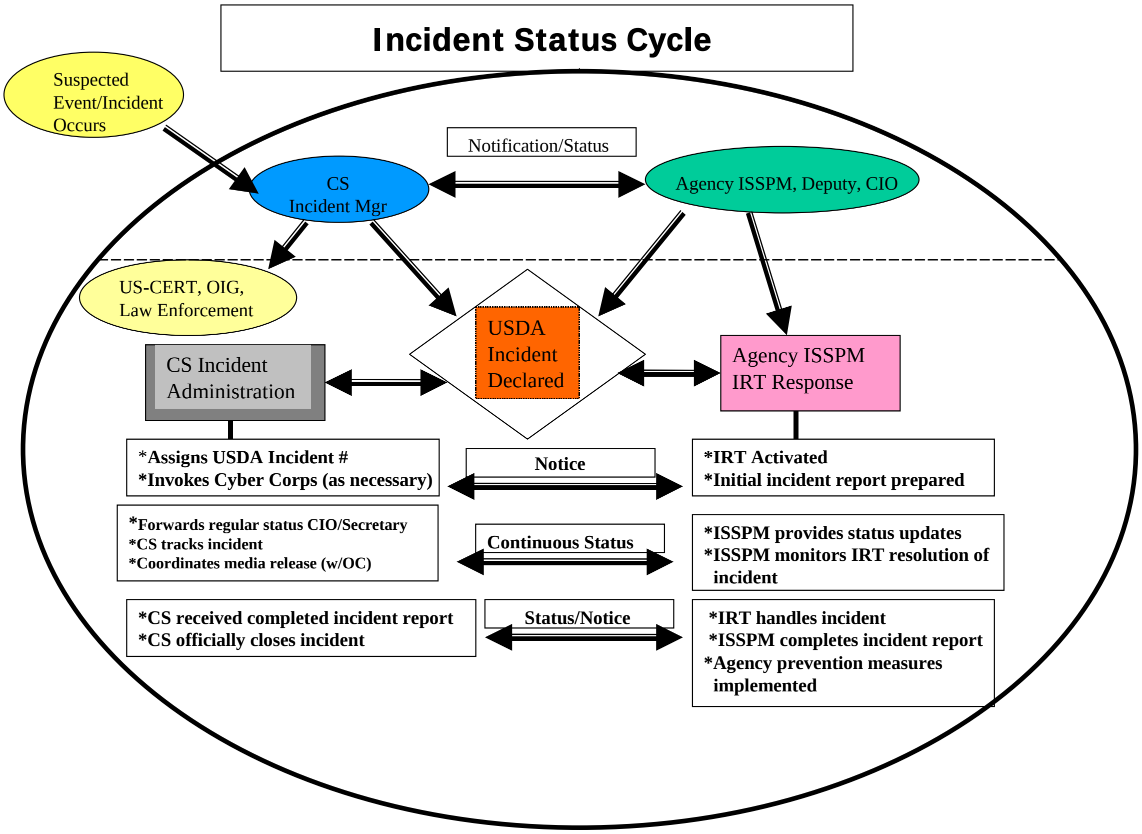

Incident Status Cycle
Suspected Event/Incident Occurs
Notification/Status
CS Incident Mgr
Agency ISSPM, Deputy, CIO
US-CERT, OIG, Law Enforcement
USDA Incident Declared
CS Incident Administration
Agency ISSPM IRT Response
*Assigns USDA Incident #
*Invokes Cyber Corps (as necessary)
Notice
*IRT Activated
*Initial incident report prepared
*Forwards regular status CIO/Secretary
*CS tracks incident
*Coordinates media release (w/OC)
Continuous Status
*ISSPM provides status updates
*ISSPM monitors IRT resolution of incident
*CS received completed incident report
*CS officially closes incident
Status/Notice
*IRT handles incident
*ISSPM completes incident report
*Agency prevention measures implemented

Figure 3

(7) Incident Closure – This process occurs when an agency IRT or manager prepares the incident report based on internal peer review of the incident, and lessons learned are developed and documented. The lessons learned are noted on the formal incident reporting form. OCIO CS shall conduct an internal peer review. If the peer review recommends closure, OCIO CS shall update its records to document closure and request close-out approval from US-CERT.

c Law Enforcement Responsibilities. Threats of harm to a USDA employee or contractor at the official duty station by someone using computer e-mail are a serious type of CS incident. All acts of violence should be promptly reported to supervisors or managers and in the case of an emergency, directly reported to the USDA Local Security Guard Command Center. Any agency ISSPM or representative who receives a report of a threat using electronic equipment should complete an intrusion report, Appendix A, and forward the information to ACIO CS for referral to the OIG. The OIG regards threats using computers as "Workplace Violence". Incidents are referred to the FBI Violent Crimes Unit. More information on Workplace Violence can be obtained from the Violence Prevention Program Website http://www.usda.gov/da/workviolence.htm.

All CS events, deemed major in nature by ACIO CS involving computer systems, websites and applications, are also reported to the OIG. The OIG will review the case (incident) and routinely advise ACIO CS if criminal referral is necessary and of the disposition within 30 days from receipt of the official report. Possible disposition includes: internal investigation, referral to the FBI, or no action by the OIG. In cases of no OIG criminal referral, the USDA organization shall be responsible for handling the incident.

The ACIO for CS, through the CIO and the Secretary, can escalate the matter to the OIG for accelerated support and case disposition in major CS incidents involving a high threat magnitude. In those instances, the OIG will respond within 5 working days from receipt of the official report.

f Incident Response Forms, Contact Lists and Time Frames. All USDA organizations must use the incident reporting forms and contact lists in the Appendices in order to properly respond to CS incidents. Each form has time frames for required agency action.

(1) CS Incident Report (Appendix A) is to be used by the ISSPM or Deputy to update major incident information throughout the entire incident response process. The final report is to be completed not later than 15 days from official notification of each major IT Incident.

(2) Agency ISSPM/Deputy ISSPM/CIO Contact List (Appendix B) contains the agency CS Incident contact information. Each agency/mission area is responsible for providing this list to OCIO CS. OCIO CS will maintain

this list electronically and use this list in their CS incident notification process. This list should include the agency ISSPM, Deputy ISSPM and CIO as the contacts responsible for maintaining/operating agency systems/networks. All individuals identified should have the technical knowledge to support USDA's overall incident response program effectively and provide internal notification to agency officials when major IT Incidents occur. The accuracy of the names, phone numbers and e-mail addresses is the responsibility of each USDA organization; agency ISSPMs will review and update this information as necessary.

4 RESPONSIBILITIES

a <u>The USDA Chief Information Officer and Deputy will:</u>

(1) Be notified immediately after confirmation that a High level CS incident has declared and assigned a USDA CS incident tracking number;
(2) Have final authority on all decisions relating to the management/response to an Major CS incident;
(3) Be responsible for notifying the Secretary all CS incidents that could become the focus of media or administration interest and provide regular updates based on the gravity of the threat; and
(4) Make determinations regarding release of information consistent with applicable Federal Statutes or regulations and serve as the contact point with the media in coordination with the Office of Communications.

b <u>The Associate Chief Information Officer for Cyber Security will:</u>

(1) Function as the Department ISSO;
(2) Coordinate incident handling management of all USDA/OCIO declared CS incidents with oversight authority to ensure that all reports and responses are prepared, appropriate personnel are involved, appropriate organizations are contacted and proper actions are taken to resolve the incident;
(3) Provide technical assistance to the OIG in support of case investigations;

(4) Notify the CIO immediately after confirmation that a CS Incident has occurred;

(5) Receive reports of suspected CS incidents from the following sources:

(a) US-CERT and other internal or external intelligence sources;

(b) ISSPM/Agency representatives;

(c) CS system engineers; or

(d) Agency employees.

(6) Review all field incident intelligence, facts surrounding the case and Level of Consequence. In coordination with the Agency ISSPM/representative, OCIO CS will make a corporate decision concerning countermeasures. Countermeasures can include a request to the SOC for blocking some/all system activity or monitoring of the system by agency engineers;

(7) Assemble and deploy the "Ad Hoc IRT" to augment agency incident response or to protect departmental information assets, if required;

(8) Review all agency requests for compromised systems/applications to ensure systems have been adequately patched/updated with security control prior to resumption of normal operations. In addition, review with the SOC the results of system scans. Approve/disapprove system/application/web page return to normal operation within 24 hours of formal agency request;

(9) Be responsible for notifying the CIO with information concerning all CS incidents; provide regular updates based on the gravity of threat;

(10) Escalate as necessary High level CS incident cases with Secretarial interest to the OIG;

(11) In cases of illegal/inappropriate activities, refer the case to the agency for administrative actions against employees/contractors, if the OIG elects not to investigate;

(12) Assure that this procedure is modified as necessary, disseminated and enforced on behalf of the CIO;

(13) Serve as the Department POC for collecting and analyzing information on incidents;

(14) Review and identify agencies that are responsible for compromises using the current centralized listing of all IP address ranges for all USDA activities;

(15) Maintain a current telephone and e-mail listing of all agency ISSPMs and their deputies;

(16) Maintain contact with internal/external parties and provide whatever assistance is needed to ensure that activities required to resolve a CS incident are taken;

(17) Review all USDA IT intrusion reports as received from reports from Firewalls/IDS;

(18) Coordinate with agencies to make an agency decision regarding the CS Incident. Possible decisions include: shut down of system, SOC blocking of external/internal activity, or careful monitoring of affected system;

(19) Assign an USDA ITN to each case. Report the incident electronically to US-CERT for review and action. US-CERT will assign an incident number, review the case and provide recommended actions via e-mail; forward the US-CERT information to the agency ISSPM;

(20) Coordinate with the SOC the deployment of the ad hoc IRT composed of ISSPMs to respond to CS incidents, when required;

(21) Advise and assist the affected agency ISSPM in the assessment and containment actions, as necessary;

(22) Provide a consolidated report on all open agency CS incidents weekly with progress on agency resolutions;

(23) Provide progress reports on all open incidents weekly;

(24) Send an electronic report daily to ISSPMs on penetration exploits that are fast paced; more routine penetration exploits will be reported weekly to the ISSPMs via e-mail;

(25) Assist in the population a current electronic database of all CS incidents and events; OCIO CS will use this database for tracking and reporting purposes;

(26) Assist the agency ISSPM with the incident response and preparation of all CS incident reports, if required;

(27) Ensure that incident handling actions taken are in accordance with established policies and procedures including incident close out; and

(28) Provide copies of the latest information on security products, breaches and alerts to the agency ISSPMs to increase their level of security awareness.

c The OCIO, CS Security Operations Center (SOC) will:

(1) Provide a POC for formally receiving notification or notifying ACIO CS of potential or actual CS incidents, 24 hours a day, seven days per week;
(2) Notify ACIO CS of potential incidents via e-mail and copy the appropriate Agency ISSPM;
(3) Manage and monitor all Departmental network backbone nodes on a 24-hour basis for network incidents/intrusions;
(4) In collaboration with OCIO CS, ensure that compromised systems have been patched and scanned before incident closure and approval to return to the network or before removal of blocked IP addresses;
(5) Provide USDA organization incident handlers and ISSPMs with technical expertise that will enable them to correctly complete the US-CERT or USDA incident report documents;
(6) Review IDS procedures including IDS reporting formats to ensure that they are meaningful to the recipients and initiate changes in the IDS reports and firewall configurations to reduce intrusions; and
(7) Survey the commercial market for the latest IDS/IPS software/hardware enhancements to ensure that USDA systems are continuously protected by an updated system.

d The Office of the Inspector General will:

(1) Provide notification of non-criminal case disposition electronically to the ACIO CS (Unless such case involves the OCIO directly, in which case only the CIO will be briefed on case disposition. Possible disposition includes: internal investigation, referral to the FBI or no action. Case disposition will be noted in the notification;
(2) Ensure that CS incidents involving threats are forwarded to the FBI, Violent Crimes Unit for action. Notification will be provided to ACIO CS of this action;

(3) Provide accelerated support and investigative assistance to the ACIO CS on all CS incidents involving a high level of magnitude as determined by the Secretary. Provide case disposition notification within 5 days from receipt of official report to include proposed investigative actions and time frames;

(4) Review and approve all USDA agencies forensic lab equipment, software and procedures;

(5) Advise ACIO CS of any investigative actions involving routine CS incidents which do not pose an immediate risk to USDA assets and on a quarterly basis; supply updates on pending cases, as often as a significant development occurs; and

(6) Provide CS intelligence information when received to the ACIO CS.

e <u>USDA Organization (Agency, Staff Office, Program Office) Chief Information Officer will:</u>

(1) Be responsible for ensuring incident handling within the organization is accomplished by:

(a) Ensuring that incident response personnel are assigned, trained, and understand their responsibilities in the organization's incident handling process;

(b) Providing ACIO CS with the names, phone numbers, e-mail addresses of the organizational personnel responsible for incident handling;

(c) Monitoring, reviewing, approving and ensuring timely incident closure;

(d) Providing adequate resources and support enabling the organization's ISSPM to comply with the requirements of this policy; and

(e) Documenting, establishing, and implementing internal tactical procedures for reporting and responding to incidents to initiate and/or request assistance in complying with this directive;

(2) Ensure procedures include the system shutdown and mitigation actions necessary to safeguard agency systems/information assets. In all cases, the safety of USDA information assets must take priority over system availability;

(3) Respond to requests from the ACIO CS for administrative action against agency

personnel/contractors as a result of unauthorized or illegal CS incidents;

(4) Establish and maintain an agency forensic capability sufficient to gather, collect, and preserve computer evidence when requested by either OIG or CS. (Note: the OIG will review and approve all agency forensic processes and procedures.);

(5) Assign telecommunications and security personnel to the agency Cyber Security Incident response team (CSIRT) as needed;

(6) Ensure that an accurate electronic listing of all IP addresses assigned to all agency activities is maintained and made available to the ISSPM, updated as changes occur and sent to OCIO CS on a monthly basis;

(7) Take the appropriate containment actions to provide adequate security in the agency environment; assume the ultimate responsibility for final resolution of all CS incidents;

(8) Collaborate with OCIO incident handling personnel promptly in making the necessary corporate and organizational level incident containment decisions;

(9) Ensure that the agency ISSPM is actively engaged in the incident process from the outset; delegating backup personnel to act for the ISSPM in their absence to handle incident responsibilities;

(10) Establish an agency IRT with the necessary skills and knowledge to quickly respond to agency threats; the organization’s ISSPM/IT staff will be responsible for this team;

(11) Make certain that system administrators, in collaboration with the organization’s ISSPM, rapidly implement the actions required to mitigate or correct any identified incident and perform interim/follow-up activities until the incident is officially closed;

(12) Assure that all respective SA, IT personnel, and agency employees are aware of the requirement to report all suspected computer attacks, virus, threats or suspicious activity to ACIO CS;

(13) Run scans on affected IP address to ensure any vulnerabilities are corrected; false positives need to be verified with OCIO CS;

(14) Request approval from the ACIO CS to return compromised systems/applications to operational

status; ensure that compromised systems/applications remain off line and disconnected from the Internet until approval is received;

(15) Ensure that system owners/business managers participate in the High level CS incident damage assessment process with regard to determination of the value/sensitivity of information and review/concurrence in the final damage report;

(16) Ensure that a privacy determination is performed to ascertain if any individual's privacy has been compromised;

(17) Determine loss of program support of the affected system;

(18) Provide oversight in the development and completion of appropriate incident reporting documentation including the formal reports identified in the figures and Appendix A of this regulation within the required time frames; and

(19) Make certain that mitigation and countermeasure actions are taken to prevent CS incident recurrences, including a formal POA&M to cover all high level intrusions that cannot be corrected immediately; and Ensure that internal controls surrounding the CS incident have been evaluated and updated as necessary to prevent the recurrence of the incident. Document this evaluation and the conclusions reached and make available to OCIO CS upon request.

f The Agency Information Systems Security Program Managers (ISSPM)/designate will:

(1) Manage and act as the focal point for the agency in the review, containment and final resolution of all CS incidents;

(2) Serve as the agency POC for all law enforcement investigations of CS incidents that were not taken on by the OIG;

(3) Promptly report and refer CS incidents involving employee threats (made or received by USDA employees/contractors) to the OIG for investigation and possible referral. The threatening e-mail (s) should be printed and faxed to the designated OIG office and the Departmental ISSPM. The printed copies will be

kept in a locked file cabinet or safe for evidentiary purposes;

(4) Ensure that all members of the organization's IRT and other incident handlers are provided with copies of all USDA CS policies and that they understand the requirements;

(5) Review and update the Agency incident contact list every as necessary to ensure accuracy of the data. Send all changes electronically to OCIO CS to use in incident notification action;

(6) Ensure that all US-CERT emergency advisories, alerts or notifications are promptly forwarded to individuals responsible for organizational systems; act as an advisor to agency IT managers regarding CS products/solutions based on own knowledge or information received from OCIO CS;

(7) Maintain a current and accurate electronic listing of IP addresses assigned to all agency activities and update as changes occur; this listing will be furnished to OCIO CS and TSO monthly and updated as changes occur;

(8) Review all intelligence reports on USDA CS incidents from all sources and in coordination with OCIO CS promptly make corporate and agency containment decisions to protect USDA IT assets;

(9) Electronically file a CS Incident report, Appendix A, within 24 hours of discovery of an event with ACIO CS, Departmental ISSPM/Deputy; provide required information in this report including IP address, type of information being processed and preliminary incident information;

(10) Begin the rapid coordination of CS incident assessment, containment, recovery, and damage analysis actions for compromised systems/applications/web pages;

(11) Provide immediate notification to the agency IRT of the incident and facts surrounding the case; participate in the overall actions of the team to effectively respond to each intrusion; take an active role in ensuring that IRT members are trained and responsive to high level intrusions;

(12) Update the CS incident report and include all required general, contact and host information, incident category data, security tools in place, and detailed descriptions of the incident as soon as possible during the assessment and containment process. Provide

verbal status updates when significant changes occur in the incident status to the Departmental ISSPM. The final report should also include agency internal controls evaluated and any changes to such controls to prevent recurrence of the same or similar incident. Interim reports using this form will be provided electronically to the Departmental ISSPM/Deputy to provide confirmed status on changes in each high level incident. Each report that is an update should be noted as such at the top. The completed electronic report is due to ACIO CS 15 business days after discovery of the incident or event and prior to the return of the compromised system/application to normal operation unless the incident involves law enforcement or adverse action which prohibits release of information. Incidents assigned to law enforcement or human resources without projected close out date will be labeled "Suspended";

(13) In coordination with the respective SA, monitor the compromised system/application if shutdown has not occurred. If the level of consequence escalates, the ISSPM will take further containment actions to include:

- Shut down or render the system unavailable to the attacker, to preclude further intrusion or damage. For systems that need to be shutdown, always bring the system to a halted state and never reboot during shutdown of a compromised system;
- Examine each affected system to determine what changes occurred, such as the addition of new user identifications or software; and
- Conduct diagnostic testing on the compromised system(s) to determine the security status using scanning tools;

(14) In concert with the SA, ensure that the penetrated system is kept offline and disconnected from the network until it has been determined how the intrusion occurred and until the vulnerabilities that allowed the penetration have been corrected or disabled. The ISSPM will make certain that log files are copied to another unaffected system. Reboot of the system will be controlled and done in "single-user mode" only;

(15) In coordination with the SA, ensure that vendor's guidelines and instructions for restarting mainframes or clustered minicomputer systems are followed. The

original operating system software will be used that represents a "trusted backup" of the operating system prior to the intrusion. All necessary system patches and authorized application software will then be reloaded. All user accounts and system privileges need to be verified for validity prior to reloading. A scan tool will be run on the system by the agency to ensure that the system is ready for operation and secure. Note all system operating software, patches, authorized applications software and data backup tapes should always be stored in a secure location in the event a system restoration is necessary. System data should be backed up on a routine basis dictated by the value or sensitivity of the information;

(16) Ensure that a proper "chain of custody" is maintained as outlined below to support the government's responsibility to prosecute intruders. Work with the SA to ensure that two backup tapes are created. These tapes will be labeled with the date, time, and description of data and signature of the person creating the tape. The ISSPM will maintain these tapes in a safe or locked file cabinet with a signed receipt that the tapes have not been reused. The original tape will be provided to investigating authorities; the second copy will be retained by the ISSPM. It is strongly recommended that a witness be present to document and attest to the events that occurred in the process of protecting evidence;

(17) Upon notification by the respective SA that the system is secure and ready for normal operation, the ISSPM will advise the ACIO CS of system recovery and request approval to resume normal operation;

(18) In concert with the systems owner or IT business manager, make a determination on the value/sensitivity of the data to the agency mission. Collaboratively develop a damage determination based on an analysis of the incident. This analysis should include the type of products used by the intruder, any apparent File Transfer Protocol (FTP)s of data, and the extent of the intrusion. This information should be used as the basis for a decision on the known potential for damage to the system. The damage determination should also be quantified in terms of loss of system availability, loss of response capability to

customer, cost of repairing hardware/software and the hours of personnel associated with repair or restoration of the system;

(19) Perform a privacy analysis to determine if individual privacy data has been compromised; if so determine the extent of the damage and advise ACIO CS;

(20) Report all suspected CS incidents to the ACIO CS to ensure that incidents are reported formally;

(21) Ensure that all CS incident reports are completed and filed in following the formats and time frames outlined in the previous Policy section, Incident Response Forms, contact lists and time frames; and

(22) Retain all incident report information, evidence tapes and other related materials in a safe or locking file cabinet; act as the official agency repository for all CS incidents.

g The Agency Systems Administrators will:

(1) In coordination with the agency ISSPM, take actions to effectively assess, contain, and recover from all CS incidents; examine the compromised system to determine what changes occurred to the system as outlined in the duties of the agency ISSPM. Remove all unknown code and software from the compromised system;

(2) Actively participate, if requested, in the internal IRT and provide subject matter expert advice in the handling of CS incidents to the agency ISSPM;

(3) Rebuild the compromised system, as outlined in the ISSPM duties above, conduct system scans, ensure that adequate security controls and countermeasures are in place or implemented and notify the agency ISSPM when the system is secure and ready to resume normal operation;

(4) Ensure that all system patches and updates have been applied;

(5) Test the system to determine that vulnerabilities have been corrected or adequately mitigated;

(6) Provide the results of the system test to the agency ISSPM to validate that the system has been restored to a trusted operating state;

(7) Assist the agency ISSPM in any research or investigation required to determine the extent of any damage done

or the impact of CS incident/event on the system(s) administered;

(8) Preserve and protect the evidence compiled as a result of the investigation or research;

(9) Ensure that forensic evidence has been maintained; and

(10) Report any suspected CS Incident to the agency ISSPM and ACIO CS immediately upon learning of the incident.

h <u>All Agency Employees will:</u>

Report all suspicious computer related activities immediately when detected on USDA Systems to the responsible SA, agency ISSPM or helpdesk personnel for investigation and determination of whether an incident has occurred or is in process.

- END -

APPENDIX A

IT INCIDENT REPORT FORM

THIS FORM MUST BE COMPLETED WITHIN 30 DAYS OF DISCOVERY OF AN IT INCIDENT. (The agency ISSPM is responsible for gathering pertinent information and completing this form.)

I. GENERAL INFORMATION [Section I, must be completed entirely]

USDA Incident Number: ___________ Date: ____________

Organization Name: _________________________________

US-CERT Incident Number: ________________

Reporting Site Organization Name:
____

Domain Name: _____________________________________

Brief Description of the affected organization: (Duties, Responsiblities)
____
____

II. CONTACT INFORMATION [* means section/item must be completed]

***** Primary Contact: ________________________
E-Mail Address: _______________________________
Telephone number: _________________________
Cell Phone Number: ______________ FAX number: ___________
Pager number: _________
Home telephone number: ________________

* Secondary Contact: _______________________
E-Mail Address: ______________________________
Telephone number: _________________________
Cell Phone Number: ______________ FAX number: ___________
Pager number: _________
Home telephone number: ________________
Secure communication Channel (yes/no):

ISSPM Name: ___________________________
E-Mail Address: ________________________________
Telephone number: __________________________
Cell Phone Number: _______________ FAX number: ____________

Pager number: __________
Home telephone number: ________________
Secure communication Channel (yes/no):

Contact from other site(s) involved in this incident

Site name: ________________________________
Contact name: __________________________________
E-Mail address: ______________________
Phone Number: _____________
Pager Number_____________
FAX Number: ________________
Security communication channel (Yes/NO):

***** Information about other USDA contacts:
USDA Organization:_________________
Organization Address: ___________________________________
Contact Name: E-Mail Address: ________________________________
Telephone number: __________________________
FAX number: ____________

***** Contact Information about site through which incident occurred:
Site name: ________________________________
Contact name: __________________________________
E-Mail address: ______________________
Phone Number: _____________
Pager Number_____________
FAX Number: ________________
Security communication channel (Yes/NO):

***** Contact Information about site from which incident began:
Site name: ________________________________
Contact name: __________________________________
E-Mail address: ______________________
Phone Number: _____________
Pager Number_____________

FAX Number: _______________
Security communication channel (Yes/NO):
Domain Name:
____

Contact Information about USDA ISSPM or OIG contact(s):
Contact name: ________________________________
E-Mail address: _____________________
Phone Number: ____________
Pager Number____________
FAX Number: _______________

III. HOST INFORMATION [Section III, must be completed entirely]

Please provide information about all host(s) involved in the incident. Each host shall be listed separately.

Host name: _________________________
IP Addresses: ____________________________________
Vendor hardware: _______________________
Operating System and version: ____________________

Security patches applied/installed as currently recommended by the vendor. List version and date of installation. (Please provide on separate sheet of paper.)

Function(s) of the involved host:
____
Router: _________________________
Server: ____
Mail Hub: ________________________
DNS - external or internal: _____________________________

Where on the network is the involved host? - Backbone; subnet:
____
____
____

Nature of the information at risk on the involved host - configuration, proprietary, personnel, financial, Privacy Act.
____

____
____

Time zone of the involved host: ____________________
Were clocks synchronized? (Yes / No)

Was the host the source or victim of the attack or both:
____

Was this host compromised as a result of the attack? (Yes / No)
# of users affected ____________ Hours system down__________
Estimated $ Loss _____________

IV. INCIDENT CATEGORIES

All categories applicable to the incident shall be documented.
Probe(s): ______________________________________
Scan(s): ______________________________________

Prank: ______________________________________
Scam: ______________________________________
E-Mail Spoof: _________________________________
E-Mail bombardment: ____________________________

Was this a denial-of-service attack?
____

Break-In:
Intruder gained “root access”: (Yes / No)
Intruder installed a Trojan horse program: (Yes / No)
Intruder installed a packet sniffer: (Yes / No)
If Yes:
What was full path name(s) of the sniffer output file(s):
____

How many sessions did the sniffer log?
(Use “grep –c ‘DATA’<filename>” to obtain this information)

In each of following, circle yes or no:

NIS (yellow pages) attack (Yes / No)
NFS attack (Yes / No)
TFTP attack (Yes / No)

FTP attack (Yes / No)
Telnet attack: (Yes / No)
Rlogin or rsh attack (Yes / No)
Cracked password (Yes / No)
Easily-guessable password (Yes / No)
Anonymous FTP abuse (Yes / No)
IP Spoofing (Yes / No)
Product vulnerability Explain:
____
Misuse of host(s) resources (Yes / No)

V. SECURITY TOOLS [* means section/item must be completed]

* At the time of the Incident, was the organization using any of the following? (Yes / No):

Banner Warning: ____________________
Network Monitoring Tools: _____________________
Authentication/Password tools: _______________
Service filtering tools: _____________________________________

Tools to scan hosts for vulnerabilities: ISS/SATAN

Multipurpose tools: C2 security COPS Tiger (Circle all that apply)
Other tools: lsof cpm smrsh append-only file systems virus scanner(s)
(Circle all that apply)
Were logs being maintained: If so, please describe.
____
____
____

VI. DETAILED INCIDENT DESCRIPTION

Detailed Incident Description: This should be as detailed as possible, especially when writing lesson learned or after the incident follow-up report. Please use separate sheets of paper to address the following:

A. Duration of Incident:
B. How was the incident discovered?
C. Method(s) used by intruders to gain access to host(s):
D. Detailed discussion of vulnerabilities exploited that are not addressed in previous sections:
E. Hidden files/directories:
F. Source of attack (if known):

G. Did system contain classified/sensitive information? What type?

H. Was the information compromised?

I. Was the matter referred to the FBI/law enforcement authorities for further action? If so, to whom?

J. How did/does your organization plan to address the incident?

K. Attach log file:

Appendix B
AGENCY ISSPM/DEPUTY ISSPM/CIO CONTACT LIST

Agency	Name	Title	Phone Number(s)	E-mail Add.