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

DEPARTMENTAL REGULATION	NUMBER: DR 3505-005
SUBJECT: Cybersecurity Incident Management	DATE: November 30, 2018
OPI: Office of the Chief Information Officer, Information Security Center	EXPIRATION DATE: November 30, 2023

1. PURPOSE

a. This Departmental Regulation (DR) establishes the United States Department of Agriculture (USDA) policy for preparing for, responding to, and reporting cybersecurity incidents. Cybersecurity incident management governs the activities for mitigating risks from such incidents before substantial harm occurs and provides timely notification to and consultation with appropriate entities.

b. It is the policy of USDA to comply with Federal requirements to establish, implement, and enforce an incident management policy to continually manage risks to USDA information resources.

c. This policy complies with the requirements of:

(1) The *Federal Information Security Modernization Act of 2014* (FISMA);

(2) The Office of Management and Budget (OMB) Circular A-130, *Responsibilities for Protecting Federal Information Resources*, Memoranda M-19-02, *Fiscal Year 2018-2019 Guidance on Federal Information Security and Privacy Management Requirements*, and M-17-12, *Preparing for and Responding to a Breach of Personally Identifiable Information*;

(3) The Federal Information Processing Standards Publication (FIPS PUB) 200, *Minimum Security Requirements for Federal Information and Information Systems*; and

(4) The National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, and NIST SP 800-61 Revision 2, *Computer Security Incident Handling Guide*.

d. This policy serves as the foundation on which USDA Mission Areas, agencies, and staff offices will develop and implement their own incident management procedures that comply with Federal and Departmental requirements and align with USDA's incident management policy.

2. SPECIAL INSTRUCTIONS/CANCELLATION

a. This policy supersedes DR 3505-005, *USDA Cyber Security Incident Management Policy*, dated October 31, 2013, in its entirety.

b. This policy is effective immediately and remains in effect until it is superseded or expires.

c. All Mission Areas, agencies, and staff offices will align their incident management procedures with this policy within 6 months of the publication date.

d. Terminology in this policy 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 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;" an example is 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 NIST SP 800-61 Revision 2, 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;

(3) The terms “response” and “incident response” may be specific and narrow or general and broad in meaning. The general and broad meaning encompasses multiple incident management activities, including analysis, notification, mitigation, or application of countermeasures, containment, eradication, and recovery. The specific and narrow meaning is any one of these activities. NIST uses the terms “incident response” and “incident handling” as synonyms; and

(4) The term “United States Computer Emergency Readiness Team” (US-CERT) will be used as a replacement for “the Federal information security incident center” identified in FISMA.

3. BACKGROUND

OMB Circular A-130 requires Federal Agencies to undertake a set of actions to ensure they can react appropriately to information security incidents. The set includes implementing policies and procedures; establishing roles and responsibilities; maintaining incident response capabilities and mechanisms; reporting; periodic testing of the procedures; documenting lessons learned; and verifying that corrective actions are implemented.

FISMA directs Federal Agencies to develop and implement cyber incident management programs. FISMA also imposes on Federal Agencies notification measures to be taken during major incidents and annual incident reporting requirements. FISMA assigns responsibility to the Secretary of the Department of Homeland Security (DHS) for developing and overseeing the implementation of binding (i.e., compulsory) operational directives to Federal Agencies to implement OMB-issued policies, principles, standards, and guidelines on information security in general.

4. SCOPE

a. This policy applies to:

(1) All USDA Mission Areas, agencies, staff offices, employees, appointees, contractors, and others who work for, or on behalf of, USDA;

(2) All Federal information, in any medium or form, 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, USDA contractors, or other organizations 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; and

(5) All incidents affecting personally identifiable information (PII), whether cyber-related or non-cyber related.

b. Nothing in this policy alters the requirements for the protection of information associated with national security systems, such as those identified in FISMA, policies, directives, instructions, and standards issued by the Committee on National Security Systems (CNSS), or the intelligence community.

5. POLICY

a. All Mission Areas, agencies, and staff offices will comply with all Federal laws and regulations, OMB policies and requirements, DHS binding operational directives, NIST standards and guidance, and Departmental directives and guidance on cybersecurity incident management.

b. Personnel with incident management responsibilities will be technically qualified and have clearances appropriate to the categorization or classification of the systems they support and the types of incident-related information they may receive.

c. The Agriculture Security Operations Division (ASOD) Cybersecurity Incident Response Team (CSIRT) will operate as USDA's central cybersecurity incident management group to:

(1) Serve as the contact and coordination point with internal USDA offices, including the USDA Privacy Office, OIG, Office of Homeland Security (OHS) Personnel and Document Security Division (PDSD), and the OHS Insider Threat Program;

(2) Serve as USDA's cybersecurity incident management operational liaison and point of contact with external entities such as US-CERT; and

(3) Act as the collection point and clearinghouse for cybersecurity incident information and have enterprise reporting responsibility related to all cybersecurity incidents, including forwarding cybersecurity incident information to US-CERT.

d. All suspected or actual incidents will be reported to the ASOD CSIRT within 1 hour of discovery. Examples of reportable incidents are:

(1) Suspected or actual spillage of classified national security information (CNSI) or suspected or actual cybersecurity incidents affecting classified systems, with concurrent reporting to OHS PDSD, the Mission Area, agency, or staff office Information Security Coordinator (ISC), and Mission Area, agency, or staff office information security support staff;

(2) Suspected or actual unauthorized release of controlled unclassified information (CUI);

(3) 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;

(4) Suspected or actual incidents related to criminal activity or misuse, in accordance with DR 1700-002, *OIG Organization and Procedures*;

(5) Suspected or actual insider threats where an insider is using or may be using his or her access 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

(6) Suspected or actual incidents of compromise to the confidentiality, integrity, or availability of USDA information, information systems, or information services.

e. Information regarding an incident and the investigation will be logged into the ASOD CSIRT and, if necessary, the Mission Area, agency, or staff office incident tracking mechanism.

f. The ASOD CSIRT will prioritize incidents using the management process identified in NIST SP 800-61 and in accordance with the impact classification factors and levels detailed in the DHS *US-CERT Federal Incident Notification Guidelines* and report to US-CERT within 1 hour:

(1) Suspected or actual exposure or compromise of cyber-based PII;

(2) Suspected or actual cyber incidents related to criminal activity or misuse; and

(3) All actual incidents of compromise to the confidentiality, integrity, or availability of USDA information, information systems, or information services.

g. The Senior Agency Official for CNSI/Director of OHS and the USDA Chief Information Security Officer (CISO) have the authority to direct any action, including shutdown, with respect to any system on which CNSI is spilled.

h. All suspected and actual breaches will be handled in accordance with Federal and Departmental requirements, including FISMA, OMB M-17-12, NIST SP 800-122, *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*, and the USDA *Personally Identifiable Information (PII) Core Incident Response Group (CIRG) PII Breach Notification & Incident Response Plan (IRP),* Revision 4.6.

i. Any technology used to capture, collect, store, analyze, transmit, or access sensitive incident information, including PII, will be properly secured to preserve confidentiality and integrity.

j. Mission Areas, agencies, and staff offices will:

(1) Regularly run automated tools that are updated with current indicators of compromise (IOC) supplied by ASOD; and

(2) Promptly analyze the results and report suspected or actual incidents as stated in Section 5d.

k. The ASOD CSIRT will scan for IOCs within 24 hours (i.e., 1 day) of issuance by US-CERT.

l. Incident management personnel will investigate all suspected and actual incidents reported by US-CERT, the ASOD CSIRT, users (whether Federal employees, contractors, or others), system, network, or database administrators, or personnel from other organizations internal or external to USDA.

m. For each major incident, including cyber-related breaches, the appropriate committees of Congress will be notified and consulted not later than 7 days after a major incident has been declared. Additional information (as defined in OMB M-19-02) will be provided to the committees within a reasonable period of time after initial notification.

n. An annual report describing major incidents, including cyber-related breaches, in unclassified form but including a classified annex if necessary will be prepared and provided to the Director of OMB, the Secretary of DHS, committees of Congress, and the Comptroller General.

o. A plan of action and milestones (POA&M) will be created for any incident and associated with either an information system or service or an information security program if:

(1) The incident remains open (unresolved) after 30 days or if the agency or staff office anticipates that it will require more than 30 days to remediate and close;

(2) A review determines remedial actions are or were inadequate for incident closure; or

(3) Required information pertaining to the incident has not been submitted.

p. Incident management personnel will finalize the Agriculture Department (AD)-3043, *ASOC Incident Report*, or the AD-3038, *Cyber Security Incident Report Personally Identifiable Information (PII) Incident*, and submit it to close the incident with the ASOD CSIRT.

q. Incident records (i.e., evidence pertaining to an incident) and records of reporting incidents both internally and externally will be destroyed 3 years after all necessary follow-up actions have been completed. Longer retention is authorized if required for business use.

r. Incident management plans and associated procedures will be documented and updated whenever significant changes affect the information in the plans or procedures.

s. Incident management plans will:

(1) Define worst-case scenarios;

(2) Include a PII section if USDA PII is generated, collected, provided, transmitted, stored, or maintained; and

(3) Be tested twice annually and if necessary updated after the test.

t. For moderate and high systems, incident response testing will be coordinated 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, and occupant emergency plans.

u. Disaster recovery plans and information system contingency plans will, in addition to physical disasters, address major cyber incidents that render information system infrastructure or systems unable to support operations.

v. Annual information security awareness training for all users will include user responsibilities for detecting and reporting cybersecurity incidents and breaches.

w. All personnel with cybersecurity incident response or incident management responsibilities will complete annual incident response role-based training.

6. ROLES AND RESPONSIBILITIES

a. The Secretary of Agriculture will:

(1) Direct the heads of USDA Mission Areas, agencies, and staff offices to implement incident management plans and procedures, and provide qualified personnel and other resources for incident management;

(2) Ensure that responsible incident management personnel notify and consult with internal and external parties in the time periods mandated and in accordance with Federal and Departmental requirements as part of responding to any incident,

including major incidents, PII or CUI incidents, actual or suspected criminal activity or misuse, insider threats, and incidents affecting national security systems;

(3) With the concurrence of the USDA CIO, the Senior Agency Official for Privacy (SAOP), the CIRG, and the Director of the Office of Communications (OC) provide notice, or designate in writing a senior-level individual to provide notice to individuals affected by a breach affecting USDA information resources;

(4) Ensure that the Department provides timely notice to individuals affected by a USDA breach in accordance with Federal and USDA requirements;

(5) Ensure that the Office of Congressional Relations (OCR) notifies Congress about each major incident within 7 days of declaration that it qualifies as a major incident; and

(6) Ensure that the USDA Chief Information Officer (CIO) and USDA CISO submit the required annual reporting of information security and cybersecurity incident and cyber-related breach information on time.

b. The Heads of Mission Areas, agencies, and Staff Offices will:

(1) Ensure that the provisions of this policy are implemented for the information resources that support the operations and assets under their control; and

(2) Ensure that personnel in their area of responsibility perform their incident management responsibilities, including notification and reporting, in a timely manner and in accordance with Federal and Departmental requirements.

c. The USDA CIO will:

(1) Ensure that Departmental policy, program, plans, procedures, and delegations of authority for incident management are developed, implemented, disseminated, maintained, and comply with FISMA and all other applicable Federal requirements;

(2) Ensure that the Department's annual information security reporting, including information on cybersecurity incidents and cyber-related breaches, is prepared and submitted on time;

(3) Determine when an incident is a major incident in consultation with the USDA CISO, ASOD Director, and appropriate senior Mission Area, agency, or staff office officials and system owners, and, if the incident is a breach, the SAOP;

(4) Ensure that the Secretary is informed promptly when a major incident is declared;

(5) Collaborate with the USDA CISO and the Assistant Secretary for Congressional Relations to provide the appropriate committees of Congress with information

about major incidents mandated by FISMA or other Federal requirements in the required timeframes;

(6) Determine if cybersecurity incident information may be released publicly, based on factors such as whether the release of information might negatively affect activities such as criminal investigations; and

(7) Provide ongoing funding for the Department's incident management program, including resources, user awareness training, role-based training for ASOD CSIRT personnel, and testing the Department's incident management plan twice annually.

d. The USDA CISO will:

(1) Inform the USDA CIO of major cybersecurity incidents;

(2) Collaborate with the USDA CIO and the Assistant Secretary for Congressional Relations to provide the appropriate committees of Congress with information about major incidents mandated by FISMA or other Federal requirements in the required timeframes;

(3) Oversee and ensure compliance with Federal and Departmental policies and requirements for incident management and provide guidance and direction to Mission Areas, agencies, and staff offices for:

(a) Compliance with Federal laws and requirements pertaining to incident management;

(b) Compliance with USDA incident management policy and procedure and other USDA guidance impacted by incident management; and

(c) Collaboration with internal and external entities and whether such collaboration is of a discretionary nature or is required by law, regulation, or policy.

(4) Ensure that the Department's incident management program and its associated resources and capabilities are developed, implemented, and maintained;

(5) Ensure that the Department's incident management plan is developed, documented, implemented, maintained, disseminated, and approved;

(6) Ensure that processes are in place to verify that the ASOD CSIRT, Mission Areas, agencies, and staff offices create POA&Ms and manage them to closure for:

(a) Incidents that do not meet criteria for closure within 30 days; and

(b) Corrective actions after incident management plan testing.

(7) Prepare USDA's annual FISMA report to include cybersecurity incident information and quarterly reports to meet OMB requirements;

(8) Notify and consult with the Inspector General (IG), the SAOP, the Senior Agency Official for CUI, the OHS PDSD Chief, the OHS Insider Threat Coordinator, the Director of the Office of Human Resources Management (OHRM), the Chief Financial Officer, the Assistant General Counsel of the Office of the General Counsel (OGC), General Law and Research Division (GLRD), the Assistant Secretary for Congressional Relations, and the Director of OC, as appropriate, regarding incidents;

(9) Serve as the Department's principal liaison with US-CERT;

(10) Serve as the Department's principal liaison with organizations outside the Department for cybersecurity incidents, notifying and consulting with (as appropriate):

(a) Law enforcement agencies, after conferring with the IG;

(b) An office designated by the President for any incident involving a national security system;

(c) The committees of Congress described in FISMA, within the time periods mandated, and in collaboration with the USDA CIO and the Assistant Secretary for Congressional Relations in the event of a major incident; and

(d) Any other agency or office, in accordance with law or as directed by the President.

(11) Ensure that required and other relevant metrics on incident management are regularly collected, analyzed, reported, and used to improve all aspects of the Department's incident management program; and

(12) Ensure that information security awareness training for Mission Area, agency, and staff office users includes user responsibilities for detecting and reporting cybersecurity incidents, including incidents involving PII and CUI.

e. The ASOD Director will:

(1) Develop and maintain the Departmental incident management plan in accordance with current NIST guidelines;

(2) Coordinate with and assist the SAOP in the development and maintenance of the USDA *Personally Identifiable Information (PII) Core Incident Response Group (CIRG) PII Breach Notification & Incident Response Plan (IRP)*;

(3) Disseminate the current Departmental incident management plans to the ASOD CSIRT and agency and staff office incident management personnel;

(4) Provide DHS with information about high value assets (HVA) and critical system architecture to help them understand the potential impact to those assets from a cyber incident and to provide assurance that robust physical and cybersecurity protections are in place for those assets;

(5) Implement a standing Federal Network Authorization with DHS to ensure DHS can rapidly access USDA's networks and deploy on-site resources to conduct incident response activities when necessary, and review the authorization semi-annually;

(6) Receive, disseminate, and track Departmentwide compliance with DHS binding operational directives;

(7) Establish and maintain relationships with external entities with incident handling expertise, resources, or whose assistance may be needed for incident response, and establish partnerships for surge resources and special capabilities through contracts, memorandums of understanding (MOU), memorandums of agreement (MOA), or service level agreements (SLA);

(8) Ensure that there is sufficient funding for resources, including equipment, software, and media, and for annual role-based training for the ASOD CSIRT to effectively support incident management activities;

(9) Manage the ASOD CSIRT and ensure that the ASOD CSIRT documents, effectively implements, and maintains comprehensive incident management procedures;

(10) Collaborate and coordinate with USDA Mission Areas, agencies, and staff offices with regard to their incident management responsibilities and provide guidance for:

(a) Compliance with Federal laws and requirements pertaining to incident management and reporting;

(b) Compliance with Departmental incident management policy and procedure and other USDA guidance impacted by incident management; and

(c) Collaboration with internal and external entities and whether such collaboration is of a discretionary nature or is required by law, regulation, or policy.

(11) Perform managerial oversight of all incidents ensuring that:

(a) All incidents affecting USDA information resources are properly documented, tracked, investigated, mitigated, and closed; and

(b) ASOD CSIRT personnel provide timely notification and reporting to US-CERT for all reportable incidents and to senior USDA officials for major incidents.

(12) Ensure that records relating to incidents and incident reporting are retained for at least 3 years, unless longer retention is required for business use, and then properly destroyed;

(13) Act as or appoint a member of the ASOD CSIRT to serve as incident commander, to direct and manage major incidents and other incidents deemed a high priority;

(14) Coordinate with:

(a) Internal entities such as OIG, the USDA Privacy Office, OHS PDSD, OHS Insider Threat Program, OHRM, Office of the Chief Financial Officer, OC, and the Office of the General Council (OGC) as appropriate; and

(b) External entities such as internet service providers (ISP), law enforcement agencies, other incident response groups, affected external parties, and vendors of information technology (IT) products and services for investigation and mitigation of incidents.

(15) Ensure that testing of USDA's incident management plans, procedures, and capabilities:

(a) Occurs at least twice annually, and if necessary, the plans and procedures are updated after each test; and

(b) Is coordinated 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, and occupant emergency plans.

(16) Ensure that incident management plan test results are documented in after-action reports and that improvement plans are developed and implemented to address any weaknesses or deficiencies;

(17) Develop an annual plan for ASOD CSIRT operations, including elements such as:

(a) Staffing and training for staff;

(b) Resources such as equipment, software tools, and media; and

(c) Collection, analysis, and reporting of performance metrics.

(18) Ensure that all ASOD CSIRT personnel are trained on USDA's incident management policy and procedure and understand incident management standards and guidelines issued by US-CERT and NIST;

(19) Ensure that all ASOD CSIRT personnel complete annual role-based training and other training as identified in the ASOD CSIRT annual operational plan and that records of the training are maintained; and

(20) Develop, track, analyze, and report metrics to meet Federal requirements and provide other relevant internal measures of ASOD CSIRT performance on incident management.

f. ASOD CSIRT Personnel will:

(1) Serve as USDA's central contact and coordination point for all cybersecurity incident management operational activities, which include notifying, consulting with, and coordinating with all USDA Mission Areas, agencies, and staff offices and external entities;

(2) Provide guidance to ensure that incident management activities at the Department, Mission Area, agency, and staff office levels comply with Federal and USDA requirements;

(3) Provide OIG and OHS PDSD with technical guidance as needed to assist with activities such as cyber investigation and analysis, incident containment, and cleanup, as instructed by the ASOD Director;

(4) Develop and maintain the ASOD CSIRT incident management standard operating procedures (SOP);

(5) Execute the ASOD CSIRT incident management SOPs for cybersecurity incidents and cyber-related breaches until the incidents are resolved and closed;

(6) Immediately perform actions to mitigate incidents or threats that have or have the potential to have severe functional or information impacts;

(7) Report incidents to US-CERT within the mandated timeframes;

(8) Ensure all incidents are thoroughly mitigated prior to incident closure;

(9) Complete required incident response training annually and when circumstances such as roles and responsibilities change; and

(10) Develop and execute incident management testing at least twice annually, update the incident management plan, when necessary after each test, document the results, and report testing results to the ASOD Director.

g. The Assistant Secretary for Administration serving as the SAOP will:

(1) Develop and maintain, in coordination with the ASOD Director, the USDA *Personally Identifiable Information (PII) Core Incident Response Group (CIRG) PII Breach Notification & Incident Response Plan (IRP)*;

(2) Be the authority for directing the identification of PII and the level of impact or sensitivity of compromised PII;

(3) Convene the USDA CIRG to coordinate USDA responses to moderate or high impact breaches per the USDA *Personally Identifiable Information (PII) Core Incident Response Group (CIRG) PII Breach Notification & Incident Response Plan (IRP)*;

(4) Provide direction and guidance to the ASOD CSIRT, Mission Areas, agencies, and staff offices, and privacy officers regarding PII and CUI incidents;

(5) Advise the USDA Secretary whether and when to notify individuals potentially affected by a breach; and

(6) Certify by email that an incident for which the CIRG has been convened is closed.

h. The USDA Chief Privacy Officer will:

(1) Direct the identification of PII and the level of impact or sensitivity of compromised PII;

(2) Inform the SAOP of moderate and high breaches;

(3) Direct the actions of the ASOD CSIRT and Mission Area, agency, and staff office incident management personnel for breaches; and

(4) Approve the closure of all other breaches by email.

i. The IG will:

(1) Review all actual or suspected criminal activity incidents and reports of fraud, waste, and abuse of information resources;

(2) Notify law enforcement agencies, after conferring with the USDA CISO; and

(3) Direct incident management personnel on methods to obtain and secure incident evidence to comply with the rules of preservation of evidence.

j. The OHS Director serving as the Senior Agency Official for CUI will consult with the Director of OC, the IG, and others, as appropriate, to determine if cybersecurity incident information pertaining to CUI may be released publicly.

k. The OHS PDSD Chief will:

(1) Be responsible for managing the security of information for incidents affecting CNSI and classified systems; and

(2) Submit final reports on CNSI incidents with recommendations to the Senior Agency Official for CNSI/Director of OHS, the USDA CISO, and the data owner.

l. The OHS Special Security Officer will:

(1) Conduct official investigations of CNSI spillage and classified system incidents, coordinating with the data owner, the ASOD CSIRT, and others as necessary; and

(2) Provide the final determination to close CNSI incidents.

m. The OHS Insider Threat Coordinator will:

(1) Implement an insider threat detection and prevention program consistent with guidance and standards outlined in Executive Order 13587, *Structural Reforms To Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information*, and the 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*;

(2) Conduct inquiries on all potential insider threat incidents;

(3) Coordinate with appointed stakeholders and the Office of the Chief Information Officer (OCIO) to obtain information necessary to identify, analyze, and resolve insider threat matters; and

(4) Serve as the USDA liaison to the intelligence community for insider threat within the Department, to include referrals to the Federal Bureau of Investigation (FBI) under the *Intelligence Authorization Act for Fiscal Year 1995*, 50 United States Code (U.S.C.) §3381, *Coordination of Counterintelligence Activities*.

n. The Assistant General Counsel, OGC GLRD 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.

o. The Director of OC will coordinate activities regarding public notification outside USDA about cyber incidents with the USDA CIO, the SAOP, the IG, and others, as appropriate.

p. Mission Area Assistant CIOs will:

(1) Fund, establish, implement, and maintain the Mission Area, agency, and staff office incident management program to include resources, capabilities, incident management plan testing, and training of incident management personnel;

(2) Ensure that management support and resources are provided and assigned to the agency and staff office incident management personnel to effectively support incident management activities;

(3) Ensure that their organization develops, documents, implements, reviews, and updates an incident management plan and associated procedures that align with Departmental policies, programs, and procedures, and comply with Federal policies, regulations, standards, and guidelines for incident reporting and management;

(4) Approve their organization's incident management plan;

(5) Provide direction and guidance to Mission Area, agency, and staff office personnel for:

(a) Compliance with Federal laws and requirements pertaining to incident management and reporting;

(b) Compliance with Departmental incident management policy and procedure and other USDA policies and procedures impacted by incident management; and

(c) Collaboration with internal and external entities (e.g., ASOD CSIRT, USDA Privacy Office, OIG, others as appropriate) to investigate, mitigate, and close incidents.

(6) 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;

(7) Ensure that their organization reports incidents to the ASOD CSIRT in the required timeframe and provides updates until incidents are closed;

(8) Formally designate one or more technically qualified points of contact with appropriate clearances to function as the CSIRT for the agency or staff office; the designee(s) may serve in a dual role such as the CISO or Information Systems Security Program Manager (ISSPM); and

(9) Ensure that Mission Area, agency, and staff office personnel with incident management responsibilities complete annual role-based training and that the training is documented and tracked.

q. Mission Area Assistant CISOs, and Mission Area, Agency, and Staff Office ISSPMs will:

(1) Ensure that this policy, all USDA incident management procedures, and binding operational directives from DHS are disseminated, implemented, enforced, and integrated within their Mission Area, agencies, and staff offices;

(2) Develop, document, disseminate, implement, and maintain the agency and staff office incident management plan for cybersecurity incidents, including incidents affecting PII;

(3) Ensure that agency and staff office incident management procedures are developed, documented, implemented, and maintained;

(4) Disseminate procedures and requirements for reporting actual and suspected incidents to users, service providers, contractors, and other organizations that own or operate information systems or services on behalf of USDA;

(5) Ensure that incidents are promptly reported to the ASOD CSIRT, properly responded to, and adequately documented;

(6) Act as the point of contact for all suspected or actual criminal activity or misuse incidents related to an OIG investigation;

(7) Inform the Mission Area, agency, and staff office head, Mission Area Assistant CIO, and USDA CIO of major incidents, including breaches or ongoing, unresolved adverse events and incidents;

(8) Verify containment, mitigation, and closure of incidents; and

(9) Plan and conduct incident management plan testing twice annually, update the plan if necessary after each test, document the results, and create POA&Ms for identified

weaknesses in accordance with DR 3565-003, *Plan of Action and Milestones Policy*.

r. Mission Area, Agency, and Staff Office CSIRTs will:

(1) Comply with all Federal and Departmental policies, regulations, standards, guidelines, and procedures for incident management and reporting, including incidents involving PII, CUI, CNSI spillage, criminal activity, misuse, or insider threats;

(2) Develop and maintain agency and staff office procedures for incident management and reporting, including incidents involving PII, CUI, CNSI spillage, criminal activity, misuse, and insider threats, ensuring that the procedures comply and align with Federal and Departmental policies, regulations, standards, guidelines, and procedures;

(3) Inform the Mission Area Assistant CIO, the Mission Area Assistant CISO, and Mission Area, agency, and staff office ISSPM of major incidents, including breaches or ongoing, unresolved adverse events and incidents;

(4) Keep the Mission Area Assistant CISO, and Mission Area, agency, and staff office ISSPM informed of incident management activities, from discovery through closure;

(5) Refrain from contacting or reporting to US-CERT directly, unless specifically requested to do so by the ASOD Director or ASOD CSIRT personnel with delegated authority;

(6) Implement the Mission Area, agency, and staff office incident management procedures, including coordinating activities with their Mission Area Assistant CISO, Mission Area, agency, and staff office ISSPM, system administrators, network managers, or other personnel, until the incident is resolved and the ASOD CSIRT validates that it is closed;

(7) Immediately perform actions to mitigate incidents or threats that have or have the potential to have severe functional or information impacts;

(8) Ensure that PII and CUI related to actual or suspected incidents are handled properly and minimized to the greatest extent possible during incident response;

(9) Create a POA&M for any incident that meets criteria described in Section 4o of this policy;

(10) Complete annual role-based training; and

(11) Participate in incident response testing and provide input into documenting the results.

s. System, Network, and Database Administrators will:

(1) Promptly report suspected and actual incidents according to the criteria defined in this policy to the ASOD CSIRT and the agency and staff office incident management personnel;

(2) Follow the directions of the ASOD CSIRT, Mission Area, agency, and staff office incident management personnel, and other authorized incident management personnel during incident response, containment, eradication, and recovery;

(3) Ensure that PII and CUI related to actual or suspected incidents is handled properly and minimized to the greatest extent possible during incident response;

(4) Document the steps taken to contain and clean up a CNSI spillage and provide that documentation to OHS PDSD as proof that the actions were taken;

(5) Take annual role-based incident management training, if required; and

(6) Participate in incident response testing and after-action reports, if requested.

t. All employees, contractors, service providers, and others working for, or on behalf of, USDA will:

(1) Promptly report actual or suspected incidents of all types to the ASOD CSIRT and properly handle PII until authorized personnel are notified and assume custody of the information;

(2) Comply with Departmental policies and procedures to safeguard PII and properly handle PII until authorized personnel are notified and assume custody of the information;

(3) Not delete, forward, or transmit any spilled information, including CNSI, CUI, or PII in any format, whether an email, an attachment, or a hyperlink, unless instructed by OHS PDSD, personnel managing CUI or breaches, or other authorized officials; and

(4) Protect all communication and limit sharing when reporting a classified or suspected classified incident, including spillage of CNSI, to minimize further exposure of the incident and damage to CNSI.

u. System Owners will establish a document (i.e., contract, SLA, MOA, or MOU) requiring contractors, service providers, and other organizations that own or operate information systems or services for, or on behalf of, USDA to:

(1) Protect USDA information resources with automated detection tools that are run regularly using updated indicators from the tool vendors or whenever requested by the ASOD CSIRT using indicators provided by the ASOD CSIRT and/or US-CERT, review the results, and provide the results to USDA or other authorized parties;

(2) Report all suspected and actual incidents in the required timeframe via methods indicated in the document governing the relationship (e.g., contract, SLA, MOA, or MOU) to the ASOD CSIRT, the system owner, the Privacy hotline number or email address if PII is affected, the contracting officer (when operating under a contract), and additional appropriate points of contact;

Note: The governing document must indicate to contractors and others working for, or on behalf of, USDA, when Mission Area, agency, or staff office points of contact are notified about a suspected or actual incident.

(3) Develop, maintain, and implement an incident management plan if they generate, collect, provide, transmit, store, or maintain USDA PII;

(4) Have and share with the system owner an incident management plan that:

(a) Integrates fully with the incident management plan of the contracting agency or staff office;

(b) Is tested twice annually, with all test results shared with the contracting agency or staff office; and

(c) Requires creating an associated POA&M for each weakness found during testing in accordance with DR 3565-003.

v. Contractors, service providers, or others acting for, or on behalf of, USDA will:

(1) Comply with all Federal and Departmental incident management policies, regulations, guidelines, and procedures indicated in the document governing the relationship (e.g., a contract, SLA, MOA, or MOU);

(2) Protect USDA information resources with automated detection tools that are run regularly using updated indicators or whenever requested by the ASOD CSIRT using indicators provided by the ASOD CSIRT and/or US-CERT, review the results, and provide the results to USDA or other authorized parties;

(3) Report all suspected and actual incidents in the required timeframe via methods indicated in the document governing the relationship (i.e., a contract, SLA, MOA, or MOU);

(4) Develop and maintain an incident management plan if USDA PII is generated, collected, provided, transmitted, stored, or maintained;

(5) Have a current incident management plan for the system or service, when required in the document governing the relationship (i.e., a contract, SLA, MOA, or MOU), share it with the responsible Mission Area, agency, or staff office, test the plan, share the test results with the responsible Mission Area, agency, or staff office, and, if authorized, create an associated POA&M for each weakness found during testing in accordance with DR 3565-003;

(6) Where non-Federal information systems or organizations process, store, or transmit USDA CUI, comply with the incident response security requirements identified in NIST SP 800-171 Revision 1, *Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations*;

(7) Ensure its personnel take annual role-based incident management training, if required; and

(8) Participate in incident response testing and after-action reports, if required.

7. PENALTIES AND DISCIPLINARY ACTIONS FOR NON-COMPLIANCE

DR 4070-735-001, *Employee Responsibilities and Conduct*, Section 16, sets forth USDA policy, procedures, and standards on employee responsibilities and conduct regarding the use of computers and telecommunications equipment. In addition, DR 4070-735-001, Section 21, Disciplinary or Adverse Action, states:

a. A violation of any of the responsibilities and conduct standards contained in this directive may be cause for disciplinary or adverse action.

b. Disciplinary or adverse action will be affected in accordance with applicable law and regulations.

Such disciplinary or adverse action will be consistent with applicable law and regulations such as Office of Personnel Management regulations, OMB regulations, and the *Standards of Ethical Conduct for Federal Employees of the Executive Branch*.

8. POLICY EXCEPTIONS

a. All USDA Mission Areas, agencies, and staff offices are required to conform to this policy. If a specific policy requirement cannot be met as explicitly stated, a waiver may be requested. Note that an approved waiver does not bring the system into compliance with policy. Requests for waivers:

(1) Are an acknowledgement of a system's non-compliance with policy and that an acceptable plan to remediate the weakness has been provided and will be implemented.

(2) Must be documented as indicated in the standard operating procedure by the Compliance and Policy Branch, CAPE-SOP-003, *Plan of Action and Milestones Management Standard Operating Procedure*, Revision 1.1.

b. Policy waiver request memoranda will be addressed to the USDA CISO and submitted to ISC.Outreach@wdc.usda.gov for review and decision. Unless otherwise specified, approved policy waivers must be reviewed and renewed every fiscal year.

9. INQUIRIES

Address inquiries concerning this DR to OCIO Information Security Center via email to the cscc@ocio.usda.gov mailbox.

-END-

APPENDIX A

AUTHORITIES AND REFERENCES

DHS, *NCCIC National Cyber Incident Scoring System*

DHS, *US-CERT Federal Incident Notification Guidelines*, April 1, 2017

Executive Order 12958, *Classified National Security Information*, April 17, 1995

Executive Order 13292, *Further Amendment To Executive Order 12958, as Amended, Classified National Security Information*, March 28, 2003

Executive Order 13526, *Classified National Security Information*, December 29, 2009

Executive Order 13556, *Controlled Unclassified Information*, November 4, 2010

Executive Order 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 United States Code (U.S.C.) §3551, et seq., December 18, 2014

Fraud and related activity in connection with identification documents, authentication features, and information, 18 U.S.C. 1028(d)(7), (2010)

Government Accountability Office (GAO), GAO Report 08-536, *Privacy: Alternatives Exist for Enhancing Protection of Personally Identifiable Information*, May 2008

Intelligence Authorization Act for Fiscal Year 1995, 50 U.S.C. §3381, *Coordination of Counterintelligence Activities*, December 17, 2004

Office of Government Ethics, *Standards of Ethical Conduct for Federal Employees of the Executive Branch*, 5 Code of Federal Regulations (CFR) §2635, et seq., (2017)

National Archives and Records Administration, *Information Systems Security Records*, General Records Schedule (GRS) 3.2, September 2016

National Archives and Records Administration (NARA), *Controlled Unclassified Information (CUI) Registry - Categories and Subcategories*

NARA, CUI Registry

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

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

Presidential Policy Directive (PPD) - 41, *United States Cyber Incident Coordination*, July 26, 2016

Annex to PPD - 41, *Federal Government Coordination Architecture for Significant Cyber Incidents*, July 26, 2016

Protected Critical Infrastructure Information, 6 CFR Part 29, January 1, 2012

Privacy Act of 1974, 5 U.S.C. 552a, December 31, 1974, as amended

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

USDA, AD-3043, *ASOD Incident Report*, June 2016

USDA, CAPE-SOP-003, *Plan of Action and Milestones Management Standard Operating Procedure*, Revision 1.1, November 2015

USDA, *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

USDA, Departmental Manual (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, DM 3505-005, *Cybersecurity Incident Management Procedures*, November 30, 2018

USDA, DR 1700-002, *OIG Organization and Procedures*, June 17, 1997

USDA, DR 3300-001, *Telecommunications & Internet Services and Use*, March 18, 2016

USDA, DR 3440-001, *USDA Classified National Security Information Program*, June 9, 2016

USDA, DR 3565-003, *Plan of Action and Milestones Policy*, September 25, 2013

USDA, DR 4070-735-001, *Employee Responsibilities and Conduct*, October 4, 2007

USDA, DR 4600-003, *USDA Insider Threat Program*, June 30, 2014

APPENDIX B

DEFINITIONS

a. 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)

b. Classified Information. See "Classified National Security Information."

c. 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)

d. 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)

e. Computer Security Incident. See "Incident."

f. Controlled Unclassified Information. Information the Government creates or possesses, or that an entity creates or possesses for or on behalf of the Government, that a law, regulation, or Government-wide policy requires or permits an agency to handle using safeguarding or dissemination controls. However, CUI does not include classified information (see definition above) or information a non-executive branch entity possesses and maintains in its own systems that did not come from, or was not created or possessed by or for, an executive branch agency or an entity acting for an agency. Law, regulation, or Government-wide policy may require or permit safeguarding or dissemination controls in three ways: Requiring or permitting agencies to control or protect the information but providing no specific controls, which makes the information CUI Basic; requiring or permitting agencies to control or protect the information and providing specific controls for doing so, which makes the information CUI Specified; or requiring or permitting agencies to control the information and specifying only some of those controls, which makes the information CUI Specified, but with CUI Basic controls where the authority does not specify. (Source: NARA, CUI Registry)

g. Cybersecurity Incident. See "Incident."

h. Event. Any observable occurrence in a network or system. (Source: NIST SP 800-61 Revision 2)

Note: Events with negative consequences are referred to as adverse events.

i. Exploit. A technique to breach the security of a network or information system in violation of security policy.

j. Federal Information. Information created, collected, processed, maintained, disseminated, or disposed of by or for the Federal Government, in any medium or form. (Source: OMB Circular A-130)

k. Functional Impact. A measure of the impact to business functionality or ability to provide services. (Source: *US-CERT Federal Incident Notification Guidelines*.) Also, see related terms "information impact" and "recoverability."

l. 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)

m. 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. (Source: OMB M-16-04)

n. 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)

o. 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 controlled unclassified information (CUI).

p. Incident Handling. The mitigation of violations of security policies and recommended practices. (Source: NIST SP 800-61 Revision 2)

q. 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 Assistant CISOs, ISSPMs, privacy office personnel

at the Departmental or agency and staff office levels, and audit or investigations personnel from the OIG.

r. 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 3d**Error! Reference source not found.** 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.

s. Indicator. A sign that an incident may have occurred or may be currently occurring. (Source: NIST SP 800-61 Revision 2)

t. Indicator of Compromise. See related term "Indicator."

u. Information Impact. Describes the type of information lost, compromised, or corrupted. (Source: *US-CERT Federal Incident Notification Guidelines*.) Also, see related terms "Functional Impact" and "Recoverability."

v. Information resources. Encompasses information, information systems, and information services.

w. Information Security Incident. See "Incident."

x. 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)

y. 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)

z. 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 (excluding a system that is to be used for routine administrative and business applications, for example, payroll, finance, logistics, and personnel management applications); 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)

aa. 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)

bb. 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*, 6 Code of Federal Regulations (CFR) Part 29)

cc. Recoverability. Identifies the scope of resources needed to recover from the incident. (Source: *US-CERT Federal Incident Notification Guidelines*.) Also, see related terms "functional impact" and "information impact."

dd. 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)

ee. Spillage. Security incident that results in the transfer of classified or CUI onto an information system not authorized for the appropriate security level. (Source: NIST IR 7298 Revision 2)

ff. Threat. The potential source of an adverse event. (Source: NIST SP 800-61 Revision 2)

gg. 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)

hh. 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)

ii. 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)

jj. 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)

kk. Vulnerability. A weakness in a system, application, or network that is subject to exploitation or misuse. (Source: NIST SP 800-61 Revision 2)

APPENDIX C

ACRONYMS AND ABBREVIATIONS

AD	Agriculture Department
ASOD	Agriculture Security Operations Division
CFR	Code of Federal Regulations
CII	Critical Infrastructure Information
CIO	Chief Information Officer
CIRG	Core Incident Response Group
CISO	Chief Information Security Officer
CNSI	Classified National Security Information
CNSS	Committee on National Security Systems
CPB	Compliance and Policy Branch
CSIP	Cybersecurity Strategy and Implementation Plan
CSIRT	Cybersecurity Incident Response Team
CUI	Controlled Unclassified Information
DHS	Department of Homeland Security
DM	Departmental Manual
DR	Departmental Regulation
FBI	Federal Bureau of Investigation
FIPS PUB	Federal Information Processing Standards Publication
FISMA	Federal Information Security Modernization Act
GAO	Government Accountability Office
GLRD	General Law and Research Division
GRS	General Records Schedule
HVA	High Value Asset
IG	Inspector General
IOC	Indicator of Compromise
IR	Interagency Report
IRP	Incident Response Plan
ISC	Information Security Coordinator
ISP	Internet Service Provider
ISSPM	Information Systems Security Program Manager
IT	Information Technology
MOA	Memorandum of Agreement
MOU	Memorandum of Understanding
NARA	National Archives and Records Administration
NCCIC	National Cybersecurity and Communications Integration Center
NIST	National Institute of Standards and Technology
OC	Office of Communications
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
PPD	Presidential Policy Directive
SAOP	Senior Agency Official for Privacy
SLA	Service Level Agreement
SOP	Standard Operating Procedure
SP	Special Publication
U.S.C.	United States Code
US-CERT	United States Computer Emergency Readiness Team
USDA	United States Department of Agriculture