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

DEPARTMENTAL REGULATION	Number: DR 3505-005
SUBJECT: Cyber Security Incident Management Policy	DATE: October 31, 2013
	OPI: Office of the Chief Information Officer

1. PURPOSE

a. This Departmental Regulation (DR) establishes the policy of the United States Department of Agriculture (USDA or "Department") for meeting the laws, regulations, and standards of a comprehensive Cyber Security Incident Management program.

b. This DR addresses guidance issued by the Office of Management and Budget (OMB), the National Institute of Standards and Technology (NIST), and the *Federal Information Security Management Act of 2002 (FISMA)*, requiring Federal agencies to develop and implement policies, plans, and procedures for detecting, reporting, and responding to cyber security incidents.

c. It is the policy of USDA to comply with Federal requirements to establish, implement, and support a Cyber Security Incident Management program. The Department confirms the commitment of its management to comply with the authorities mandating and governing cyber security incidents.

2. SPECIAL INSTRUCTIONS/CANCELLATIONS

a. This directive replaces Departmental Manual (DM) 3505-000, *USDA Computer Incident Response Procedures* and DM 3505-001, *USDA Cyber Security Incident Handling Procedures*, in their entirety.

b. The terms "cyber security incident" and "computer security incident" are intended to convey the same meaning for the purposes of this policy.

3. BACKGROUND

a. The USDA is required to manage any and all incidents as categorized by the United States Computer Emergency Response Team (US-CERT). This requirement is part of the Comprehensive National Cybersecurity Initiative (CNCI) launched by President George W. Bush in National Security Presidential Directive 54/Homeland Security Presidential Directive 23 (NSPD-54/ HSPD-23) in January 2008, to create a unified defense around the United States digital infrastructure.

b. FISMA specifically directs Federal agencies to develop and implement procedures for detecting, reporting, and responding to cyber security events and incidents as mandated by the Department of Homeland Security. Additionally, OMB directs Federal agencies to identify and report within one hour of discovery any security incidents (physical or virtual) involving the suspected or confirmed compromise of personally identifiable information (PII).

c. USDA defines a security incident in accordance with NIST Special Publication (SP) 800-61 Revision 2, *Computer Incident Handling Guide*, as "…a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices" and is required to manage any and all cyber incidents occurring within its own cyber environment.

4. SCOPE

This policy applies to all USDA agencies, staff offices, employees, appointees, contractors, and others working for or on behalf of the USDA.

5. POLICY

a. The Agriculture Security Operations Center (ASOC) Computer Security Incident Response Team (CSIRT) shall communicate and coordinate cyber security incident management for all systems, assets, and data with internal and external entities, as required, to manage USDA incidents. The ASOC CSIRT shall coordinate incidents and

communication related to classified systems or data in coordination with the USDA Director of Homeland Security and Emergency Services.

b. The ASOC CSIRT shall assign incident prioritization in accordance with US-CERT as defined by NIST SP 800-61.

c. The ASOC CSIRT is the incident management liaison and point of contact (POC) with US-CERT. The ASOC CSIRT is solely responsible for forwarding applicable incident information to US-CERT.

d. The ASOC CSIRT has enterprise reporting responsibility for all cyber security and PII incidents.

e. The ASOC CSIRT shall coordinate with the USDA Core Incident Response Group (CIRG) on applicable PII incidents and notify affected personnel of any PII breach in accordance with OMB Memorandum M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*.

f. All information security incidents confirmed as exposing or compromising PII shall be reported to ASOC CSIRT immediately upon discovery/detection to allow USDA to meet the one hour reporting requirement mandated by OMB M-07-16. US-CERT will be notified by ASOC CSIRT and those incidents become part of an agency's annual FISMA reporting.

g. All information security incidents related or potentially related to criminal activity shall be referred by ASOC CSIRT to the Office of the Inspector General (OIG) as soon as an incident is suspected of or identified as being criminal in nature, in accordance with DR 1700-002, *OIG Organization and Procedures*.

h. ASOC CSIRT, under the direction of the USDA Chief Information Security Officer (CISO), is authorized to take possession of government furnished equipment (GFE) in coordination with applicable entities (e.g., OIG, State or Federal law enforcement, the Office of Human Resources Management (OHRM), or other USDA agencies and staff offices) for investigations involving actual or suspected criminal activity or misuse that may lead to adverse personnel action.

i. Agencies and staff offices shall use the applicable Computer Security Incident forms to detail information surrounding reported incidents. The forms can be found on the Office of the Chief Information Officer intranet Web site.

j. In the event that a USDA 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)*, the agency/staff office is responsible for alerting the ASOC CSIRT that data covered by the law is resident on the GFE and shall provide specific handling requirement guidance.

k. Agencies and staff offices shall comply with the guidance provided in this policy and any associated USDA incident management procedures. Agencies and staff offices shall incorporate the aforementioned policies and procedures into their respective agency/staff office CSIRT incident management procedures for processing all incidents, including breaches involving PII.

6. ROLES AND RESPONSIBILITIES

a. The USDA Chief Information Officer (CIO) shall:

(1) Ensure the Departmentwide information security program incorporates procedures for detecting, reporting, and responding to security incidents consistent with standards and guidelines issued pursuant to Section 3546 of FISMA, including mitigating risks associated with such incidents before substantial damage is done; and

(2) Notify and consult with appropriate law enforcement agencies, relevant OIG, and offices designated by the President for any incident involving a national security system and any other agency or office, in accordance with law or as directed by the President.

b. The USDA CISO shall:

(1) Report directly to the USDA CIO and be the principal advisor for information security matters;

(2) Manage the USDA Information Security Program to ensure compliance with applicable Federal laws, Executive orders, directives, policies, and regulations, to include:

(a) Issue Department information security policy, guidance, and architecture requirements for all USDA unclassified and classified systems, data, and networks (in coordination with the Office of Homeland Security and Emergency Coordination);

(b) Serve as the principal Departmental liaison with organizations outside the USDA for matters relating to information security;

(c) Develop and implement procedures for detecting, reporting, and responding to computer security incidents; and

(d) Refer activities requiring adverse action to OHRM.

c. The Associate Chief Information Officer (ACIO) for ASOC shall:

(1) Direct the creation, update, implementation, and compliance with this policy;

(2) Direct, manage, and document all cyber security incidents;

(3) Support the enforcement of policy; and

(4) Ensure sufficient resources are provided and assigned to effectively support incident management activities within its organizations.

d. The ASOC Incident Management Director shall:

(1) Manage the USDA ASOC CSIRT;

(2) Collaborate with USDA agencies/staff offices and other Federal agencies with regard to information security incident management policies and procedures;

(3) Coordinate with external entities such as Internet Service Providers, webmasters, and/or law enforcement as necessary to investigate and/or mitigate USDA incidents;

(4) Provide direction to USDA agencies/staff offices in support of their information security incident management responsibilities;

(5) Manage, document, report, coordinate, and track all reportable information for security incidents;

(6) Designate a primary and secondary POC for all interactions with US-CERT;

(7) Develop the Departmental incident response plan in accordance with current NIST SP 800-61, and NIST SP 800-53 Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations* guidelines;

(8) Ensure that the ASOC Information Systems Security Program Manager (ISSPM), ASOC CSIRT, and agency/staff office incident managers are trained on USDA incident management policies and procedures and are familiar with NIST incident-related standards and guidance; and

(9) Ensure sufficient resources are provided and assigned to effectively support incident management activities within its organizations.

e. The ASOC CSIRT shall:

(1) Coordinate with USDA agencies and staff offices as required to mitigate USDA information security incidents;

(2) Coordinate with the USDA CIRG on applicable PII related incidents; and

(3) Ensure equipment that is identified as containing malicious code or suspected of suspicious activity is removed from the USDA network and appropriately analyzed and restored, as applicable.

f. Agency and Staff Office CIOs shall:

(1) Implement this policy and associated procedures within their respective agency or staff office;

(2) Ensure that any agency/staff office-specific incident management policies and procedures are complete, up-to-date, and in compliance with FISMA, NIST, and USDA policies and procedures for incident management and response;

(3) Designate cyber incident managers and incident handlers to coordinate with the ASOC CSIRT in response to cyber security incidents impacting their respective agencies/staff offices;

(4) Ensure that their agency/staff office ISSPMs and incident managers are trained on USDA incident management policies and procedures and are familiar with NIST incident-related standards and guidance;

(5) Ensure sufficient resources are provided and assigned to effectively support incident management activities within their organizations; and

(6) Utilize the Department's enterprise Internet Protocol (IP) management system to maintain a current and accurate inventory of IP and Media Access Control addresses for all devices in their agency/staff office’s inventory.

g. Agency and Staff Office ISSPMs or designated specialists shall:

(1) Ensure this policy and any related procedures are enforced, implemented and integrated within their agency or staff offices;

(2) Ensure agency/staff office policies and procedures are in accordance with USDA guidance for information security incident management response;

(3) Ensure corrective actions identified by the ASOC CSIRT are implemented in accordance with USDA policies and procedures;

(4) Ensure agency/staff office PII incidents are reported to ASOC CSIRT in accordance with USDA policies and procedures;

(5) Act as the agency/staff office POC for all misuse or potential criminal activity incidents related to an OIG investigation;

(6) Ensure contact information for agency/staff office incident handlers is up-to-date, accurate, and submitted to the ASOC CSIRT POC as changes occur;

(7) Ensure all US-CERT advisories, alerts, and notifications are coordinated with the ASOC CSIRT for handling and response; and

(8) Ensure all agency/staff office incident documentation is complete, accurate, and kept open until approved for closure by the ASOC CSIRT.

h. The USDA Privacy Officer shall:

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

(2) Provide direction and guidance to agency/staff offices and Privacy Officers concerning PII incidents; and

(3) Approve the closure of all significant or sensitive PII incidents.

i. The USDA CIRG shall:

(1) Be responsible for directing the handling of PII incidents and developing the Department's response to a PII breach in coordination with the ASOC CSIRT; and

(2) Be convened when the risk factors identified in NIST SP 800-122, *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)* or OMB M-07-16, are determined to be high or moderate-high.

j. Agency and Staff Office incident managers shall:

(1) Lead coordination with the ASOC CSIRT in handling all phases of the incident management lifecycle and keep the appropriate ISSPM informed of activities;

(2) Coordinate with ISSPMs, system administrators, and network managers to perform corrective actions such as reimaging infected or compromised computers or servers, retrieving backup media to restore a system, or assisting in an investigation;

(3) Report incidents to ASOC CSIRT and coordinate activities with ISSPMs, agency/staff office Human Resources personnel, and the OIG to take possession of a computer or server for analysis and forensics investigation; and

(4) Not report or contact US-CERT directly unless specifically requested to do so by the ASOC CSIRT Director or their delegated agent.

7. PENALTIES AND DISCIPLINARY ACTIONS FOR NON-COMPLIANCE

DR 4070-735-001, *Employee Responsibilities and Conduct,* Section 16, sets forth the USDA's policies, procedures, and standards on employee responsibilities and conduct relative to the use of computers and telecommunications equipment, with further delineation provided in DR 3300-001, *Telecommunications and Internet Services and Use,* Section 3. 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 shall be effected in accordance with applicable law and regulations.

Such disciplinary or adverse action shall be effected in accordance with applicable law and regulations such as the Code of Ethics for Government Employees, Office of Personnel Management regulations, OMB regulations, and Standards of Conduct for Federal Employees.

8. POLICY EXCEPTIONS

All USDA agencies and staff offices are required to conform to this policy; however, in the event that a specific policy requirement cannot be met as explicitly stated, agencies/staff offices may submit a waiver request. The waiver request shall explain the reason for the request, identify compensating controls/actions that meet the intent of the policy, and identify how the compensating controls/actions provide a similar or greater level of defense or compliance than the policy requirement. Agencies and staff offices shall address all policy waiver request memorandums to the USDA CISO and submit the request to asoc.outreach@asoc.usda.gov for review and decision.

Unless otherwise specified, agencies/staff offices shall review and renew approved policy waivers every fiscal year. Approved waivers shall be associated with a NIST security control and tracked as a plan of action and milestones item in the Department's FISMA data management and reporting tool. The ACIO-ASOC shall monitor and approve waivers to this policy.

-END-

APPENDIX A

ACRONYMS AND ABBREVIATIONS

ACIO	Associate Chief Information Officer
ASOC	Agriculture Security Operations Center
CIO	Chief Information Officer
CIPSEA	Confidential Information Protection and Statistical Efficiency Act of 2002
CIRG	Core Incident Response Group
CISO	Chief Information Security Officer
CNCI	Comprehensive National Cybersecurity Initiative
CSIRT	Computer Security Incident Response Team
DM	Departmental Manual
DR	Departmental Directive
FISMA	Federal Information Security Management Act
GFE	Government Furnished Equipment
HSPD	Homeland Security Presidential Directive
IP	Internet Protocol
ISSPM	Information Systems Security Program Manager
NIST	National Institute of Standards and Technology
NSPD	National Security Presidential Directive
OHRM	Office of Human Resources Management
OIG	Office of the Inspector General
OMB	Office of Management and Budget
PII	Personally Identifiable Information
POC	Point of Contact
SP	Special Publication
USDA	United States Department of Agriculture
US-CERT	United States Computer Emergency Response Team

APPENDIX B

REFERENCES AND AUTHORITIES

Comprehensive National Cybersecurity Initiative (CNCI), March 2, 2010

Computer Fraud and Abuse Act of 1986, 18 United States Code (U.S.C.) 1030, (2013)

Confidential Information Protection and Statistical Efficiency Act of 2002 (CIPSEA), 44 U.S.C. 3501

DM 3440-001, *USDA Classified National Security Information Program Manual*, May 1, 2008

DM 3525-003, *Telework & Remote Access Security*, February 17, 2005

DM 3545-001, *Information Security Awareness and Training Policy*, October 22, 2013

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

DR 3140-001, *USDA Information Systems Security Policy*, May 15, 1996

DR 3140-002, *USDA Internet Security Policy*, March 7, 1995

DR 3160-001, *Computer Software Piracy*, March 29, 2007

DR 3300-001, *Telecommunications & Internet Services and Use*, March 23, 1999

DR 3440-001, *USDA Classified National Security Information Program Regulation*, October 5, 2011

DR 3440-002, *Control and Protection of "Sensitive Security Information"*, January 30, 2003

DR 4070-735-001, *Employee Responsibilities and Conduct*, October 04, 2007

E-Government Act of 2002, Public Law 107-347, 116 Statute 2899, December 17, 2002

Executive Order 13103, *Computer Software Piracy*, September 30, 1998

Federal Information Security Management Act of 2002 (FISMA), 44 U.S.C. 3541, et seq. (2013)

FIPS PUB 200, Minimum Security Requirements for Federal Information and Information Systems, March, 2006

NIST SP 800-37 Revision 1, *Guide for Applying the Risk Management Framework to Federal Information System: A Security Life Cycle Approach*, February 2010

NIST SP 800-53 Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations,* August 2009 (Errata as of May 1, 2010)

NIST SP 800-53A Revision 1, *Guide for Assessing the Security Controls in Federal Information Systems and Organizations, Building Effective Security Assessment Plans*, June 2010

NIST SP 800-61 Revision 2, *Computer Security Incident Handling Guide*, August 2012

NIST SP 800-83, *Guide to Malware Incident Prevention and Handling*, November 2005

NIST SP 800-86, *Guide to Integrating Forensic Techniques into Incident Response*, August 2006

NIST SP 800-100, *Information Security Handbook: A Guide for Managers*, October 2006

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

NIST SP 800-137, *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations*, September 2011

NSPD-54/HSPD-23, *Cyber Security and Monitoring*, January 8, 2008, as amended

OMB Circular A-130, Appendix III, *Management of Federal Information Resources,* as amended

OMB M-06-19, *Reporting Incidents Involving Personally Identifiable Information Incorporating the Cost for Security in Agency Information Technology Investments*, July 12, 2006

OMB M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*, May 22, 2007

OMB M-07-19, *FY 2007 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*, July 25, 2007

USDA Computer Security Incident Forms