

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

<b>DEPARTMENTAL MANUAL</b>	NUMBER: DM 3505-005
SUBJECT: Cybersecurity Incident Management Procedures	DATE: November 30, 2018
OPI: Office of the Chief Information Officer, Information Security Center	EXPIRATION DATE: November 30, 2023

<u>Section</u>	<u>Page</u>
1. Purpose	1
2. Special Instructions/Cancellations	2
3. Background	3
4. Scope	3
5. Procedures	4
6. Departmental Incident Management Procedures	4
7. Agency and Staff Office Incident Management Procedures	15
8. Notification to Congress about Incidents Procedures	30
9. Annual and Quarterly Incident Reporting Procedures	31
10. Incident Management Preparation Procedures	32
11. Roles and Responsibilities	39
12. Inquiries	46
Appendix A Authorities and References	A-1
Appendix B Definitions	B-1
Appendix C Acronyms and Abbreviations	C-1

1. PURPOSE

- a. This Departmental Manual (DM) provides guidance for cybersecurity incident management and reporting and describes essential preparations for effective incident management.
- b. This DM supports compliance by the United States Department of Agriculture (USDA) with Federal laws, regulations, and guidance on cybersecurity incident management.
- c. This DM serves as the foundation for Mission Areas, agencies, and staff offices to develop and implement cybersecurity incident management procedures and plans that comply with Federal and Departmental requirements.
- d. Major objectives of the cybersecurity incident management procedures in this manual are to:

- (1) Mitigate risks from incidents before substantial harm occurs;
- (2) Ensure coordination of and good communication about incident management activities within USDA and with external stakeholders; and
- (3) Provide timely notification and reporting to appropriate entities.

## 2. SPECIAL INSTRUCTIONS/CANCELLATIONS

- a. This manual is effective immediately and remains in effect until it is superseded or expired.
- b. All Mission Areas, agencies, and staff offices will align their procedures with this manual within 6 months of the publication date.
- c. The DM aligns with the Department's cybersecurity incident management policy, Departmental Regulation ([DR](#) 3505-005, *Cybersecurity Incident Management*).
- d. Terminology in this DM will be used and interpreted as follows:
  - (1) The term "misuse" broadly refers to improper usage of information or information resources in violation of rules, regulations, or policies;
  - (2) The term "operational security" encompasses techniques and processes that protect less valuable information from disclosure to an adversary to protect more valuable information. For example, disclosing only to those with a need to know that an incident has occurred so that an investigation to identify the intruder, and the information sought by the intruder can be investigated. Operational security techniques focus on preventing information from being inadvertently disclosed to an adversary. The objective of operational security techniques and processes prevent an adversary, for example, of knowing where information is located, how it is protected, or learning about mitigation plans;
  - (3) The terms "potential," "suspected," and "imminent" with respect to threats and incidents are distinct. "Potential" refers to a currently unrealized ability and is nearly synonymous with "possible" (e.g., a potential threat). "Suspected" implies a slight indication that something might be true or there is a reasonable basis for believing so; in other words, incidents may be suspected, as opposed to being confirmed (positively identified) or actual. "Imminent," as explained by National Institute of Standards and Technology (NIST) [Special Publication \(SP\) 800-61 Revision 2](#), *Computer Security Incident Handling Guide*, refers to a situation in which there is a factual basis for believing that a specific event is about to occur; attacks from a zero-day exploit of a vulnerability can be imminent;
  - (4) The terms "response" and "incident response" may be broad or narrow in meaning. The broad meaning encompasses multiple incident management activities, including analysis, notification, mitigation or application of countermeasures,

containment, eradication, and recovery. The narrow meaning is any one of these activities. NIST uses the terms “incident response” and “incident handling” as synonyms; and

- (5) The term “US-CERT” is used in this manual as a replacement for “the Federal information security incident center” identified in FISMA.

### 3. BACKGROUND

USDA experiences suspected and actual cybersecurity incidents daily, necessitating a framework for managing incidents supported by incident management plans, procedures, resources, testing, and training. This DM draws on Federal requirements for incident management found in Office of Management and Budget (OMB) Circular [A-130](#), *Responsibilities for Protecting Federal Information Resources*, July 28, 2016; FISMA; NIST [SP 800-53 Revision 4](#), *Security and Privacy Controls for Federal Information Systems and Organizations*; NIST SP 800-61 Revision 2; and other Federal regulations.

### 4. SCOPE

a. This DM applies to:

- (1) All USDA Mission Areas, agencies, staff offices, employees, appointees, contractors, subcontractors, and others who work for, or on behalf of, USDA;
- (2) All Federal information generated, collected, provided, transmitted, stored, maintained, or accessed by, or on behalf of, USDA;
- (3) Information systems or services (including cloud-based services) used or operated by USDA, a USDA contractor, or other organization on behalf of or funded by USDA, and interconnections between or among systems or services;
- (4) Cyber-based information, including electronic data, voice, and video data; and
- (5) All incidents affecting personally identifiable information (PII), which may or may not be cyber-related. This manual encompasses reporting both cyber-related and non-cyber breaches.
  - (a) All breaches that must be reported within USDA to the Agriculture Security Operations Division (ASOD) cybersecurity incident response team (CSIRT) and the USDA Privacy Office;
  - (b) All cyber-related breaches that are reportable to the United States Computer Emergency Readiness Team (US-CERT); and
  - (c) All major breaches that are reportable to Congress.

- b. Nothing in this DM will alter the requirements for the protection of information associated with national security systems (NSS) such as those in the *Federal Information Security Modernization Act of 2014* ([FISMA](#)), policies, directives, instructions, and standards issued by the Committee on National Security Systems (CNSS), or the intelligence community.

## 5. PROCEDURES

The procedures in this DM expand upon DR 3505-005, which addresses:

- a. Appropriately managing suspected and actual incidents affecting USDA information resources, including specialized incident types such as breaches, criminal activity, or misuse, and classified national security information (CNSI) spillage;
- b. Safeguarding sensitive incident information;
- c. Detecting potential compromises and exploits;
- d. Timely reporting of incidents internally to the ASOD CSIRT, externally to US-CERT, and notifying Congress of major incidents;
- e. Maintaining well-tested incident management plans and procedures and providing appropriate resources for incident management; and
- f. Providing awareness and training for incident management personnel and general users.

## 6. DEPARTMENTAL INCIDENT MANAGEMENT PROCEDURES

This Section describes Department-level incident management activities that should be leveraged to produce organization-specific incident management procedures.

The ASOD CSIRT operates as USDA's central cybersecurity incident management group, coordinating incident management activities, sharing information with both internal USDA offices and external entities, and providing assistance to agencies and staff offices when requested. For certain types of incidents, the USDA Privacy Office, Core Incident Response Group (CIRG), OIG, Office of Homeland Security (OHS) Personnel and Document Security Division (PDSD), OHS Insider Threat Program, and other offices have incident management responsibilities.

Notification and reporting to Congress and OMB are covered in Sections 8 and 9.

### a. Incident Command.

- (1) The ASOD CSIRT coordinates incident management activities with other USDA offices. It is staffed 24 hours a day, 7 days a week.

- (2) The ASOD CSIRT is USDA's designated operational liaison with US-CERT. The ASOD Director designates a primary and secondary point of contact in the ASOD CSIRT for all interactions with US-CERT.
  - (3) The ASOD Director has the authority to appoint an incident commander for a major incident (which may be declared by USDA, Department of Homeland Security (DHS), or OMB) or when warranted by other circumstances. The incident commander is then responsible for directing and managing the incident.
  - (4) The ASOD Director or the designated incident commander, during complex or crisis-level incidents (that is, those that require non-routine response operations), sets priorities based on factors such as functional impact, information impact, recoverability, and resource availability and communicates those priorities and requirements for additional assistance or resources to the USDA Chief Information Security Officer (CISO) or US-CERT.
- b. Coordination and Assistance.
- (1) The ASOD CSIRT coordinates with and provides, upon request, technical and non-technical assistance to agencies and staff offices when there are actual or suspected cybersecurity incidents.
  - (2) The ASOD Director or authorized ASOD CSIRT personnel may request, through appropriate management channels, agency and staff office incident management personnel to provide technical or investigation assistance to other agencies or staff offices.
- c. Recordkeeping and Metrics. The ASOD CSIRT must produce metrics about incidents for reporting to the President's Management Council, OMB, or other Federal organizations such as:
- (1) Whether an incident or an attack successfully resulted in unauthorized access to, exfiltration of, manipulation of, harm to, or impaired the integrity, confidentiality, or availability of an information system or information that is stored on, processed by, or transiting an information system; and
  - (2) Any public and internal notifications about an incident and the dates of those notifications.
- d. Detection and Analysis.
- (1) The ASOD CSIRT deploys automated tools such as intrusion detection systems and network analysis software to support detection and analysis and runs them on a regular schedule. The tools are configured to receive updates to indicators from their vendors.
  - (2) When US-CERT issues an alert about a suspected or actual compromise with the potential to affect U.S. Government systems and provides indicators of compromise

(IOC), the ASOD CSIRT must start IOC scans using the provided indicators within 24 hours. If the ASOD CSIRT confirms a compromise has occurred, this information must be reported back to US-CERT.

- (3) The ASOD CSIRT also participates in DHS's EINSTEIN program to detect security incidents and collect incident information for analysis.

e. Reporting Cyber-Related Incidents to US-CERT.

- (1) The ASOD CSIRT reports only cyber-related incidents to US-CERT. Non-cyber incidents (such as exposure of printed documents containing PII) are not reported to US-CERT.
- (2) The ASOD CSIRT must report the following to US-CERT within 1 hour:
  - (a) Suspected or actual exposure or compromise of cyber-based PII;
  - (b) Suspected or actual cyber incidents related to criminal activity or misuse;
  - (c) Suspected or actual incidents of CNSI spillage and compromise of classified systems; and
  - (d) All confirmed incidents of compromise to the confidentiality, integrity, or availability of USDA information, information systems, or information services.
- (3) Reporting to US-CERT within 1 hour is mandatory and must not be delayed to provide or gather other details about the incident such as root cause, threat vector, or mitigation actions taken.
- (4) The ASOD CSIRT must report each incident separately because US-CERT does not accept reports of multiple incidents in a single submission. The ASOD CSIRT emails the reports to US-CERT from its incident ticketing system.
- (5) Required information for reporting to US-CERT can be found in the DHS, [US-CERT Federal Incident Notification Guidelines](#). The ASOD CSIRT ensures that each reported incident is categorized, prioritized, and contains all other required information prior to sending it to US-CERT. As additional information is discovered and gathered about an incident, the ASOD CSIRT provides updates to US-CERT.
- (6) The ASOD Director or the incident commander may, based on the severity of an incident, activate the standing Federal Network Authorization, authorizing US-CERT to access relevant USDA networks and, if necessary, to provide on-site technical assistance.

f. General Incident Handling.

See the following Sections for specific incident handling guidance:

Section 6g for specific guidance about breaches;

Section 6h for OIG related incidents; and

Section 6i for CNSI spillage.

- (1) For incidents involving spillage of CNSI, PII, or controlled unclassified information (CUI), all personnel must minimize damage to or further exposure of the information. The ASOD CSIRT reminds personnel of the following protective actions when suspected or actual incidents involving these types of sensitive information are reported to them. Specifically, personnel reporting spillage of CNSI, PII, or CUI must:
  - (a) Not delete or forward any spilled information in any format, whether it is an email, attachment, hyperlink attachment, or hardcopy document; and
  - (b) Take custody of the information to safeguard it from further unauthorized access until it can be secured by the proper authority.
- (2) The ASOD CSIRT ensures that the correct forms are used and properly completed for reporting incident details: Agriculture Department [\(AD\)-3043](#), *ASOC Incident Report*, or [AD-3038](#), *Cyber Security Incident Report Personally Identifiable Information (PII) Incident*.
- (3) The ASOD CSIRT ensures that actions are immediately performed to mitigate incidents or threats that have or potentially will have:
  - (a) High functional impacts to all critical services and system users; or
  - (b) Severe impacts to the integrity of USDA information or to information deemed to be classified, privacy-related, or proprietary.
- (4) The ASOD CSIRT ensures that compromised devices are disconnected from the USDA network, appropriately analyzed, and, if appropriate, restored to service in a secure configuration only after malware or other types of compromise are eradicated.
- (5) ASOD CSIRT personnel, at the direction of the ASOD Director or the designated incident commander, collaborate and coordinate on a need-to-know basis with external entities such as Internet Service Providers (ISP), other incident response groups, affected external parties, or vendors of information technology (IT) products and services, about investigation and mitigation of incidents.

- (6) ASOD CSIRT personnel, with the concurrence of the USDA CISO, the ASOD Director, or the designated incident commander, notify external organizations affected by an actual or suspected incident (exploit or threat) originating from USDA.
  
- (7) External Notifications about Incidents. Different agencies, offices, and the CIRG have different responsibilities for issuing external notifications about incidents. The responsibility varies depending on the type of incident and the audience for the notification. Examples of external communications include informing the public in general; notifying individuals affected by a breach; or alerting external parties affected by an actual or suspected incident originating from USDA. This Section covers general information about external notifications; subsequent Sections describe the responsibilities for special types of incidents.
  - (a) When external notifications are to be issued, the responsible agency or office must inform or consult with the Director of the Office of Communications (OC).
  - (b) The USDA Chief Information Officer (CIO) and the Director of OC are jointly responsible for notification about major incidents at USDA that are issued to general public, the media, and external entities not directly affected by the incident.
  
- (8) Incident Closure Activities.
  - (a) The ASOD CSIRT:
    - 1 Monitors and tracks agency and staff office mitigation efforts;
    - 2 Validates completion of the mitigation efforts;
    - 3 Verifies that affected systems and devices are no longer a threat to the USDA network; and
    - 4 Validates that all required reporting information has been provided.
  - (b) The ASOD Director or the designated incident commander provides another level of oversight, ensuring that all incident handling activities are validated as complete, including additional reporting to US-CERT.
  - (c) Reopening Incidents. Incidents may be reopened at the request of ASOD CSIRT personnel, the ASOD Director, the Senior Agency Official for Privacy (SAOP), the USDA Chief Privacy Officer (CPO), the Inspector General, or the Chief of OHS PDSO.

g. Handling Breaches.

- (1) The ASOD CSIRT must provide notifications of suspected or actual exposure or compromise of PII to the following within 1 hour:
  - (a) For cyber-related breaches, notify the US-CERT, the USDA Privacy Office, the agency or staff office CSIRT, and the OIG; and
  - (b) For non-cyber breaches (e.g., hardcopy only), notify the USDA Privacy Office, the agency or staff office CSIRT, and the OIG.
- (2) All incident management personnel receive direction and guidance regarding breaches, whether or not they are cyber-related, from:
  - (a) The USDA CPO when the incidents are low impact;
  - (b) The SAOP when the breaches are moderate and high impact; or
  - (c) The CIRG when convened.
- (3) The ASOD CSIRT provides email notification of breaches to the USDA CPO and others, as directed by the CPO. Files or emails containing PII should not be emailed or forwarded.
- (4) Details about breaches are documented on form AD-3038; the form has Sections to report unauthorized access and equipment containing PII that is lost or stolen (including seizure by a foreign government).
- (5) Care must be taken to ensure that PII related to actual or suspected incidents is handled properly and its use and disclosure is minimized to the greatest extent possible.
- (6) Procedures in the USDA [\*Personally Identifiable Information \(PII\) Core Incident Response Group \(CIRG\) PII Breach Notification & Incident Response Plan \(IRP\)\*](#) must be followed.
- (7) Actions directed by the CIRG or the USDA Privacy Office must be completed in the prescribed timeframe to meet notification guidance prescribed in [OMB M-17-12, Preparing for and Responding to a Breach of Personally Identifiable Information.](#)
- (8) Breach Notifications.
  - (a) The SAOP will be responsible for advising the Secretary of Agriculture whether and when to notify individuals potentially affected by a breach, in coordination with the:
    - 1 CIRG when convened; or
    - 2 CPO, when the CIRG is not convened.

- (b) The Secretary of Agriculture will make a final decision regarding whether to provide notification to individuals affected by a breach.
- (c) The CIRG, when convened, is responsible for requiring notifications to be developed, and reviewing and approving the content of notifications to all individuals impacted by exposure of their PII by USDA employees or contractors.
- (d) When the CIRG has not been convened, OC is responsible for breach notifications. OC may delegate this responsibility to agency and staff office communication or public affairs offices.
- (e) Office of the General Counsel (OGC) must review and approve any notifications to individuals impacted by a breach in which the individuals are or were litigants.
- (f) Office of Human Resources Management (OHRM), in coordination with OC, is responsible for breach notifications to current and former USDA employees, retirees, and retirees' survivors or designated dependents (e.g., spouses and minor or adult children).
- (g) Other types of breach notifications for which OC is responsible include:
  - 1 Notifications to other impacted individuals, such as customers, grant recipients, or contractors; and
  - 2 Notifications to the general public, the media, and external entities not directly affected by the incident.

(9) Closure of Breaches.

- (a) The SAOP must certify by email that a moderate or high impact breach is closed.
- (b) The USDA CPO must approve closure of all other breaches.

h. Handling OIG-Related Incidents.

- (1) ASOD CSIRT coordinates with OHS PDSO regarding all incidents involving foreign actors;
- (2) The ASOD CSIRT must immediately escalate to the OIG Technical Crimes Division (TCD), Special Agent in Charge via email or the OIG Hotline (800-424-9121):
  - (a) All cyber investigations and incidents related to or potentially related to criminal activity;

- (b) Incidents related to fraud, waste, and abuse of information resources; and
  - (c) Any incidents that involve law enforcement from any level of government (Federal, State, local, tribal, or territorial).
- (3) The ASOD CSIRT must report suspected or actual cyber incidents of criminal activity or misuse to US-CERT within 1 hour of notification or detection.
- (4) The ASOD CSIRT must report to OIG every incident that is reported to US-CERT.
- (5) The ASOD CSIRT and other incident management personnel must cooperate with OIG and law enforcement personnel to provide any support needed for criminal investigations and prosecutions.
- (6) OIG and the ASOD CSIRT collaborate prior to taking possession of government furnished equipment (GFE) for investigations involving actual or suspected criminal activity or misuse.
- (a) Mission Area Assistant CISOs and Information Systems Security Program Managers (ISSPM) must inform the ASOD CSIRT and provide specific guidance for handling GFE and information on that GFE when the agency or staff office is operating under a law specific to its mission, such as the [Confidential Information Protection and Statistical Efficiency Act of 2002](#) (CIPSEA).
  - (b) The ASOD CSIRT must coordinate with agency and staff office personnel responsible for incident management, and employee relations or adverse personnel actions prior to taking possession of GFE for investigations or confirmed incidents.
- (7) Seizures of GFE. OIG and the ASOD CSIRT will coordinate with other entities as applicable when taking possession of GFE. Examples of applicable entities include:
- (a) Federal, State, local, tribal, or territorial levels of law enforcement agencies;
  - (b) Other USDA agencies and staff offices affected or potentially affected by the incident; or
  - (c) In cases that may lead to adverse personnel action, OHRM or agency or staff office personnel responsible for employee relations or adverse actions.
- (8) Notifications about Criminal and Foreign Actor Incidents. OIG is responsible for notifications about suspected and actual incidents with a connection or link to criminal or foreign actors.
- (a) The OIG or the ASOD CSIRT, after conferring and when appropriate, will notify law enforcement agencies;

- (b) The Inspector General (IG) is responsible for providing notifications, as appropriate:
  - 1 To external parties affected by the incident; and
  - 2 In coordination with OC and only when notification will not impact open criminal investigations, the general public, the media, and external entities not directly affected by the incident.
- i. Handling Classified System Incidents and CNSI Spillage.
  - (1) OHS PDSD:
    - (a) Coordinates incident management with the ASOD CSIRT; and
    - (b) Conducts official investigations of suspected or actual CNSI spillage incidents and incidents affecting classified systems. Contact information is:
      - 1 OHS PDSD: Call 202-720-7373 or email [pdsd@dm.usda.gov](mailto:pdsd@dm.usda.gov); the phone is staffed Monday through Friday, 7 a.m. until 5 p.m. (Eastern Time); and
      - 2 ASOD CSIRT: Call 866-905-6890 or email [cyber.incidents@usda.gov](mailto:cyber.incidents@usda.gov); ASOD is staffed 24x7x365.
  - (2) Notifications about Classified System Incidents and CNSI Spillage Incidents.
    - (a) The incident is reported promptly to the ASOD CSIRT, OHS PDSD, and the OHS Insider Threat Program (if pertinent). The OHS Special Security Officer (SSO) is often the person who reports the incident and notifies the ASOD CSIRT. If the ASOD CSIRT learns of the incident first, it notifies OHS PDSD.
    - (b) OHS PDSD is responsible for notifying and coordinating with the security staff of any external network owner if any external network may have been contaminated by a USDA CNSI spillage incident.
  - (3) Operational security discipline must be used for all communication to minimize further exposure of the incident and damage to CNSI. Specifically:
    - (a) Provide only the minimum amount of information to convey that there has been an incident, then request a face-to-face meeting or a secure call;
    - (b) Avoid indicating what the information is or its classification, unless using approved secure methods of communication;
    - (c) Only discuss the incident or potential incident with personnel who have an appropriate security clearance and a need to know; and

- (d) Refrain from contacting any individuals associated with the incident, as it may inhibit inquiry processes into potential security violations or insider threats.
- (4) Coordination of Incident Management.
- (a) OHS PDSD collaborates with the OHS National Security System Program (NSSP) as needed, the ASOD CSIRT, and network and system administrators who handle containment and cleanup activities, and consults with the OHS Insider Threat Program on any potential insider threat concerns.
  - (b) OHS PDSD contacts the data owner of CNSI and agrees on details of steps needed for containment and cleanup.
  - (c) OHS NSSP assists and advises in the containment and cleanup strategies and activities and coordination with classified network owners, as appropriate. The contact information is 202-720-0594 or [OHSEC-NSSP-SupportTeam@dm.usda.gov](mailto:OHSEC-NSSP-SupportTeam@dm.usda.gov).
  - (d) The ASOD CSIRT and OHS PDSD coordinate with US-CERT on all incident response activities and communications related to classified systems and CNSI spillage, sharing information about incidents, threats, and vulnerabilities to the extent consistent with standards and guidelines for NSS, issued in accordance with law and as directed by the President.
- (5) Mitigating CNSI Spills.
- (a) Identify and report the information system or system component contaminated by a potential or actual spillage, along with the specific information involved in the spillage, using operational security discipline.
  - (b) Promptly isolate and secure the contaminated information system or system component. The ASOD CSIRT, OHS PDSD, and OHS NSSP advise network owners and administrators on how to contain and isolate classified or potentially classified information.
  - (c) Safeguard the information at all times.
  - (d) The Senior Agency Official for CNSI/Director of OHS and the USDA CISO have the authority to direct any action, including shutdown, with respect to any system on which CNSI is spilled.
  - (e) The data owner may provide input on containment and cleanup strategies, over which OHS PDSD has approval authority.
  - (f) The ASOD CSIRT investigates to determine if other information systems or system components may have been subsequently contaminated and communicates that information to OHS PDSD.

- (g) If an external network may have been contaminated by the spillage, the OHS NSSP and the ASOD CSIRT consult with the external network provider or providers to contain and isolate classified or potentially classified information.
  - (h) Eradicate the spilled information from all contaminated information systems and system components. Other cleanup activities may also be required. Note that CNSI spillages involving cloud computing environments present unique challenges for eradication.
  - (i) System, network, and database administrators document the steps taken to contain and clean up a CNSI spillage and provide that documentation to the ASOD CSIRT and OHS PDSO as proof that the actions were taken.
  - (j) Certification is required to verify that the spilled information has been eradicated from the contaminated system(s) and device(s) and that the network is clean.
- (6) Closure of CNSI Spillage Incidents. The following information pertains only to the cybersecurity aspects of a CNSI spillage. Other investigative aspects may continue separately after the cybersecurity portion of the incident is closed.
- (a) The OHS SSO submits final security incident reports to the Senior Agency Official for CNSI, the USDA CISO, and the data owner, along with recommendations such as making changes to security controls or training.
  - (b) The OHS SSO also submits recommendations for changes or improvements to the Senior Agency Official for CNSI and the USDA CISO.
  - (c) OHS PDSO provides the final determination to close the CNSI spillage incident to the Senior Agency Official for CNSI and the USDA CISO.
  - (d) For the ASOD CSIRT, the USDA CISO may deem the cybersecurity incident closed or identify additional steps to be taken before closure.

j. Handling Insider Threat Incidents.

- (1) OHS's Insider Threat Program must be involved:
  - (a) As soon as an issue is identified; and
  - (b) In all incidents and inquiries potentially or actually relating to an insider's use of access privileges to do harm, wittingly or unwittingly, to the security of the United States through espionage, terrorism, unauthorized disclosure of national security information, or the loss or degradation of Departmental resources or capabilities. OHS Insider Threat Program's contact information is 202-720-3487 or [insider@dm.usda.gov](mailto:insider@dm.usda.gov).

- (2) The Insider Threat Program Coordinator conducts inquiries on all potential insider threat incidents and coordinates with appointed stakeholders, including within the Office of the Chief Information Officer (OCIO), to obtain information, including electronic records and files, necessary to identify, analyze, and resolve insider threat matters.
  - (3) The Insider Threat Program serves as the USDA liaison to the intelligence community for insider threat and counterintelligence activities within the Department, to include referrals to the Federal Bureau of Investigation (FBI).
- k. Handling Miscellaneous Incident Types.
- (1) Incidents Affecting USDA’s Financial Systems or Records. The Office of the Chief Financial Officer (OCFO) is consulted when an incident affects a financial system or financial records. After informing OC, OCFO is responsible for issuing notifications to financial services institutions such as banks, credit unions, payment card companies, and insurance companies about incidents affecting USDA’s financial systems or records.
  - (2) Adverse Personnel Actions; Seizure of GFE. OHRM, or agency and staff office personnel responsible for employee relations or adverse personnel actions must be notified when:
    - (a) Incidents may require adverse personnel action due to actual or suspected misuse of information resources; or
    - (b) It is necessary to take possession of GFE for investigations or confirmed incidents. See Section 6h, Handling OIG-Related Incidents.
  - (3) Other Government Entities. OGC provides legal advice for incidents involving other Government entities at the Federal, State, local, tribal, or territorial levels.
  - (4) Exposure of CUI. The ASOD CSIRT coordinates with the USDA CUI program office when CUI is exposed to an unauthorized person or persons.
- l. Correlation and Analysis of Incident Data. The ASOD CSIRT must correlate and analyze current and historical incident information and responses to incidents to achieve a Departmentwide perspective on incident awareness and response.

## 7. AGENCY AND STAFF OFFICE INCIDENT MANAGEMENT PROCEDURES

This Section describes incident management procedures from the perspective of agencies and staff offices. Section 6 covers incident management procedures at the Departmental level.

Agencies and staff offices should leverage these procedures to produce their own tailored incident management procedures.

Incident preparation procedures are discussed in Section 10. Incident management activities include incident detection; reporting incidents; investigating and analyzing incidents; gathering evidence and protecting sensitive incident information; mitigating incidents through activities such as containment, eradication, and recovery; documenting incidents; incident closure; and post-incident after-action reviews and improvement planning. Many of these activities take place concurrently (e.g., investigating, mitigating, documenting) or occur multiple times (e.g., reporting with updates to original information).

a. Incident Detection.

Prompt detection can improve incident response and recovery, thereby minimizing the resulting damage.

- (1) Incident management personnel receive indications, warnings, alerts, and notifications from a variety of sources about events that may be suspected and actual incidents. The sources include automated tools such as intrusion detection systems, anti-malware software, and log analyzers and reports from the ASOD CSIRT, other incident response groups, or users.
- (2) Incident management personnel and other personnel such as system, network, and database administrators must take actions directed by the ASOD CSIRT to detect potential or imminent threats and exploits.
- (3) Incident management personnel must expect to deal with false positives from any type of source. NIST SP 800-61 Revision 2, Section 3.2, Detection and Analysis, provides extensive details on the challenges, differences between precursors and indicators as signs of potential incidents, and tools or other sources that provide such signs.
- (4) Incident management personnel must log into the agency or staff office incident tracking mechanism all suspected and actual incidents, appropriate details, and conclusions of their investigations.

b. Incident Reporting.

This Section describes reporting topics that must be incorporated into agency and staff office procedures. Procedures must indicate the types of suspected and actual incidents that must be reported immediately to the ASOD CSIRT. Details about each incident must also be submitted using the forms described in this Section. All required information on the reporting forms must be finalized before an incident may be closed; supporting information may also be required.

- (1) Report all suspected or actual incidents affecting USDA information resources to the ASOD CSIRT through the ASOD 24-Hour Hotline (866-905-6890) or the Cyber mailbox ([cyber.incidents@ASOC.usda.gov](mailto:cyber.incidents@ASOC.usda.gov)). Either communication method may be used to convey additional information about the reported incident.

- (2) Report all suspected or actual incidents to the ASOD CSIRT within 1 hour of discovery. Examples of reportable incidents are:
- (a) Suspected or actual spillage of CNSI or suspected or actual cybersecurity incidents affecting classified systems, with concurrent reporting to OHS PDSD, the agency or staff office Information Security Coordinator (ISC), and agency or staff office information security support staff. See Section 7b(3) for guidance to protect CNSI;
  - (b) Suspected or actual unauthorized release of CUI;
  - (c) Suspected or actual exposure or compromise of PII (a category of CUI) in all forms (e.g., cyber-based, verbal discussions of PII with unauthorized persons, loss of hardcopy documents that contain PII), whether the exposure is inadvertent or intentional;
- Caution: When reporting a PII breach, do not forward the subject PII to the ASOD CSIRT. Do not delete emails or email attachments containing PII until receiving instructions on what to do.
- (d) Suspected or actual incidents related to criminal activity or misuse;
  - (e) Suspected or actual insider threats where an insider is using or may be using access privileges to do harm, wittingly or unwittingly, to the security of the United States, including damage to the United States through espionage, terrorism, unauthorized disclosure of national security information, or the loss or degradation of Departmental resources or capabilities; and
  - (f) Suspected or actual incidents of compromise to the confidentiality, integrity, or availability of USDA information, information systems, or information services.

(3) Protection of CNSI. When reporting a classified or potentially classified incident, including spillage of CNSI, use operational security discipline for all communication to minimize further exposure of the incident and damage to CNSI. Specifically:

- (a) Do not delete emails or email attachments with CNSI until receiving instructions on what to do;
- (b) Do not forward the CNSI to the ASOD CSIRT, or anyone else;
- (c) Provide only the minimum amount of information to convey that there has been an incident and request a face-to-face meeting or a secure call to follow up;
- (d) Avoid indicating what the information is or its classification, unless using approved secure methods of communication; and

- (e) Only discuss the incident or potential incident with personnel who have an appropriate security clearance and a need to know.
  - (4) Notify others with a need to know about the incident, based on the type of incident and the information resources affected. Examples include the system owner, network, system, or database administrators, or the Mission Area Assistant CIO or Privacy Officer.
  - (5) As incident investigation and mitigation continue, incident management personnel are to provide the ASOD CSIRT with additional information such as the threat vector, functional and information impacts, mitigation details, or recoverability.
  - (6) Incident Reporting Forms. An incident report is submitted to the ASOD CSIRT using these Departmental forms to close an incident:
    - (a) AD-3038 for incident reports involving unauthorized access to PII or equipment with PII that is lost or stolen (including seizure by a foreign government; or
    - (b) AD-3043 for all other incidents.
  - (7) Reportable Information. Fill in the information using the appropriate form. If the investigation determines that a reported incident is a false positive, only Section 1 of AD-3043 needs to be completed. All required information must be submitted before an incident may be closed.
  - (8) When PII is inadvertently released to a person or organization, at the discretion of management in collaboration with CPO and ASOD, outside USDA, the responsible agency or staff office in coordination with the CPO may send the recipient or recipients a tailored copy of form [AD-3050](#), *PII Incident Non Disclosure Agreement*. The form must be tailored by modifying the paragraphs:
    - (a) To describe the circumstances of the incident to indicate how the control of PII was lost (e.g., PII being sent in an email, as an attachment to an email, or on a lost hardcopy document);
    - (b) To describe a set of actions the recipient should take to delete or destroy the email, file, or document containing PII and not to discuss or disclose the PII; and
    - (c) To provide instructions where to return the completed form.
  - (9) Log this activity and any responses in the tracking mechanism of the responsible agency or staff office.
- c. Incident Investigation, Analysis, and Cooperation.
- (1) All suspected and actual incidents must be investigated.

- (2) Agency and staff offices must coordinate and collaborate with the ASOD CSIRT. They must not directly contact external entities such as US-CERT unless specifically requested to do so by the ASOD Director or ASOD CSIRT personnel to whom that authority has been delegated.
- (3) Agency and staff office incident management personnel may request assistance, as needed, from the ASOD CSIRT; US-CERT or other support resources for incident handling must be requested through the ASOD CSIRT.
- (4) The ASOD Director or authorized ASOD CSIRT personnel may request agency and staff office incident management personnel to provide technical or investigation assistance to other agencies or staff offices.
- (5) Investigations of some incidents need the involvement or leadership of other entities with specialized authorities and capabilities. Agency and staff office personnel are expected to cooperate in these investigations. The other entities include:
  - (a) OIG or law enforcement from any level of government (Federal, State, local, tribal, or territorial) for criminal activity;
  - (b) OIG for instances of fraud, waste, and abuse;
  - (c) OHS PDSO for actual or potential compromises of CNSI;
  - (d) OHS's Insider Threat Program for all incidents and inquiries potentially or actually relating to an insider's use of access privileges to do harm, wittingly or unwittingly, to the security of the United States;
  - (e) The OHRM and agency or staff office responsible for employee relations or adverse actions; and
  - (f) The USDA Privacy Office and agency or staff office responsible for privacy.
- (6) Perform all incident investigative actions advised by the ASOD CSIRT or other authorized USDA offices in a timely manner.
- (7) Analysis. Incident analysis begins with detection of an incident and continues until the incident investigation is complete. Analysis also serves as an input to incident documentation and reporting. Through analysis, incident management personnel determine whether an event represents a suspected or actual incident and the type of incident. The analysis must also address questions such as these:
  - (a) Information Impact. What types of information are affected, including classified, proprietary, or privacy? What is the extent of compromise or effect on information confidentiality, integrity, or availability?
  - (b) Functional Impact. What are the functional impacts of the incident?

- (c) Incident Scale. Which networks, systems, or applications are affected? What is the extent and magnitude of the incident?
- (d) Root Cause. How the incident is occurring? For example, what vulnerabilities are being exploited or what tools or attack methods are being used?
- (e) Evidence. What is the evidence (e.g., logs, files, emails, devices)? How should the evidence be protected and preserved?
- (f) Recoverability. What resources and strategies/potential courses of action are needed to respond to and recover from the incident? How long will it take to recover from the incident?

For more information about Information Impact, Functional Impact, and Recoverability, see the *US-CERT Federal Incident Notification Guidelines* and NIST SP 800-61 Revision 2.

- (8) Breaches. Incident management personnel are to follow the procedures in the *USDA Personally Identifiable Information (PII) Core Incident Response Group (CIRG) PII Breach Notification & Incident Response Plan (IRP)* and complete actions directed by the CIRG, the USDA Privacy Office, or the ASOD CSIRT in the prescribed timeframe.
- (9) Scanning for IOCs. Either the US-CERT or another Federal agency, from time to time, issue alerts and provide indicators regarding suspected or actual compromises with the potential to affect U.S. Government systems. Agencies and staff offices that have scanning capabilities must perform IOC scans using the provided indicators within 24 hours and report the scan results to the ASOD CSIRT. If the ASOD CSIRT confirms a compromise has occurred, this information is reported to US-CERT.
- (10) Investigating Incidents Identified from Various Sources. Various sources may identify that an agency or staff office is experiencing a suspected or actual incident or compromise. Sources include the ASOD CSIRT; another USDA agency or staff office; users (whether Federal employees, contractors, or others); system, network, or database administrators; US-CERT, a law enforcement agency, or another external entity. The procedures are as follow:
  - (a) The ASOD CSIRT creates and sends an inquiry or a ticket to the agency or staff office incident management personnel, who must acknowledge receipt by responding to the ASOD CSIRT through the ASOD 24-Hour Hotline (866-905-6890) or the Cyber mailbox ([cyber.incidents@ASOC.usda.gov](mailto:cyber.incidents@ASOC.usda.gov)).
  - (b) The agency or staff office incident management personnel investigate the reported incident or compromise.
  - (c) If the investigation confirms an incident or compromise:

- 1 Immediately notify the ASOD CSIRT (as indicated in Section 7c(10)(a)) with known details.
- 2 Perform recommended mitigation measures in the timeframe directed by the ASOD CSIRT.
- 3 Continue the investigation to discover the threat vector and, when that is determined, notify the ASOD CSIRT of the updated information.

(d) If the investigation determines that the reported incident or compromise is a false positive, agency or staff office incident management personnel complete only Section 1 of AD-3043 and submit it to the ASOD CSIRT via the Cyber mailbox ([cyber.incidents@ASOC.usda.gov](mailto:cyber.incidents@ASOC.usda.gov)).

(11) Adverse Personnel Actions; Seizure of GFE. The agency and staff office incident management personnel must notify OHRM or their organization responsible for employee relations or adverse personnel actions when:

- 1 Incidents may require adverse personnel action due to actual or suspected misuse of information resources; or
- 2 It is necessary to take possession of GFE for investigations or confirmed incidents.

d. Evidence Gathering and Handling.

Incident information is considered sensitive and may be considered as evidence in personnel disciplinary matters or legal actions.

- (1) Protection of Sensitive Incident Information. Protect the confidentiality and integrity of all sensitive incident information by employing sufficient security controls and procedures.
  - (a) Minimize damage to or further exposure of information such as PII, CUI, and CNSI. Also protect documentation about the incident and incident management activities.
  - (b) Protection is to be applied to information in any form or medium, such as hardcopy or softcopy format, when collected, stored, processed, or transmitted.
  - (c) Employ security controls such as the following:
    - 1 Restrict access to automated or manual incident tracking tools to authorized persons. In addition, all accesses and actions to add, update, or delete information should be logged.
    - 2 Have a secure storage container within a facility for securing incident evidence and other sensitive materials.

- 3 Optionally, encrypt softcopy incident records, documents, and PII information by implementing encryption software that uses an algorithm validated to the Federal Information Processing Standards Publication ([\(FIPS PUB\) 140-2](#), *Security Requirements for Cryptographic Modules*).
  - 4 Optionally, incident communications via email may be encrypted and digitally signed, especially if the email contains sensitive information.
- (2) PII Protection Requirements. These requirements apply for both suspected and actual breaches:
  - (a) All employees, contractors, and others who work on behalf of USDA are to protect and properly handle PII, until authorized personnel assume custody of the information; and
  - (b) Incident management personnel are to ensure that PII is handled properly and its exposure is minimized to the greatest extent possible.
- (3) Suspected or Known Criminal Activity or Misuse. All incident management personnel must comply with [DR 1700-002](#), *OIG Organization and Procedures*. The evidence and supporting incident documentation may be needed for further investigation by law enforcement or for legal proceedings. Compromised systems or devices also serve as evidence and must be secured and preserved. The following standards should be adhered to so that evidence can be admissible in court:

Note: When OIG wants to collect evidence, the OIG (most likely a Special Agent) will do so by initiating an *Evidence Receipt* (Exhibit B of Form OIG-8440-1; also known as a chain of custody form) in person. The *Evidence Receipt* should not be used, or issued, on behalf of the OIG.

- (a) Have documented procedures that meet all (Federal, State, local, tribal, or territorial) applicable laws and regulations and that are based on guidance from OIG.
- (b) Follow the procedures when collecting evidence and document any deviations from the procedures;
- (c) Forensically protect evidence, using enterprise, agency or staff office-provided tools and techniques to collect, examine, and analyze evidence;
- (d) Document all activities and steps taken to collect evidence, who performed them, how they were performed, and the date and time performed;
- (e) Keep a detailed log of all evidence collected;
- (f) Seal all devices and other collected evidence in containers and label the containers;

- (g) Label all evidence, indicating who secured and validated the evidence and the date and time; and
- (h) Account for evidence at all times:
  - 1 Whenever evidence is transferred from person to person, establish a formal chain of custody using form OIG-8440-1. *Evidence Receipt* (provided by the OIG) to detail the transfer and capture each person's signature.
  - 2 Securely store evidence, documenting when it is stored and by whom.
- (4) OIG criminal investigators or the OIG TCD, in collaboration with the ASOD CSIRT, will direct incident management personnel on securing incident evidence to comply with the rules of preservation of evidence.
- (5) Seizure of GFE.
  - (a) Mission Area Assistant CISOs and ISSPMs are to inform the ASOD CSIRT and provide specific guidance for handling GFE and information on that GFE when the agency or staff office is operating under a law specific to its mission, such as the CIPSEA.
  - (b) Agency and staff office incident management personnel must notify their employee relations organization and the ASOD CSIRT prior to taking possession of GFE for investigations or confirmed incidents.
- e. Mitigating Incidents or Threats.
  - (1) Immediately perform actions to mitigate incidents or threats that have or potentially will have:
    - (a) High functional impacts to critical services and system users; or
    - (b) Severe impacts to the integrity of USDA information or to information deemed to be classified, privacy-related, or proprietary.
  - (2) Promptly disconnect service to devices that are reported lost, stolen, or seized by a foreign government.
  - (3) Perform these actions for compromised devices (e.g., equipment identified or suspected of containing malicious code or exhibiting suspicious activity):
    - (a) Report the incident to the ASOD CSIRT;
    - (b) Disconnect the equipment from the network, unless otherwise instructed by the ASOD CSIRT; and

- (c) Follow instructions from the ASOD CSIRT on subsequent handling of the equipment.
- (4) Agency and staff office incident management personnel and others such as system, network, and database administrators are to perform, in a timely manner, all incident mitigation actions in advisories sent by the ASOD CSIRT or other authorized USDA offices. Advisories may apply to actual incidents or to potential or imminent threats and exploits.
- (5) Mitigating Breaches.
  - (a) Instruct those who report or handle a breach that they must:
    - 1 Not delete or forward any of the information in any format, whether an email, an attachment, or a hyperlink; and
    - 2 Properly protect the information until authorized personnel assume custody of the information.
  - (b) When PII is inadvertently sent in the body of an email or in an email attachment to one or more external parties, at the discretion of management in collaboration with the CPO and ASOD the responsible office may send the recipient or recipients a tailored copy of form AD-3050. The form must be tailored by modifying the paragraphs:
    - 1 To describe the circumstances of the incident to indicate how the control of PII was lost (e.g., PII being sent in an email, as an attachment to an email, or on a lost hardcopy document);
    - 2 To describe a set of actions the recipient should take to delete or destroy the email, file, or document containing PII and not to discuss or disclose the PII; and
    - 3 To provide instructions where to return the completed form.
  - (c) Log this activity and any responses in the tracking mechanism of the responsible agency or staff office.
- (6) Mitigating Spillage of CNSI.
  - (a) The Senior Agency Official for CNSI/Director of OHS and the USDA CISO each has the authority to direct any action, including shutdown, with respect to any system on which CNSI is spilled.
  - (b) The contaminated information system or system component is to be promptly isolated.

- (c) The spilled information must be eradicated from all contaminated information systems and system components. Other cleanup activities may also be required.
- (d) System, network, and database administrators document the steps taken to contain and clean up a CNSI spillage and provide that documentation to the ASOD CSIRT and OHS PDSD as proof that the actions were taken.

f. Incident Information and Documentation.

Documentation is an ongoing activity throughout an incident. It serves as an input to incident reporting and continues until the incident is closed. Incident documentation may be put to uses such as briefing personnel brought in to assist with handling the incident, evidence for legal proceedings, or input to an after-action review of the incident.

Incident information may be recorded with a combination of manual methods (such as a logbook) and automated tracking mechanisms. Incident information and documentation are considered sensitive and must be protected appropriately during storage and transmission in any form or medium (i.e., electronic, hardcopy, or orally). Incident-related documents are Federal records and subject to records management life cycle processes, including retention and destruction.

(1) General requirements for documenting incidents are:

- (a) Accurately and completely document all suspected and actual incidents and communicate incident information to the ASOD CSIRT;
- (b) Document all activities taken to handle the incident (i.e., each step taken and the outcome(s)) from the time the incident was detected to its final resolution;
- (c) Document communications, such as interviews with a user who reported a suspicious event, notifications to the ASOD CSIRT or senior managers, or requests for assistance; and
- (d) Include a date and timestamp (Coordinated Universal Time (UTC) when possible) for all key actions and the identity of the person making the entry.

(2) Documenting the following incident information is strongly recommended:

- (a) A summary of the incident, including dates and times (including time zone) when the incident occurred and it was detected (which may be after the date of occurrence);
- (b) Periodic status of the incident (e.g., new, in progress, forwarded for investigation, resolved);

- (c) Actions taken by all incident handlers and significant observations or comments by incident handlers;
  - (d) A list of evidence gathered during the incident investigation;
  - (e) Actions taken to protect impacted equipment or sensitive information and, if applicable, chain of custody for equipment and sensitive information;
  - (f) Contact information for other involved stakeholders (e.g., system owners, system administrators) or for any impacted organizations, whether internal or external to USDA;
  - (g) Incoming and outgoing communications with other groups or personnel, and the date and time of the communication;
  - (h) Locations of documents related to the incident, such as log files;
  - (i) Assessments of primary and secondary impacts of the incident;
  - (j) Mitigating factors (e.g., full disk encryption, two-factor authentication) that may reduce the impacts;
  - (k) Sources, methods, or tools used to identify the incident (e.g., intrusion detection system, audit log analysis, reported by system administrator or user).
  - (l) Indicators related to the incident (e.g., host names, domain names, network traffic characteristics, registry keys, X.509 certificates, hashes of attack signatures);
  - (m) Technical information about affected systems such as source and destination Internet Protocol (IP) addresses, port numbers, and protocols, if applicable;
  - (n) Details describing any vulnerabilities involved such as Common Vulnerabilities and Exposures (CVE) identifiers; and
  - (o) Next steps to be taken (e.g., rebuild the host, upgrade an application, harden the system configuration).
- (3) CNSI Spillage Documentation. System, network, and database administrators and agency and staff office incident management personnel are to:
- (a) Document the steps taken to contain, clean up, and mitigate a CNSI spillage; and
  - (b) Provide that documentation as proof of actions taken to OHS PDSO, taking care to store, handle, and transmit the documentation using secure methods appropriate to the classification level of the information.

- (4) Records Retention. Keep incident records and records of reporting incidents (both internal and external incidents) for 3 years after all necessary follow-up actions have been completed. Longer retention is authorized if the records are required for business use.

g. Incident Closure.

(1) General Incident Closure Process.

- (a) Any incident that is not a false positive remains open until:

- 1 All necessary mitigation actions (e.g., containment, eradication, and recovery) are complete; and
- 2 AD-3043 or AD-3038 with all required information and all incident documentation supporting the investigation and findings (e.g., logs, screen captures, output from scans, law enforcement reports, user awareness training certificates, credit monitoring offer letters for breaches) are submitted to the ASOD CSIRT.

The completed form and supporting documentation must be submitted to the ASOD CSIRT to close an incident. If additional details are required, the ASOD CSIRT will contact the responsible incident management personnel.

- (b) Mission Area Assistant CISOs or ISSPMs verify that criteria for containment and closure of incidents have been met. This verification is simply a step towards closure, but does not actually close the incident. Criteria for containment and closure for example includes the following activities:
  - 1 Containment. Reset of all user authentication credentials; compromised systems disconnected and undergoing analysis or being held for forensic analysis.
  - 2 Closure. Restored systems validated as compliant with required configurations; systems and devices scanned and no further traces of malware discovered.
- (c) The ASOD CSIRT validates completion of the mitigation efforts, verifies that affected systems and devices are no longer a threat to the USDA network, and validates that all required reporting information has been provided. Until these activities are completed, the incident remains open.
- (d) Reopening Incidents. Incidents may be reopened at the request of the ASOD CSIRT, the ASOD Director, the SAOP, the USDA CPO, or other senior officials from OIG or OHS.

(2) Plans of Action and Milestones (POA&M).

- (a) The FISMA data entry and reporting tool is used as follows for creating and managing PO&AMs:
  - 1 Create the POA&M in the information system or service, or the program that was affected; or
  - 2 Create the POA&M in the agency or staff office information security program for non-cyber breaches (e.g., loss of hardcopy) or for incidents that affect devices not associated with an information system or service.
- (b) POA&Ms for classified incidents are outside the scope of this document.
- (c) Agency and staff office incident management personnel must create a POA&M for unclassified incidents, whether system-related or program-related, when:
  - 1 An incident remains open (unresolved) for more than 30 days;
  - 2 Remedial actions are determined to be inadequate for incident closure for more than 30 days; or
  - 3 Required information on AD-3043 or AD-3038 has not been submitted.

(3) Closing Breaches.

- (a) The SAOP must certify by email that a moderate- or high-impact breach is closed.
- (b) The USDA CPO must approve closure of all other breaches.

(4) Closing CNSI Spillage Incidents.

- (a) OHS PDSO provides the final determination to close the CNSI spillage incident to the Senior Agency Official for CNSI/ Director of OHS and the USDA CISO.
- (b) For the ASOD CSIRT, the USDA CISO may deem the cybersecurity incident closed or identify additional steps to be taken before closure.

h. Post-incident Activities.

Post-incident activities include: producing after-action reports and improvement plans, particularly after major incidents; correlating and analyzing data across multiple past and recent incidents; and responding to requests for information about incidents.

- (1) Incident management personnel should conduct a post-incident review after each major incident or as instructed by the ASOD Director to produce an after-action report and identify lessons learned and good practices. Reviews may also be conducted for other actual or suspected incidents or for tests and exercises of the incident management plan.

- (a) Inputs to the post-incident review include:
    - 1 Debriefs with incident management personnel; users who reported the incident; system, network, or database administrators; or other offices or groups who participated in the response; and
    - 2 Analysis of information documenting the incident, whether in an automated tracking system or in hardcopy form such as logbooks.
  - (b) The after-action report should explain how the incident was detected and mitigated.
  - (c) The lessons learned should discuss insights into the incident management processes, including reporting, detection, and mitigation.
  - (d) The after-action report and lessons learned should be shared with appropriate stakeholders.
  - (e) After-action reports from similar incidents and tests or exercises of the incident management plan should be compared and analyzed for patterns of both strengths and weaknesses in capabilities.
- (2) Improvement Plans. All agencies and staff offices should develop and implement improvement plans for their incident management procedures, resources, and capabilities, based on post-incident reviews.
- (3) Correlation and Analysis of Incident Data.
- (a) Agencies and staff offices responsible for one or more high impact systems are required to correlate current and historical incident information and responses to individual incidents to achieve an organizationwide perspective on incident awareness and response, in compliance with NIST SP 800-53 incident response control “IR-4,” Enhancement 4.
  - (b) Examples of areas for correlation and analysis include:
    - 1 Indicator patterns;
    - 2 Similar attack actions and tactics, techniques, and procedures (TTP);
    - 3 Malware found; and
    - 4 Common vulnerabilities or misconfigurations exploited.
- (4) Ad Hoc Reporting. Agency and staff office incident management personnel must respond in a timely manner, using information from their incident records and other sources, to:

- (a) Data calls regarding actual or suspected cybersecurity incidents issued by the CISO or ASOD;
- (b) Requests from the USDA OIG; and
- (c) Requests from the Government Accountability Office (GAO).

## 8. NOTIFICATION TO CONGRESS ABOUT INCIDENTS PROCEDURES

USDA organizations should leverage these procedures to produce their own tailored procedures to notify Congress of an incident.

- a. Notification to Congress occurs on an incident-by-incident basis. This notification is mandated by FISMA for major incidents.
- b. The ASOD CSIRT provides the Office of Congressional Relations (OCR), the USDA CIO, the USDA CISO, and the ASOD Director with initial information about the incident as soon as possible after notifying US-CERT. The ASOD CSIRT also helps OCR prepare to answer possible questions from Congressional committees and members of Congress.
- c. OCR distributes the initial notification to the responsible Congressional committees not later than 7 days after the date on which there is a reasonable basis to conclude that the major incident has occurred. OCR informs the USDA CIO, the USDA CISO, and the ASOD Director when the notification has been sent.
- d. After the initial notification and within a reasonable period of time after additional information relating to the incident is discovered, the ASOD CSIRT updates the incident information for OCR, the USDA CIO, the USDA CISO, and the ASOD Director, and OCR provides the additional information to the responsible committees of Congress. The information update must include:
  - (1) A description of the major incident or related set of incidents;
  - (2) A summary of threats and threat actors, vulnerabilities, and impacts relating to the incidents;
  - (3) A summary of risk assessments conducted on the affected information systems before the date on which the incident occurred;
  - (4) A summary of the status of compliance of the affected information systems with applicable security requirements at the time of the incident; and
  - (5) A summary of the detection, response, and remediation actions.

## 9. ANNUAL AND QUARTERLY INCIDENT REPORTING PROCEDURES

USDA organizations should leverage these procedures to produce their own tailored annual and quarterly reporting procedures. The Department provides additional guidance for organizations when issuing requests for information.

- a. Annual FISMA Reporting. In compliance with the requirements of FISMA, an annual report, in unclassified form but including a classified annex if necessary, must be prepared and provided to the Director of OMB, the Secretary of DHS, committees of Congress, and the Comptroller General. The report must contain the following information:
  - (1) A description of each major incident or related sets of incidents, including summaries of:
    - (a) The threats and threat actors, vulnerabilities, and impacts relating to the incidents;
    - (b) The risk assessments conducted on the affected information systems before the date on which the incident occurred;
    - (c) The status of compliance of the affected information systems with applicable security requirements at the time of the incident; and
    - (d) The detection, response, and remediation actions.
  - (2) A description of each major incident that involved PII, including:
    - (a) The number of individuals whose information was affected by the major incident; and
    - (b) A description of the information that was breached or exposed.
  - (3) The total number of cyber incidents, including a description of incidents resulting in significant compromise of information security, system impact levels, types of incidents, and locations of affected systems.
- b. Quarterly Reporting.
  - (1) Quarterly reports must be prepared and submitted to meet OMB requirements and the President's Management Council's assessment criteria. The assessment criteria include metrics and not all assessment criteria pertain to incident management.
  - (2) Currently required incident management metrics are:
    - (a) Trending of percentage of successful incidents and attacks decreasing year over year; and

- (b) Number or percentage of public and internal notifications conducted within 30 days of detection and discovery of an incident.

## 10. INCIDENT MANAGEMENT PREPARATION PROCEDURES

USDA organizations should leverage these procedures to produce their own tailored incident management procedures.

Substantial preparation contributes to successful incident handling. Preparation includes, at a minimum, well documented procedures, an incident management plan, documentation and resources, identified and properly trained personnel, and testing of the plan and procedures at least annually. While the information in this Section applies specifically to agencies and staff offices, much of it is also pertinent to the ASOD CSIRT's incident management activities.

### a. Incident Management Procedures.

Each agency and staff office must develop, implement, and maintain incident management procedures based on the activities described in Section 7, Agency and Staff Office Incident Management Procedures, and supplemented with information from Section 6, Departmental Incident Management Procedures, as follows:

- (1) Formally document incident management procedures to contribute to effective responses to incidents. Good procedures:
  - (a) Are tailored to reflect the organization's size, structure, and functions, in addition to the types of information resources it is responsible for;
  - (b) Define requirements for reporting incidents and doing so in a timely manner;
  - (c) Identify incident management personnel and include current and accurate contact information for all personnel, group email addresses, or USDA organizations with incident management roles or equities;
  - (d) Identify non-USDA organizations that provide or support the information systems and services on behalf of USDA and any incident management roles and responsibilities of their personnel; and
  - (e) List other organizations, along with their contact information, that can provide support services during incident response or recovery, such as ISPs or hardware and software suppliers. IT vendors may, for example, provide support such as emergency patches for vulnerabilities in systems, devices, or software.
- (2) Align agency and staff office incident management procedures with the procedures described in this DM;

- (3) Detail specific technical and operational processes and techniques to be used by incident management personnel;
- (4) Include checklists (to minimize errors) and required forms or links to those forms;
- (5) Review and update procedures annually to reflect:
  - (a) Changes to the Department's incident management policy or procedures;
  - (b) Changes in the organization, its information resources, or personnel;
  - (c) Lessons learned from exercises or responses to incidents; and
  - (d) Must include all contact information, to ensure that the information remains current and accurate.
- (6) Disseminate or make available copies of the incident management procedures to incident management personnel within the organization; and
- (7) Ensure users and, where pertinent, service providers, contractors, subcontractors, and other organizations that own or operate information systems or services on behalf of USDA are aware of requirements for reporting all actual and suspected incidents to the ASOD CSIRT.

b. Incident Management Plans.

- (1) Each agency and staff office must have an incident management plan that includes, at a minimum, the following information:
  - (a) The information systems and services covered by the incident management plan and the interconnections with other information systems and services;
  - (b) Business-impact criticality of the organization's information resources and priorities for managing incidents and recovering information systems and services;
  - (c) Realistic worst-case scenarios and strategies for handling them;
  - (d) A PII Section if USDA PII is generated, collected, provided, transmitted, stored, or maintained;
  - (e) The organizational structure used for incident response (including other organizations such as the ASOD CSIRT, the USDA Privacy Office, and OIG), the roles and responsibilities of the agency or staff office incident management personnel and support personnel such as network and system administrators, and contact information for all identified organizations and individuals;
  - (f) Requirements for reporting incidents and the timeframes for reporting;

- (g) Requirements for documenting and tracking incidents and protection of sensitive incident information;
  - (h) Resources to support incident management and whether the resources are on hand or available by request;
  - (i) Requirements for training personnel with incident management responsibilities; and
  - (j) Requirements for testing the incident management plan.
- (2) The plan should be disseminated to the ASOD CSIRT or other offices having incident management equities or related responsibilities.
  - (3) Review the incident management plan at least twice annually (and update if necessary), including after incident response testing or any major incident.
    - (a) The review and update must include all contact information, to ensure that the information remains current and accurate.
    - (b) After each update, disseminate the contact information to each person with incident management responsibilities, technical personnel such as network and system administrators, group email addresses, and hotline numbers.

c. Inventory, System Documentation, and Technical Resources.

Current, accurate, and complete information in documentation and other file-based resources facilitate incident analysis, response, and recovery. Resources, such as hardware and software tools, help incident management personnel analyze, respond to, and recover from incidents.

- (1) Inventory. USDA's enterprise inventory system must have a current and accurate inventory of all agency and staff office IT devices and systems including their IP and Media Access Control (MAC) addresses, and high value assets (HVA).
- (2) Essential Information. Agency and staff office incident management personnel must have access to documentation and file-based resources including:
  - (a) Network diagrams;
  - (b) Inventory of all authorized hardware devices and ports and protocols for those devices, identified by criticality in the incident management plan;
  - (c) Inventory of all software and applications, including custom-developed code, open-source software, and vendor-provided software, identified by criticality in the incident management plan;
  - (d) All system installation or system administrator guides;

- (e) Vendor documentation for operating systems, databases, applications, appliances, and other information resources;
  - (f) Vendor documentation for cybersecurity products such as antivirus software, intrusion detection systems, or scanning tools;
  - (g) Configuration management baselines for all systems; and
  - (h) Cryptographic hashes of critical files such as operating systems and applications.
- (3) Recommended Information. Baselines of expected network, system, and application activity help to detect and analyze anomalous behaviors.
- (4) Resources for Incident Management. Resources, some essential and others desirable, are needed to effectively support incident management activities. The Mission Area Assistant CIO is responsible for funding the resources identified in the incident management plan. Examples of resources include:
- (a) Sufficient and secure system storage for logging events and tools for log analysis and correlation;
  - (b) Tools and supplies (e.g., incident tracking database, laptops, logbooks, evidence bags, digital cameras, encryption software) to document, track, and report incidents;
  - (c) Equipment, software, media, and other supplies for incident detection, analysis, response, and recovery (e.g., laptops for incident management personnel; spare workstations, servers, and networking equipment; backup devices; packet sniffers and protocol analyzers; cables; forensics workstations);
  - (d) Images of clean operating system and application installations for restoration and recovery purposes; and
  - (e) Any external services such as forensics expertise.
- (5) Tracking Mechanisms and Metrics.
- (a) An incident tracking mechanism supports effective incident management and is a necessary prerequisite for documenting incidents, reporting them, and conducting good analyses. Tracking mechanisms may be automated (e.g., a database, a service desk ticketing system) or manual (e.g., an incident logbook). A combination of manual and automated methods is often used.
    - 1 An automated tracking system is mandatory for agencies and staff offices responsible for moderate and high impact systems.

2 Agencies and staff offices responsible for low impact systems may use an automated or a manual tracking mechanism.

(b) Metrics. Incident management personnel should use the incident tracking mechanism to generate and report on incident management metrics. The types and amounts of information tracked shape the metrics that can be produced. Missing data elements in an incident record, however, reduce the usefulness of the metrics. Examples of metrics include the following:

- 1 Numbers of incidents by type within a defined time period;
- 2 Percent of incidents reported meeting mandatory reporting requirements;
- 3 Percent of incidents reported meeting the 1-hour reporting requirement;
- 4 Efficiency in resolving incidents (time to resolution);
- 5 Rate of successful incidents and attacks as a percentage of all incidents;
- 6 Trending of percentage of successful incidents and attacks;
- 7 Number or percentage of public and internal notifications about incidents conducted within 30 days of detecting or discovering the incidents; and
- 8 Resources expended in incident response (e.g., personnel, dollar amounts, supplies).

d. Personnel and Training.

- (1) Incident Management Personnel. Mission Area Assistant CIOs must formally designate members of their CSIRT, who may serve in a dual role such as the Mission Area Assistant CISO or ISSPM.
- (2) Personnel Qualifications. Incident management personnel, including CISOs, ISSPMs, and CSIRT members, must be technically qualified (meet agency or staff office knowledge, skill, or experience requirements for the various roles) to perform their responsibilities and have clearances appropriate to the categorization or classification of the systems they support.
- (3) CSIRT Staffing. Because incidents may occur or be discovered at any time, agency and staff CSIRT personnel must provide 24 hours a day, 7 days a week incident handling coverage for information systems and services owned or operated by the agency or staff office or by a contractor, subcontractor, or other organization on behalf of the agency or staff office. Agencies and staff offices may achieve this coverage by having and publicizing normal and after-hours contact information, in addition to information about the ASOD CSIRT hotline and mailbox.
- (4) Training and Awareness for Incident Management Personnel.

- (a) General. All personnel with identified incident management responsibilities must be aware of USDA's incident management policies and procedures and their organization's plan and procedures, including those for incidents involving PII and criminal activity or misuse.
  - 1 Annual role-based training is mandatory. In addition, these personnel may be required to take out-of-cycle training when changes occur in responsibilities, plans or procedures, threat vectors or exploit types, or the organization's information resources.
  - 2 Training may be accomplished through on-the-job training, role-based (formal, specialized, or functional) or certification training, participation in testing and exercises, or other means.
- (b) High Impact Systems. When an agency or staff office is responsible for one or more high-impact systems, training must incorporate simulated events for crisis situations and employ automated mechanisms (e.g., videos, online training environments, use of online support tools).
- (5) Training and Awareness for IT Staff. Personnel such as application developers, systems integrators, network administrators, system administrators, and database administrators must be aware of how they can develop and maintain their networks, systems, and applications in accordance with USDA's security standards. Properly developed and maintained networks, systems, and applications reduce the risk of vulnerabilities being exploited. Training may be accomplished through on-the-job training, role-based (formal, specialized, or functional) or certification training.
- (6) Awareness Training for Users. Incident management awareness training for users should encompass these topics:
  - (a) Policies and procedures regarding appropriate use of networks, systems, and applications;
  - (b) Incident management policies and procedures; and
  - (c) Their responsibilities for detecting and reporting all types of incidents.Applicable lessons learned from previous incidents may also be shared with users so they can see how their actions could affect the organization.
- e. Testing and Exercises.
  - (1) Testing and exercises are used to:
    - (a) Validate the accuracy, completeness, and usefulness of plans and procedures;
    - (b) Improve the skills and capabilities of incident management personnel;

- (c) Determine the adequacy of incident management resources; and
  - (d) Understand the effects on organizational operations (e.g., reduction in mission capabilities), organizational assets, and individuals.
- (2) Types of testing include use of checklists, walk-through or tabletop exercises, simulations, and functional exercises.
- (3) Requirements for Testing.
- (a) Test incident management plans and the associated procedures at least twice annually. This requires adequate funding and a set schedule for the testing.
  - (b) The type and complexity of the testing must be commensurate with the highest security impact level of any information system in the agency or staff office inventory.
  - (c) As part of the testing:
    - 1 Verify roles and responsibilities;
    - 2 Exercise a worst-case incident scenario;
    - 3 Exercise detection of or protection from phishing attempts, attempts to access large volumes of data, or attempts to exfiltrate data; and
    - 4 Exercise recovery from (not just response to) a breach, a destructive malware campaign, or any scenario based on recent events and available threat data.
  - (d) Coordinate testing for moderate and high impact systems with organizational elements responsible for related plans; such as business continuity plans, contingency plans, disaster recovery plans, continuity of operations plans, crisis communications plans, critical infrastructure plans, or occupant emergency plans.
  - (e) Document the results of the testing, including the weaknesses discovered in the plan, procedures, resources, personnel knowledge or skills, or coordination.
  - (f) Create a POA&M for any weakness discovered during the testing that is not mitigated within 30 days.
  - (g) Develop an after-action report summarizing lessons learned and best practices and share this with appropriate stakeholders.
- f. Information Resources, Situational Awareness, and Information Sharing.

It is very important for incident management personnel to stay informed about cybersecurity threats and exploits, incidents, attack methods, and appropriate courses of action such as mitigation techniques.

- (1) Methods for obtaining information include education and training; information from US-CERT; participation in the Government Forum of Incident Response and Security Teams (GFIRST); and open source information on the web.
  - (a) US-CERT provides technical information in the form of alerts about security issues, vulnerabilities, and exploits; a current activity report on high-impact types of security incidents; and bulletins summarizing vulnerabilities and any available patch information. The website is [National Cyber Awareness System](#).
  - (b) GFIRST is a peer group for information security personnel responsible for securing U.S. Government information systems. Through GFIRST, incident management personnel can stay informed on the latest technologies and exploits. The GFIRST Compartment in the US-CERT Portal provides a secure collaborative system to share sensitive cyber-related information. Additional information is available at [Government Forum of Incident Response and Security Teams \(GFIRST\)](#).
  - (c) Examples of open source information include cybersecurity firms; communities of incident responders and cybersecurity experts; cybersecurity blogs; media reports; academic and think tank literature and reports; conference presentations; or reports from other government agencies.
- (2) Disseminate cyber threat and exploit warning information to appropriate personnel in a timely manner. For example, CISOs, ISSPMs, and CSIRT personnel are expected to distribute information appropriate for system owners or system, network, or database administrators and other information (such as about phishing attacks) appropriate for all users.
- (3) The ASOD Director or designees from the ASOD CSIRT disseminate:
  - (a) Information derived from analysis and correlation of USDA incident management data to appropriate stakeholders; and
  - (b) Information from US-CERT and other external sources.

## 11. ROLES AND RESPONSIBILITIES

- a. The Secretary of Agriculture will make a final decision regarding whether to provide notification to individuals affected by a breach.
- b. The USDA CIO will:

- (1) Notify Congress about major incidents initially within 7 days and with follow-up information within a reasonable period of time, in collaboration with the USDA CISO and the Assistant Secretary for Congressional Relations; and
  - (2) Determine if cybersecurity incident information may be released publicly, based on factors such as whether the release of information might negatively affect factors such as criminal investigations or CNSI or delegate this authority to the USDA CISO.
- c. The USDA CISO will:
- (1) Notify Congress about major incidents initially within 7 days and with follow-up information within a reasonable period of time, in collaboration with the USDA CIO and the Assistant Secretary for Congressional Relations; and
  - (2) Direct any action, including shutdown, with respect to any system on which CNSI is spilled.
- d. The ASOD Director will:
- (1) Designate a primary and secondary point of contact in the ASOD CSIRT for all interactions with US-CERT;
  - (2) Appoint an incident commander for a major incident or when warranted by other circumstances;
  - (3) Set priorities based on factors such as functional impact, information impact, recoverability, and resource availability during complex or crisis-level incidents;
  - (4) Activate the standing Federal Network Authorization so US-CERT can access USDA networks and provide on-site technical assistance or delegate this authority to the incident commander;
  - (5) Authorize ASOD CSIRT personnel to collaborate and coordinate, on a need-to-know basis, with external entities or delegate this authority to the incident commander;
  - (6) Request agency and staff office incident management personnel to provide technical or investigation assistance to other agencies or staff offices or delegate this authority to ASOD CSIRT personnel;
  - (7) Ensure that all incident handling activities are validated as complete, including additional reporting to US-CERT;
  - (8) Reopen closed incidents when warranted;
  - (9) Ensure that the Department incident management plan and associated procedures are tested at least annually; and

- (10) Disseminate analytical products about incidents and incident management to appropriate stakeholders.
- e. The ASOD CSIRT and ASOD CSIRT Personnel will:
- (1) Serve as USDA's 24 hours a day, 7 days a week central cybersecurity incident management group, and the central contact and coordination point to US-CERT;
  - (2) Promptly report incidents to:
    - (a) US-CERT in accordance with *US-CERT Federal Incident Notification Guidelines*;
    - (b) The USDA CIO, USDA CISO, and the OCR for all major incidents; and
    - (c) Responsible USDA offices and external organizations based on the type of incident.
  - (3) Ensure actions are immediately performed to mitigate significant incidents or threats;
  - (4) Ensure that the correct incident reporting forms are used and properly completed;
  - (5) Provide technical and non-technical assistance to agencies and staff offices upon request and collaborate with appropriate USDA and external entities to manage incidents;
  - (6) Disseminate information derived from incident analysis and correlation and cyber threat and exploit warning, and provide direction to detect, investigate, and mitigate potential or imminent threats and suspected or actual exploits;
  - (7) Deploy automated tools to support detection and analysis and run them on a regular schedule;
  - (8) Coordinate IOC scanning activities with US-CERT and with agencies and staff offices when US-CERT issues an alert about a suspected or known compromise with the potential to affect U.S. Government systems;
  - (9) Collaborate with the OIG TCD on securing incident evidence;
  - (10) Validate completion of incident mitigation efforts, verify that affected systems and devices are no longer a threat to the USDA network, and validate that all required reporting information has been provided by agency and staff office incident management personnel;
  - (11) Ensure that agencies and staff offices create POA&Ms for incidents when any of the criteria for incident-related POA&Ms are not met;

- (12) Test the Departmental incident management plan and associated procedures at least annually; and
  - (13) Correlate and analyze current and historical incident information and responses to incidents and produce metrics for internal and external reporting purposes.
- f. The SAOP will:
- (1) Provide direction and guidance to all incident management personnel responding to cyber and non-cyber breaches involving privacy information;
  - (2) Convene the USDA CIRG to coordinate USDA responses to moderate or high impact breaches;
  - (3) Advise the Secretary of Agriculture on whether and when to notify individuals potentially affected by a breach;
  - (4) With concurrence of the Secretary of Agriculture, require notification be sent to individuals affected by a breach and review and approve the content of those notifications; and
  - (5) Certify by email that an incident for which the CIRG has been convened is closed.
- g. The USDA CPO will:
- (1) Provide direction and guidance to all incident management personnel regarding cyber and non-cyber breaches;
  - (2) Escalate moderate and high impact breaches to the SAOP; and
  - (3) Approve closure of all major breaches or reopen closed incidents when warranted.
- h. The IG and/or the IG of the TCD will:
- (1) Investigate all suspected or actual criminal activity incidents and fraud, waste, and abuse of information resources;
  - (2) Direct incident management personnel on securing incident evidence to comply with the rules of preservation of evidence; and
  - (3) Coordinate taking possession of GFE.
- i. The Senior Agency Official for CNSI/Director of OHS will direct any action, including shutdown, with respect to any system on which CNSI is spilled.
- j. The OHS PDSO Chief will:
- (1) Coordinate incident management with the ASOD Director;

- (2) Conduct official investigations of suspected or actual CNSI spillage incidents and incidents affecting classified systems, and be responsible for managing the security of the information;
  - (3) Coordinate with the data owner during CNSI spillage incidents and approve containment and cleanup strategies;
  - (4) Notify and coordinate with the security staff of any external network owner if an external network may have been contaminated by a USDA CNSI spillage incident; and
  - (5) Provide final determination to close CNSI spillage incidents.
- k. The OHS Insider Threat Coordinator will:
- (1) Conduct inquiries on all potential insider threat incidents;
  - (2) Coordinate with appointed stakeholders, including within OCIO, to obtain relevant electronic records, files and other information necessary to identify, analyze, and resolve insider threat matters; and
  - (3) Serve as the USDA liaison to the intelligence community for insider threat and counterintelligence activities within the Department, to include referrals to the FBI.
- l. The Assistant General Counsel of OGC, General Law and Research Division will:
- (1) Review and approve any communications to individuals impacted by a breach in which the individuals are or were litigants; and
  - (2) Provide legal advice for incidents involving other government entities at the Federal, State, local, tribal, and territorial levels.
- m. The Director of OHRM or agency and staff office personnel responsible for employee relations or adverse personnel actions will:
- (1) Become involved when incidents may require adverse personnel action; and
  - (2) Coordinate with OC to provide breach notifications to current and former USDA employees, retirees, and retirees' survivors or designated dependents.
- n. The CFO will:
- (1) Be consulted when an incident affects a financial system or financial records; and
  - (2) Issue notifications to financial institutions about incidents affecting financial systems at USDA.
- o. The Director of OC will:

- (1) Coordinate public notification of cybersecurity incidents outside of USDA with the USDA CIO and other USDA officials, depending on the type of incident; and
- (2) Be responsible for breach notifications when the CIRG has not been convened or, optionally, delegate this responsibility to agency and staff office public affairs offices.

OCR and the Assistant Secretary for Congressional Relations will collaborate with the USDA CIO, the USDA CISO, and the Director of OC when Congress must be notified about major incidents at USDA and forward notifications to the appropriate Congressional committees.

p. Mission Area Assistant CIOs will:

- (1) Formally designate one or more technically qualified points of contact (POC) with appropriate clearances to function as the CSIRT for that agency or staff office. The POC may also serve in a dual role such as the Mission Area Assistant CISO or ISSPM; and
- (2) Ensure that USDA's enterprise inventory system has a current and accurate inventory of all IT devices and systems in the scope of their responsibility and identify those that are HVAs to support incident management.

q. Mission Area Assistant CISOs and ISSPMs will:

- (1) Ensure that detection tools are run regularly using automatically updated indicators and, when notified by the ASOD CSIRT, that IOC scans are conducted using provided indicators within 24 hours of notification;
- (2) Inform the ASOD CSIRT and provide specific guidance for handling GFE and information on that GFE when the agency or staff office is operating under a law specific to its mission; and
- (3) Verify that criteria for containment and closure of incidents have been met.

r. Mission Area Assistant CISOs, ISSPMs, and Incident Management Personnel (CSIRT Members) will:

- (1) Document their organization's incident management plan and procedures, test them twice annually, and review and update them whenever there are significant changes or identified shortcomings;
- (2) Provide 24 hours a day, 7 days a week incident handling coverage, which can include publicizing after-hours contact information;
- (3) Promptly report to the ASOD CSIRT in the required timeframe suspected and actual incidents of all types (e.g., suspected malicious code, inadvertent release of PII, suspected criminal activity, possible spillage of CNSI);

- (4) Promptly respond to all inquiries and tickets issued by the ASOD CSIRT;
  - (5) Disseminate procedures and requirements for reporting suspected and actual incidents to users and, where pertinent, to contractors, subcontractors, service providers, and other organizations that own or operate information systems or services on behalf of USDA;
  - (6) Maintain complete and accurate current and historical records of actual and suspected incidents;
  - (7) Cooperate with and perform all incident investigative actions advised by the ASOD CSIRT or other authorized internal or external entities in a timely manner;
  - (8) Request assistance, as needed, from the ASOD CSIRT and provide technical or investigation assistance to other agencies and staff offices when requested by the ASOD CSIRT;
  - (9) Refrain from directly contacting external entities, such as US-CERT, unless specifically requested to do so by the ASOD CSIRT;
  - (10) Ensure that sensitive incident information is handled properly and appropriately protected to maintain confidentiality and integrity;
  - (11) Disseminate cyber threat and exploit warning information to appropriate personnel in a timely manner;
  - (12) Create POA&Ms in accordance with [DR 3565-003](#), *Plan of Action and Milestones Policy* for any incident that is not remediated and for weaknesses discovered during incident management plan testing;
  - (13) Be familiar with and follow Departmental incident management policies and procedures and their organization's plans and procedures;
  - (14) Take annual role-based training on incident management; and
  - (15) Respond to data calls regarding actual or suspected security incidents in a timely manner.
- s. System, Network, and Database Administrators will:
- (1) Perform incident management actions as directed by the ASOD CSIRT and other authorized officials in a timely manner; and
  - (2) Document the steps taken to contain, clean up, and mitigate a CNSI spillage and provide that documentation to the ASOD CSIRT and OHS PDSD.

- t. All employees, contractors, subcontractors, service providers, and others who work on behalf of USDA will:
  - (1) Protect and properly handle incident information (e.g., control PII until authorized personnel assume custody of the information); and
  - (2) Refrain from deleting or forwarding emails, attachments, or hyperlinks with sensitive information such as PII, CUI, or CNSI.

## 12. INQUIRIES

Direct all questions concerning this DR to the OCIO, Information Security Center via email to the [csc@ocio.usda.gov](mailto:csc@ocio.usda.gov) mailbox.

-END-

## APPENDIX A

### AUTHORITIES AND REFERENCES

[AD-3038](#), *Cyber Security Incident Report Personally Identifiable Information (PII) Incident*, June 2016

[AD-3043](#), *ASOC Incident Report*, June 2016

[AD-3050](#), *PII Incident Non Disclosure Agreement*, June 2013

[Confidential Information Protection and Statistical Efficiency Act of 2002](#) (CIPSEA), 44 United States Code (U.S.C.) §3501 (2017)

[Critical Infrastructure Information Act of 2002](#), 6 U.S.C. 121, et seq.

Department of Homeland Security (DHS), [Federal Information Security Modernization Act](#), required reporting requirements

DHS, [US-CERT Federal Incident Notification Guidelines](#), September 2016

DHS, [US-CERT Government Forum of Incident Response and Security Teams \(GFIRST\)](#)

DHS, [US-CERT National Cyber Awareness System](#)

DHS, [NCCIC National Cyber Incident Scoring System](#)

[Executive Order \(EO\) 12958](#), *Classified National Security Information*, April 17, 1995

[E.O. 13292](#), *Further Amendment to Executive Order 12958, as Amended, Classified National Security Information*, March 25, 2003

[E.O. 13556](#), *Controlled Unclassified Information*, November 4, 2010

[E.O. 13587](#), *Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information*, October 7, 2011

*Federal Information Security Modernization Act of 2014*, ([FISMA](#)), 44 U.S.C. §3551, et seq.

GAO, [GAO Report 08-536](#), *Privacy: Alternatives Exist for Enhancing Protection of Personally Identifiable Information*, May 2008

General Services Administration, [President's Management Council](#)

National Archives and Records Administration (NARA), *Information Systems Security Records*, [General Records Schedule \(GRS\) 3.2](#), September 2014

NIST, Federal Information Processing Standard Publication, [\(FIPS PUB\) 140-2](#), *Security Requirements for Cryptographic Modules*, May 25, 2001

NIST, [FIPS PUB 200](#), *Minimum Security Requirements for Federal Information and Information Systems*, March 2006

NIST, Interagency Report ([IR](#)) [7298](#) Revision 2, *Glossary of Key Information Security Terms*, May 2013

NIST, [SP 800-53 Revision 4](#), *Security and Privacy Controls for Federal Information Systems and Organizations*, April 2013 with updates as of January 22, 2015

NIST, [SP 800-61 Revision 2](#), *Computer Security Incident Handling Guide*, August 2012

NIST, [SP 800-122](#), *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*, April 2010

NIST, [SP 800-150](#), *Guide to Cyber Threat Information Sharing*, October 2016

NIST, [SP 800-171 Revision 1](#), *Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations*, December 2016

OIG, Form OIG-8440-1, *Evidence Receipt*, October 1995

Office of the Director of National Intelligence (ODNI), National Counterintelligence and Security Center, [National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs](#), November 21, 2012

OMB, Circular [A-130](#), *Managing Information as a Strategic Resource*, July 28, 2016

OMB, Memorandum [M-16-04](#), *Cybersecurity Strategy and Implementation Plan (CSIP) for the Federal Civilian Government*, October 30, 2015

OMB, Memorandum [M-17-12](#), *Preparing for and Responding to a Breach of Personally Identifiable Information*, January 3, 2017

OMB, Memorandum [M-19-02](#), *Fiscal Year 2018-2019 Guidance on Federal Information Security and Privacy Management Requirements*, October 25, 2018

[Protected Critical Infrastructure Information](#), 6 Code of Federal Regulations Part 29, 2018

[Privacy Act of 1974](#), 5 U.S.C. 552a, December 31, 1974

USDA, [DM 3300-005](#), *Policies for Planning and Managing Wireless Technologies in USDA*, November 10, 2010

USDA, [DM 3440-001](#), *USDA Classified National Security Information Program Manual*, June 9, 2016

USDA, [DR 1700-002](#), *OIG Organization and Procedures*, June 17, 1997

USDA, [DR 3080-001](#), *Records Management*, June 16, 2016

USDA, [DR 3085-001](#), *Vital Records Management Program*, August 19, 2011

USDA, [DR 3090-001](#), *Litigation Retention Policy for Documentary Materials including Electronically Stored Information*, May 28, 2008

USDA, [DR 3440-001](#), *USDA Classified National Security Information Program Regulation*, June 9, 2016

USDA, [DR 3440-002](#), *Control and Protection of Sensitive Security Information*, January 30, 2003

USDA, [DR 3505-005](#), *Cybersecurity Incident Management*, November 30, 2018

USDA, [DR 3545-001](#), *Information Security Awareness and Training Policy*, October 22, 2013

USDA, [DR 3565-003](#), *Plan of Action and Milestones Policy*, September 25, 2013

USDA, [DR 4600-003](#), *USDA Insider Threat Program*, June 30, 2014

USDA, Memorandum, [Minimum Safeguards for Protecting Personally Identifiable Information \(PII\)](#), August 5, 2016

USDA, [Personally Identifiable Information \(PII\) Core Incident Response Group \(CIRG\) PII Breach Notification & Incident Response Plan \(IRP\)](#), Revision 4.6, November 23, 2017

## APPENDIX B

### DEFINITIONS

- a. Automated Tracking System. A software system capable of collecting, analyzing, monitoring, or tracking incident information.
- b. Breach. The loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar occurrence where (1) a person other than an authorized user accesses or potentially accesses personally identifiable information or (2) an authorized user accesses or potentially accesses personally identifiable information for an other than authorized purpose. (Source: OMB M-17-12)
- c. Classified Information. See “classified national security information.”
- d. Classified National Security Information. Information that has been determined pursuant to Executive Order 13526 or any predecessor order to require protection against unauthorized disclosure and is marked to indicate its classified status when in documentary form. (Source: NIST IR 7298 Revision 2)
- e. Compromise. Disclosure of information to unauthorized persons, or a violation of the security policy of a system in which unauthorized intentional or unintentional disclosure, modification, destruction, or loss of an object may have occurred. (Source: NIST IR 7298 Revision 2)
- f. Computer Security Incident. See “incident.”
- g. Controlled Unclassified Information. Information that requires safeguarding or dissemination controls pursuant to and consistent with applicable law, regulations, and government-wide policies but is not classified under Executive Order 13526 or the *Atomic Energy Act*, as amended. (Source: Executive Order 13556)
- h. Cybersecurity Incident. See “incident.”
- i. Data Breach. See “breach.”
- j. Event. Any observable occurrence in a network or system. Events with negative consequences are referred to as adverse events. (Source: NIST SP 800-61 Revision 2)
- k. Exploit. A technique to breach the security of a network or information system in violation of security policy.
- l. Federal Information. Information created, collected, processed, maintained, disseminated, or disposed of by or for the Federal Government, in any medium or forum. (Source: OMB Circular A-130)

- m. Federal Information System. An information system used or operated by an executive agency, by a contractor of an executive agency, or by another organization on behalf of an executive agency. (Source: NIST, SP 800-53 Revision 4)
- n. Functional Impact. Adverse impacts to business functionality provided by the affected systems. (Source: *US-CERT Federal Incident Notification Guidelines*, see related terms “information impact” and “recoverability.”)
- o. Harm. Any adverse effects that would be experienced by an individual (i.e., that may be socially, physically, or financially damaging) or an organization if the confidentiality of PII were breached. (Source: NIST, SP 800-122)
- p. High Value Asset. Those assets, systems, facilities, data and datasets that are of particular interest to potential adversaries. These assets, systems, and datasets may contain sensitive controls, instructions or data used in critical Federal operations, or house unique collections of data (by size or content) making them of particular interest to criminal, politically-motivated, or state-sponsored actors for either direct exploitation of the data or to cause a loss of confidence in the U.S. Government. (Sources: OMB M-16-04)
- q. Improper Usage. Any incident resulting from a violation of an organization’s acceptable use policies by an authorized user. (Source: NIST, SP 800-61 Revision 2)
- r. Incident. An occurrence that (1) actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or (2) constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies. (Source: FISMA)  
  
Note: An occurrence may be identified as an incident, but later identified as a breach once it is determined that PII is involved. Also, “incident” encompasses more specific terms such as “cybersecurity incident,” “information security incident,” “computer security incident,” spillage of CNSI, or exposure of CUI.
- s. Incident Handling. The mitigation of violations of security policies and recommended practices. (Source: NIST, SP 800-61 Revision 2)
- t. Incident management personnel. Personnel who are part of a CSIRT, those who manage CSIRT personnel, and potentially other personnel with incident handling responsibilities. Examples include Mission Area Assistant CISOs, ISSPMs, privacy office personnel at the Departmental or agency and staff office levels, and audit or investigations personnel from the OIG.
- u. Incident Management Plan. Provides a roadmap for implementing an incident response program based on the organization’s policy. The plan indicates both short- and long-term goals for the program, including metrics for measuring the program. The incident response plan should also indicate how often incident handlers should be trained and the requirements for incident handlers. (Source: Adapted from NIST, SP 800-61 Revision

2). See Section 3c**Error! Reference source not found.** in this DM for additional information.

Note: The term “incident management plan” is used in this DR instead of “incident response plan,” unless the title of a referenced source specifically uses the latter term. An incident management plan is different from an “incident response plan” or “cyber incident response plan,” which are contingency planning procedures for systems.

- v. Indicator. See “indicator of compromise.”
- w. Indicator of Compromise. A sign that an incident may have occurred or may be currently occurring. (Source: NIST, SP 800-61 Revision 2)
- x. Information Impact. The extent of compromise or effect on information confidentiality, integrity, or availability, covering one or more information types (classified, proprietary, or privacy). (Source: *US-CERT Federal Incident Notification Guidelines*)
- y. Information resources. Encompasses information, information systems, and information services.
- z. Information Security Incident. See “Incident.”
- aa. Insider Threat. The threat that an insider will use her/his authorized access, wittingly or unwittingly, to do harm to the security of United States. This threat can include damage to the United States through espionage, terrorism, unauthorized disclosure of national security information, or through the loss or degradation of departmental resources or capabilities. (Source: NIST, SP 800-53 Revision 4)
- bb. Major Incident. Is either:
  - (1) Any incident that is likely to result in demonstrable harm to the national security interests, foreign relations, or the economy of the United States or to the public confidence, civil liberties, or public health and safety of the American people. Using the DHS [NCCIC National Cyber Incident Scoring System](#) this includes Level 3 events (orange), defined as those that are “likely to result in a demonstrable impact to public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence”; Level 4 events (red), defined as those that are “likely to result in a significant impact to public health or safety, national security, economic security, foreign relations, or civil liberties”; and Level 5 events (black), defined as those that “pose an imminent threat to the provision of wide-scale critical infrastructure services, national government stability, or the lives of US persons”. Agencies should determine the level of impact of the incident by using the existing incident management process established in NIST SP 800-61 Revision 2; or
  - (2) A breach that involves personally identifiable information (PII) that, if exfiltrated, modified, deleted, or otherwise compromised, is likely to result in demonstrable harm to the national security interests, foreign relations, or the economy of the

United States, or to the public confidence, civil liberties, or public health and safety of the American people. (Source: OMB M-19-02)

- (3) Note: A major incident determination is required for any unauthorized modification of, unauthorized deletion of, unauthorized exfiltration of, or unauthorized access to the PII of 100,000 or more people. (Source: OMB M-19-02)
- cc. National Security System. Any information system (including any telecommunications system) used or operated by an agency or by a contractor of an agency, or other organization on behalf of an agency (1) the function, operation, or use of which involves intelligence activities; involves cryptologic activities related to national security; involves command and control of military forces; involves equipment that is an integral part of a weapon or weapons system; or is critical to the direct fulfillment of military or intelligence missions; or (2) is protected at all times by procedures established for information that have been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept classified in the interest of national defense or foreign policy. (Source: NIST IR 7298 Revision 2)
- dd. Personally Identifiable Information. Any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information. (Source: NIST, SP 800-122)
- ee. Protected Critical Infrastructure Information. Information not customarily in the public domain and related to the security of critical infrastructure or protected systems that has been validated and voluntarily submitted, directly or indirectly, to DHS for its use regarding the security of critical infrastructure and protected systems, analysis, warning, interdependency study, recovery, reconstitution, or other appropriate purpose, and any information, statements, compilations or other materials reasonably necessary to explain the critical infrastructure information (CII), put the CII in context, describe the importance or use of the CII, when accompanied by an express statement indicating an expectation of protection from disclosure as provided by the provisions of the *Critical Infrastructure Information Act of 2002*. (Source: Adapted from [Protected Critical Infrastructure Information](#))
- ff. Recoverability. The amount of time and resources needed to recover from the incident, factoring in the size of the incident and the types of information and information systems and services affected. (Source: *US-CERT Federal Incident Notification Guidelines*, See related terms "functional impact" and "information impact.")
- gg. Sensitive Information; also, Sensitive Incident Information. Information where the loss, misuse, or unauthorized access or modification could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under the *Privacy Act of 1974*; that has not been specifically authorized under

criteria established by an Executive Order or an Act of Congress to be kept classified in the interest of national defense or foreign policy. (Source: NIST, SP 800-53 Revision 4)

- hh. Spillage. Security incident that results in the transfer of classified or controlled unclassified information onto an information system not authorized for the appropriate security level. (Source: NIST, IR 7298 Revision 2)
- ii. Threat. The potential source of an adverse event. (Source: NIST, SP 800-61 Revision 2)
- jj. Unauthorized Access. The act or process of logical or physical access without permission to a Federal agency information, information system, application, or other resource. (Source: OMB M-19-02)
- kk. Unauthorized Deletion. The act or process of removing information from an information system without authorization or in excess of authorized access. (Source: OMB M-19-02)
- ll. Unauthorized Exfiltration. The act or process of obtaining, without authorization or in excess of authorized access, information from an information system without modifying or deleting it. (Source: OMB M-19-02)
- mm. Unauthorized Modification. The act or process of changing components of information and/or information systems without authorization or in excess of authorized access. (Source: OMB M-19-02)
- nn. Vulnerability. A weakness in a system, application, or network that is subject to exploitation or misuse. (Source: NIST, SP 800-61 Revision 2)
- oo. X.509 Certificate. The X.509 public-key certificate or the X.509 attribute certificate, as defined by the ISO/ITU-T X.509 standard. Most commonly (including in this document), an X.509 certificate refers to the X.509 public-key certificate. (Source: NIST IR 7298 Revision 2)

## APPENDIX C

### ACRONYMS AND ABBREVIATIONS

AD	Agriculture Department
ASOD	Agriculture Security Operations Division
CII	Critical Infrastructure Information
CIO	Chief Information Officer
CIPSEA	Confidential Information Protection and Statistical Efficiency Act
CIRG	Core Incident Response Group
CISO	Chief Information Security Officer
CNSI	Classified National Security Information
CNSS	Committee on National Security Systems
CPO	Chief Privacy Officer
CSIP	Cybersecurity Strategy and Implementation Plan
CSIRT	Cyber Security Incident Response Team
CUI	Controlled Unclassified Information
CVE	Common Vulnerabilities and Exposures
DHS	Department of Homeland Security
DM	Departmental Manual
DR	Departmental Regulation
E.O.	Executive Order
FBI	Federal Bureau of Investigation
FIPS PUB	Federal Information Processing Standards Publication
FISMA	Federal Information Security Modernization Act
GAO	Government Accountability Office
GFE	Government Furnished Equipment
GFIRST	Government Forum of Incident Response and Security Teams
GRS	General Records Schedule
HVA	High Value Asset
IOC	Indicator of Compromise
IG	Inspector General
IP	Internet Protocol
IR	Interagency Report
IRP	Incident Response Plan
ISC	Information Security Coordinator
ISP	Internet Service Provider
ISSPM	Information Systems Security Program Manager
IT	Information Technology
MAC	Media Access Control
NARA	National Archives and Records Administration
NCCIC	National Cybersecurity and Communications Integration Center
NIST	National Institute of Standards and Technology
NSS	National Security System
NSSP	National Security System Program
OC	Office of Communications

OCFO	Office of the Chief Financial Officer
OCIO	Office of the Chief Information Officer
OCR	Office of Congressional Relations
ODNI	Office of the Director of National Intelligence
OGC	Office of the General Counsel
OHRM	Office of Human Resources Management
OHS	Office of Homeland Security
OIG	Office of the Inspector General
OMB	Office of Management and Budget
PDSD	Personnel and Document Security Division
PII	Personally Identifiable Information
POA&M	Plan of Action and Milestones
POC	Point of Contact
SAOP	Senior Agency Official for Privacy
SP	Special Publication
SSO	Special Security Officer
TCD	Technical Crimes Division
TTP	Tactics, Techniques, and Procedures
U.S.C.	United States Code
US-CERT	United States Computer Emergency Readiness Team
USDA	United States Department of Agriculture
UTC	Coordinated Universal Time