EPA INFORMATION PROCEDURES

OFFICE OF ENVIRONMENTAL INFORMATION

EPA Classification No.:	CIO-2150.3-P-06.1	CIO Approval Date:	08/06/2012
CIO Transmittal No.:	12-003	Review Date:	08/06/2015

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

INFORMATION SECURITY – INTERIM CONTINGENCY PLANNING PROCEDURES

V3.2

JULY 13, 2012

1. PURPOSE

The purpose of this procedure is to facilitate the implementation of Environmental Protection Agency (EPA) security control requirements for the Contingency Planning control family, as identified in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Revision 3 *Recommended Security Controls for Federal Information Systems and Organizations.*

2. SCOPE AND APPLICABILITY

These 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.

These procedures apply to all EPA employees, contractors, and all other users of EPA information and information systems that support the operations and assets of EPA.

3. AUDIENCE

These procedures apply to all EPA employees, contractors, and all other users of EPA information and information systems that support the operations and assets of 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 must meet the security requirements through the use of the security controls defined in the NIST SP 800-53, Revision 3 *Recommended Security Controls for Federal Information Systems and Organizations*. This chapter addresses the procedures and standards set forth by EPA, and in compliance with, the contingency planning family of controls found in NIST SP 800-53, Revision 3.

5. AUTHORITY

- E-Government Act of 2002, Public Law 107-347, Title III, *Federal Information Security Management Act (FISMA)* as amended
- Clinger-Cohen Act of 1996, Public Law 104-106
- Privacy Act of 1974, Public Law 93-579, as amended
- Freedom of Information Act (FOIA), 5 U.S.C. § 552, as amended by Public Law 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

6. PROCEDURES

CP-2 –Contingency Plan

a. NIST SP 800-34, Revision 1 and NIST SP 800-84 must 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.

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.

b. A contingency planning program must be developed as follows:

i. Designate, in writing, a knowledgeable individual as Contingency Planning

Coordinator for the system or organization for multiple systems, as appropriate to the system criticality, organizational resources, and geographic distribution of the resources.

ii. Conduct a Business Impact Analysis (BIA) in order to focus the scope of the Contingency Plan.
   - The BIA must be included as an appendix to the Contingency Plan.

iii. Address eventual, full information system restoration without deterioration of the security measures originally planned and implemented.
   - Identify preventative controls, both in place and planned.
   - Develop recovery strategies, both in place and planned, and determine associated costs.
     - Recovery strategies include backups, alternate sites and associated resources, and replacement of equipment at the primary processing (i.e., operational) site.
     - Refer to *Information Security – Security Planning* for requirements on in place and planned controls.

iv. Develop the Contingency Plan document.

v. Create plans for training, testing, and exercising the contingency plans.

vi. Plan for maintenance of all elements of the contingency planning program.

c. The BIA must incorporate the following:

i. Identify essential missions and business functions and associated contingency requirements.

ii. Identify critical resources for each business process.

iii. Determine the impacts of disruptions, damages to resources, and the maximum tolerable downtime (MTD) for each resource in each business process, should an adverse event occur.

iv. Develop recovery priorities for each resource, considering criticality and dependencies or interdependencies of resources.

d. The BIA must be reviewed at least annually and updated with new information, as applicable, to identify new contingency planning requirements, recovery objectives, restoration priorities, and metrics.

i. The BIA findings, particularly the MTD times and disruption impacts, must serve as inputs to develop and maintain the Contingency Plan’s recovery time objective (RTO) and recovery point objective (RPO) requirements.

ii. Application recovery requirements must be shared and coordinated with associated GSS owners.

iii. GSS owners shall consider the application recovery requirements and incorporate these requirements into their continuity of support considerations of their contingency planning program.

e. Information system recovery objectives must be consistent with applicable laws, Executive Orders, directives, policies, standards, and regulations.

f. Reviews of the Contingency Plan should be conducted annually or when a major change has occurred to the information system.

g. Copies of the Contingency Plan shall be distributed based on the information system.

   i. At a minimum, distribute to personnel with contingency plan responsibilities and organizations with support functions in the plan, to include but not limited to, the Authorizing Official (AO), Information Security Officer (ISO), Information System Security Officer (ISSO), Program Manager (PM), Senior Agency Information Security Officer (SAISO), and CSIRC Manager.

h. The approved Contingency Plan template for EPA must be used when developing the information system's Contingency Plan.

   i. All required components and key objectives identified in the Contingency Plan template must be adequately addressed. These include, but are not limited to, the following:

      - The procedures in this document must be addressed.
      - Contingency activity roles and responsibilities must be identified.
      - Individuals must be assigned to appropriate roles and responsibilities.
        - Responsibilities may be identified by teams.
      - Contact information (e.g., home number, mobile number) for the identified individuals must be included.
      - Maintaining essential missions and business functions despite an information system disruption, compromise, or failure must be addressed.
      - Activities that must be documented include:
        - Plan activation
        - Notification
        - Outage assessment
        - Recovery
        - Reconstitution
        - Return to normal operations
        - Plan deactivation
      - Procedures for restoration/reconstitution of normal operations by transitioning from the alternate processing site to the original or new primary processing facility must be included.
      - Procedures for testing security both during recovery at the alternate processing site and during restoration/reconstitution at the original or new primary processing facility must be included.

i. The Contingency Plan must be reviewed and approved by designated officials within the organization.

j. The Contingency Plan must be reviewed within an organizational component (i.e., region or program office) to determine opportunities for consolidation, efficiencies, and cost savings across the organization. Recommendations for further enterprise-wide consolidation, efficiencies and cost savings must be forwarded to the Chief

Information Officer (CIO) for consideration.

k. Copies of the Contingency Plan must be distributed to organizational management. At a minimum, distribute to personnel with contingency plan responsibilities and organizations with support functions in the plan.

    i. Because the Contingency Plan contains potentially sensitive operational and personnel information, its distribution must be marked accordingly and be controlled.

l. Weaknesses found in the Contingency Plan during development, testing, or implementation must be listed and tracked using the Plan of Action and Milestones (POA&M) for the information system.

m. An emergency response data repository must be established for each organizational entity.

    i. This repository must include all documentation pertaining to the actions necessary during emergency situations and must allow the tracking of the actions' implementation (e.g., security violation, security deficiency, incident, contingency, continuity, disaster situation and response for GSS and MA).

n. The contingency planning activities must be coordinated with incident handling activities.

    i. Refer *to Information Security – Incident Response Procedures* for requirements on incident reporting.

Note: Examples of actions to call out in contingency plans include, for example, graceful degradation, information system shutdown, fall back to a manual mode, alternate information flows, or operating in a mode that is reserved solely for when the system is under attack.

o. The Contingency Plan must be reviewed, tested, and updated at least annually to address information system, environment of operations, or organizational changes and problems encountered during plan implementation, execution, or testing.

    i. The purpose of updating the plan is to ensure that it accurately reflects the current information system. The plan must include the following components:

        - Requirements
        - Policies
        - Procedures
        - Equipment
        - Software
        - Alternate and offsite facilities
        - Points of contact

p. The Contingency Plan must be reviewed and revised, if necessary, prior to each exercise.

    i. The revisions must include workable plans and procedures to promote success of the overall testing effort.

q. The Contingency Plan must be updated whenever one (1) or more of the following criteria is present:

- i. Following a major/significant change to the software or hardware of the information system.
- ii. Following organizational changes in mission, functions, or business processes supported by the information system.
- iii. When there is a change to the RTO or RPO identified in the BIA for an information system.
- iv. Following a Contingency Plan test that uncovered problems (whether major or minor) in the Contingency Plan, to incorporate revisions identified or recommended in the Contingency Plan test report.
- v. Following a Contingency Plan activation that revealed problems (whether major or minor) in the Contingency Plan, to incorporate revisions identified or recommended in the After Action Report.

r. The Contingency Plan update must use the most current Contingency Plan template.

s. Changes must be communicated to organizational management and 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).

For moderate and high information systems

t. Contingency Plan development must be coordinated with organizational elements responsible for related plans (e.g., Business Continuity Plan, Disaster Recovery Plan (DRP), Continuity of Operations Plan (COOP), Crisis Communications Plan, Critical Infrastructure Plan, Cyber Incident Response Plan, and Occupant Emergency Plan).

For high information systems

u. Capacity planning must be conducted so that necessary capacity for information processing, telecommunications, and environmental support exists during contingency operations.

v. The resumption of essential missions and business functions must be planned for within 24 hours of Contingency Plan activation.

CP-3 – Contingency Training

a. All personnel must be trained in their contingency roles and responsibilities with respect to the information system and attend annual refresher training.

b. A comprehensive log of all Contingency Plan related training must be maintained and monitored by the System Owner (SO).

- i. The log must include participant, information system name(s), type of training, date of completion, and whether the training was initial training or refresher training.

c. Contingency training plans must be developed and maintained for all information systems.

- i. Refer *to Information Security –Awareness and Training Procedures* for requirements on creating training plans.

d. The training plan must meet the following criteria.

i. Training objectives and requirements must be identified and documented.

ii. All personnel with Contingency Plan responsibilities must be identified and included in the contingency training plan.

iii. The training plan must identify the mandatory training activities for personnel with contingency roles and responsibilities.

iv. The training plan must identify the types of training to be provided, such as classroom training, table top exercises, or full test simulations. However, actual plan testing may serve as a training activity.

v. The training plan may include both team-specific and cross-team training exercises, spanning orientation, drills, tabletop, functional, and full-scale methods.

e. Contingency Plan training must be provided by a qualified and certified commercial or internal source.

f. NIST SP 800-50 must be used for creating a security awareness training program.

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

For high information systems

h. Simulated events must be incorporated into contingency training to facilitate effective response by personnel in crisis situations.

CP-4 – Contingency Plan Testing and Exercises

a. The Contingency Plan must be tested on an annual using agency -approved tests and exercises (checklist or table-top exercises) to determine the plan’s effectiveness and the agency’s readiness to execute the plan.

b. The Contingency Plan must be tested before the system goes into production.

c. Results of the contingency plan test must be reviewed and as necessary corrective actions initiated. Significant deficiencies must be remediated prior to production deployment.

d. Costs of testing must be budgeted.

e. Commensurate with the budget planning cycle, a three-year Contingency Plan testing cycle must be established.

i. Requirements for the testing cycle must be identified and documented.

ii. The plan for the three-year testing cycle must incorporate a variety of drills and exercises that address key aspects and objectives of the Contingency Plan.

iii. The following is an example of a three-year plan:

- Year 1: Communications exercise/notification drill (phone tree) AND Contingency Plan readiness exercise (table-top scenario).
- Year 2: Communications exercise/notification drill (phone tree) AND Backup/recovery test.
- Year 3: Communications exercise/notification drill (phone tree) AND Contingency Plan readiness exercise (table-top scenario).

iv. The schedule for the tests and exercises in the three-year cycle must be documented.

f. An exercise plan for each scheduled test or exercise must be developed. The exercise plan must identify:

i. Objectives for the test or exercise; these must be based on objectives in the Contingency Plan.

ii. The type of test or exercise (e.g., checklist, walk-through/table-top, simulation: parallel, full interrupt).

iii. The scenario(s) for the test or exercise; see below for more information.

iv. Participants.

v. Logistics for the test or exercise.

vi. Documentation for implementing the test or exercise.

vii. Development of an After Action Report and any improvement plan to correct weaknesses uncovered by the test or exercise.

g. Contingency Plan testing objectives must include a determination of the effects on organization operations and assets (e.g., reduction in mission capability) and individuals arising due to contingency operations in accordance with the plan.

h. Test or exercise scenarios must include, but are not limited to, one or more of the following:

i. Equipment damage/failure.

ii. COOP emergency relocation, when applicable.

iii. Data loss/corruption.

iv. Network outage.

v. Staff shortage due to pandemic influenza.

vi. Localized or larger scale natural or man-made disaster scenarios relevant to potential or expected occurrences of the locality (e.g., earthquakes, floods, hazardous materials releases, etc.).

vii. Restoration of user-level and system-level files from backup media.

i. Testing may include a real-time exercise that tests the Contingency Plan's execution against critical systems' RTO and RPO.

j. The results of the Contingency Plan testing must be reviewed.

k. The results of Contingency Plan testing must be used to identify and remediate weaknesses within the Contingency Plan. All weaknesses found must also be documented and corrected through the POA&M process.

i. A test report, also known as an After Action Report, must be maintained on file with the Contingency Plan or in an appendix of the plan for historical reference.

l. Only appropriate personnel are permitted access to review the Contingency Plan test results. These must be limited to:

i. Personnel responsible for the Contingency Plan or identified as having a role in implementing the Contingency Plan.

ii. Agency information security oversight and audit personnel conducting authorized oversight and audit activities.

m. NIST SP 800-84 must be used for guidelines on designing, developing, conducting, and evaluating TT&E events.

For moderate and high information systems

n. Contingency Plan testing must be coordinated with organizational elements 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).

o. For GSSs that support mission-critical applications, Contingency Plan testing must be performed 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.

p. A full (simulation) recovery and reconstitution of the information system to a known state must be included as part of Contingency Plan testing.

For high information systems

q. Contingency Plan testing must be performed 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.

r. A full (interrupted simulation) recovery and reconstitution of the information system to a known state must be included as part of Contingency Plan testing.

CP-6 – Alternate Storage Sites

For moderate and high information systems

a. An alternate storage site must be established for the storage and recovery of the information system’s backup information.

b. The alternate storage site must be in a location that is separate from the primary facility.

    i. It must be separated from the primary facility to ensure that the risk of a disruption impacting both the primary and alternate site is low or otherwise is at an acceptable level, based on an assessment of risk.

    - Refer *to Information Security – Risk Assessment Procedures* for requirements on developing risk assessments.

    ii. Equivalent or related hazards or risks associated with the primary site must be absent or mitigated at the alternate storage site.

    iii. Potential problems with access to the alternate storage site in the event of an area-wide disruption or disaster must be identified and explicit mitigation actions must 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.

c. Agreements must be in place with the alternate storage site.

i. The agreements must detail service levels to be provided.

ii. The agreements must include confidentiality requirements per federal guidelines.

d. The Contingency Plan for the information system must document the following:

i. The location of the alternate storage site, including the full address and contact information.

ii. The agreements for use of the alternate storage site.

iii. Hazards or risks associated with the alternate storage site and mitigations to address them.

iv. Mitigation actions to address potential problems with access to the alternate storage site.

e. A log of all backup information stored at or retrieved from the alternate storage facility must be maintained.

For high information systems

f. The alternate storage site must be configured to facilitate recovery operations in accordance with RTOs and RPOs of the information system.

<u>CP-7 – Alternate Processing Sites</u>

For moderate and high information systems

a. An alternate processing site for the information system must be established to permit the resumption of information system operations for essential missions and business functions.

b. A timeframe for resuming those essential functions when the primary processing capabilities are unavailable must be established.

i. The timeframe to resume information system operations must be consistent with RTOs for the information system established in the BIA.

ii. This timeframe must be documented in the System Security Plan (SSP) for the information system, in the implementation description for this control.

c. Agreements must be in place with the alternate processing site.

i. The alternate processing site must 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.

- 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.

ii. The alternate processing site agreement must include testing time that is sufficient to test the longest RTO of the critical MAs.

iii. The agreements must include confidentiality requirements per federal guidelines.

d. Alternate processing site personnel must be experienced in restoring operating systems as well as applications and data.

e. The alternate processing site must be far enough away from the primary site to ensure that the alternate site is not susceptible to the same risks or hazards.

i. The risk assessment process must be used to determine the area, accessibility requirements, security requirements, environmental conditions, and cost factors necessary for selecting a safe and practical off-site facility.

- Refer to *Information Security – Risk Assessment Procedures* for requirements on developing risk assessments.

ii. Potential problems with access to the alternate processing site in the event of an area-wide disruption or disaster must be identified and explicit mitigation actions must be outlined.

f. The Contingency Plan for the information system must address the following:

i. The location of the alternate processing site, including the full address and contact information.

ii. The agreements for use of the alternate processing site.

iii. The criteria for activating the plan and achieving recovery at the alternate site.

iv. Hardware, software, and telecommunications requirements for recovery at the alternate site.

v. Strategies for recovery at the alternate site.

Note: Strategies range from having the equipment, telecommunications, and supplies in place to purchasing some or all of the equipment, supplies, and services These are not mutually exclusive strategies.

vi. Vendor contacts.

g. Arrangements must be made to ensure the necessary equipment and supplies required to resume operations identified as priorities in the Contingency Plan are available in time to support the organization-defined time period for resumption.

i. Equipment needs at the alternate processing site must be based on minimum critical function requirements identified through the BIA.

ii. The equipment requirements must match the supporting hardware, software, and connectivity requirements of the identified information systems.

iii. The equipment and supplies must be in place at the alternate processing site or appropriate contracts or agreements must be in place or initiated when the Contingency Plan is activated.

h. The alternate processing site must provide information security measures equivalent to that of the primary site.

For high information systems

i. The alternate processing site must be configured to support essential missions and business functions and ready to function as the operational site.

<u>CP-8 – Telecommunications Services</u>

For moderate and high information systems

a. Alternate telecommunications services must be established.

    i. Telecommunications restoration plans and related operational procedures must provide adequate capabilities for channels of communication between EPA and other organizations involved in the coordination and support of the Contingency Plan.

b. Alternate telecommunications services must be obtained with consideration for reducing the likelihood of sharing a single point of failure with primary telecommunications services.

c. The timeframe for resuming information system operations for essential missions and business functions using the alternate telecommunications services when the primary telecommunications capabilities are unavailable must be available immediately.

d. The necessary telecommunications agreements must be developed with both primary and alternate service providers.

    i. Primary and alternate telecommunications service agreements must contain priority-of-service provisions in accordance with the information system's availability requirements.

    ii. The terms of the agreement must 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.

    iii. Agreements with the primary and alternate telecommunications providers must each include an SLA and a notification process should the SLA not be met.

    iv. Telecommunications Service Priority (TSP) must be requested for all telecommunications services required and used for National Security and Emergency Preparedness (NSEP) in the event that the primary and/or alternate telecommunications services are provided by a common carrier.

    - The TSP program prioritizes requests for restoring telecommunications services or establishing new services during emergencies or events of national significance.

e. The Contingency Plan must document the following:

    i. The timeframe for the alternate telecommunications services to begin providing telecommunications capabilities when the primary telecommunications capabilities are unavailable.

    ii. Channels for necessary communications within EPA and between EPA and other organizations involved.

    iii. The names of the primary and the alternate telecommunications services providers and points of contact.

    iv. The agreements with the primary and alternate telecommunications service providers.

For high information systems

f. Alternate telecommunications service providers must be separated from primary service providers so as not to be susceptible to the same hazards or risks.

g. Primary and alternate telecommunications service providers must have contingency plans.

<u>CP-9 – Information System Backup</u>

a. Backups of user-level and system-level information contained in the information system must be conducted.

Note: System-level information includes, for example, system-state information, operating system and application software, and licenses.

b. Backups of information system documentation including security-related documentation must be conducted.

c. The frequency of information system backups must be consistent with the information systems' RTOs and RPOs.

   i. Incremental backups must be conducted daily.

   ii. Full backups must be conducted at least weekly.

d. The confidentiality and integrity of the system backup information must be protected at the storage location.

   i. The information system's assessment of risk or information content must guide the use of encryption 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.

e. If the information system includes personally identifiable information (PII), the SO must ensure that the information system's backup uses an encryption module that is validated as meeting federal standards (i.e., FIPS 140-2 as amended), and complies with the *Information Security – Systems and Communications Protection Procedures*.

f. Procedures for backing up and restoring the information system must be documented and included as attachments to the Contingency Plan.

g. Backup and restoration procedures must address the following:

   i. Backups must be performed outside of regular business hours.

   ii. A routine schedule must be established for backing up user-level and system-level information.

   iii. All backup media must include markings that address the contents of the media, date created, and sequence number, if multiple media were used.

      - Refer to *Information Security – Media Protection Procedures* for requirements on media protection.

   iv. The priorities and sequencing of restoration must be established.

   v. Utilities must be used by personnel responsible for storage management in order to perform system backups and disk file restorations on production systems.

   vi. Each network access control device's configuration (e.g., system software, configuration data, and database files) must be backed up via a scheme that provides 100% recovery in case of system failure.

- Backup files for network access control devices must be stored securely on read-only media so that data in storage is not over-written inadvertently.
- Backup media for network access control devices must be accessible only to the appropriate and approved personnel.

h. Backup information must be retained as follows:

   i. Daily backups must be retained for at least two weeks.

   ii. Weekly backups must be retained for at least 90 days or in accordance with records retention requirements before being reused.

For moderate and high information systems

i. Backup information must be tested at least monthly to ensure media reliability and information integrity.

   i. This testing may be on random files versus full system restoration.

   ii. Test results for backup information must be documented and must include findings for media reliability and information integrity.

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

j. Full system restoration must be tested when new backup technologies are initially implemented.

k. As part of Contingency Plan testing, a sample of backup information must be used to restore selected information system functions.

   i. This may be a full restoration or a restoration of selected files.

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

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

CP-10 – Information System Recovery and Reconstitution

a. The information system must be recovered and reconstituted to a known state after a disruption, compromise, or failure.

   i. Recovery and reconstitution mechanisms and procedures must be documented in the Contingency Plan.

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

b. The information system's recovery and reconstitution procedures must follow the priorities identified in the information system's BIA and Contingency Plan.

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

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

iii. Reconstitution must 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.

c. Personnel responsible for the information system must ensure the following both during disruptions and during recovery and reconstitution:

i. Essential operations must be continued.

ii. Vital records must be protected in accordance with EPA's Vital Records Program.

iii. Essential equipment and assets must be protected.

For moderate and high information systems

d. The information system must be configured 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.

e. Compensating security controls must be provided 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.

For high information systems

f. The capability must be provided to reimage information system components immediately from configuration-controlled and integrity-protected disk images representing a secure, operational state for the components.

7. RELATED DOCUMENTS

- NIST SP 800-34, Revision 1, *Contingency Planning Guide for Information Technology Systems*, May 2010
- NIST SP 800-50*, Building an Information Technology Security Awareness and Training Program,* October 2003
- NIST SP 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations,* August 2009
- NIST SP 800-84*, Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities*, September 2006

8. ROLES AND RESPONSIBILITIES

Chief Information Officer (CIO)

a. The CIO has the following responsibilities with respect to contingency planning:

i. Accept risks to the organization related to contingency planning.

ii. Ensure the organization has necessary resources to plan and enact Contingency Plans for information systems within their organization.

iii. Negotiate contingency planning requirements with other CIOs in support of their information systems.

Information Owner (IO)

b. The IO has the following responsibilities with respect to contingency planning:

i. Assist the CIO in contingency planning responsibilities.

System Owner (SO)

c. The SO has the following responsibilities with respect to contingency planning:

i. Ensure that the Contingency Plan is developed, reviewed, and updated annually.

ii. Communicate changes to appropriate elements responsible for related plans.

iii. Conduct capacity planning so that necessary capacity for information processing, telecommunications, and environmental support exists during crisis situations.

iv. Establish a three-year Contingency Plan testing cycle.

v. Ensure that the Contingency Plan is developed, budgeted for, and implemented in accordance with requirements for the system.

vi. Ensure that all personnel with contingency roles and responsibilities receive both initial and refresher training.

vii. Ensure that the Contingency Plan is properly implemented when a disruption, compromise, or failure occurs.

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

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

x. Ensure that 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.

Information System Security Officer (ISSO)

d. The ISSO has the following responsibilities with respect to contingency planning:

i. Assist the CIO, IO, and SO in understanding their responsibilities for contingency planning.

ii. Assist in the coordination and oversight of information system contingency planning.

iii. Support and assist the SO in their contingency planning responsibilities.

9. DEFINITIONS

- After Action Report – a document containing findings and recommendations from an exercise or a test or from an 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.
- Cold Site – a backup facility that has the necessary electrical and physical components of a computer facility, but does not have the computer equipment in place. The site is ready to receive the necessary replacement computer equipment in the event that the user has to move from their main computing location to an alternate site.
- 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' contingency plans.
- Continuity of Support Plan/IT 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

disaster. From the standpoint of GSS, a Contingency Plan is the documentation of a predetermined set of instructions or procedures that describe how to sustain major applications and GSS 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.
- General Support System (GSS) – an interconnected set of information resources under the same direct management control that shares common functionality. A general support system normally includes hardware, software, information, data, applications, communications, facilities, and people and provides support for a variety of users and/or applications. A general support system, for example, can be a (i) LAN including smart terminals that support a branch office, (ii) backbone (e.g., agency-wide), (iii) communications network, (iv) Agency data processing center including its operating system and utilities, (v) tactical radio network, or (vi) shared information processing service facility. A general support system can have a FIPS 199 impact level of low, moderate, or high in its security categorization depending on the criticality or sensitivity of the system and any major applications the general support system is supporting. A general support system is considered a major information system when special management attention is required, they are high development, operating, or maintenance costs; and the system/information has a significant role in the administration of agency programs. When the general support system is a major information system, the system's FIPS 199 impact level is either moderate or high.
- Hot Site – a fully operational off-site data processing facility equipped with hardware and system software to be used in the event of a disaster.
- 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 Security Policy – an aggregate of directives, regulations, rules, and practices that prescribe how an organization manages, protects, and distributes information.
- Information System – a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.
- Information Technology – any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or

reception of data or information by the executive agency. For purposes of the preceding sentence, equipment is used by an executive agency if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency which (i) requires the use of such equipment or (ii) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. The term information technology includes computers, ancillary equipment, software, firmware, and similar procedures, services (including support services), and related resources.

- Integrity – guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.
  - *Major Application* – an application that requires special attention to security due to the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application. *Note: All federal applications require some level of protection. Certain applications, because of the information in them, however, require special management oversight and should be treated as major. Adequate security for other applications should be provided by security of the systems in which they operate.*
  - *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, 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, 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).
- Mobile Site – a self-contained, transportable shell custom-fitted with the specific IT equipment and telecommunications necessary to provide full recovery capabilities upon notice of a significant disruption.
- 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 contingency plan activation.
- Recovery – executing information system contingency plan 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.
- Warm Site – an environmentally conditioned workspace that is partially equipped with IT and telecommunications equipment to support relocated IT operations in the event of a significant disruption.
- Written – or “in writing” means to officially document the action or decision and includes a signature. The documentation can be accomplished manually or electronically.

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 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 Manual, Directive 2195A1, 1999 Edition, Section 13 and Appendix A

13. ADDITIONAL INFORMATION

NA

Malcolm D. Jackson
Assistant Administrator and Chief Information Officer
Office of Environmental Information

APPENDIX A: ACRONYMS

BIA	Business Impact Analysis
BCP	Business Continuity Plan
CIO	Chief Information Officer
COOP	Continuity of Operations Plan
DRP	Disaster Recovery Plan
EPA	Environmental Protection Agency
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
GSS	General Support System
IO	Information Owner
ISSO	Information System Security Officer
IT	Information Technology
LSI	Large Scale Integration
MA	Major Application
MTD	Maximum Tolerable Downtime
NIST	National Institute of Standards and Technology
NSEP	National Security and Emergency Preparedness
OMB	Office of Management and Budget
PII	Personally Identifiable Information
POA&M	Plan of Action and Milestones
RPO	Recovery Point Objective
RTO	Recovery Time Objective
SAISO	Senior Agency Information Security Officer
SLA	Service Level Agreement
SO	System Owner
SP	Special Publication
SSP	System Security Plan
TSP	Telecommunications Service Priority
TT&E	Test, Training, and Exercise
USC	United States Code

DOCUMENT CHANGE HISTORY

Version	Release Date	Summary of Changes	Author of Changes	DCN
0.6	1/14/08	Initial draft	Heather Flager	Procedures-CP-Draft_TO62_020_1
2.0	5/13/09	Incorporated EPA comments and metrics Final	Heather Flager	Procedures-CP-Final_TO62_020_2
2.9	8/16/10	Updated per NIST SP 800-53 Rev 3	Heather Flager	Procedures_CP_Draft.TO-062_050_1.0
3.0	1/11/11	Final TISS Review	Charleen Johnson	Procedures_CP_Draft.TO-062_050_1.0
3.1	5/1/12	SAISO Final Review	Jabran Malik	Procedures_CP_Draft.TO-062_050_1.0
3.2	7/13/12	Document Review	LaToya Gordon	Procedures_CP_Draft.TO-062_050_1.0