

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

|                                                                                    |                                                                                               |
|------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------|
| <b>DEPARTMENTAL REGULATION</b>                                                     | Number:<br>DR 3571-001                                                                        |
| SUBJECT: Information System Contingency Planning<br>and Disaster Recovery Planning | DATE:<br>June 1, 2016                                                                         |
|                                                                                    | OPI:<br>Office of the Chief Information<br>Officer, Agriculture Security<br>Operations Center |

| <u>Section</u>                                           | <u>Page</u> |
|----------------------------------------------------------|-------------|
| 1. Purpose                                               | 1           |
| 2. Scope                                                 | 2           |
| 3. Special Instructions/Cancellations                    | 2           |
| 4. Background                                            | 3           |
| 5. Policy                                                | 4           |
| 6. Roles and Responsibilities                            | 8           |
| 7. Penalties and Disciplinary Actions for Non-Compliance | 12          |
| 8. Policy Exceptions                                     | 13          |
| Appendix A Definitions                                   | A-1         |
| Appendix B Acronyms and Abbreviations                    | B-1         |
| Appendix C Authorities and References                    | C-1         |

## 1. PURPOSE

- a. This Departmental Regulation (DR) establishes the United States Department of Agriculture (USDA) policy to guide agencies and staff offices in developing, implementing, and maintaining Information System Contingency Plans (ISCPs) and facility Disaster Recovery Plans (DRPs). This contingency planning policy governs the activities designed to sustain or restore information system operations, possibly at alternate sites, in the event of disruptions. In this context, contingency planning helps ensure the availability of information systems and the services and business processes supported by information technology (IT).
- b. This policy complies with the requirements of United States Code (U.S.C.) in the *Federal Information Security Modernization Act of 2014* ([FISMA](#)), 44 U.S.C. § 3541, et seq.; Federal Information Processing Standards Publication ([FIPS PUB](#)) 200, *Minimum*

*Security Requirements for Federal Information and Information Systems*; Office of Management and Budget (OMB) Circular A-130, Appendix III, *Responsibilities for Protecting Federal Information Resources*; 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*; NIST [SP 800-37](#) Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*; and NIST [SP 800-34](#) Revision 1, *Contingency Planning Guide for Federal Information Systems*.

## 2. SCOPE

- a. This policy applies to all USDA agencies, staff offices, employees, appointees, contractors, and others who work for or on behalf of USDA and are responsible for establishing and maintaining contingency plans or performing contingency planning activities, specifically for ISCPs, DRPs, or both.
- b. This policy applies to:
  - (1) Information systems owned or operated by USDA, a USDA contractor, subcontractor, or by another organization on behalf of or funded by USDA; and
  - (2) Facilities from which these systems operate.
- c. Nothing in this policy shall alter the requirements for the protection of information associated with national security systems such as those in *Federal Information Security Modernization Act of 2014* ([FISMA](#)), policies and standards issued by the Committee on National Security Systems (CNSS), or Intelligence Community Directives (ICDs).
- d. NIST SP 800-34 Revision 1 identifies various types of contingency plans. Of those, this policy applies only to ISCPs and DRPs and where ISCPs and DRPs may intersect with those other plans, such as during a disruption or plan testing. This document does not apply to:
  - (1) Organizational mission continuity plans defined in National Security Presidential Directive-51/Homeland Security Presidential Directive-20 ([NSPD-51/HSPD-20](#)), *National Continuity Policy*, except where it is required to restore information systems and their processing capabilities; or
  - (2) Other plans mentioned in NIST SP 800-34 Revision 1, specifically, business continuity plans (BCPs), continuity of operations plans (COOPs), occupant emergency plans (OEPs), or crisis communications plans.

## 3. SPECIAL INSTRUCTIONS/CANCELLATIONS

- a. This policy supersedes in their entirety:
  - (1) DM 3570-000, *IT Contingency and Disaster Planning*, dated February 17, 2005; and
  - (2) DM 3570-001, *Disaster Recovery and Business Resumption Plans*, dated February 17, 2005.
- b. This policy is effective immediately when published and will remain in effect until superseded.
- c. All agencies and staff offices shall align their policies and procedures with this DR within six months of the publication date.

#### 4. BACKGROUND

In the NIST SP 800-34 Revision 1, Executive Summary, contingency planning is described as “...[the] interim measures to recover information system services after a disruption. Interim measures may include relocation of information systems and operations to an alternate site, recovery of information system functions using alternate equipment, or performance of information system functions using manual methods.”

This document focuses on ISCPs and DRPs. An ISCP, also known as a contingency plan, addresses information system disruptions, whether physical or cyber, and procedures to recover that system regardless of the system’s operating site or sites. The ISCP identifies roles and responsibilities, details inventory information, and provides established procedures for assessing the situation, restoring and recovering the system, and validation testing of the system to resume secure functions and operations.

A DRP addresses relocation of essential information system functions and operations to an alternate site in the event of a major disruption or damage that renders the information system infrastructure (electric power, telecommunications connections, and environmental controls) or a facility unable to support operations. This includes physical events that make a facility or operating site inaccessible or uninhabitable and cyber incidents that make systems processing infeasible at the facility. Note a DRP does not have to address information systems such as radio-based telecommunications that are not housed in a facility.

Continuity plans are related to, but distinct from, contingency plans. The focus of continuity planning is mission and business functions or processes, whether these functions are supported by information systems or not. A COOP focuses on restoration of mission essential functions at an alternate site. A BCP addresses sustaining mission or business processes according to established priorities.

Conducting a business impact analysis (BIA) is an initial process linking continuity and contingency planning. The BIA associates an information system with the critical mission or

business processes and services provided, which in turn characterizes the impacts of a disruption on those processes and services. The results of a BIA drive priorities for continuity and recovery and the strategies and resources needed to meet those priorities. Information resulting from a BIA includes the maximum tolerable downtime (MTD) for each mission or business process, the recovery time objective (RTO), and the recovery point objective (RPO); the MTD, RTO, and RPO can serve as metrics for actual disruptions and tests of contingency plans.

A cyber security incident may affect availability (such as a denial of service attack), or may impact the confidentiality and/or integrity of cyber-based information. A cyber security incident response plan (IRP) provides procedures for identifying, analyzing, and categorizing cyber security incidents, and then containing, eradicating, and recovering from incidents. A cyber security incident that renders information system infrastructure at a facility unable to support operations may trigger activation of one or more ISCPs as well as the facility's DRP.

Crisis communications plans provide guidance on communicating with both internal and external parties in the event of a disruption or an incident. These plans also designate who is authorized to communicate with the public and the media or issue statements.

Although this policy addresses only ISCPs and DRPs, all planners must collaborate to coordinate strategies in the various plans to ensure they are effective and efficient in ensuring critical information, systems, and services are maintained or recoverable in the event of an emergency.

Contingency plans are tested in two ways. Tabletop exercises are discussion-based and do not involve deploying equipment or other resources. Functional exercises test recovery and restoration of system operations and processing and allow personnel to practice their roles and responsibilities. The complexity and scope of functional exercises vary: they may focus on parts of the plan, specific procedures, or teams, or they may be full-scale, in which all elements of the plan are exercised.

## 5. POLICY

- a. All agencies and staff offices shall use the security categorization impact level (high, moderate, or low) from [FIPS PUB 199](#), *Standards for Categorization of Federal Information and Information Systems*, to determine the effort and rigor of ISCP/DRP development, implementation, and testing.
- b. Agencies and staff offices shall acquire and maintain sufficient funding and personnel to ensure viable development, implementation, testing, and maintenance of their ISCPs and facility DRPs.
- c. Each contingency planning/disaster recovery planning program shall identify one or more ISCP/DRP Coordinators, and the ISCPs and DRPs shall include complete and

current contact information for the responsible coordinator(s) and any alternate coordinator(s).

- d. Agencies and staff offices shall assign specific ISCP/DRP responsibilities to designated positions or personnel and identify the personnel in a contact list with complete and current contact information.
- e. Annual ISCP/DRP training shall be conducted for all personnel with implementation or execution responsibilities identified in an ISCP or a DRP.
- f. A BIA shall be:
  - (1) Created for each new information system;
  - (2) Updated and revised if major changes are made to the system or to the business processes and functions that the system supports; and
  - (3) Used to determine contingency planning requirements and priorities.
- g. All USDA information systems, including those at contractor or other facilities, owned or operated by or on behalf of USDA, shall be covered by a current ISCP to meet the needs of critical system operations in the event of a disruption.
- h. Agencies and staff offices shall use ISCP templates as follows:
  - (1) For cloud-hosted systems, the current template available from the Federal Risk and Authorization Management Program (FedRAMP) website at <https://www.fedramp.gov/resources/templates-3/>; and
  - (2) For all other systems, the current template available from the FISMA data management and reporting tool or the Compliance, Audit, Policy, and Enforcement (CAPE) Resources [SharePoint page](#) for contingency planning documentation.
- i. While cyber security incident management and incident response planning are addressed in other USDA documents (DR 35XX-XXX, *Cyber Security Incident Management*, and Departmental Manual (DM) 35XX-XXX, *Cyber Security Incident Management*), the scope of ISCP and DRP planning shall include cyber incidents in addition to physical incidents, to enable response to and recovery from major cyber incidents that render information system infrastructure or systems unable to support operations.
- j. The scope of the ISCP shall include:
  - (1) All IT components within the system boundary, as described in the security plan for the information system; and

- (2) Major cyber incidents that render the information system or its supporting infrastructure unable to support operations.
- k. Operators of USDA facilities that serve as the primary or alternate processing site for one or more moderate or high impact systems shall develop and maintain a current DRP, ensuring that the contents of the DRP:
  - (1) Identify all systems that rely upon the DRP;
  - (2) Describe response activities to be taken for physical events that could significantly disrupt operations, including making the site inaccessible or uninhabitable, and major cyber incidents that render information system infrastructure at the facility unable to support operations;
  - (3) Reference or include the site or facility physical emergency or security plan, the OEP, cyber security IRP, and the COOP; and
  - (4) Identify the ISCP/DRP Coordinator(s) and other personnel with significant disaster recovery roles.
- l. ISCPs and DRPs shall be reviewed and updated at least annually to:
  - (1) Reflect system, organizational, personnel, or operating site changes, or changes to the mission or business functions supported;
  - (2) Address problems encountered during contingency plan implementation, execution, or testing; and
  - (3) Resolve issues noted in after-action reports.
- m. ISCPs and DRPs shall be tested at least annually. The type of test (tabletop or functional) shall be based on the FIPS PUB 199 categorization of the system or systems covered by the test. Test guidance is provided in the [Contingency Plan Exercise Handbook](#), available for download from the FISMA data management and reporting tool.
  - (1) For a new system, no matter what its system categorization is, a tabletop test of the ISCP is acceptable.
  - (2) For systems categorized as moderate or high impact, a functional test of the ISCP/DRP shall be conducted.
  - (3) For low impact systems, the ISCP/DRP test may be a tabletop exercise or a functional test.

- (4) An unscheduled disruption may serve as a test, but only if the scope of the disruption equals or exceeds the required type of test.
  - (5) The annual test may cover multiple systems, provided that:
    - (a) The type of test meets or exceeds the testing requirements for the highest impact system included in the test; and
    - (b) The test results are documented individually for each system included in the test.
- n. An after-action report shall be produced for each test of an ISCP or DRP.
  - (1) For ISCP tests, the *Contingency Plan Exercise Handbook*, Appendix A, provides a report template.
  - (2) Protection of after action reports shall be commensurate with the sensitivity or classification of the contents.
  - (3) The after-action reports shall identify all corrective actions needed to address deficiencies in the plan, associated procedures, staff training, or resources.
- o. Any corrective actions that cannot be remediated within 30 days following the publication of the after-action report shall be entered as plans of action and milestones (POA&Ms) in the FISMA data management and reporting tool, per [DR 3565-003](#), *Plan of Action and Milestones Policy*.
- p. Current ISCPs, DRPs, test plans, test results, and after-action reports shall be uploaded to and maintained in the FISMA data management and reporting tool.
- q. Agencies and staff offices shall ensure each information system and its data are backed up with a frequency consistent with the RTO and RPO for the system, unless a waiver for this requirement has been approved. Backups shall be tested at least annually to ensure system and data recovery requirements are achieved.
- r. For all moderate and high impact level systems, agencies and staff offices shall establish and maintain alternate storage and alternate processing sites and ensure copies of ISCPs are available at the alternate processing sites.
- s. System owners shall ensure that primary and alternate telecommunications service agreements are in place for each facility and designed to support the RTO of essential mission and business functions, including priority-of-service provisions for moderate and high systems.

- t. System owners of high impact systems shall ensure that primary and alternate telecommunications service providers have contingency plans, test the plans at least annually, and train their personnel in contingency plan responsibilities.

## 6. ROLES AND RESPONSIBILITIES

- a. The USDA Chief Information Officer (CIO) shall:
  - (1) Provide guidance and direction for a standardized Departmentwide process for contingency planning; and
  - (2) Direct agencies and staff offices to take risk-reducing corrective actions to remediate problems found during activation of ISCPS or DRPs or when testing those plans.
- b. The USDA Chief Information Security Officer (CISO) shall:
  - (1) Ensure the development and maintenance of Departmental contingency planning policies and guidance;
  - (2) Ensure dissemination of Federal and Departmental contingency planning requirements and guidance to agencies and staff office CIOs, CISOs, and Information Systems Security Program Managers (ISSPMs);
  - (3) Ensure the development and maintenance of a framework for evaluating and reporting compliance with contingency planning policy;
  - (4) Evaluate and report to the USDA CIO contingency planning compliance levels at least annually; and
  - (5) Ensure that all ISCPs and facility DRPs are tested annually.
- c. Agency and Staff Office CIOs shall:
  - (1) Ensure agency and staff office contingency planning activities are consistent with Federal guidance and Departmental policy and that the NIST contingency planning process is integrated into system life cycle activities;
  - (2) Ensure that adequate resources are budgeted for all contingency planning activities within their area of responsibility;
  - (3) Ensure that ISCP/DRP Coordinators are designated and trained annually on their responsibilities; and

- (4) Identify and align the RTO and RPO for each information system with the MTD of business functions and services in coordination with system owners.
- d. Agency and Staff Office System Owners shall:
  - (1) Ensure that program managers:
    - (a) Are provided with a copy of this policy and take annual awareness training on contingency planning; and
    - (b) Request adequate budget funding for contingency planning activities for all information systems in their portfolio.
  - (2) Identify and align the system RTO and RPO with the MTD of business functions and services in coordination with the agency CIO;
  - (3) Ensure BIAs are conducted for all information systems and are reviewed and updated at least annually to reflect changes, including MTD, RTO, or RPO;
  - (4) Designate a ISCP/DRP Coordinator for each system and ensure that each coordinator is trained annually on system/facility-specific contingency planning responsibilities;
  - (5) Ensure that for all information systems in their respective portfolio:
    - (a) ISCPs are developed and maintained using the current applicable templates, correctly implemented, and updated at least annually to reflect system, organizational, personnel, or operating site changes, or changes to the mission or business functions that the systems support;
    - (b) Interconnection security agreements (ISAs), memoranda of agreement (MOAs) or memoranda of understanding (MOUs), and cybersecurity IRPs do not conflict with ISCP requirements;
    - (c) ISCPs document the responsibilities of the ISCP/DRP Coordinator and their alternate;
    - (d) ISCPs are disseminated to personnel with ISCP responsibilities, and current copies are kept at each primary and alternate processing sites for those systems;
    - (e) ISCPs are tested annually with a rigor consistent with the system security categorization, as described in Section 5 of this policy;
    - (f) An after-action report is produced for every test and that POA&Ms for uncorrected weaknesses are created as required in Section 5; and

- (g) Current and approved ISCPs, test plans, test results, and after-action reports are uploaded to the FISMA data management and reporting tool as part of the required documentation for assessment and authorization.
- (6) Review and approve ISCPs for the systems for which they are responsible, ensuring that plans are complete, up-to-date, and compliant with this policy;
- (7) Review and approve after-action reports for ISCP activation and tests;
- (8) Provide contractors, subcontractors, or other facilities (e.g., data centers operated by another Federal department or a state agency) with applicable contingency planning documents and templates; and
- (9) Ensure personnel at primary and alternate facilities are aware of the operational security requirements that must be maintained when an ISCP is activated or tested.
- e. Agency and Staff Office CISOs and ISSPMs shall:
  - (1) Communicate the responsibilities for managing, implementing, and maintaining compliance with this policy to all personnel with ISCP/DRP responsibilities;
  - (2) Ensure Federal and Departmental requirements for ISCP/DRP activities are being met;
  - (3) Review and provide security input to and guidance on the contingency planning process, development, and implementation of ISCPs/DRPs, testing of ISCPs/DRPs, and ISCP/DRP training;
  - (4) Assist and support ISCP/DRP Coordinators, system owners, and program managers with:
    - (a) Developing contingency planning strategies that support the mission or business functions and processes;
    - (b) Identifying resources and interdependencies needed to implement and sustain contingency planning activities;
    - (c) Identifying and resolving competing priorities and resource requirements in ISCPs/DRPs; and
    - (d) Mitigating any issues identified in ISCPs/DRPs.
  - (5) Ensure proper cross-references between different types of security documentation and contingency plans, including system security plans, privacy impact assessments, ISCPs, DRPs, and continuity plans;

- (6) Review and approve DRPs and ensure that:
    - (a) The DRPs are available to all personnel with responsibilities identified therein and current copies are kept at each primary and alternate processing site; and
    - (b) Current DRPs, associated test plans, test results, and after-action reports are uploaded to the FISMA data management and reporting tool.
  - (7) Ensure that an after-action report is produced after each ISCP/DRP activation or test and POA&Ms for uncorrected weaknesses are created as required in Section 5.
- f. ISCP/DRP Coordinators shall:
- (1) Coordinate and conduct contingency planning activities in compliance with this policy;
  - (2) Work with system owners and other internal and external stakeholders to identify and validate mission or business functions and processes that support or depend on the information system or systems;
  - (3) Work with system owners, process owners, and business managers to determine the MTD for each system or process and the optimum RTO and RPO for each system;
  - (4) Use BIA results to define ISCP requirements, strategies, and priorities;
  - (5) Understand interdependencies of infrastructure and systems and the effects of those interdependencies on plans;
  - (6) Identify and document for system owners potential recovery strategies, recovery procedures, and technologies to meet recovery priorities;
  - (7) Analyze identified processing methods and approaches (e.g., employing alternate equipment or manual means, relocating to an alternate site) to ensure that they are compatible with the system's management, operational, technical, and privacy controls;
  - (8) Analyze the selected recovery strategies, measures, and technologies to ensure they can:
    - (a) Be implemented effectively in a timely manner with available personnel and financial resources: and
    - (b) Provide for recovery and reconstitution of information systems to a known state after a disruption, compromise, or failure.

- (9) Document the formal ISCP/DRP using the current template, describing specific responsibilities, facilities or alternate processing methods, and other required elements;
  - (10) Review and update the ISCP/DRP at least annually and ensure that:
    - (a) Weaknesses discovered during actual disruptions or tests have been corrected; and
    - (b) The information is current and valid regarding procedures, resources, roles and responsibilities, operating sites, and alternative processing methods.
  - (11) Plan and ensure annual testing is consistent with the FIPS PUB 199 categorization, as described in Section 5 of this document;
  - (12) Coordinate recovery testing of backups, including testing of backups maintained at alternate sites; and
  - (13) Conduct or facilitate training for personnel with responsibilities identified in the ISCP/DRP, including providing awareness of policies and procedures.
- g. ISSOs shall:
- (1) Review and approve the after-action reports from ISCP/DRP testing; and
  - (2) Ensure that POA&Ms for uncorrected weaknesses discovered during actual disruptions or tests are created as required in Section 5.

## 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 regarding the use of wireless technologies.

[DR 4070-735-001](#), *Employee Responsibilities and Conduct*, Section 16, sets forth the USDA's policies, procedures, and standards on employee responsibilities and conduct regarding 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; 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 memoranda to the USDA CISO and submit the request to [asoc.outreach@asoc.usda.gov](mailto: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 FISMA data management and reporting tool. The Associate Chief Information Officer (ACIO), Agriculture Security Operations Center (ASOC) shall monitor and approve waivers to this policy.

-END-

## APPENDIX A

### DEFINITIONS

- a. After Action Report. A document containing findings and recommendations from an exercise or a test. (Source: NIST [SP 800-84](#))
- b. Authorization. The official management decision given by a senior organizational official to authorize operation of an information system and to explicitly accept the risk to the 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 [Interagency Report \(IR\) 7298](#) Revision 2)
- c. Contingency Plan. Management policies and procedures used to guide an enterprise response to a perceived loss of mission capability. The Contingency Plan is the first plan used by enterprise risk managers to determine what happened, why, and what to do. It may point to the COOP or a DRP for major disruptions. (Source: NIST IR 7298 Revision 2)
- d. Disaster Recovery Plan. A written plan for recovering one or more information systems at an alternative facility in response to a major hardware or software failure or destruction of facilities. (Source: NIST IR 7298 Revision 2)
- e. Disruption. An unplanned event that causes an information system to be inoperable for a length of time (e.g., minor or extended power outage, extended unavailable network, or equipment or facility damage or destruction). (Source: NIST [SP 800-34](#) Revision 1)
- f. Exercise. A simulation of an emergency designed to validate the viability of one or more aspects of an information technology (IT) plan. (Source: NIST SP 800-84)
- g. Functional Testing. Segment of security testing in which advertised security mechanisms of an information system are tested under operational conditions. (Source: NIST SP 800-34 Revision 1)
- h. Impact. The magnitude of harm that can be expected to result from the consequences of unauthorized disclosure of information, unauthorized modification of information, unauthorized destruction of information, or loss of information or information system availability. (Source: NIST SP 800-34 Revision 1)
- i. Impact Level. High, moderate, or low security categories of an information system established in FIPS PUB 199, which classify the intensity of a potential impact that may occur if the information system is jeopardized. (Source: NIST SP 800-34 Revision 1)

- j. Information System. A discrete set of resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. (Source: NIST SP 800-34 Revision 1)
- k. Information System Contingency Plan (also see Contingency Plan). Management policy and procedures designed to maintain or restore business operations, including computer operations, possibly at an alternate location, in the event of emergencies, system failures, or disasters. (Source: NIST SP 800-34 Revision 1)
- l. Maximum Tolerable Downtime. The amount of time mission or business process can be disrupted without causing significant harm to the organization's mission. (Source: NIST SP 800-34 Revision 1)
- m. Memorandum of Understanding /Agreement. A document established between two or more parties to define their respective responsibilities in accomplishing a particular goal or mission, e.g., establishing, operating, and securing a system interconnection. (Source: NIST IR 7298 Revision 2)
- n. Recovery Point Objective. The point in time to which data is to be recovered after an outage. (Source: NIST SP 800-34 Revision 1)
- o. Recovery Time Objective. The overall length of time an information system's components can be in the recovery phase before negatively impacting the organization's mission or business processes. (Source: NIST SP 800-34 Revision 1)
- p. 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 SP 800-34 Revision 1)
- q. Significant Change. Modifications to an information system or common controls that may trigger an event-driven reauthorization include, but are not limited to: (i) installation of a new or upgraded operating system, middleware component, or application; (ii) modifications to system ports, protocols, or services; (iii) installation of a new or upgraded hardware platform; (iv) modifications to cryptographic modules or services; or (v) modifications to security controls. Significant changes to environments of operation that may trigger an event-driven authorization include, but are not limited to: (i) moving to a new facility; (ii) adding new missions or business functions; (iii) acquiring specific and credible threat information that the organization is being targeted by a threat source; or (iv) establishing new or modified laws, directives, policies, or regulations. Risk assessment results and/or the results from a security impact analysis may be used to help determine if changes to information systems or common controls are significant enough to trigger a reauthorization action. (Source: NIST [Supplemental Guidance on Ongoing Authorization: Transitioning to Near Real-Time Risk Management](#))

- r. System Development Life Cycle. The scope of activities associated with a system, encompassing the system's initiation, development and acquisition, implementation, operation and maintenance, and ultimately its disposal that instigates another system initiation. (Source: NIST SP 800-34 Revision 1)
- s. Tabletop Exercise. A discussion-based exercise where personnel with roles and responsibilities in a particular IT plan meet in a classroom setting or in breakout groups to validate the content of the plan by discussing their roles during an emergency and their responses to a particular emergency situation. A facilitator initiates the discussion by presenting a scenario and asking questions based on the scenario. (Source: NIST SP 800-34 Revision 1)
- t. Test. A type of assessment method that is characterized by the process of exercising one or more assessment objects under specified conditions to compare actual with expected behavior, the results of which are used to support the determination of security control effectiveness over time. (Source: NIST IR 7298 Revision 2)

## APPENDIX B

### ACRONYMS AND ABBREVIATIONS

|          |                                                     |
|----------|-----------------------------------------------------|
| ACIO     | Associate Chief Information Officer                 |
| ASOC     | Agriculture Security Operations Center              |
| BCP      | Business Continuity Plan                            |
| BIA      | Business Impact Analysis                            |
| CAPE     | Compliance, Audits, Policy and Enforcement          |
| CIO      | Chief Information Officer                           |
| CISO     | Chief Information Security Officer                  |
| CNSS     | Committee on National Security Systems              |
| COOP     | Continuity of Operations Plan                       |
| CP       | Contingency Planning                                |
| DHS      | Department of Homeland Security                     |
| DM       | Departmental Manual                                 |
| DR       | Departmental Regulation                             |
| DRP      | Disaster Recovery Plan                              |
| FCD      | Federal Continuity Directive                        |
| FedRAMP  | Federal Risk and Authorization Management Program   |
| FIPS PUB | Federal Information Processing Standard Publication |
| FISMA    | Federal Information Security Modernization Act      |
| HSPD     | Homeland Security Presidential Directive            |
| ICD      | Intelligence Community Directive                    |
| IR       | Interagency Report                                  |
| IRP      | Incident Response Plan                              |
| ISA      | Interconnection Security Agreement                  |
| ISCP     | Information Security Contingency Plan               |
| ISSPM    | Information Systems Security Program Manager        |
| IT       | Information Technology                              |
| MOA      | Memorandum of Agreement                             |
| MOU      | Memorandum of Understanding                         |
| MTD      | Maximum Tolerable Downtime                          |
| NIST     | National Institute of Standards and Technology      |
| NSPD     | National Security Presidential Directive            |
| OCD      | Oversight & Compliance Division                     |
| OEP      | Occupant Emergency Plan                             |
| OMB      | Office of Management and Budget                     |
| POA&M    | Plan of Action and Milestones                       |
| RMF      | Risk Management Framework                           |
| RPO      | Recovery Point Objective                            |
| RTO      | Recovery Time Objective                             |
| SP       | Special Publication                                 |
| U.S.C.   | United States Code                                  |
| USDA     | United States Department of Agriculture             |

## APPENDIX C

### AUTHORITIES AND REFERENCES

ASOC, Compliance, Audits, Policy and Enforcement (CAPE) Division Standard Operating Procedure, [CAPE-SOP-004](#), *USDA Six-Step Risk Management Framework (RMF) Process Guide*, Revision 2.44, May 2015

Department of Homeland Security (DHS), [Federal Continuity Directive 1 \(FCD 1\)](#), *Federal Executive Branch National Continuity Program and Requirements*, October 2012

DHS, [Federal Continuity Directive 2 \(FCD 2\)](#), *Federal Executive Branch Mission Essential Function and Candidate Primary Mission Essential Function Identification and Submission Process*, July 2013

DHS, [National Disaster Recovery Framework](#), September 2011

DHS, [National Response Framework](#), 2<sup>nd</sup> edition, May 2013

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

DM 35XX-XXX, *Cyber Security Incident Management*, forthcoming

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

DR 35XX-XXX, *Cyber Security Incident Management*, forthcoming

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

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

*E-Government Act of 2002*, [40 U.S.C. § 11331](#)

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

[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

[NSPD-51/HSPD-20](#), *National Continuity Policy*, May 9, 2007

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

NIST [SP 800-34](#) Revision 1, *Contingency Planning Guide for Federal Information Systems*, May 2010

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 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, April 2013 with updates as of January 22, 2015

NIST [SP 800-84](#), *Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities*, September 2006

NIST, [Supplemental Guidance on Ongoing Authorization: Transitioning to Near Real-Time Risk Management](#), June 2014

OMB Circular A-130, Appendix III, *Responsibilities for Protecting Federal Information Resources*, forthcoming

[USDA Contingency Plan Template](#), Version 1.5, October 2014

[USDA Disaster Recovery Plan Template](#), Version 1.0, September 2015

USDA Office of the Chief Information Officer Oversight & Compliance Division (OCD), [Contingency Plan Exercise Handbook](#), Version 2.0, October 2014