INFORMATION PROCEDURE

Information Security – Contingency Planning Procedures	
EPA Classification No.: CIO 2150-P-06.2	CIO Approval Date: 9/11/2015
CIO Transmittal No.: 15-012	Review Date: 9/11/2018

Issued by the EPA Chief Information Officer,
Pursuant to Delegation 1-19, dated 07/07/2005

INFORMATION SECURITY – CONTINGENCY PLANNING PROCEDURES

1. PURPOSE

To implement the security control requirements for the Contingency Planning (CP) control family, as identified in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations.*

2. SCOPE AND APPLICABILITY

The procedures cover all EPA information and information systems to include information and information systems used, managed, or operated by a contractor, another agency, or other organization on behalf of the agency. The procedures apply to all EPA employees, contractors, and all other users of EPA information and information systems that support the operations and assets of the EPA.

3. AUDIENCE

The audience is all EPA employees, contractors, and all other users of EPA information and information systems that support the operations and assets of the EPA.

4. BACKGROUND

Based on federal requirements and mandates, the EPA is responsible for ensuring that all offices within the agency meet the minimum security requirements defined in the *Federal Information Processing Standards* (FIPS) Publication 200, *Minimum Security Requirements for Federal Information and Information Systems*. All EPA information systems shall meet the security requirements through the use of the security controls defined in the NIST SP 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*. This document addresses the procedures and standards set forth by the EPA, and complies with the family of Contingency Planning controls.

5. AUTHORITY

- E-Government Act of 2002, Public Law (PL) 107-347, Title III, Federal Information Security Management Act (FISMA) as amended
- Federal Information Security Modernization Act of 2014, PL 113-283, chapter 35 of title 44, United States Code (U.S.C.)
- Clinger-Cohen Act of 1996, PL104-106

- Privacy Act of 1974, PL 93-579, as amended
- Freedom of Information Act (FOIA), 5 U.S.C. § 552, as amended by PL 104-231, 110 Stat. 3048, Electronic Freedom of Information Act Amendments of 1996
- Paperwork Reduction Act of 1995 (as amended) (44 USC 3501-3519)
- Privacy Act of 1974 (as amended) (5 USC 552a)
- USA PATRIOT Act of 2001, Public Law 107-56
- Code of Federal Regulations, Part 5 Administrative Personnel, Subpart C—Employees Responsible for the Management or Use of Federal Computer Systems, Section 930.301 through 930.305 (5 C.F.R 930.301-305)
- Office of Management and Budget (OMB) Memorandum M-06-16, "Protection of Sensitive Agency Information," June 2006
- OMB Circular A-130, "Management of Federal Information Resources," Appendix III, "Security of Federal Automated Information Resources," November 2000
- Federal Information Processing Standards (FIPS) 199, Standards for Security Categorization of Federal Information and Information Systems, February 2004
- FIPS 200, Minimum Security Requirements for Federal Information and Information Systems, March 2006
- EPA Information Security Program Plan
- EPA Information Security Policy
- EPA Information Security – Roles and Responsibilities Procedures
- CIO Policy Framework and Numbering System

6. PROCEDURES

For the following section titles, the "CP" designator identified in each procedure represents the NIST-specified identifier for the Contingency Planning *control family* and the number represents the control *identifier,* as identified in NIST SP 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations.*

Abbreviations including acronyms are summarized in Appendix A.

CP-2 –Contingency Plan

For All Information Systems:

1) System Owners (SO), in coordination with Information Security Officers (ISO), Information Management Officers (IMO), Service Managers (SM), Information Owners (IO), and Information System Security Officers (ISSO), for EPA-operated systems shall; and Service Managers (SM), in coordination with IOs, for systems operated on behalf of the EPA, shall ensure service providers:
   a) Develop a contingency plan (CP) that satisfies the following EPA requirements:

i) Identifies essential missions and business functions and associated contingency requirements;

ii) Provides recovery objectives, restoration priorities and metrics;

iii) Addresses contingency roles and responsibilities, to include contact information for individuals with assigned responsibilities;

(1) The plan shall include a detailed contact list. At a minimum, the contact list shall include primary (office) and secondary (home/personal) telephone numbers. The contact list shall also describe the contact escalation process. The contact list shall be reviewed annually as part of the CP review. The contact list shall also be updated out-of-cycle to address changes to CP personnel.

iv) Addresses how essential missions and business functions will be maintained during an information system disruption, compromise, or failure;

v) Addresses the eventual, full information system restoration without deterioration of the security safeguards originally planned and implemented; and

vi) Is reviewed and approved by the Senior Information Official (SIO) as part of the authorization package.

2) SOs, in coordination with ISOs, IMOs, SMs, IOs, and ISSOs, for EPA-operated systems shall; and SMs, in coordination with IOs, for systems operated on behalf of the EPA, shall ensure service providers:

a) Maintain all aspects of the CP to include:

i) Updating the CP due to any changes to the system and the system environment that affect contingency and recovery operations. If changes have been made to the CP, they need to be communicated to all parties involved. Additionally, the updated CP shall be made available in hardcopy or softcopy, as applicable.

ii) Uploading the CP into the agency Information Security Repository. Subsequent updates to the plan will also be maintained and managed in the agency Information Security Repository.[1]

(1) ISOs are responsible for authorizing access to the agency Information Security Repository to personnel with a need to know.

iii) Coordinating contingency planning activities with incident handling activities in coordination with the Computer Security Incident Response Center (CSIRC);

iv) Protecting the CP from unauthorized disclosure and modification;

v) Reviewing the CP annually;

vi) Updating the CP to address changes to the organization, information system or operational environment as they occur;

vii) Updating the CP to address problems encountered during plan implementation, execution or testing; and

[1] *For systems processed under FedRAMP procedures by non-EPA entities, documentation will be housed at GSA and does not need to be duplicated in the agency Information Security Repository. However, any portions of controls for which EPA is responsible shall be documented in the agency Information Security Repository.*

viii) Communicating changes to the plan to personnel responsible for CP roles.

CP-2(1) Contingency Plan | Coordinate with Related Plans

For Moderate and High Information Systems:

1) SOs, in coordination with ISOs, IMOs, SMs, IOs and ISSOs, for EPA-operated systems shall; and SMs in coordination with IOs, for systems operated on behalf of the EPA, shall ensure service providers:
   a) Coordinate the development of the CP with those responsible for developing related plans (e.g., Business Continuity, Disaster Recovery Plans, Continuity of Operations Plans, Crisis Communications Plans, Critical Infrastructure Plans, Cyber Incident Response Plans and Occupant Emergency Plans).

CP-2(2) Contingency Plan | Capacity Planning

For High Information Systems:

1) SOs, in coordination with ISOs, IMOs, SMs, IOs and ISSOs, for EPA-operated systems shall; and SMs, in coordination with IOs, for systems operated on behalf of the EPA, shall ensure service providers:
   a) Conduct capacity planning to ensure necessary capacity for information processing, telecommunications and environmental support exists during contingency operations.

For FedRAMP[2] Moderate Information Systems:

1) SMs, in coordination with IOs, shall ensure service providers:
   a) Conduct capacity planning so that necessary capacity for information processing, telecommunications, and environmental support exists during contingency operations.

CP-2(3) Contingency Plan | Resume Essential Missions / Business Functions

For Moderate and High Information Systems:

1) SOs, in coordination with ISOs, IMOs, SMs, IOs and ISSOs, for EPA-operated systems shall; and SMs, in coordination with IOs, for systems operated on behalf of the EPA, shall ensure service providers:
   a) Define within the CP and Business Impact Analysis (BIA) the time period in which the system needs to be operational to support essential mission and business functions:
      i) Working directly with mission/business process owners, departmental staff, managers, and other stakeholders, estimate the following three downtime factors for consideration as a result of a disruptive event.
         (1) *Maximum Tolerable Downtime (MTD)* - The MTD represents the total amount of time leaders/managers are willing to accept for a mission/business process outage or disruption and includes all impact considerations.

[2] *The Federal Risk and Authorization Management Program (FedRAMP) is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services.*

(2) *Recovery Time Objective (RTO)* - RTO defines the maximum amount of time that a system resource can remain unavailable before there is an unacceptable impact on other system resources, supported mission/business functions, and the MTD.

(3) *Recovery Point Objective (RPO)* - The RPO represents the point in time, prior to a disruption or system outage, to which mission/business process data shall be recovered (given the most recent backup copy of the data) after an outage.

b) Plan for the resumption of operation to be within the defined time period in which the system needs to be operational after activating the CP; and

c) Ensure that information system assets supporting essential mission and business functions are identified and included in the organization-wide CP.

CP-2(4) Contingency Plan | Resume All Missions / Business Functions

For High Information Systems:

1) SOs, in coordination with ISOs, IMOs, SMs, IOs and ISSOs, for EPA-operated systems shall ; and SMs, in coordination with IOs, for systems operated on behalf of the EPA, shall ensure service providers:

   a) Develop plans to resume essential mission and business within the time period defined under CP-2(3) of activating the CP.

CP-2(5) Contingency Plan | Resume All Missions / Business Functions

For High Information Systems:

1) SOs, in coordination with ISOs, IMOs, SMs, IOs, and ISSOs, for EPA-operated systems shall; and SMs, in coordination with IOs, for systems operated on behalf of the EPA, shall ensure service providers:

   a) Develop plans to transfer essential mission and business functions with the objective of minimizing the loss of operational continuity until restoration to the primary processing site.

CP-2(6) Contingency Plan | Alternate Processing / Storage Site

Not selected as part of the control baseline.

CP-2(7) Contingency Plan | Coordinate with External Service Providers

Not selected as part of the control baseline.

CP-2(8) Contingency Plan, Identify Critical Assets

For Moderate and High Information Systems:

1) SOs, in coordination with ISOs, IMOs, SMs, IOs, and ISSOs, for EPA-operated systems shall; and SMs, in coordination with IOs, for systems operated on behalf of the EPA, shall ensure service providers:

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

Note: Contingency planning for information systems is part of an overall organizational program for achieving continuity of operations for critical mission/business operations. Contingency planning addresses both information system restoration and implementation of alternative mission/business processes when systems are compromised. A Contingency Plan is just one element of that program. NIST SP 800-34, Revision 1 and NIST SP 800-84 shall be used for more detailed procedural steps and guidance on contingency planning activities ranging across developing and documenting analyses, strategies and plans; training people in their responsibilities; conducting testing and exercises; using exercise results to make improvements to the plans through corrective actions; and maintaining plans, procedures and other documents.

CP-3 – Contingency Training

For All Information Systems:

1) SOs, in coordination with ISOs, IMOs, SMs, IOs, and ISSOs, for EPA-operated systems shall; and SMs, in coordination with IOs, for systems operated on behalf of the EPA, shall ensure service providers:
   a) Train all personnel in their contingency roles and responsibilities within 30-days of being assigned a role. All CP personnel shall receive annual refresher training or training when the information system undergoes a significant change.

CP-3(1) – Contingency Training | Simulated Events

For High Information Systems:

1) SOs, in coordination with ISOs, IMOs, SMs, IOs, and ISSOs, for EPA-operated systems shall; and SMs, in coordination with IOs, for systems operated on behalf of the EPA, shall ensure service providers:
   a) Include simulated events into contingency training to facilitate effective response by personnel in crises.

CP-3(2) – Contingency Training | Automated Training Environments

Not selected as part of the control baseline.

CP-4 – Contingency Plan Testing

For All Information Systems:

1) SOs, in coordination with ISOs, IMOs, SMs, IOs, and ISSOs, for EPA-operated systems shall; and SMs, in coordination with IOs, for systems operated on behalf of the EPA, shall ensure service providers:
   a) Maintain the effectiveness of the information system CP and readiness of the program office or region to execute the plan by:
      i) Developing a test plan and uploading it into the agency Information Security Repository;

ii) Performing annual testing using agency approved tests and exercises (checklist or table-top exercises);

iii) Testing the CP for all new systems prior to production deployment;

iv) Documenting in the agency Information Security Repository and reviewing CP test results; and

v) Documenting in the agency Information Security Repository and implementing corrective actions.

(1) Significant deficiencies shall be remediated prior to production deployment.

(2) Corrective actions shall be documented using the Plan of Action and Milestones (POA&M) in the agency Information Security Repository.

2) SOs shall ensure service providers:

a) Document and review the results of the test/exercise with the ISSO.

i) NIST SP 800-84 shall be used for guidelines on designing, developing, conducting, and evaluating test, training, and exercise (TT&E) events.

CP-4(1) – Contingency Plan Testing | Coordinate with Related Plans

For Moderate and High Information Systems:

1) SOs, in coordination with ISOs, IMOs, SMs, IOs, and ISSOs, for EPA-operated systems shall; and SMs, in coordination with IOs, for systems operated on behalf of the EPA, shall ensure service providers:

a) Coordinate CP testing appropriately with those responsible for related plans (e.g., Business Continuity Plan, Disaster Recovery Plan, Continuity of Operations Plan, Crisis Communications Plan, Critical Infrastructure Plan, Cyber Incident Response Plan, and Occupant Emergency Plan);

b) Include a full (simulation) recovery and reconstitution of the information system to a known state as a part of the CP testing.

CP-4(2) – Contingency Plan Testing | Alternate Processing Site

For High Information Systems:

1) SOs, in coordination with ISOs, IMOs, SMs, IOs, and ISSOs, for EPA-operated systems shall; and SMs, in coordination with IOs, for systems operated on behalf of the EPA, shall ensure service providers:

a) Perform CP testing at the alternate processing site to familiarize contingency personnel with the facility and available resources and to evaluate the site's capabilities to support contingency operations.

b) Include a full (interrupted simulation) recovery and reconstitution of the information system to a known state as part of CP testing.

CP-4(3) – Contingency Plan Testing | Automated Testing

Not selected as part of the control baseline.

CP-4(4) – Contingency Plan Testing | Full Recovery / Reconstitution

Not selected as part of the control baseline.

CP-5 Contingency Plan Update

Incorporated into CP-2.

CP-6 – Alternate Storage Sites

For Moderate and High Information Systems:

1) SOs, in coordination with ISOs, IMOs, SMs, IOs, and ISSOs, for EPA-operated systems shall; and SMs, in coordination with IOs, for systems operated on behalf of the EPA, shall ensure service providers:
   a) Establish an alternate storage site for the storage and recovery of the information system's backup information with the following requirements:
      i) Service and Support Agreements shall be in place with the alternate storage site and uploaded into the agency Information Security Repository.
         (1) The agreements shall detail service levels to be provided.
         (2) The agreements shall include confidentiality requirements per federal guidelines.
      ii) The CP for the information system shall include the following:
         (1) Alternate storage site location: street address, city/town, state, zip code, and site contact information.
         (2) Terms of use for the alternate storage site.
         (3) Hazards or risks associated with the alternate storage site and mitigations to address them.
         (4) Mitigation actions to address potential problems associated with physically accessing the alternate storage site.
      iii) A log of all information system backup data stored at, or retrieved from, the alternate storage facility shall be maintained.

CP-6(1) – Alternate Storage Sites | Separation from Primary Site

For Moderate and High Information Systems:

1) SOs, in coordination with ISOs, IMOs, SMs, IOs, and ISSOs, for EPA-operated systems shall; and SMs, in coordination with IOs, for systems operated on behalf of the EPA, shall ensure service providers:
   a) Establish an alternate storage site for the storage and recovery of the information system's backup information with the following requirements:

i) Establish the site in a location that is separate from the primary facility to ensure that the risk of a disruption affecting both the primary and alternate site is low or otherwise is at an acceptable level, based on an assessment of risk.[3]

CP-6 (2) – Alternate Storage Sites | Recovery Time / Point Objectives

For High Information Systems:

1) SOs, in coordination with ISOs, IMOs, SMs, IOs and ISSOs, for EPA-operated systems shall; and SMs, in coordination with IOs, for systems operated on behalf of the EPA, shall ensure service providers:
   a) Configure the alternate storage site to facilitate recovery operations in accordance with RTOs and RPOs established for the information system in the BIA and CP.

CP-6(3) – Alternate Storage Sites | Accessibility

For Moderate and High Information Systems:

1) SOs, in coordination with ISOs, IMOs, SMs, IOs and ISSOs, for EPA-operated systems shall; and SMs, in coordination with IOs, for systems operated on behalf of the EPA, shall ensure service providers:
   a) Establish an alternate storage site for the storage and recovery of the information system's backup information where potential problems that occur accessing the alternate storage site during an area-wide disruption or disaster shall be identified and explicit mitigation actions shall be outlined.

      Note: Explicit mitigation actions include, for example, duplicating backup information at another alternate storage site if access to the first alternate site is hindered; or, if electronic accessibility to the alternate site is disrupted, planning for physical access to retrieve backup information.

CP-7 – Alternate Processing Site

For Moderate and High Information Systems:

1) SOs, in coordination with ISOs, IMOs, SMs, IOs, and ISSOs, for EPA-operated systems shall; and SMs, in coordination with IOs, for systems operated on behalf of the EPA, shall ensure service providers:
   a) Establish an alternate processing site for the information system to permit the transfer and resumption of information system operations necessary to support essential missions and business functions within the RTOs and RPOs established in the CP and BIA, when the primary processing capabilities are unavailable;
      i) Alternate processing sites are geographically distinct from the primary processing sites.
   b) Ensure the equipment and supplies required to transfer and resume operations are available at the alternate processing site or contracts are in place to support delivery to the site within the organization-defined time period for transfer/resumption; and

[3] *Refer to the latest version of the EPA Information Security – Risk Assessment Procedures for updated guidance.*

c) Ensure the alternate processing site provides information security safeguards equivalent to that of the primary site.

CP-7(1) – Alternate Processing Site | Separation from Primary Site

For Moderate and High Information Systems:

1) SOs, in coordination with ISOs, IMOs, SMs, IOs, and ISSOs, for EPA-operated systems shall; and SMs, in coordination with IOs, for systems operated on behalf of the EPA, shall ensure service providers:
   a) Identify an alternate processing site that is separated from the primary processing site to reduce susceptibility to the same threats and hazards.
      i) The risk assessment process shall be used to determine area, accessibility requirements, security requirements, environmental conditions, and cost factors necessary for selecting a safe and practical off-site facility.

CP-7(2) – Alternate Processing Site | Accessibility

For Moderate and High Information Systems:

1) SOs, in coordination with ISOs, IMOs, SMs, IOs, and ISSOs, for EPA-operated systems shall; and SMs, in coordination with IOs, for systems operated on behalf of the EPA, shall ensure service providers:
   a) Identify potential accessibility problems to the alternate processing site in the event of an area-wide disruption or disaster that is broad in geographic scope (e.g., hurricane, regional power outage).
   b) Outline and document explicit mitigation actions within the CP.

CP-7(3) – Alternate Processing Site | Priority of Service

For Moderate and High Information Systems:

1) SOs, in coordination with ISOs, IMOs, SMs, IOs, and ISSOs, for EPA-operated systems shall; and SMs, in coordination with IOs, for systems operated on behalf of the EPA, shall ensure service providers:
   a) Develop alternate processing site agreements that contain priority-of-service provisions in accordance with organizational availability requirements including defined RTO and RPO objectives as defined in the BIA and CP.
      i) Arrangements shall be made to ensure the necessary equipment and supplies required to resume operations identified as priorities in the CP are available in time to support the organization-defined time period for resumption.
      ii) Service and Support Agreements shall be in place with the alternate processing site.
         (1) The alternate processing site shall provide a Service Level Agreement (SLA) that contains priority-of-service provisions in accordance with the information system's requirements in the event of a disruption or disaster.
         (2) This may be in the form of a priority-of-service provision or through a provider with a sufficient network of facilities to ensure available capacity.

(3) The alternate processing site agreement shall include testing time that is sufficient to test the longest RTO of the critical systems.

(4) The agreements shall satisfy confidentiality requirements per federal guidelines.

CP-7(4) – Alternate Processing Site | Preparation for Use

For High Information Systems:

1) SOs, in coordination with ISOs, IMOs, SMs, IOs and ISSOs, for EPA-operated systems shall; and SMs, in coordination with IOs, for systems operated on behalf of the EPA, shall ensure service providers:
   a) Configure the alternate processing site to support essential missions and business functions and to be ready to function as the operational site.

CP-7(5) – Alternate Processing Site | Equivalent Information Security Safeguards

Incorporated into CP-7.

CP-7(6) – Alternate Processing Site | Inability to Return to Primary Site

Not selected as part of the control baseline.

CP-8 – Telecommunications Services

For Moderate and High Information Systems:

1) SOs, in coordination with ISOs, IMOs, SMs, IOs, and ISSOs, for EPA-operated systems shall; and SMs, in coordination with IOs, for systems operated on behalf of the EPA, shall ensure service providers:
   a) Establish alternate telecommunications services that satisfy the following requirements:
      i) Telecommunications restoration plans and related operational procedures shall provide adequate capabilities for channels of communication between the EPA and other organizations involved in the coordination and support of the CP. The CP shall document the following:
         (1) The timeframe for the alternate telecommunications services to begin providing telecommunications capabilities when the primary telecommunications capabilities are unavailable.
         (2) Channels for necessary communications within the EPA and between EPA and other organizations involved.
         (3) The names of the primary and the alternate telecommunications services providers and points of contact.
         (4) The agreements with the primary and alternate telecommunications service providers.

CP-8(1) – Telecommunications Services | Priority of Service Provisions

For Moderate and High Information Systems:

1) SOs, in coordination with ISOs, IMOs, SMs, IOs and ISSOs, for EPA-operated systems shall; and SMs, in coordination with IOs, for systems operated on behalf of the EPA, shall ensure service providers:
   a) Establish alternate telecommunications services that satisfy the following requirements:
      i) The necessary telecommunications agreements shall be developed with both primary and alternate service providers.
         (1) Primary and alternate telecommunications service agreements shall contain priority-of-service provisions in accordance with the information system's availability requirements.
         (2) The terms of the agreement shall permit the resumption of information system operations for essential missions and business functions within the time period required for the information system and related applications and functions requiring telecommunications support.
         (3) Agreements with the primary and alternate telecommunications providers shall each include an SLA and a notification process should the SLA not be met.
         (4) Telecommunications Service Priority (TSP) shall be requested for all telecommunications services required and used for National Security Emergency Preparedness (NSEP) in the event that the primary and/or alternate telecommunications services are provided by a common carrier.

         Note: The TSP program, operated under the auspices of DHS, prioritizes requests for restoring telecommunications services or establishing new services during emergencies or events of national significance.

CP-8(2) – Telecommunications Services | Single Points of Failure

For Moderate and High Information Systems:

1) SOs, in coordination with ISOs, IMOs, SMs, IOs, and ISSOs, for EPA-operated systems shall; and SMs, in coordination with IOs, for systems operated on behalf of the EPA, shall ensure service providers:
   a) Obtain alternate telecommunications services with consideration for reducing the likelihood of sharing a single point of failure with primary telecommunications services.

CP-8(3) – Telecommunications Services | Separation of Primary / Alternate Providers

For High Information Systems:

1) SOs, in coordination with ISOs, IMOs, SMs, IOs, and ISSOs, for EPA-operated systems shall; and SMs, in coordination with IOs, for systems operated on behalf of the EPA, shall ensure service providers:
   a) Select diverse alternate telecommunications service providers to ensure separation from primary service providers so as not to be susceptible to the same hazards or risks.

CP-8(4) – Telecommunications Services | Provider Contingency Plan

For High Information Systems:

1) SOs, in coordination with ISOs, IMOs, SMs, IOs, and ISSOs, for EPA-operated systems shall; and SMs, in coordination with IOs, for systems operated on behalf of the EPA, shall ensure service providers:
   a) Have current CPs for primary and alternate telecommunications service providers.
   b) Have telecommunications providers' CPs that are consistent with EPA's CP requirements.
   c) Ensure primary and alternate telecommunication service providers provide contingency testing and training evidence on an annual basis.

CP-8(5) – Telecommunications Services | Alternate Telecommunications Service Testing

Not selected as part of the control baseline.

CP-9 – Information System Backup

For All Information Systems:

1) SOs, in coordination with ISOs, IMOs, SMs, IOs, and ISSOs, for EPA-operated systems shall; and SMs, in coordination with IOs, for systems operated on behalf of the EPA, shall ensure service providers:
   a) Backup data residing on information systems including, but not limited to, the following:
      i) Backups of user-level information contained in the information system shall be conducted at least weekly.
      ii) Backups of system-level information contained in the information system shall be conducted at least weekly. System-level information includes, for example, system-state information, operating system and application software, and licenses.
      iii) Backups of information system documentation including security-related documentation shall be conducted at least weekly.
      iv) The frequency of information system backups shall be consistent with the information systems' RTOs and RPOs.
      v) The confidentiality and integrity of the system backup information shall be protected at the storage location.
         (1) Sensitive information such as the information system's assessment of risk and similar information content shall determine the use of encryption or other measures for protecting backup information.

         Note: Digital signatures and cryptographic hashes are examples of mechanisms that can be employed by organizations to protect the integrity of information system backups.
      vi) Information systems that include backups of sensitive personally identifiable information (SPII) shall use an encryption module that is certified to meet Federal Information Processing Standards (FIPS) 140-2, as amended, and complies with the controls outlined in the latest version of the *EPA Information Security – Systems* and

Communications Protection Procedures and *EPA Information Security – Privacy Procedures* documents.

vii) Procedures for backing up and restoring the information system shall be documented and included in, or as attachments to, the information system CP.

viii) Backup and restoration procedures shall address the following:

(1) A routine schedule shall be established for backing up user-level and system-level information.

(2) All backup media shall include markings that address the contents of the media; date created, and sequence number, if multiple media were used. Refer to the *EPA Information Security – Media Protection Procedures* document for requirements on media protection.

(3) The priorities and sequencing of restoration shall be established.

ix) Backup information shall be retained as follows:

(1) Backups shall be retained for at least 90 days or in accordance with records retention requirements.

CP-9(1) – Information System Backup | Testing for Reliability / Integrity

For Moderate and High Information Systems:

1) SOs, in coordination with ISOs, IMOs, SMs, IOs, and ISSOs, for EPA-operated systems shall; and SMs, in coordination with IOs, for systems operated on behalf of the EPA, shall ensure service providers:

a) Test backup information at least annually for media reliability and information integrity.

i) Testing may be conducted on random files versus entire system restoration.

ii) Test results shall be documented and shall include findings for media reliability and information integrity.

iii) Virus scans shall be performed on backups each month unless real-time scanning is performed on the information system.

(1) Full system restoration shall be tested when new backup technologies are initially implemented.

(2) As part of CP testing, a sample of backup information shall be used to restore selected information system functions.

(a) This may be a full restoration or a restoration of selected files.

(3) Backup copies of the operating system and other critical information system software, as well as copies of the information system inventory (e.g., hardware, software, and firmware components), shall be stored in a separate secure facility or in a fire-rated container that is not collocated with the operational system.

(a) At least one set of backups shall be rotated off-site on a schedule that is in accordance with the information system's availability requirements and determination of acceptable risk.

CP-9(2) – Information System Backup | Test Restoration using Sampling

For High Information Systems:

1) SOs, in coordination with ISOs, IMOs, SMs, IOs, and ISSOs, for EPA-operated systems shall; and SMs, in coordination with IOs, for systems operated on behalf of the EPA, shall ensure service providers:
   a) Use sample backup information during the restoration of selected information systems functions as part of CP testing.

CP-9(3) – Information System Backup | Separate Storage for Critical Information

For High Information Systems:

1) SOs, in coordination with ISOs, IMOs, SMs, IOs, and ISSOs, for EPA-operated systems shall; and SMs, in coordination with IOs, for systems operated on behalf of the EPA, shall ensure service providers:
   a) Store backup copies of the operating system and other critical information system software, as well as copies of the information system inventory in a separate facility or in a fire-rated container that is not collocated with the operational system. Information system inventory includes operating systems, cryptographic key management systems, and intrusion detection/prevention systems. Security-related information includes organizational inventories of hardware, software, and firmware components.

For FedRAMP Moderate Information Systems:

1) SMs, in coordination with IOs, shall ensure service providers:
   a) Store backup copies of the operating system and other critical information system software, as well as copies of the information system inventory appropriately in a separate facility or in a fire-rated container that is not collocated with the operational system. Information system inventory includes operating systems, cryptographic key management systems, and intrusion detection/prevention systems. Security-related information includes organizational inventories of hardware, software, and firmware components.

CP-9(4) – Information System Backup | Protection From Unauthorized Modification

Incorporated into CP-9.

CP-9(5) – Information System Backup | Transfer to Alternate Storage Site

For High Information Systems:

1) SOs, in coordination with ISOs, IMOs, SMs, IOs, and ISSOs, for EPA-operated systems shall; and SMs, in coordination with IOs, for systems operated on behalf of the EPA, shall ensure service providers:
   a) Transfer information system backup information to the alternate storage site on a monthly basis. The information system backup information will be available to ensure compliance with system specific recovery time and recovery point objectives.

CP-9(6) – Information System Backup | Redundant Secondary System

Not selected as part of the control baseline.

CP-9(7) – Information System Backup | Dual Authorization

Not selected as part of the control baseline.

CP-10 – Information System Recovery and Reconstitution

For All Information Systems:

1) SOs, in coordination with ISOs, IMOs, SMs, IOs, and ISSOs, for EPA-operated systems shall; and SMs, in coordination with IOs, for systems operated on behalf of the EPA, shall ensure service providers:
   a) Ensure the information system can be recovered and reconstituted to a known state after a disruption, compromise, or failure.[4]

      Note: System recovery is executing information system CP activities to restore essential missions and business functions. System reconstitution takes place following recovery and includes activities for returning the information system to its original functional state before CP activation.

      i) Recovery and reconstitution mechanisms and procedures shall be documented in the CP.

         Note: Refer to Section 9 for recovery and reconstitution definitions.

   b) Ensure the information system's recovery and reconstitution procedures follow the priorities identified in the information system's BIA and CP.[5]

      i) Recovery and reconstitution procedures shall be based on organizational priorities, established RPO, RTO, and reconstitution objectives, and appropriate metrics.

      ii) Reconstitution shall include the deactivation of any interim information system capability that may have been needed during recovery operations.

      iii) Reconstitution shall include an assessment of the fully restored information system capability, a potential system reauthorization and the necessary activities to prepare the system against another disruption, compromise, or failure.

         Note: Recovery and reconstitution capabilities employed by the organization can be combination of automated mechanisms and manual procedures.

         (1) Personnel responsible for the information system shall ensure the following during disruptions and during recovery and reconstitution:

[4] *Refer to the latest version of the EPA Information Security – Security Assessment and Authorization Procedures for updated guidance.*

[5] *NIST SP 800-34, Revision 1 and NIST SP 800-84 shall be used for more detailed procedural steps and guidance on contingency planning activities ranging across developing and documenting analyses, strategies, and plans; training people in their responsibilities; conducting testing and exercises; using exercise results to make improvements to the plans through corrective actions; and maintaining plans, procedures, and other documents.*

iv) Essential operations shall be continued.

v) Vital records shall be protected in accordance with EPA's Vital Records Program.

vi) Essential equipment and assets shall be protected.

CP-10(1) – Information System Recovery and Reconstitution | Contingency Plan Testing

Incorporated into CP-4.

CP-10(2) – Information System Recovery and Reconstitution, Transaction Recovery

For Moderate and High Information Systems:

1) SOs, in coordination with ISOs, IMOs, SMs, IOs, and ISSOs, for EPA-operated systems shall; and SMs, in coordination with IOs, for systems operated on behalf of the EPA, shall ensure service providers:
   a) Configure the information system to implement transaction recovery for systems that are transaction-based.

      Note: Database management systems and transaction processing systems are examples of information systems that are transaction-based. Transaction rollback and transaction journaling are examples of mechanisms supporting transaction recovery.
   b) Provide compensating security controls for circumstances that can inhibit recovery and reconstitution to a known state.
      i) At a minimum, compensating controls for corrupt or inaccessible backups and loss of critical personnel or hardware should be established.

CP-10(3) – Information System Recovery and Reconstitution | Contingency Plan Testing

Addressed through tailoring procedures.

CP-10(4) – Information System Recovery and Reconstitution | Restore Within Time Period

For High Information Systems:

1) SOs, in coordination with ISOs, IMOs, SMs, IOs and ISSOs, for EPA-operated systems shall; and SMs, in coordination with IOs, for systems operated on behalf of the EPA, shall ensure service providers:
   a) Have the capability to reimage information system components immediately from configuration-controlled and integrity-protected disk images representing a secure, operational state for the components. The restoration time-period of the information system shall be consistent with the information systems' RTOs and RPOs.

CP-10(5) – Information System Recovery and Reconstitution | Failover Capability

Incorporated into SI-13.

CP-10(6) – Information System Recovery and Reconstitution | Component Protection

Not selected as part of the control baseline.

CP-11 – Alternate Communications Protocols

Not selected as part of the control baseline.

CP-12 – Safe Mode

Not selected as part of the control baseline.

CP-13 – Alternate Security Mechanisms

Not selected as part of the control baseline.

7. RELATED DOCUMENTS

- NIST Special Publications, 800 series

8. ROLES AND RESPONSIBILITIES

Chief Information Officer (CIO)

1) The CIO has the following responsibilities with respect to contingency planning:
   a) Accept risks to the organization related to contingency planning.
   b) Ensure the organization has necessary resources to plan and enact CPs for information systems within their organization.
   c) Negotiate contingency planning requirements with other CIOs in support of their information systems.

Senior Agency Information Security Officer (SAISO)

1) The SAISO has the following responsibilities with respect to contingency planning:
   a) Develop, maintain and distribute agency-wide information security policies, procedures and control techniques to provide direction for implementing the requirements of the information security program.
   b) Provide oversight to the agency's contingency planning and testing processes.
   c) Notify SIO, IMO, ISO, SO and ISSO of compliance issues.

Information Owner (IO)

1) The IO has the following responsibility with respect to contingency planning:
   a) Assist the CIO in contingency planning responsibilities.

Information Management Officers (IMO)

1) The IMO has the following responsibilities with respect to contingency planning:
   a) Develop and issue local information security procedures, control techniques, and processes for local systems and operations as necessary to support and implement the CP requirements.

b) Ensure all employees within their organizations designated as having significant information security responsibilities, with respect to the CP, complete role based information security training as defined under the EPA Information Security Program.

Information Security Officer (ISO)

1) The ISO has the following responsibilities with respect to contingency planning:
   a) Provide guidance on CP roles and responsibilities to ISSOs, system owners, system administrators, and others with significant security responsibilities.
   b) Ensure personnel with CP roles and responsibilities complete role based information security training and credentialing, as defined under the EPA Information Security Program.
   c) Review the agency Information Security Repository periodically and ensure all system information security information, such as the CP and related plans of actions and milestones are current.
   d) Coordinate with CSIRC as a first responder for incidents affecting the assigned organization's information, systems, or personnel.
   e) Provide expert advice in developing and updating enterprise and local information security documents to include policy, procedures, standards, and guides.

Information System Security Officer (ISSO)

1) The ISSO has the following responsibilities with respect to contingency planning:
   a) Assist the CIO, IO and SO in understanding their responsibilities for contingency planning.
   b) Assist in the coordination and oversight of information system contingency planning.
   c) Support and assist the SO in their contingency planning responsibilities.

System Owner (SO)

1) The SO has the following responsibilities with respect to contingency planning:
   a) Ensure that the CP is developed, reviewed, and updated annually.
   b) Communicate changes to appropriate elements responsible for related plans.
   c) Conduct capacity planning so that necessary capacity for information processing, telecommunications and environmental support exists during crises.
   d) Establish an annual CP testing cycle.
   e) Ensure the CP is developed, budgeted for, and implemented in accordance with requirements for the system.
   f) Ensure all personnel with contingency roles and responsibilities receive both initial and refresher training.
   g) Ensure the CP is properly implemented when a disruption, compromise, or failure occurs.
   h) Ensure that an After Action Report, including recommendations for corrective actions, is produced and acted upon, whenever there has been a disruption or failure.

i) Ensure the alternate storage site, alternate processing site, and telecommunications services providers meet all requirements in these procedures and that appropriate agreements are in place.

j) Ensure the information system's backup uses encryption that meets FIPS 140-2 standards, and complies with the Information Security – Systems and Communications Protection Procedures if the information system includes PII.

Service Manager (SM)

1) The SM has the following responsibilities with respect to contingency planning:

a) Ensure the CP is developed, reviewed, and updated annually.

b) Communicate changes to appropriate elements responsible for related plans.

c) Conduct capacity planning so that necessary capacity for information processing, telecommunications and environmental support exists during crises.

d) Establish a three-year CP testing cycle.

e) Ensure the CP is developed, budgeted for, and implemented in accordance with requirements for the system.

f) Ensure all personnel with contingency roles and responsibilities receive both initial and refresher training.

g) Ensure the CP is properly implemented when a disruption, compromise, or failure occurs.

h) Ensure that an After Action Report, including recommendations for corrective actions, is produced and acted upon, whenever there has been a disruption or failure.

i) Ensure the alternate storage site, alternate processing site, and telecommunications services providers meet all requirements in these procedures and that appropriate agreements are in place.

j) Ensure the information system's backup uses encryption that meets FIPS 140-2 standards and complies with the Information Security – Systems and Communications Protection Procedures if the information system includes PII.

9. DEFINITIONS

- *After Action Report* – a document containing findings and recommendations from an exercise, test, or analysis of an actual disruption or failure and the response to and recovery from it.
- *Alternate Processing Site* – a facility that is able to support system operations by restoring critical systems to an acceptable level as defined in the Disaster Recovery Plan. Sites are referred to as cold, warm, hot, mobile, or mirrored.
- *Alternate Storage Site* – a secure location, remote from the primary location, at which backup hardware, software, data files, documents, equipment, or supplies are stored.
- *Availability* – ensuring timely and reliable access to and use of information.
- *Business Continuity Plan (BCP)* – the documentation of a predetermined set of instructions or procedures that describe how an organization's business functions will be sustained during and after a significant disruption.

- *Business Impact Analysis (BIA)* – an analysis of an information system's requirements, processes, and interdependencies used to characterize system contingency requirements and priorities in the event of a significant disruption.
- *Confidentiality* – preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information.
- *Contingency Training* – the dynamic development and implementation of a coordinated training strategy for contingency personnel on information systems or applications' CPs.
- *Continuity of Support Plan/IT Contingency Plan (CP)* – 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 disaster. From the standpoint of information systems, a CP is the documentation of a predetermined set of instructions or procedures that describes how to sustain operations in the event of a significant disruption.
- *Continuity of Operations Plan (COOP)* – a predetermined set of instructions or procedures that describe how an organization's essential functions will be sustained for up to 30 days as a result of a disaster event before returning to normal operations.
- *Disaster Recovery Plan (DRP)* – a written plan for processing critical applications in the event of a major hardware or software failure or destruction of facilities.
- *Incident* – an occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system, or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.
- *Incident Response Plan* – the documentation of a predetermined set of instructions or procedures to detect, respond to, and limit consequences of a malicious cyber-attack against an organization's IT systems.
- *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.
- *Information System* – a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.
- *Integrity* – guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.
- *Maximum Tolerable Downtime (MTD)* – the total amount of time the System Owner/Authorizing Official is willing to accept for a mission/business process outage or disruption and includes all impact considerations.
- *Media* – physical devices or writing surfaces including, but not limited to, magnetic tapes, optical disks, magnetic disks and Large-Scale Integration (LSI) memory chips, printouts (but not including display media) onto which information is recorded, stored or printed within an information system. Digital media include diskettes, tapes, removable hard drives, flash/thumb drives, compact disks, and digital video disks. Examples of non-digital media are paper or microfilm. This term also applies to portable and mobile computing

and communications devices with information storage capability (e.g., notebook computers, personal digital assistants, cellular telephones).

- *National Security Emergency Preparedness (NSEP) Telecommunications* Services – telecommunication services which are used to maintain a state of readiness or to respond to and manage any event or crisis (local, national or international), which causes or could cause injury or harm to the population, damage to or loss of property, or degrades or threatens the NSEP posture of the United States. These services fall into two specific categories, Emergency NSEP and Essential NSEP, and are assigned priority levels pursuant to Section 9 of 47 C.F.R. Pt. 64, App. A.
- *Organization* – a federal agency or, as appropriate, any of its operational elements.
- *Reconstitution* – takes place following recovery and includes activities for returning the information system to its original functional state before CP activation.
- *Recovery* – executing information system CP activities to restore essential missions and business functions.
- *Recovery Point Objective (RPO)* – the point in time, prior to a disruption or system outage, to which mission/business process data can be recovered (given the most recent backup copy of the data) after an outage.
- *Recovery Time Objective (RTO)* – the maximum amount of time that a system resource can remain unavailable before there is an unacceptable impact on other system resources, supported mission/business functions, and the MTD.
- *Risk* – the level of impact on organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals resulting from the operation of an information system given the potential impact of a threat and the likelihood of that threat occurring.
- *Service Level Agreement (SLA)* – part of a service contract in which a certain level of service is agreed upon. An SLA is not a type of service contract, but rather a part of a service contract. A service contract can contain zero, one or more SLAs. A contract containing SLAs is usually referred to as a performance contract.
- *Signature* (of an individual) – a mark or sign made by an individual to signify knowledge, approval, acceptance, or obligation (can be accomplished manually, sometimes referred to as a “wet signature,” or electronically).
- *Telecommunications Service Priority (TSP)* – a program that provides NSEP users priority authorization in restoring or establishing telecommunications services that are vital to coordinating and responding to crises. A telecommunications service with a TSP assignment is assured of receiving full attention by the service vendor before a non-TSP service.
- *User* – individual or (system) process authorized to access an information system.
- *Vital Records* – also termed Essential Records -- Records essential to the continued functioning or reconstitution of an organization during and after an emergency and also those records essential to protecting the legal and financial rights of that organization and of the individuals directly affected by its activities.

- *Written* (or in writing) – to officially document the action or decision, either manually or electronically, and includes a signature.

10. WAIVERS

Waivers may be requested from the CIO by submitting a justification based on:

- Substantive business case need(s)
- Demonstration of, or a proposal for, establishment of adequate compensating controls that provide a suitable alternative to the mandated protection

The CIO may grant a waiver for sufficient reasons exercising judgment in the best interests of the agency.

The SAISO and Director, OTOP shall coordinate to maintain a central repository of all waivers.

11. RELATED POLICY, PROCEDURES, STANDARDS AND GUIDELINES

Related policy and procedures are available on OEI's Policy Resources website.

http://intranet.epa.gov/oei/imitpolicy/policies.htm

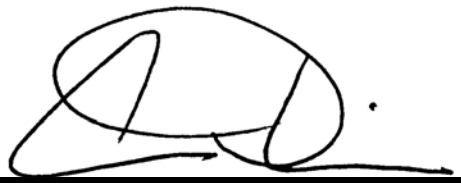
Related standards and guidelines are available on OEI's website.

12. MATERIAL SUPERSEDED

- EPA Information Security – Interim Contingency Planning Procedures, Version 3.2, July 13, 2012

13. ADDITIONAL INFORMATION

N/A



Ann Dunkin
Chief Information Officer
U.S. Environmental Protection Agency

APPENDIX A: ACRONYMS & ABBREVIATIONS

BIA	Business Impact Analysis
BCP	Business Continuity Plan
CFR	Code of Federal Regulations
CIO	Chief Information Officer
COOP	Continuity of Operations Plan
CP	Contingency Plan
CSIRC	Computer Security Incident Response Center
DRP	Disaster Recovery Plan
EPA	Environmental Protection Agency
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
FOIA	Freedom of Information Act
IMO	Information Management Officers
IO	Information Owner
ISO	Information Security Officer
ISSO	Information System Security Officer
LSI	Large Scale Integration
MTD	Maximum Tolerable Downtime
NIST	National Institute of Standards and Technology
NSEP	National Security Emergency Preparedness
OMB	Office of Management and Budget
PII	Personally Identifiable Information
PL	Public Law
POA&M	Plan of Action and Milestones
RPO	Recovery Point Objective
RTO	Recovery Time Objective
SAISO	Senior Agency Information Security Officer
SIO	Senior Information Official
SLA	Service Level Agreement
SM	Service Manager
SO	System Owner
SP	Special Publication
SPII	Sensitive Personally Identifiable Information
SSP	System Security Plan
TSP	Telecommunications Service Priority
TT&E	Test, Training, and Exercise
USC	United States Code