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

DEPARTMENTAL REGULATION	Number: DR 3540-003
SUBJECT: Security Assessment and Authorization	DATE: August 12, 2014
	OPI: Office of the Chief Information Officer – Agriculture Security Operations Center

1. PURPOSE

a. This Departmental Regulation (DR) establishes the Security Assessment and Authorization (A&A) policy of the United States Department of Agriculture (USDA or "Department") for meeting the applicable laws, regulations, and standards of the Federal Government.

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 to continually assess the risk and magnitude of the harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information or information systems.

c. This policy establishes formal, documented security assessment and authorization (A&A) policies that address purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. Formal documented procedures facilitating the implementation of the security A&A policy controls are contained in the Agriculture Security Operations Center (ASOC) Oversight and Compliance Division (OCD) standard operating procedure (SOP) OCD-SOP-004, *USDA Six Step Risk Management Framework (RMF) Process Guide (RMF Process Guide.)*

d. It is the policy of USDA to comply with federal requirements to establish, implement, and support A&A to continually manage risk to USDA information systems.

2. SCOPE

a. This policy applies to all USDA information technology (IT) programs and systems, including cloud services, that are developed, maintained, and operated by USDA agencies, staff offices, employees, contractors, and other individuals working for or on behalf of the USDA.

b. This policy applies to systems operated by entities not under the jurisdiction of the USDA Secretary that are employed or contracted to process, transmit, or store USDA information through services such as (but not limited to), platform as a service (PaaS), infrastructure as a service (IaaS), and software as a service (SaaS.)

c. This DR adheres to the guidance identified in NIST Special Publication (SP) 800-53 Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations*, specifically the security assessment and authorization family of management controls applicable to all USDA systems with a Federal Information Processing Standard Publication (FIPS PUB) 199, *Standards for Security Categorization of Federal Information and Information Systems* security classification of low, moderate, or high.

3. SPECIAL INSTRUCTIONS/CANCELLATIONS

This policy supersedes the following directives in their entirety, unless otherwise noted:

a. Departmental Manual (DM) 3540-000, *Risk Management Program*, February 17, 2005;

b. DM 3540-001, *Risk Assessment Methodology*, February 17, 2005;

c. DM 3540-002, Risk Assessment and Security Checklists, August 19, 2004;

d. DM 3555-000, Certification and Accreditation (C&A) of Information Systems, October 18, 2005;

e. DM 3555-001, Certification and Accreditation Methodology, October 18, 2005;

f. DM 3565-000, *Cyber Security Plans*, February 17, 2005;

g. DM 3565-001, Annual Security Plan Guide for IT Systems, February 17, 2005; and

h. DM 3575-000, *Security Controls*, May 27, 2005.

4. BACKGROUND

This DR addresses requirements and responsibilities mandated by FISMA under Section 3544 (a) (2) (A-D). Federal agency responsibilities include:

a. Assessing the risk and magnitude of the harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of such information or information systems;

b. Determining the levels of information security appropriate to protect such information and information systems in accordance with standards issued under FIPS PUB 199 categorization and required minimum security controls as defined in FIPS PUB 200, *Minimum Security Requirements for Federal Information and Information Systems*, for information security classifications and related requirements;

c. Implementing policies and procedures to cost-effectively reduce risks to an acceptable level; and

d. Periodically testing and evaluating information security controls and techniques to ensure that they are effectively implemented.

5. POLICY

a. All USDA IT programs, systems, contractor provided systems, including cloud systems and services, require an authorization to operate (ATO) following the procedures outlined in the *RMF Process Guide* prior to being placed into operation. All systems shall be entered into the USDA FISMA data management and reporting tool (currently the Cyber Security Assessment and Management (CSAM) tool) by the end of the initiation phase of the project.

b. Authorized systems shall be continually monitored for risk using the ongoing assessment and authorization processes throughout the system lifecycle, based on the relevant procedures associated with the system categorization as outlined in the *RMF Process Guide*, and re-authorized every three years.

c. A&A documentation for all USDA systems, IT programs, and cloud services, including those operated by contractor and cloud service providers, shall be maintained in the USDA FISMA data management and reporting tool (CSAM) in accordance with the *RMF Process Guide* and its associated templates, as required by the system's categorization.

d. All FISMA-reportable USDA system and IT program deficiencies shall be recorded in the USDA FISMA data management and reporting tool. These deficiencies shall be managed in accordance with the USDA Plan of Action and Milestones (POA&M) guidance (located in the USDA Cyber Security 3500 Series of directives) and in accordance with OCD-SOP-003 *Plan of Action and Milestones Management Standard Operating Procedure*, Revision 1.

e. All contracts and statements of work for USDA systems, IT programs, and cloud services, including those operated by contractor and cloud service providers, shall include a requirement for completion of the A&A process in accordance with the *RMF Process Guide* to ensure the appropriate security controls and configuration baselines are implemented commensurate with the information system's categorization.

f. All interconnected systems, including those operated by contractor and cloud service providers, shall contain nondisclosure language in the Interconnection Security Agreement (ISA) and Memorandum of Understanding/Agreement (MOU/A) and require a nondisclosure agreement to be signed by all contractors who will access USDA information or information systems. *The Whistleblower Protection Enhancement Act* (WPEA) of 2012, 5 United States Code (U.S.C.) § 2301 et seq. (June 11, 2014) makes it a prohibited personnel practice for Federal agencies to enter into any "nondisclosure policy, form, or agreement" that does not include the following specific language:

"These provisions are consistent with, and do not supersede, conflict with, or otherwise alter the employee obligations, rights, or liabilities created by existing statute or executive order relating to:

(1) Classified information;

(2) Communications to Congress;

(3) The reporting to the Inspector General of a violation of any law, rule, or regulation, or mismanagement, a gross waste of funds, an abuse of authority, or a substantial and specific danger to public health or safety; or

(4) Any other whistleblower protection. The definitions, requirements, obligations, rights, sanctions, and liabilities created by controlling Executive orders and statutory provisions are incorporated into this agreement and are controlling."

6. ROLES AND RESPONSIBILITIES

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

(1) Develop and maintain a Departmentwide information security program, part of which defines assessment and authorization activities;

(2) Ensure that information security policies, procedures, and control techniques to address all A&A activities are developed and issued;

(3) Ensure compliance with applicable information security requirements; and

(4) Report annually to the Secretary of Agriculture, in coordination with other senior Departmental officials, on the effectiveness of the Department's information security program, including progress of remediation actions.

b. The USDA Chief Information Security Officer (CISO) / ASOC Associate Chief Information Officer (ACIO) 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 / ASOC ACIO reports directly to the USDA CIO and is the principal advisor for information security matters;

(2) Provide guidance, direction, and oversight for the security of processes and systems in USDA agencies and staff offices;

(3) Maintain information security policies, procedures, and control techniques to address all applicable A&A requirements;

(4) Provide direction, oversight, and concurrency review functions for the USDA A&A process, including maintaining and publishing the *RMF Process Guide* and schedules;

(5) Review agency and staff office exception requests to this policy and make approval or denial determination per Section 8 of this DR;

(6) Perform information security duties assigned by the CIO with the mission and resources to ensure compliance with information security requirements;

(7) Establish, develop, and maintain a process for planning, implementing, evaluating, and documenting remediation actions to address deficiencies in the Department's information security A&A policies, procedures, practices, and controls;

(8) Support the USDA CIO in annual reporting to the Secretary of Agriculture on the effectiveness of the Department's information security program, including progress of remediation activities;

(9) Track the status of IT systems and the associated A&A functions to ensure that systems are assessed, authorized and continually monitored;

(10) Review risk-based decisions (RDB) and approve as needed;

(11) Conduct concurrency reviews and issue concurrence memoranda prior to systems receiving an ATO;

(12) Establish, develop, and oversee the Department's A&A process;

(13) Ensure timely action(s) are taken to resolve all open POA&Ms;

(14) Provide administration, technical support, and training in the use of the Department's USDA FISMA data management and reporting tool; and

(15) Provide guidance, tools, schedules, and strategies to assist USDA agencies and staff offices in complying with the requirements of this policy.

c. Agency and Staff Office CIOs shall:

(1) Provide security for the information and information systems that support the operations and assets of the agency or staff office, including those provided or managed by another agency, staff office, contractor, or other source;

(2) Ensure that their agency or staff office complies with USDA's A&A policy and procedures in support of this policy;

(3) Initiate any needed waiver/exception requests to this policy per Section 8 of this DR;

(4) Ensure that an authorizing official (AO) is designated for each IT system, and that the AO understands and accepts the responsibility for system risk and operation;

(5) Ensure all agency and staff office IT professionals understand their role in the A&A process, with special emphasis on system owners, developers, Information Systems Security Program Managers (ISSPMs) and system administrators;

(6) Ensure corrective actions are taken to resolve or accept risk for all identified vulnerabilities related to their respective mission areas;

(7) Ensure adequate resources and funding, as required by OMB, are allocated to the mitigation of security vulnerabilities;

(8) Ensure timely action(s) are taken to resolve all POA&Ms; and

(9) Ensure this policy is available to any individual who will be involved in the A&A process to ensure they understand and can fulfill their roles and responsibilities.

d. Agency and Staff Office ISSPMs and CISOs shall:

(1) Keep the agency or staff office head informed of status, actions, and unresolved issues for continuous A&A through agency and staff office-level communication channels;

(2) Support and facilitate the work of A&A teams to ensure that agency and staff office IT systems are assessed and authorized in accordance with NIST per the process delineated in the *RMF Process Guide*;

(3) Review and ensure that A&A packages are complete before they are submitted for concurrency review;

(4) Ensure that system and program risks are mitigated or compensated for by appropriate security controls based on FIPS PUB 199, categorization and required minimum security controls, as defined in FIPS PUB 200, and NIST SP 800-53, Revision 3;

(5) Monitor A&A progress of agency and staff office systems and provide bi-weekly and ad hoc status to ASOC;

(6) Participate in IT system and program configuration control boards to ensure that system changes are reviewed to determine if the changes require A&A action;

(7) Ensure timely action(s) are taken to resolve all open POA&Ms:

(8) Ensure all security control assessments are performed by an independent assessor; and

(9) Disseminate, review, and provide input for this policy, as needed, to implement USDA A&A successfully.

e. Agency and Staff Office Information System Security Officers shall:

(1) Ensure that system compliance with this policy and the *RMF Process Guide*;

(2) Assist the system owner with the implementation and documentation of A&A activities as outlined within this policy and *RMF Process Guide*, specifically perform oversight and ensure security controls are documented, tested, and effective;

(3) Ensure that controls and/or compensating security controls are in place and effective; and

(4) Ensure that compensating security controls are removed, according to established processes, when no longer needed.

f. Agency and staff office system owners shall:

(1) Manage the prompt resolution of identified information security weaknesses, significant deficiencies, and non-conformance conditions, including the development, maintenance, monitoring, and reporting of corrective actions;

(2) Maintain accurate records of the status of the identified information security material weaknesses, deficiencies, and non-conformance throughout the entire corrective action process; and

(3) Ensure that the tracking, remediation, verification, and closure of information security weaknesses adhere to the USDA POA&M policies in the USDA Cyber Security 3500 Series of directives.

g. AOs shall:

(1) Review accreditation packages, specify any required changes, authorize systems for operation, and accept all operational risk;

(2) Oversee and approve the implementation of the security controls for the system;

(3) Review/validate risk, POA&M, and ATO constraints with the system owner and submit an RBD to ASOC OCD;

(4) Generate authorization recommendations or denials with system owner involvement;

(5) Review/validate risk, POA&M, system changes, and documentation of authorized systems with the system owner throughout the lifecycle of the system; and

(6) Determine whether a major change has been made to the system that impacts the risk and ATO status.

7. PENALTIES AND DISCIPLINARY ACTIONS FOR NON-COMPLIANCE

DM 3300-005, *Policies for Planning and Managing Wireless Technologies in USDA,* Chapter 3, sets forth USDA's policies and standards on employee responsibilities and conduct relative to the use of wireless technologies.

DR 4070-735-001, *Employee Responsibilities and Conduct*, Section 16, sets forth 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

a. All USDA agencies and staff offices are required to conform to this policy. In the event that a specific policy requirement cannot be met as explicitly stated, agencies and 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 memoranda to the USDA CISO / ASOC ACIO and submit the request to asoc.outreach@asoc.usda.gov for review and determination.

b. Agencies and 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 POA&M item in the Department's FISMA data management and reporting tool. The USDA CISO / ASOC ACIO shall render decision and monitor waivers to this policy.

-END-

APPENDIX A
DEFINITIONS

a. Assessment. See Security Control Assessment.
(Source: NIST Interagency or Internal Report (IR) 7298, Revision 2)

b. Authorizing Official. Official with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals. Synonymous with Accreditation Authority.
(Source: NIST IR 7298, Revision 2)

c. Authorization (to operate). The official management decision given by a senior organizational official to authorize operation of an information system and to explicitly accept the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation based on the implementation of an agreed-upon set of security controls.
(Source: NIST IR 7298, Revision 2)

d. Cloud Services. Shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.
(Source: NIST SP 800-145)

e. Cloud System. Collection of network-accessible computing resources that customers (i.e., cloud consumers) can access over a network.
(Source: NIST SP 800-145)

f. Independent Assessor. Any individual or group capable of conducting an impartial assessment of security controls employed within or inherited by an information system. Impartiality implies that assessors are free from any perceived or actual conflicts of interest with respect to the development, operation, and/or management of the information system or the determination of security control effectiveness. Independent security control assessment services can be obtained from other elements within the organization or can be contracted to a public or private sector entity outside of the organization. Contracted assessment services are considered independent if the information system owner is not directly involved in the contracting process or cannot unduly influence the independence of the assessor(s) conducting the assessment of the security controls.
(Source: NIST SP 800-37, Revision 1)

g. Information Security. The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.
(Source: NIST IR 7298, Revision 2)

h. Information System/System. A discrete set of resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.
(Source: NIST IR 7298, Revision 2)

i. Infrastructure as a Service (IaaS). The capability provided to the consumer to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure, but has control over operating systems, storage, deployed applications, and possibly select networking components (e.g., firewalls, load balancers).
(Source: NIST SP 800-145)

j. Interconnection Security Agreement (ISA). An agreement established between organizations that own and operate connected IT systems to document the technical requirements of the interconnection. The ISA also supports an MOU/A between the organizations.
(Source: NIST IR 7298, Revision 2)

k. Memorandum of Understanding/Agreement (MOU/A). A document established between two or more parties to define their respective responsibilities in accomplishing a particular goal or mission. In this guide, an MOU/A defines the responsibilities of two or more organizations in establishing, operating, and securing a system interconnection.
(Source: NIST IR 7298, Revision 2)

l. Platform-as-a-Service (PaaS). The capability provided to the consumer to deploy onto the cloud infrastructure consumer-created applications using programming languages and tools supported by the provider (e.g., Java, Python, .NET). The consumer does not manage or control the underlying cloud infrastructure, network, servers, operating systems, or storage, but the consumer has control over the deployed applications and possibly application hosting environment configurations.
(Source: NIST SP 800-145)

m. Security Control Assessment. The testing and/or evaluation of the management, operational, and technical security controls in an information system to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for system and/or enterprise. (Source: NIST IR 7298, Revision 2)

n. Security Controls. The management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information.
(Source: NIST IR 7298, Revision 2)

o. Service Providers. This category encompasses typical outsourcing of system or network operations, telecommunications services, or other managed services (including those provided by another agency or staff office and subscribing to software services). (Source: NIST SP 800-37, Revision 1)

p. Software-as-a-Service (SaaS). The capability provided to the consumer to use the provider's applications running on a cloud infrastructure and accessible from various client devices through a thin client interface such as a Web browser (e.g., Web-based email). The consumer does not manage or control the underlying cloud infrastructure, network, servers, operating systems, storage, or individual application capabilities, with the possible exception of limited user-specific application configuration settings. (Source: NIST SP 800-145)

APPENDIX B
ACRONYMS AND ABBREVIATIONS

A&A	Assessment and Authorization
AO	Authorizing Official
ACIO	Associate Chief Information Officer
ASOC	Agriculture Security Operations Center
ATO	Authorization to Operate
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CSAM	Cyber Security Assessment and Management Tool
DM	Departmental Manual
DR	Departmental Regulation
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act of 2002
IaaS	Infrastructure as a Service
IR	Interagency or Internal Report
ISA	Interconnection Security Agreement
ISSPM	Information Systems Security Program Manager
IT	Information Technology
MOU/A	Memorandum of Understanding/Agreement
NIST	National Institute of Standards and Technology
OCD	Oversight and Compliance Division
OMB	Office of Management and Budget
PaaS	Platform as a Service
POA&M	Plan of Action and Milestones
PUB	Publication
RBD	Risk-Based Decision
RMF	Risk Management Framework
SaaS	Software as a Service
SOP	Standard Operating Procedure
SP	Special Publication
U.S.C.	United States Code
USDA	United States Department of Agriculture
WPEA	Whistleblower Protection Enhancement Act

APPENDIX C
AUTHORITIES AND REFERENCES

DM 3300-005, *Policies for Planning and Managing Wireless Technologies in USDA*, November 10, 2010

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

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

Federal Information Security Management Act of 2002 *(FISMA)*, 44 U.S.C. § 3541 et seq. (2014)

FIPS PUB 199, *Standards for Security Categorization of Federal Information and Information Systems*, February 2004

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

NIST IR 7298, Revision 2, *Glossary of Key Information Security Terms*, May 2013

NIST SP 800-37, Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems*, February 2010

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

SP 800-145, *The NIST Definition of Cloud Computing*, September 2011

OCD-SOP-003, *Plan of Action and Milestones Management Standard Operating Procedure*, Revision 1, July 2013

OCD-SOP-004, *USDA Six Step Risk Management Framework (RMF) Process Guide*, Revision 2.38, December 2012

USDA Cyber Security Directives, 3500 Series

Whistleblower Protection Enhancement Act (WPEA) of 2012, 5 U.S.C. § 2301 et seq. (June 11, 2014)