

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

DEPARTMENTAL REGULATION	Number: DR 3565-003
SUBJECT: Plan of Action and Milestones Policy	DATE: September 25, 2013
	OPI: Office of the Chief Information Officer

<u>Section</u>	<u>Page</u>
1. Purpose	1
2. Scope	2
3. Special Instructions/Cancellations	2
4. Background	2
5. Policy	2
6. Procedures and guidance	3
7. Roles and Responsibilities	4
8. Penalties and Disciplinary Actions for Non-Compliance	6
9. Policy Exceptions	6
Appendix A Acronyms and Abbreviations	A-1
Appendix B Authorities and References	B-1
Appendix C Footnotes	C-1

1. PURPOSE

- a. This Departmental Regulation (DR) establishes the policy of the United States Department of Agriculture (USDA) for identifying, assessing, prioritizing, and monitoring the progress of corrective efforts for security vulnerabilities found in USDA programs, applications and systems. National Institute of Standards and Technology (NIST) Special Publication [\(SP\) 800-30 Revision 1, Guide for Conducting Risk Assessments](#), defines vulnerability as a weakness in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source.
- b. A plan of action and milestones (POA&M), also referred to as a corrective action plan, is a tool that identifies tasks that need to be accomplished to remediate security vulnerabilities. The goal of a POA&M should be to reduce the risk of the vulnerability identified.

- c. This policy adheres to the guidance identified in the NIST (SP) 800-53, Revision 3, Recommended Security Controls for Federal Information Systems and Organizations, August 2009.

2. SCOPE

This DR applies to all USDA Information Technology (IT) systems owned, operated, or maintained by, for, or on behalf of USDA. This includes contractor and cloud systems. This DR also applies to IT programs that provide security controls for use (inheritance) by any USDA IT system.

3. SPECIAL INSTRUCTIONS/CANCELLATIONS

- a. This regulation supersedes all references to the POA&M Process in Departmental Manual 3555-001, *Certification and Accreditation Methodology*, dated October 18, 2005.
- b. This policy is effective as of the publication date of this document and will remain in effect until superseded.

4. BACKGROUND

- a. The Office of Management and Budget (OMB) directs agency Chief Information Officers (CIOs) and agency program officials to develop, implement, and manage POA&Ms for all programs and systems they operate and control as part of compliance to the Federal Information Security Management Act (FISMA). In addition, POA&Ms must be shared with the USDA Office of the Inspector General (OIG) to ensure independent evaluation and verification of identified vulnerabilities and proposed mitigation strategies.
- b. POA&Ms are used at the program level to identify and track vulnerabilities across enterprise-level initiatives and at the system level to identify and track system-specific vulnerabilities. Agencies are required to update POA&Ms to reflect the current progress against planned remediation efforts.

5. POLICY

- a. A POA&M is an agency's primary management tool for tracking mitigation of IT security program, application, and system-specific vulnerabilities.
- b. All identified IT security vulnerabilities which represent risk to the USDA, its programs, systems, and information require a planned mitigation strategy in the form of a POA&M. Sources of weaknesses include, but are not limited to, IT and non-IT audits, testing security controls, continuous monitoring, and assessment and authorization activities.

- c. POA&Ms shall be created in the Department's official system of record when vulnerabilities are discovered during any review performed by, for, or on behalf of an agency, including, but not limited to, program and system audits and critical infrastructure vulnerability assessments. (See Appendix C: 1,2,3)
- d. POA&Ms shall be entered into and managed in the Department's official system of record when a vulnerability is identified (and evaluated for severity) and cannot be remediated within 30 days; however, vulnerabilities found that can be resolved within 30 days do not require the creation of a POA&M. (See Appendix C: 1,2,4) This record shall contain the resources required to accomplish the elements of the plan, any milestones in meeting the tasks, and scheduled completion dates for the milestones. Note: All vulnerabilities must have an approved POA&M before completion of Step 4 concurrency review.
- e. In the case of vulnerabilities generated by automated tools/scanners the finding, remediation, closure and reporting may be managed in an automated tool (such as a vulnerability scanner and/or trouble ticket system, etc.). This also accommodates control of the need to know nature of the identifying information (e.g., Internet Protocol (IP) address, server name), location and detailed function of the device. Utilizing a system other than the system of record is at the sole discretion of the USDA Chief Information Security Officer (CISO) and access to these tools for oversight must be provided to the USDA CISO. In these instances, a single POA&M should be entered into the Department's official system of record identifying the location of the externally managed vulnerability information and should be closed/renewed at least annually.
- f. The agency shall determine the costs and timeframes associated with mitigating the vulnerabilities identified in the POA&Ms. These costs shall be captured in the Department's System of Record and/or in the program's annual [OMB Exhibit 300](#), *Planning, Budgeting, Acquisition, and Management of IT Capital Assets*, and in the enterprise-wide [OMB Exhibit 53](#), *Information Technology and E-Government*, which are the funding vehicles submitted to OMB to secure an operating budget.
- g. All POA&Ms shall contain a unique investment identifier (UII) which is the default entered for the system. If the system UII is not providing the funding for the remedial action then the correct one must be provided as part of the POA&M entry.
- h. Agencies shall add POA&Ms as vulnerabilities are discovered, and closed when remediated thereby reflecting the latest vulnerability mitigation status for the agency.
- i. In some cases, a Risk Based Decision (RBD) (i.e., a determination) may be made that the existence of vulnerability is an acceptable risk, hence entered into the Department's official system of record as an RBD, not as a POA&M. These RBDs shall be reviewed and concurred with by ASOC management and documented accordingly per the Department's POA&M Standard Operating Procedure (SOP). These RBDs shall be

reviewed at least annually to ensure the associated risk remains acceptable. The CISO retains the right to refuse renewal of all RBDs.

6. PROCEDURES AND GUIDANCE

This DR may be further shaped by other USDA regulations, manuals, or guides that contain clarifying procedures. USDA Departmental regulations and manuals can be found on the [Department's Directives Web page](#). Additional information can also be found in Appendix B of this document.

7. ROLES AND RESPONSIBILITIES

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

- (1) Develop, implement, and maintain the Department's Information Security Program.
- (2) Develop and maintain information security policies and procedures to address all applicable requirements.
- (3) Ensure compliance with applicable information security requirements.
- (4) Report annually, in coordination with the other senior agency officials, to the Secretary of Agriculture on the effectiveness of the agency information security program, including progress of remedial actions.

b. The USDA Chief Information Security Officer (CISO) shall:

- (1) Implement and manage the USDA Information Security Program to ensure compliance with applicable Federal laws, Executive Orders, directives, policies, and regulations. The USDA CISO reports directly to the USDA CIO and is the principal advisor for information security matters.
- (2) Perform information security duties including, but not limited to, waiver and Risk Based Decision (RBD) approval/denial responsibilities reserved for USDA CISO.
- (3) Establish, implement, maintain and review annually the Department's process for planning, implementing, evaluating, and documenting remedial actions for addressing deficiencies in the information security systems, policies, procedures, and practices of the agency.
- (4) Review the department's POA&M policy annually.
- (5) Support the agency CIO in annual reporting to the agency head on the effectiveness of the agency POA&M programs.

- c. The Associate CIO for Agriculture Security Operations Center (ACIO-ASOC) shall:
 - (1) Establish and implement a POA&M program and process as part of the USDA IT Security Program.
 - (2) Ensure guidance, tools, and strategies to assist USDA agencies in complying with the requirements of this policy are in place and documented.
 - (3) Ensure the POA&M program provides administration, technical support, and training in the use of the Department's official system of record.
 - (4) Ensure management and oversight activities related to POA&Ms are in place and functioning in accordance with Federal guidelines.

- d. The Agency and Staff Office CIOs shall:
 - (1) Establish procedures to implement this policy.
 - (2) Provide component-level annual assurance statements and a summary of material vulnerabilities, non-compliance and corrective actions to support the Secretary's annual assurance statements.
 - (3) Share accountability and responsibility for corrective actions with agency Program Officials and Chief Financial Officers, as appropriate.
 - (4) Maintain a POA&M management program.
 - (5) Assess and monitor all identified vulnerabilities within their agency which include, but are not limited to, deficiencies identified through OIG or General Accounting Office audit findings; risk or self assessments; Independent Verification and Validation assessments; or internal or external scans.
 - (6) Ensure corrective actions are taken to resolve all identified vulnerabilities related to their respective mission areas.
 - (7) Ensure adequate resources and funding is allocated for the mitigation of identified security vulnerabilities.
 - (8) Ensure that POA&Ms are tied to the agency's capital planning and investment control process, and identified by the system's OMB UII.

- e. The Agency/Staff Office Information Systems Security Program Managers shall:
 - (1) Ensure corrective actions are consistent with laws, regulations, and USDA policy.

(2) Keep the Agency/Staff Office CIO informed of status, unresolved issues, and required actions through agency-level identified communication channels.

(3) Ensure that POA&Ms are managed according to the USDA POA&M SOP

f. The Agency/Staff Office System Owners shall:

(1) Manage the prompt and proper resolution of identified material weaknesses, significant deficiencies, control deficiencies, and non-conformance conditions that exist in the official's functional area, including the development, maintenance, monitoring, and reporting of corrective actions.

(2) Maintain accurate records of the status of the identified material vulnerabilities, significant deficiencies, and non-conformance throughout the entire corrective action process.

8. 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.

9. POLICY EXCEPTIONS

a. 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 may submit a waiver request. The waiver request must 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.

- b. Unless otherwise specified, agencies must review and renew approved policy waivers every fiscal year. Approved waivers must be associated with a NIST security control and tracked as a POA&M 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
CISO	Chief Information Security Officer
DR	Departmental Regulation
FISMA	Federal Information Security Management Act
IP	Internet Protocol
IT	Information Technology
NIST	National Institute of Standards and Technology
OCIO	Office of the Chief Information Officer
OIG	Office of Inspector General
OMB	Office of Management and Budget
POA&M	Plan of Action and Milestones
POC	Point of Contact
RBD	Risk Based Decision
SOP	Standard Operating Procedure
SP	Special Publication
UUI	Unique Investment Identifier
USDA	United States Department of Agriculture

APPENDIX B

AUTHORITIES AND REFERENCES

ASOC [OCD-SOP-003](#), *Plan of Action and Milestones Management Standard Operating Procedure*

Federal Information Security Management Act of 2002 ([FISMA](#)), 44 U.S.C. 3531 et seq. (2013)

[NIST SP 800-100](#), *Information Security Handbook: A Guide for Managers*, October 2006

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

[NIST SP 800-30 Revision 1](#), *Guide for Conducting Risk Assessments*, September, 2012

[NIST SP 800-37 Revision 1](#), *Guide for Applying the Risk Management Framework to Federal Information Systems: 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 May 1, 2010)

[NIST SP 800-65](#), *Integrating IT Security into the Capital Planning and Investment Control Process*, January 2005

[OMB Exhibit 53](#), *Information Technology and E-Government*, as amended

[OMB, Exhibit 300](#), *Planning, Budgeting, Acquisition, and Management of IT Capital Assets*, as amended

[OMB M-04-25](#), *FY 2004 Reporting Instructions for the Federal Information Security Management Act*, August 23, 2004

[OMB M-11-33](#), *FY 2011 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*, September 14, 2011

[DR 4070-735-001](#), *Employee Responsibilities and Conduct*, October 4, 2007

[DR 3300-001](#), *Telecommunications and Internet Services and Use*, March 23, 1999

APPENDIX C

FOOTNOTES

1. The Department's official system of record for management of FISMA activities is currently the Cyber Security and Assessment (CSAM) tool.
2. If an automated tool/scanner has been approved for use in managing vulnerabilities the remediation, tracking and reporting protocol will be specified in the agency's continuous monitoring policy and/or procedures.