FSIS DIRECTIVE

1306.15 Revision 1	9/20/16

INFORMATION SYSTEMS CONTINGENCY PLANNING

I. PURPOSE

This directive lists information systems contingency planning (CP) requirements as stated in the National Institute of Science and Technology (NIST) Special Publication (SP) 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations* and provides general information concerning how the Office of the Chief Information Officer (OCIO) implements them. This revision updates references and security controls required by the NIST.

II. CANCELLATION

FSIS Directive 1306.15, *Information Systems Contingency Planning (CP)*, 12/1/11

III. BACKGROUND

A. CP is a process, with accompanying documentation for an information system that addresses roles, responsibilities, assigned individuals with contact information, and activities associated with restoring the system after a disruption or failure.

B. FSIS ensures information security controls are in place to protect FSIS information systems and data in compliance with Public Law 107-347, Title III, *E-Government Act of 2002*; Public Law 93-579, *Privacy Act of 1974*, as amended; and USDA regulations.

C. The President signed Public Law 113-283 into law as the *Federal Information Security Modernization Act of 2014* (FISMA). The goals of FISMA include the development of a comprehensive framework to protect the Government's information, operations, and assets. FISMA assigns specific responsibilities to Federal agencies, and particularly to the NIST and the Office of Management and Budget (OMB), to strengthen IT system security. In particular, FISMA requires the head of each agency to implement policies and procedures to cost-effectively reduce information security risks to an acceptable level.

D. NIST SP 800-53, Revision 4, outlines the controls addressed by CP. The selection and employment of appropriate security controls for an information system is an important task that can have major implications on the operations and assets of an organization. To adhere to the NIST SP 800-53, Revision 4, FSIS has established the requirements stated in Section VI. of this directive.

IV. ROLES AND RESPONSIBILITIES FOR FSIS EMPLOYEES

A. **System Users.** All employees, to include program areas outside of OCIO, contractors, other Federal agencies, state and local governments, and authorized private organizations or individuals who use FSIS IT resources are to:

1. Be knowledgeable of CP and the requirements in this directive; and

2. Ensure their duties are performed in accordance with this directive.

B. **FSIS System Owners.** System owners are FSIS employees that are designated by their specific program area and may be from program areas outside of OCIO. They are to:

1. Assist in the development and maintenance of detailed operating procedures to satisfy appropriate CP security requirements in this directive; and

2. Approve the IT CP on an annual basis with support from the Information System Security Program Manager (ISSPM).

V. ROLES AND RESPONSIBILITIES FOR OCIO

A. **OCIO Chief Information Officer (CIO).**

1. Supports and promotes CP throughout the Agency;

2. Establishes the IT CP Program within the Agency;

3. Ensures that the positions and staff years are established within OCIO to develop, implement, and maintain the disaster recovery plan (DRP) and business resumption plans (BRPs) for each major system;

4. Designates a CP Coordinator in OCIO; and

5. Advises and recommends to senior management within OCIO, solutions regarding the DRP and BRPs based on USDA cyber security reviews.

B. **Associate CIOs.**

1. Ensures that OCIO develops the DRP and BRPs and that they are:

   a. Developed using the Departmental enterprise software or an approved equivalent for major systems identified;

   b. Ranked according to priority with the maximum system outage appropriate to the delivery of products and services; and

   c. Reviewed annually and executable in the event of a major incident or disaster.

2. Ensures that there is an alternate backup site with operating procedures and personnel designated to run specific applications at the site;

3. Ensures that DRP and BRP recovery solutions are closely coordinated and integrated with all emergency preparedness plans for major systems, interconnected systems, and business processes as part of the system development life cycle;

4. Ensures that recovery procedures are developed and implemented; and

5. Provides specialized training and certification opportunities to the CP Coordinator and appropriate general disaster training to all DRP and BRP team personnel.

C. **CP Coordinator.**

1. Identifies and coordinates with internal and external points of contact for each major system to characterize the ways that they depend on or support IT systems;

2. Ensures that data backup is implemented daily of critical files or tapes and stored offsite in the event of an incident or disaster;

3. Identifies disruption impacts and allowable outage times;

4. Identifies the maximum allowable time that a resource may be denied before it prevents or inhibits the performance of an essential function;

5. Develops and prioritizes recovery strategies that personnel will implement during CP activation and considers issues such as:

   a. Cost;

   b. Allowable outage time;

   c. Security; and

   d. Integration with larger Agency-level plans.

6. Coordinates with officials to establish contingency teams and team leaders for damage assessment and recovery teams; and

7. Reviews and updates plans annually.

D. **ISSPM.** Ensures collaboration among OCIO organizational entities and compliance of the CP requirements in this directive. In addition the ISSPM:

1. Ensures that the OCIO Network Security Operations Center and the FSIS Service Desk:

   a. Work in concert to ensure all maintenance adheres to the CP requirements in this directive; and

   b. Provide effective controls on tools, techniques, mechanisms, personnel used, and the integrity of the information and information systems.

2. Provides guidance and strategies to OCIO staff offices to assist them in establishing an Information Survivability Program; this includes CP actions, developing, testing, and implementing an executable DRP and BRP.

3. Reviews the Agency DRP and BRPs and tracks and monitors Agency compliance with these policies;

4. Tests the DRP and BRPs at least annually or when a significant change occurs to the system unless an approved waiver has been obtained from OCIO directly;

5. Provides an assessment report of the IT contingency plan to each FSIS Assistant Administrator;

6. Directs, coordinates, and performs oversight reviews in accordance with this directive;

7. Observes DRP and BRP testing in accordance with this directive;

8. Evaluates and recommends a specific course of action to remedy deficiencies found during review of plans or tests; and

9. Ensures that the OCIO CP Coordinator reviews and approves all DRP and BRPs.

VI. NIST SP 800-53, REVISION 4 REQUIREMENTS FOR OCIO

A. **CP.**

1. Develop and implement a CP that identifies essential mission and business functions and associated contingency requirements that address:

   a. Recovery objectives;

   b. Restoration priorities;

   c. Metrics;

   d. Roles and responsibilities;

   e. Activities associated with restoring information systems after a disruption or failure; and

   f. Maintaining essential mission and business functions despite an information system disruption, compromise, or failure.

2. Review and approve a CP through designated officials and distribute it to key contingency personnel;

3. Review and update, at least annually, the CP to address changes to the organization, information system, or environment of operation and problems encountered during CP implementation, execution, or testing;

4. Communicate contingency plan changes to CP team members, Data Center CP personnel, and officials responsible for related plans;

5. Coordinate CP activities with incident handling activities;

6. Coordinate and develop a CP with officials responsible for related plans;

7. Protect the contingency plan from unauthorized disclosure and modification; and

8. The categorization of “HIGH,” “MODERATE,” or “LOW” systems is defined in Federal Information Processing Standards (FIPS) Publication (PUB) 199, *Standards for Security Categorization of Federal Information and Information Systems*. The following applies to HIGH systems only:

a. Conduct capacity planning to ensure necessary capacity for information processing, telecommunications, and environmental support exists during crisis situations;

b. Plan for the resumption of all missions and business functions within the timeframe identified in the system CP, of CP activation;

c. Plan for the continuance of essential missions and business functions with little or no loss of operational continuity until full information system restoration at primary processing or storage sites; and

d. Identify critical information system assets supporting essential missions and business functions.

B. **Contingency Training.**

1. Ensure contingency personnel are trained upon assignment, in their roles and responsibilities and provide refresher training annually.

2. For HIGH systems only:

a. Incorporate simulated events into contingency training to facilitate effective responses by personnel in crisis situations; and

b. Employ automated mechanisms to provide a more thorough and realistic training environment.

C. **CP Testing.**

1. Test the CP annually using the CP testing plan to determine its effectiveness and readiness to execute the plan;

2. Review CP test results and initiate corrective actions if needed;

3. Coordinate CP testing with organizational elements responsible for related plans;

4. For HIGH systems only:

a. Test the CP at the alternate site to familiarize contingency personnel with the facility and available resources. Evaluate the site's capabilities to support contingency operations; and

b. Employ automated mechanisms to more thoroughly and effectively test the contingency plan.

D. **Alternate Storage Site.**

1. Identify an alternate storage site and initiate necessary agreements to permit the storage of information system backup information;

2. Ensure the frequency of information system backups and the transfer rates of backup information to the alternate storage site (if so designated) are consistent with recovery time objectives and recovery point objectives;

3. Identify an alternate storage site that is geographically separated from the primary storage site so as not to be susceptible to the same hazards;

4. Identify potential accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster and outline explicit mitigation actions; and

5. Configure the alternate storage site to facilitate timely and effective recovery operations. This requirement is only applicable to HIGH systems.

E. **Alternate Processing Site.**

1. Identify an alternate processing site and initiate necessary agreements to permit the resumption of information system operations for critical mission and business functions in accordance with the enterprise data center (EDC) service level agreement (SLA) if the primary processing capabilities are unavailable;

2. Ensure that equipment and supplies required to resume operations in accordance with the EDC SLA are either available at the alternate processing site or that contracts are in place to support delivery to the site within the time period defined in the CP or EDC SLA;

3. Identify an alternate processing site that is geographically separated from the primary processing site, not susceptible to the same hazards;

4. Identify potential accessibility problems to the alternate processing site in the event of an area-wide disruption or disaster and outline explicit mitigation actions;

5. Ensure alternate processing site agreements contain priority-of-service provisions in accordance with the EDC SLA; and

6. Fully configure the alternate processing site so that it is ready to be used as the operational site supporting the minimum required operational capability. This requirement is only applicable to HIGH systems.

F. **Telecommunications Services.**

1. Identify primary and alternate telecommunications services to support the information systems and initiate necessary agreements to permit the resumption of system operations for critical mission and business functions in accordance with the EDC SLA if the primary telecommunications capabilities are unavailable. In the event that the primary and alternate telecommunications services are provided by a common carrier, OCIO is to request a “Telecommunications Service Priority” for all telecommunications services used for national security emergency preparedness in accordance with USDA regulations;

2. Ensure primary and alternate telecommunications service agreements contain priority-of-service provisions in accordance with USDA regulations for availability requirements;

3. Obtain alternate telecommunications services that do not share a single point of failure with primary telecommunications services;

4. For HIGH systems only:

a. Obtain alternate telecommunications service providers that are sufficiently separated from primary service providers so as not to be susceptible to the same hazards;

b. Require primary and alternate telecommunications service providers to have adequate contingency plans in accordance with USDA regulations;

c. Review provider contingency plans to ensure that the plans meet organizational contingency requirements; and

d. Obtain evidence of contingency testing or training by providers at least annually.

G. **Information System Backup.**

1. Conduct backups of user-level information on a daily basis and system-level information on a weekly basis (including system state information) contained in the information system and protect the backup information at the storage location;

2. Test backup information on a quarterly basis to verify media reliability and information integrity;

3. Protect the confidentiality, integrity, and availability of backup information at storage locations;

4. Employ appropriate mechanisms (e.g., digital signatures, cryptographic hashes) to protect the integrity of information system backups;

5. For HIGH systems only:

   a. Selectively use backup information in the restoration of information system functions as part of CP testing;

   b. Store backup copies of the operating system and other critical information system software in a separate facility or in a fire-rated container that is not collocated with the operational software; and

   c. Transfer information system backup information to the alternate storage site as defined in the system CP.

H. **Information System Recovery and Reconstitution.**

1. Employ mechanisms with supporting procedures to allow the information system to be recovered and reconstituted to a known secure state after a disruption or failure;

2. Implement transaction recovery for transaction-based information systems such as database management and processing systems;

3. Protect backup and restoration hardware, firmware, and software such as router tables, compilers, and other security-relevant system software; and

4. Maintain the capability to restore information system components from configuration-controlled and integrity-protected disk images representing a secure, operational state for the components. This requirement is only applicable to HIGH systems.

VII. PENALTIES AND DISCIPLINARY ACTIONS FOR NON-COMPLIANCE

FSIS Directive 1300.7, *Managing Information Technology (IT) Resources*, sets forth the FSIS policies, procedures, and standards on employee responsibilities and conduct relative to the use of computers and telecommunications equipment. In addition, FSIS Directive 4735.3, *Employee Responsibilities and Conduct*, outlines the disciplinary action that FSIS may take when an employee fails to fulfill responsibilities or adhere to standards of conduct.

VIII. QUESTIONS

A. For questions regarding CP, contact the Agency ISSPM at: FSIS_Information_Security@fsis.usda.gov.

B. USDA Departmental directives are located at: http://www.ocio.usda.gov/policy-directives-records-forms.

C. FSIS Directives and Notices are located at: http://www.fsis.usda.gov/wps/portal/fsis/topics/regulations.

Assistant Administrator
Office of Policy and Program Development