DHS Management Directive, "Information Technology Security Program, Sensitive Systems"

Instructions K

IT Contingency Plan Template

Version 1.0

September 1, 2022

This page intentionally blank

Document Change History

Version	Date	Description
1.0	September 1, 2022	Final Draft

Contents

1.0 OVERVIEW

The intent of a contingency plan, as described by Section 3.5.2 of the DHS Management Directive 140-01-001, "*Information Technology Security Program, Sensitive Systems*", is to ensure the availability of critical information systems under all circumstances. A Contingency Plan provides for capability to respond to emergencies, to recover from them, and to resume normal operations, possibly at an alternate location, in the event of emergency, system failure, or disaster.

Specific control requirements for emergency situations, and level of effort expended, are determined based on the information system's security categorization. The level of resources for the Contingency Plan is based on the security categorization for the availability security objective:

- For systems with a low impact for availability, the system owner can determine the Contingency Plan format and content that is appropriate for the system and its environment. The Contingency Plan generated in the Cyber Security Assessments and Management system (CSAM) automated Security Authorization tool can also be used.
- For systems with a moderate impact level for availability, the default Contingency Plan template in CSAM should be used.
- Systems with a high impact level for availability should develop a rigorous Contingency Plan. The template to be used for such a plan is provided in this attachment and can also be found in IACS. The high impact plan can be received in IACS when creating a package, by answering "Yes" to additional documents in the questionnaire.

The DHS *Security Authorization Process Guide* provides detailed information on developing the Contingency Plan within CSAM.

The template included in this attachment is for ***high impact availability information systems only***. The template contains instructions for completing specific sections where practical. Text is added in certain sections, but the text is only intended to suggest the type of information for the section. The suggestive text is not comprehensive and should be modified to meet specific agency and system considerations. The Information System Contingency Plan should be marked with the appropriate security label, such as For Official Use Only.

2.0 RELATIONSHIP TO CONTINUITY OF OPERATIONS PLAN

Information System Contingency Plans, for critical systems identified within a Continuity of Operations (COOP) Plan, should be developed and included as appendices to the COOP Plan.

COOP Plans and associated Information System Contingency Plans should cross-reference each other.

Allowable outage times identified in Information System Contingency Plans should coincide with the business functionality Minimum Allowable Outage/Downtime (MAO) identified in the COOP Plans.

3.0 GUIDANCE FOR TEMPLATE USAGE

Throughout the attached template, angle brackets – < > – enclose guidance; when the template is complete, remove all such material.

Generic terms in braces – **{ }** – must be replaced with appropriate specific terms. Some, such as {system name} can be globally replaced by word processor software functions. For terms whose replacements do not begin with a capital letter, errors may occur when those terms are at the beginning of a sentence. Most spell checkers will find these errors.

Adjust the version number of the plan on the cover and in headers and footers. Versions that are distributed should be whole numbers in the form 1.0, 2.0, 3.0, etc.

The plan, when completed, is "FOR OFFICIAL USE ONLY." Remove the words "(when completed)" from the headers and footers.

Enter the Component name, system name, and date in the headers.

It is recommended that SharePoint filename be entered as a field code in the footer if possible. This will help simplify version control.

Insert a table of contents on page v.

Run a spell and grammar check. Note that some correct constructions and spellings will be cited as grammar or spelling "errors."

Before distributing the completed template, remove this and all preceding pages.

Homeland Security

{Component Name}

{System name}
Information System Contingency Plan

Version <n.n>

{Month dd, yyyy}

This page intentionally blank

Document Change History

Version	Date	Author	Description
1.0			Initial Publication

1.0 PLAN APPROVAL

As the designated authority for {system name}, I hereby certify that this information system Contingency Plan (CP)is complete and in accordance with DHS Management Directive 140-01-001, "*Information Technology Security Program, Sensitive Systems,*" and that the information contained in this CP provides an accurate representation of hardware, software, and telecommunications components.

I further certify that this document identifies the criticality of the system as it relates to the mission of {Component name}, and that the recovery strategies identified will provide the ability to recover the system's functionality using the most expedient and cost-efficient methods in keeping with the system's level of criticality.

Further, I attest that this CP for {system name} will be tested at least annually. This CP was last tested on {exercise date}; the Test, Training, and Exercise (TT&E) material associated with this test can be found {location of TT&E results}. This document will be modified as changes occur and will remain under version control in accordance with DHS Management Directive 140-01-001, "*Information Technology Security Program, Sensitive Systems,*".

_____ Date _____

{system owner name}

{system owner title}

<add other applicable approving authorities if appropriate>

This page intentionally blank

<insert table of contents>

This page intentionally blank

1.0 INTRODUCTION

Information systems are vital to the mission business processes of {Component name}; therefore, it is critical that services provided by {system name} can operate effectively without excessive interruption. This Contingency Plan (CP) establishes comprehensive procedures to recover {system name} quickly and effectively following disruption of service.

1.1 Authorities

U.S. Department of Homeland Security Office of the Chief Information Officer (OCIO) Devolution Plan 8/5/2020

U.S. Department of Homeland Security (DHS) Order Delegation of Authority Updated Date: 01/19/2021

U.S. Department of Homeland Security (DHS) Office of Chief Information Officer (OCIO) Continuity of Operations Annex August 14, 2020

U.S. Department of Homeland Security Management Directorate (MGMT) Devolution Plan

Department of Homeland Security (DHS) Headquarters Reconstitution Plan March 2016

Federal Law

Federal Information Security Modernization Act of 2014 (FISMA), Public Law 113-283; 128 Stat 3073

National Defense Authorization Act for Fiscal Year 2001, Title X, Subtitle G, Pub L 106-398, 114 Stat 1564 “Government Information Security Reform,”

Federal Continuity Directive 1 (FCD 1), "Federal Executive Branch National Continuity Program and Requirements"

Presidential Decision Directive

Presidential Decision Directive (PDD) 67, “Enduring Constitutional Government and Continuity of Government Operations,” October 1998

National Institute of Standards and Technology Federal Information Processing Standards

NIST FIPS 199, “Standards for Security Categorization of Federal Information and Information Systems,” February 2004

National Institute of Standards and Technology Special Publications

NIST Special Publication (SP) 800-34 “Contingency Planning Guide for Federal Information Systems,” November 11, 2010

Federal Preparedness Circular

Federal Preparedness Circular (FPC) 65, “Federal Executive Branch Continuity of Operations (COOP),” June 15, 2004

1.2 Background

This {system name} CP establishes procedures to recover {system name} following a disruption. The following objectives have been established for this plan:

- In an emergency, the Department of Homeland Security {Component name} top priority and objective is to preserve the health and safety of its staff.
- Maximize the effectiveness of contingency operations through an established plan that consists of the following phases:
    - ***Notification/Activation phase*** to detect and assess damage and to activate the plan.
    - ***Recovery phase*** to restore temporary information system operations and recover damage done to the original system.
    - ***Reconstitution phase*** to restore information system processing capabilities to normal operations.
- Identify the activities, resources, and procedures needed for {system name} processing during prolonged interruptions of normal operations.
- Assign responsibilities to designated {Component name} personnel and provide guidance for recovering {system name} during prolonged interruptions of normal operations.
- Ensure coordination among all personnel responsible for {Component name} contingency planning strategies.
- Ensure coordination with external points of contact and vendors whose involvement is necessary to the execution of this CP.

1.3 Scope

Guidance, direction, and authority for DHS Component information system contingency planning is provided by the DHS Office of the Chief Information Officer (CIO). This Contingency Plan was developed using the requirements of DHS Management Directive 140-01, *Information Technology Security Program* together with implementation guidance provided in the *DHS Management Directive 140-01-001, "Information Technology Security Program, Sensitive Systems"* instructions and NIST SP 800-53 baseline control matrix, as well as NIST SP 800-34, "*Contingency Planning Guide for Information Technology (IT) Systems*," which details planning principles universally applicable to all federal information systems. The rigor of information system contingency planning, training, testing and capabilities is dependent upon the FIPS 199 defined potential impact level.

This CP has been developed for {system name}, which is classified as a Low, medium, or high system as defined by Federal Information Processing Standard (FIPS) 199, "Standards for Security Categorization of Federal Information and Information Systems." Procedures detailed in this CP are for {level of impact} impact systems and designed to recover {system name} within Recovery Time Objective {RTO hours}. This plan does not address replacement or purchase of new equipment; short-term disruptions lasting less than {RTO hours}; or loss of data at the onsite facility or at the user-desktop levels.

This CP does not apply in the following situations:

- Overall recovery and continuity of mission business operations: The Business Continuity Plan (BCP) and Continuity of Operations Plan (COOP) address continuity of business operations.
- Emergency evacuation of personnel: The Occupant Emergency Plan (OEP) addresses employee evacuation.

1.4 Assumptions

This plan is based on the following assumptions:

- {System name} is a {level of impact} impact system according to FIPS 199 criteria.
- <for high impact systems> Alternate processing sites and offsite storage are required and have been established for this system.
- <for high impact systems> Current backups of system software and data are intact and available at the offsite storage facility in {City, State} and are available if needed for relocation of {system name}.
- <*For high impact systems*> Alternate facilities have been established at {City, State} and are available if needed for relocation of {system name}.
- <For high impact systems> The equipment, connections, and capabilities required are available at the alternate site in {CITY, STATE}. Service agreements are maintained with Not Specified hardware, software, and communications providers to support the emergency system recovery.
- <For high impact systems> A valid {plan or contract} exists with an alternate site which designates the site in {City, State} as the alternate operating facility for {system name}. The {plan or contract} contains provisions such that:
  - DHS will use the alternate site building and resources to recover {system name} functionality during an emergency that prevents access to the original facility.
  - The designated computer system at the alternate site has been configured to begin processing {system name} information.
- The alternate site will be used to continue {system name} recovery and processing throughout the period of disruption, until the return to normal operations.
- {system name} is inoperable at {Component name} and cannot be recovered within 48 hours.
- Key {system name} personnel have been identified and trained in their emergency response and recovery roles and are available to activate the {system name} CP.
- The DHS facility in {City, State} is inaccessible; therefore, DHS is unable to perform {system name} processing for the {DHS, DHS Component or DHS organization}.
- Preventive controls (e.g., generators, uninterruptible power supply (UPS), environmental controls, waterproof tarps, sprinkler systems, fire extinguishers, and fire department assistance) are, or may not be fully operational at the time of the disaster. Existing preventive controls are documented and are provided as an attachment to this plan, {attachment name}.
- Current backups of the application software and data are intact and available at the offsite storage facility or alternate processing site.

- <additional assumptions as appropriate>
-

The {SYSTEM NAME}Contingency Plan does not apply to the following situations:

- **Overall recovery and continuity of business operations.** The Business Resumption Plan (BRP) and Continuity of Operations (COOP) Plans are appended to this plan.
- **Emergency evacuation of personnel.** The Occupant Emergency Plan (OEP) is appended to this plan. As stated, this appended {System name} addresses occupant emergencies and is not the information system Contingency Plan.
-

2.0 CONCEPT OF OPERATIONS

<The concept of operations section provides details about {system name}*; an overview of the three phases of the CP (Activation and Notification, Recovery, and Reconstitution); and a description of roles and responsibilities of {Component name}'s personnel during contingency plan execution.>*

2.1 System Description

<Information for this section should be available from the system's Security Plan (SP). Attach the latest version of the SP to this CP, referencing this section's content to specific sections of the SP.

- Provide a general description of system architecture and functionality.
- Indicate the operating environment, physical location, general location of users, and partnerships with external organizations/systems.
- Include information regarding backup procedures. The DHS recommended procedures are daily incremental backups and weekly full backups.
- Include a list of preventive controls that deter, detect, and/or reduce impacts to the system.
- Include information regarding any other technical considerations that are important for recovery purposes.
- Provide a diagram of the architecture, including security controls and telecommunications connections.

Full size image can in found in CSAM project artifacts as {SYSTEM NAME} Diagram.

Add the image is located at:

Facility Name

Address

On share: \\

-

2.2 Order of Succession

DHS sets forth an order of succession to ensure that decision-making authority for the {system name} CP is uninterrupted. The {facility manager or security officer} is responsible for ensuring the safety of personnel. The {system owner, information system contingency plan coordinator and/or delegated personnel} is responsible for execution of procedures documented within this CP. If the {system owner or contingency plan coordinator} is unable to function as the overall authority or chooses to delegate this responsibility to a successor, the person delegated responsibility by the system owner shall function as that authority. Documented orders of succession and/or delegations are attached to this plan for reference.

The Under Secretary for Management and his or her successors, identified below, have the authority to activate the OCIO Devolution Plan.

- Under Secretary for Management (USM)
- Chief Financial Officer
- Chief Human Capital Officer
- Chief Procurement Officer
- Chief Readiness Support Officer
- Chief Security Officer
- Chief of Staff (CoS)
- Deputy Director, Federal Law Enforcement Training Center (FLETC)

The OCIO will ensure the OCIO Order of Succession is current. The CIO Order of Succession is as follows:

- Chief Information Officer
- Deputy Chief Information Officer
- Executive Director, Information Technology Services Office
- Chief Information Security Officer
- Executive Director, Information Sharing and Services Office
- Chief Information Officer, FLETC
- Deputy Chief Information Officer, FLETC

Order of Succession for System (s)				
Title	**Name**	**Phone**	**Pager**	**Cell**
Authorizing Official (AO)				
Service Delivery Manager HSD				
System Owner				
Site A Continuity Operations Manager				
Chief Information Security Officer				

{SYSTEM NAME} Information Systems Security Manager (ISSM)				
HQ SOC Lead				
Information Systems Security Officer (ISSO)				

2.3 Overview of the Three Phases

This CP has been developed to recover the {system name} in three phases. This approach ensures that system recovery is performed in a methodical sequence that maximizes effectiveness of recovery effort and minimizes system outage time due to errors and omissions. The three system recovery phases are:

(1) Activation and Notification Phase

- This CP is activated following an outage or disruption that may be reasonably expected to extend beyond 48 hours. The outage event may result in severe damage to the facility housing the system; severe damage or loss of equipment; or other damage that typically results in long-term loss.
- After activation of the CP, system owners and users are notified of a possible long-term outage, and a thorough outage assessment if performed for the system. Results of the outage assessment are presented to system owners and may be used to modify recovery procedures to specifically address the cause of the outage.

(2) Recovery Phase

- During the recovery phase, activities and procedures for recovery are written for use by appropriately skilled technicians in recovering the system without intimate system knowledge. This phase includes notification and awareness escalation procedures for communication of recovery status to system owners and users.

(3) Reconstitution Phase

- Define the actions taken to test and validate system capability and functionality at the original or new permanent location. Validation procedures may include functionality or regression testing, concurrent processing, and/or data validation. Upon completion of validation, the system is declared recovered and operational by system owners.
- Plan deactivation is the final step, during which users are notified of the system's operational status; recovery effort documentation is finalized; activity logs are finalized; and lessons learned are documented for incorporation into plan updates. Resources are readied for any future events.

2.4 Roles and Responsibilities

In addition to the Senior Management Official identified in this section, this CP establishes several teams trained to participate in recovering {system name} operations, environment, and all applications. Team members include personnel who are responsible for daily operations of the system.

<Describe the responsibilities of each individual and team, with narrative and bulleted lists similar to those in the typical text that follows. Include responsibilities, leadership, and coordination with other individuals and teams during the recovery process. Highlight overall recovery objectives and specific responsibilities. Do not detail procedures that will be used to execute the responsibilities; those procedures will be included in the appropriate phase sections. Rewrite and modify the typical text where needed.>

The relationships of the team leaders involved in system recovery and their member teams are illustrated in Figure *{nn}.*

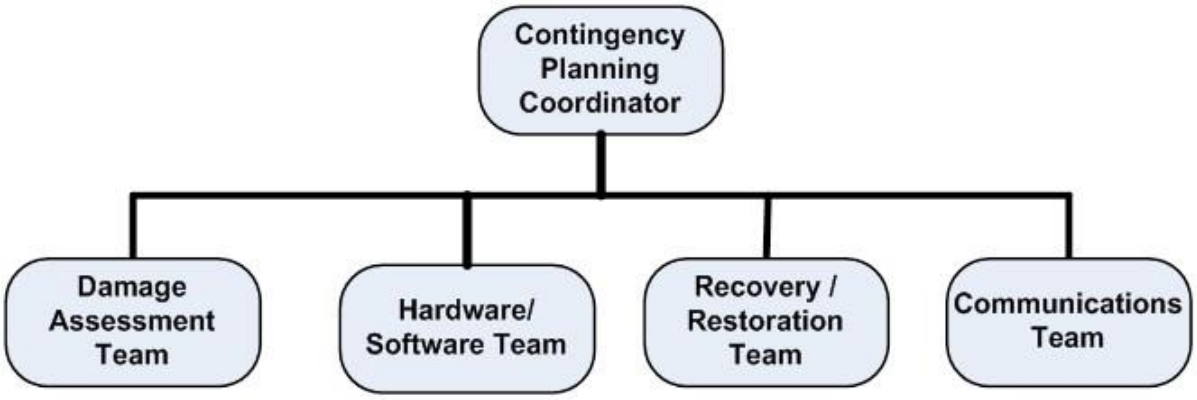
<Insert hierarchical diagram of recovery teams. Show team names and leaders; do not include actual names of personnel.>

The information system Contingency Plan establishes several teams assigned to participate in recovering {SYSTEM NAME}operations. The (Component) (Division) and the Management Group is responsible for obtaining business needs, reviewing requirements, defining the user impact, developing image pre-build plans and communication plans, approving the release content, reviewing test results, submitting revision requests, and approved the final image release.

The relationships of the team leaders involved in system recovery and their member teams are illustrated in Figure below.

The Image Management Group works directly with the Customer Relationship Managers (CRMs), Federal Engineering team, Security team, Accessibility (OAST) team, Communications team, and the O&M testing team, providing actionable recommendations with supporting documentation, throughout the image build life cycle to achieve organizational goals.

These groups may work independently of the {SYSTEM NAME}ISSO/ISSM during the day-to-day operations and maintenance of {SYSTEM NAME}systems. In the case of a large-scale event such as a massive malware infection, the {SYSTEM NAME} ISSO/ISSM would work in coordination with these teams to coordinate events and track progress until the threat has been eradicated and systems return to normal operation.



2.4.1 Senior Management Official

This individual is a Senior Manager is responsible to Executive Management for all facets of contingency planning and exercises, as well as for recovery operations.

- Pre-event
  - Approve the plan.
  - Ensure the plan is maintained.
  - Ensure training is conducted.
  - Authorize periodic plan testing exercises.
  - Support the Contingency Management Team Leader and all other participants prior to and during scheduled and unscheduled exercises and plan tests.
- Post-event
  - Declaration of a disaster.
  - Authorize travel and housing arrangements for team members.
  - Authorize expenditures through the Administration Team.
  - Manage and monitor the overall recovery process.
  - Periodically advise senior staff, customers, and media relations personnel of the status.
  - Support the Contingency Management Team Leader and all other participants during debilitating conditions/situations.

2.4.2 Contingency Management Team

<The responsibilities described may also be those of a team called the Alternate Site Recovery Coordination Team>

The Contingency Management Team is responsible for managing the total recovery effort; for ensuring that other teams and personnel perform all checklist items; for providing a "Command Center" for coordination and overall communications; and for ensuring that activities are accomplished among all teams within planned time frames and for providing assistance in resolving problems that may arise. This team is activated by the Senior Management Official or System Owner. establishes several teams trained to participate in recovering {system name}

operations, environment, and all applications. Team members include personnel who are responsible for daily operations of the system.

<Describe the responsibilities of each individual and team, with narrative and bulleted lists similar to those in the typical text that follows. Include responsibilities, leadership, and coordination with other individuals and teams during the recovery process. Highlight overall recovery objectives and specific responsibilities. Do not detail procedures that will be used to execute the responsibilities; those procedures will be included in the appropriate phase sections. Rewrite and modify the typical text where needed.>

The relationships of the team leaders involved in system recovery and their member teams are illustrated in Figure *{nn}.*

<Insert hierarchical diagram of recovery teams. Show team names and leaders; do not include actual names of personnel.>

Emergency Management Team is responsible for managing the total recovery effort, ensuring other teams and personnel perform all detailed checklist activities, providing a "Command Center" for coordination and overall communications, ensuring that activities are accomplished among all teams within planned time frames and assisting in resolving problems that arise. This team is activated by the Senior Management Official/CIO/System Owner/Contingency Planning Coordinator. All other teams report directly to the Contingency/Emergency Management Team. Specific duties are:

2.4.2.1 Contingency Management Team Leader /Emergency Management Team

- **Pre-event**
  - Maintain and update the plan as needed or scheduled but not less than annually.
  - Distribute copies of plan to team members.
  - Coordinate testing as needed or scheduled but not less than annually.
  - Train team members.
- **Post-event**
  - Accomplish initial notification of Team members.
  - Establish a command center for recovery operations.
  - Assist in damage assessment.
  - Coordinate activities of recovery teams.
  - Notify alternate site of activation.
  - Notify Team Leaders of other Teams of CP activation.
  - Authorize the Administration Team to make the necessary travel and hotel accommodations for recovery team members.
  - Periodically report to the Senior Management Official status of recovery efforts and details as required.

2.4.2.2 Contingency Management Team Members:

- **Pre-event**
  - Assist the Team Leader as directed.
  - Participate in contingency exercises.

- Understand all CP roles and responsibilities.

- **Post-event**
  - Perform command center functions.
  - Maintain a record of all communications using the provided log forms.

2.4.3 Damage Assessment Team

The Damage Assessment Team is responsible for damage assessment of the computer facilities as quickly as possible following CP activation, and for reporting the level of damage to the Contingency/Emergency Management Team. The Team also provides assistance when possible in the cleanup and repair of the facility. Specifically, the team responsibilities are:

- **Pre-event**
  - Understand role and responsibilities under the CP.
  - Work to reduce the likelihood of events that could require CP activation.
  - Train employees in emergency preparedness.
  - Participate in CP exercises and tests.
  - Have a thorough understanding of damage assessment procedures.
- **Post-disaster**
  - Determine accessibility to facility, building, offices, and work areas/stations.
  - Assess extent of damage to the system and computer center.
  - Assess need and/or adequacy of physical security/guards.
  - Estimate time to recover primary facility and system.
  - Identify salvageable hardware.
  - Inform Contingency Management Team about the extent of damages, estimated recovery time, the need for physical security, and salvageable equipment details.
  - Maintain a salvageable equipment log.
  - Coordinate with suppliers restoring, repairing, or replacing equipment not under the purview of another CP.
  - Support data center cleanup following an incident.

2.4.4 Hardware Team

<With appropriate modifications, the typical content below may be relevant to:

Hardware Salvage Team

Original Site Restoration/Salvage Coordination Team>

The Hardware team is responsible for site preparation, physical planning, and installation of data processing equipment to provide required processing capability when the CP is activated. The Team's responsibilities include ordering and installing hardware and software necessary at the alternate and permanent sites.

- **Pre-event**
  - Understand roles and responsibilities under the CP.
  - Work closely with the Contingency Management Team to reduce the likelihood of events that could require CP activation.

- Work closely with the Contingency Management Team to reduce the likelihood of events that could require CP activation.
- Train employees in emergency preparedness.
- Participate in contingency plan exercises and tests.
- Thoroughly understand CP procedures.
- Maintain current system configuration information in an off-site storage facility and in this plan.

- **Post-event**
  - Verify pending occupancy requirements with alternative site.
  - Inspect physical space at the alternative site.
  - Interface with Software, Communications and Operations Team members on space configuration for the alternative site.
  - Coordinate transportation of salvageable equipment to the alternative site.
  - Notify the Administration Team of equipment requirements.
  - Ensure installation of required temporary terminals and workstations connected to the alternative site hardware.
  - Plan the hardware installation at the alternative site.
  - Plan and coordinate transportation of and installation of hardware at the permanent site, when available.

2.4.5 Software Team

<With appropriate modifications, the typical responsibilities enumerated below may also be applicable to the following teams:

Systems Software Team
Server Recovery Team (e.g., client server, Web Server)
LAN/WAN Recovery Team
Database Recovery Team
Application Recovery Team(s)
Telecommunications Team
Test Team
Network Operations Recovery Team
Operating Systems Administration Team>

The Software Team is responsible for installation and configuration of all system and application software not installed by other administrators.

- **Pre-event**
  - Understand roles and responsibilities under the CP.
  - Work closely with the Contingency Management Team to reduce the likelihood of events that could require CP activation.
  - Train employees in emergency preparedness.
  - Participate in CP exercises and tests.
  - Thoroughly understand CP procedures.
  - Maintain current system software configuration information in an off-site storage facility and in an appendix to this plan.

- **Post-event**
  - Arrange for delivery of off-site storage containers containing backup media.
  - Receive, inventory and control access to the off-site storage containers and media
  - Restore system/application software data files not installed in conjunction with .another plan's personnel.
  - Test and verify operating system and application software functions as required.
  - Return backup media storage containers to the off-site storage facility.

2.4.6 Communications Team

The Communications Team is responsible for establishing voice and data links to/from the alternative site. This includes connecting local and remote users/customers to the alternate site.

- **Pre-event**
  - Understand roles and responsibilities under the CP.
  - Work closely with the Contingency Management Team to reduce the likelihood of events that could require CP activation.
  - Train employees in emergency preparedness.
  - Participate in contingency plan exercises and tests.
  - Thoroughly understand CP procedures.
  - Maintain current communications configuration information in an off-site storage facility and in this CP.
- **Post-event**
  - Assist the Damage Assessment Team in evaluating communications equipment.
  - Plan, coordinate, and install the communications equipment required at the alternative site.
  - Plan, coordinate, and install the necessary cabling at the alternative sire not accomplished by another plan's recovery personnel.

2.4.7 Physical and Personnel Security Team

The Physical and Personnel Security Team is responsible for providing personnel identification and access limitations to the building and floors and acts as liaison with emergency personnel. This is crucial during the time of an incident because of the uncommonly large number of vendors, contractors and other visitors requiring access to the facility.

- **Pre-event**
  - Understand roles and responsibilities under the CP.
  - Work closely with the Contingency Management Team to ensure physical security of existing system and facilities.
  - Train employees in emergency preparedness.
  - Participate in CP exercises and tests.
  - Thoroughly understand CP procedures.
- **Post-event**
  - Cordon off the facility including offices to restrict unauthorized access.
  - Coordinate with Building Management for authorized personnel access.

- Provide additional physical security/guards.
- Act as liaison with emergency personnel, such as fire and police departments.
- Schedule and provide transportation security for files, reports, and equipment.
- Provide assistance to officials investigating the damaged facility and site.

2.4.8 Administration and Procurement Support Team

<Depending on potential workload, other teams might be formed as appropriate to assume some of the responsibilities listed below. Such teams could be these:

- Transportation and Relocation Team
- Media Relations Team
- Legal Affairs Team>

The Administration and Procurement Support Team is responsible for providing secretarial, procurement, travel, housing, off-site storage, and other administrative matters not performed by other teams. The Team has limited authority to fund emergency expenditures other than capital equipment and salaries. This Team is also responsible for conveying pertinent information to the Department's Media Relations Officer, will work with the Department's Legal Representation staff on related matters.

- **Pre-event**
  - Understand roles and responsibilities under the CP.
  - Work closely with the Contingency Management Team to ensure that all administrative functions are accomplishable.
  - Work closely with the Contingency Management Team to reduce the likelihood of events that could require CP activation.
  - Work closely with the Contingency Management Team to ensure all potential means of transportation are understood and provided for.
  - Train employees in emergency preparedness.
  - Participate in contingency exercises.
  - Know the procedures to be followed.
  - Ensure details of administering emergency funds expenditures are known.
  - Assess need for alternative means of communication (other than normal telephone service) is available to all employees involved.
  - Ensure that current listings of viable means of transportation to the alternate site are maintained both at the off-site storage facility and included in an appendix to this plan.
  - Ensure that current contact information for the Department's Media Relations Officer and for the Department's Legal Representation is maintained both at the off-site storage facility and included in an appendix to this plan.
- **Post-event**
  - Prepare, coordinate, and obtain approval for all procurement requests.
  - Coordinate deliveries.
  - Process requests for payment for all invoices related to the incident.
  - Arrange for travel and lodging of Team members.

- Provide for acquisition of telephone equipment and services including voice, dial-up, and leased lines.
- Provide for alternative means of communication among the teams in the event that normal telephone services are unavailable.
- Arrange for temporary secretarial support for filing, and other administrative services required by the teams.
- Coordinate with other teams to provide transportation as required.
- Plan, coordinate and provide transportation to the alternate site and for teams as required in the accomplishment of their missions.
- Support activities of the Department's Media Relations Officer and Legal Representation staff as directed by the Contingency Management Team.

2.5 Activation and Notification Phase

The Activation and Notification Phase defines initial actions taken once a {system name} disruption has been detected or appears to be imminent. This phase includes activities to notify recovery personnel, conduct an outage assessment, and activate the CP. At the completion of the Activation and Notification Phase, {system name} CP staff will be prepared to perform recovery measures. Based on the assessment of the event, the plan may be activated by the CIO or Contingency Planning Coordinator.

In an emergency, the top priority for DHS is to preserve the health and safety of its staff before proceeding to the Notification and Activation procedures.

2.5.1 Activation Criteria and Procedure

The {system name} CP may be activated if one or more of the following criteria are met:

- The type of outage indicates {system name} will be down for more than {RTO hours}
- The facility housing {system name} is damaged and may not be available within {RTO hours}
- <Other criteria, as appropriate>

The following persons or roles may activate the CP if one or more of these criteria are met:

<Establish one or more roles that may activate the plan based on activation criteria. Authorized persons may include the system or business owner, or the operations point of contact (POC) for system support.>

If the plan is activated, the system owner/contingency plan coordinator is to notify all Team Leaders and inform them of the details of the event and if relocation is required. Upon notification from the system owner/contingency plan coordinator, team leaders are to notify their respective teams. Team members are to be informed of all applicable information and prepare to respond and relocate if necessary. The system owner/contingency plan coordinator is to notify the off-site storage facility that a contingency event has been declared and to ship the necessary materials (as determined by damage assessment) to the alternate site. The system owner/contingency plan coordinator is to notify the alternate site a contingency event has been declared and to prepare the facility for the Organization's arrival. The system owner/contingency

plan coordinator is to notify remaining personnel (via notification procedures) on the general status of the incident.

2.5.2 Notification

The first step upon activation of the {system name} CP is notification of appropriate mission/business and system support personnel. Contact information for appropriate POCs is included in Appendix <*specify> Contact List Appendix*>.

<Describe CP notification procedures, to include who makes the initial notifications, the sequence in which personnel are notified (e.g., system owner, technical POC, CP Coordinator, business unit or user unit POC, and recovery team POC). Describe notification methodology (email blast, call tree, automated notification system, etc.).>

Contact information for key personnel is located in the Appendix of this plan. The notification sequence is listed below:

- The first responder is to notify the System Owner/Contingency Planning Coordinator. All known information must be relayed to the System Owner/Contingency Planning Coordinator.
- The systems manager is to contact and inform the Damage Assessment Team (DAT) Leader of the event. The System Owner/Contingency Planning Coordinator is to instruct the DAT Leader to begin assessment procedures.
- The DAT Leader is to notify team members and direct them to complete the assessment procedures outlined below to determine the extent of damage and estimated recovery time. If damage assessment cannot be performed locally because of unsafe conditions, the DAT is to follow the outline below.
- The first responder will notify the System Owner conveying all known information regarding the event
- The System Owner will inform the DAT Leader of the event and direct initiation of assessment procedures
- The DAT Leader will notify Team members and direct them to complete the assessment procedures prescribed by this CP.

2.5.3 Damage Assessment

Following notification, the DAT will determine the extent of damage and estimate recovery time. Assessment results are provided to the Contingency Management Team Leader. If damage assessment cannot be performed due to dangerous conditions, alternative steps will be taken as prescribed by this CP. For {system name}, the following method and procedure for notifications are used:

<Outline detailed procedures to include how to determine the cause of the damage; identification of potential for additional disruption or damage; affected physical area(s); and determination of the physical infrastructure status, IT equipment functionality, and inventory. Procedures should include recording items that will need to be replaced and the estimated time to restore normal operations. Identify alternate procedures in the event primary procedures cannot be carried out.>

Upon notification from the {SYSTEM NAME} ISSM, the DAT is to

assess the nature and extent of damage. This will include:

1. Cause of the emergency or disruption
2. Potential for additional disruptions or damage
3. Areas affected by the emergency
4. Review the scope and scale of damage or infection across {SYSTEM NAME} UE,
5. Coordinate efforts with IT Support and HSD to begin identifying affected systems for re-imaging

Contact information for key personnel is located in the Appendix of this plan. The notification sequence is listed below:

- The first responder is to notify the System Owner/Contingency Planning Coordinator. All known information must be relayed to the System Owner/Contingency Planning Coordinator.
- The systems manager is to contact and inform the DAT Leader of the event. The System Owner/Contingency Planning Coordinator is to instruct the DAT Leader to begin assessment procedures.

The DAT Leader is to notify team members and direct them to complete the assessment procedures outlined below to determine the extent of damage and estimated recovery time. If damage assessment cannot be performed locally because of unsafe conditions, the DAT is to follow the outline below.

- Upon notification from the {system owner/contingency plan coordinator}, the DAT leader, is to notify the DAT to begin assessment.
- The DAT is to:
  - Begin damage assessment in accordance with the procedures outlined above.
  - When damage assessment has been completed, the DAT leader is to notify the {system owner/contingency plan coordinator} of the results.
  - The {system owner/contingency plan coordinator} is to evaluate the results and determine whether the contingency plan is to be activated and if relocation is required.
  - Based on assessment results, the {system owner/contingency plan coordinator} is to notify civil emergency personnel (e.g., police, fire) assessment of the results, as appropriate.

Alternate Assessment Procedures

N/A or add if applicable

The information system Contingency Plan is to be activated if one or more of the following criteria are met:

1. A large number of {SYSTEM NAME}systems are compromised (malware infection, botnet, etc) and untrusted for normal use and operations.
2. The scale and scope of the infection is such that normal operations cannot be maintained within an acceptable timeframe, as determined by the System Owner.

If the plan is to be activated, the {SYSTEM NAME} ISSM is to notify all Team Leaders and inform them of the details of the event and if relocation is required.

Upon notification from the {SYSTEM NAME} ISSM, Team Leaders are to notify their respective teams. Team members are to be informed of all applicable information and prepare to respond and relocate if necessary.

The CP Coordinator is to notify remaining personnel (via notification procedures) on the general status of the incident.

2.6 Recovery Phase

During the Recovery Phase formal recovery operations are undertaken, beginning after the CP has been activated and notification accomplished; outage assessments have been completed (if possible); and appropriate teams have been mobilized. Recovery Phase activities focus on implementation of recovery strategies to restore system capabilities, repair damage, and resume operational capabilities at the original or alternative location. Upon completion of the Recovery Phase, {system name} will be functional and capable of performing the functions identified in Section 2.1 of this plan.

2.6.1 Recovery Goals

The following goals are for recovering the {system name}. Procedures are outlined per team required. Each procedure should be executed in the sequence it is presented to maintain efficient operations within the allowable outage time of {number of hours/days} as determined by the System Owner.

Recovery Goal #1 *{State the recovery objective as determined by the system owner, if available. For each team responsible for executing a function to meet this objective, state the team names and list their respective procedures.}*

- [Team Name]
  - {Provide an overview of Team Recovery Procedures as it pertains to the goal.}
- [Team Name]
  - {Provide an overview of Team Recovery Procedures as it pertains to the goal.}
- [Team Name]
  - {Provide an overview of Team Recovery Procedures as it pertains to the goal.}

Roles:

Contingency Plan Coordinator

- Determine and direct acquisition efforts

Hardware/Software Team

- Coordinate and manage re-imaging of {SYSTEM NAME}.

Recovery/Restoration Team

- Test and verify system and data recovery
- Coordinate connectivity testing with end-user.
- Communicate recovery results across all teams

2.6.2 Sequence of Recovery Activities

The following activities occur during recovery of {system name}*:*

<Modify the following list as appropriate for the recovery strategy

- Identify recovery location (if not at original location).
- Identify required resources to perform recovery procedures.
- Retrieve backup and system installation media.
- Recover hardware and operating system (if required).
- Recover system from backup and system installation media.>

2.6.3 Recovery Procedures

The following procedures are provided for recovery of {system name} at the original location. Recovery procedures are outlined per team and will be executed in the prescribed sequence to maintain an efficient recovery effort.

<Provide general procedures for system recovery from backup media. If there is an alternative site, include procedures for recovery to that site. Specific keystroke level procedures may be provided in an appendix referenced in this section. Teams or persons responsible for each procedure should be identified.>

Recovery Goal #2
Restore User Data if available. User data is only available if it was backed up to the user's network share drive. Users can retrieve backups on their own, or may contact IT Support for assistance.
Some email data may be available through Office 365(O365)/Enterprise Vault. Using its Archiving Service, the Enterprise Vault logs data into Exchange Mailboxes on O365.

2.7 Reconstitution Phase

Reconstitution is the process during which normal system operations are resumed. The goal is to provide a seamless transition from the alternate site to the original location. If the original facility is not recoverable, activities in this phase can be applied to preparation of a new permanent location to support system requirements. A determination must be made as to whether the system has undergone significant change and will require reassessment and reauthorization. The phase consists of two major activities: validating successful reconstitution and deactivation of the CP. The imaging process and procedures are kept on SharePoint and are available from Component by request, as well as a copy is kept in CSAM artifacts as Imaging Process.

The Image Management Group is responsible for maintaining the {SYSTEM NAME}images,

and testing the imaging and recovery capabilities. Due to the nature of this operation, it is exercised on an almost daily basis through:

- Imaging new systems as they are purchased and brought into the environment
- Re-imaging systems that have become corrupted, infected, or otherwise found to not be in compliance with {SYSTEM NAME}standards.

The process of testing and validating data ensures that data files or databases have been completely recovered at the permanent location. The procedures in this process are found in this CP section.

<Outline procedures for testing and validation to ensure that data is correct and up to date. This section may be combined with the Functionality Testing section if one set of procedures tests both functionality and data validity. Identify the teams or persons responsible for each procedure. An example of a validation data test for a low-impact system would be to test whether the last known complete transaction was updated in the database. Detailed data test procedures may be provided in the Appendix E, System Validation Test Plan. >

2.7.1 Validation of Reconstitution

2.7.1.1 Validation Data Testing

The process of testing and validating data ensures that data files or databases have been completely recovered at the permanent location. The procedures in this process are found in this CP section.

<Outline procedures for testing and validation to ensure that data is correct and up to date. This section may be combined with the Functionality Testing section if one set of procedures tests both functionality and data validity. Identify the teams or persons responsible for each procedure. An example of a validation data test for a low-impact system would be to test whether the last known complete transaction was updated in the database. Detailed data test procedures may be provided in Appendix E, System Validation Test Plan. >

2.7.1.2 Validation Functionality Testing

The process of testing and validating functionality ensures that the system is ready to return to normal operations.

<Outline procedures for system functionality testing and validation to ensure that the system is operating correctly. This section may be combined with the Data Testing section if one set of procedures tests both functionality and data validity. Identify the teams or persons responsible for each procedure. An example of a functional test for a low-impact system is logging onto the system and running a report or performing a transaction. Detailed functionality test procedures may be provided in Appendix E, System Validation Test Plan.>

2.7.2 Contingency Plan Deactivation

Once all of the activities outlined in this section have been completed, the {system owner} will formally deactivate the CP recovery and reconstitution effort. Notification of this declaration will be provided to all business and technical POCs.

{Activities should be outlined, per necessary team, to clean the alternate site of any equipment or other materials belonging to the organization, with a focus on handling sensitive information. Materials, equipment, and backup media should be properly packaged, labeled, and shipped to the appropriate location(s). Team members should be instructed to return to the original or new site.}

- [Team Name]
  - {Describe Contingency Plan Deactivation activities.}
- [Team Name]
  - {Describe Contingency Plan Deactivation activities.}
- [Team Name]
  - {Describe Contingency Plan Deactivation activities.}

2.7.2.1 Recovery Declaration

Upon successfully completing both functionality and data testing and validation, the {system owner} will formally declare that recovery efforts are complete, and that {system name} is in normal operations. {System name} business and technical POCs will be notified of the declaration by the CP Coordinator.

2.7.2.2 Notification of Users

When normal operations are restored, users will be notified by {role} using predetermined notification procedures (email, broadcast message, phone calls, etc.).

2.7.2.3 Cleanup

Cleaning up temporary recovery locations, dismantling temporary equipment, restocking supplies used, returning manuals or other documentation to their original locations, and readying the system for future contingency events will be accomplished by the Cleanup Team.

<Provide any specific cleanup procedures for the system including preferred locations for manuals and documents and returning backup or installation media to its original location.>

2.7.2.4 Data Backup

As soon as reasonably practical after recovery, the system will be fully backed up and a new copy of the current operational system stored for future recovery efforts. This full backup is then kept with other system backups. The procedures for conducting a full system backup are:

<Provide appropriate procedures for ensuring that a full system backup is conducted within a reasonable time, ideally at the next scheduled backup time. >

2.7.2.5 Event Documentation

It is important to thoroughly document all recovery steps and changes in status, including actions taken and problems encountered during the recovery and reconstitution effort. Record lessons learned for inclusion when this CP is updated. It is the responsibility of each CP team and

responsible individual to provide their documentation to the Contingency Management Team Leader.

<Provide details about the types of information each CP team leader is required to provide or collect for updating the CP with lessons learned. Types of documentation that should be collected after CP execution include but might not be limited to:

- Activity logs (including recovery steps performed and by whom, the time the steps were initiated and completed, and any problems or concerns encountered while executing activities)
- Functionality and data testing results
- Lessons learned documentation
- After Action Report>

Event documentation procedures should detail responsibilities for development, collection, approval, and maintenance.>

3.0 SUGGESTED APPENDIXES

<The attached CP appendixes are recommended. Other appendixes may be included based on system and plan requirements.>

Appendix A: Personnel Contact List

<Include contact information for the CP's Senior Management Official, and the leader and members of each team. For each contact, list name, title, address, and telephone numbers for work, home, and mobile.

Note that a special "Residual/Other" Team Contact List should be prepared for individuals not already included in other teams. This special contact list will be used to keep the uninvolved personnel aware of status and activities that may require action on their part.

In the team member contact list(s), names should be indented to indicate the organization of the calling tree (who calls who). Calling trees for a large group of personnel should be designed to limit the number of individuals that are called by a single individual to no more than 3 or 4. This will provide for expeditious communications with all team members. It will also minimize and provide for those situations where an individual must contact subordinates of those individuals that cannot be directly contacted. >

Team: *{Contingency Management Team}*

Name (Team Position)	Phone Numbers (Home/Cell/Office)	Contacted (Date and Time)	Comments
ISSO			
ISSM			
Federal Engineer			
Asset MGMT			
Service Delivery Manager			
Software Manager			
SOC Lead			

Appendix B: Vendor and Supplier Contact List

<Include contact information for all key maintenance or support vendors. For each list name, title, address, and telephone numbers for work, home, and mobile. Include contract numbers and contractual response and onsite times.>

Vendor Product / Service	Contact Name / Address	Phone Numbers (Home, Cell, Office, FAX, 24 hr)	Contacted (Date/Time)	Comments

Vendor Product / Service	Contact Name / Address	Phone Numbers (Home, Cell, Office, FAX, 24 hr)	Contacted (Date/Time)	Comments

Appendix C: Detailed Recovery Procedures

<This appendix includes detailed recovery procedures for the system, perhaps including:

- Keystroke-level recovery steps
- System installation instructions from tape, CD, or other media; Required configuration settings
- or changes
- Recovery of data from tape and audit logs
- Other system recovery procedures, as appropriate

<If the system's recovery and reconstitution is solely reliant on another group or supporting system (such as a mainframe system), provide contact information and locations of detailed written recovery procedures for that supporting system.>

Appendix D: Alternate Processing Procedures

<This section should identify any alternate manual or technical processing procedures that can be used to allow the business unit to continue some processing of information that would normally be done by the affected system. Examples of alternate processes include manual forms processing, input into workstations to store data until it can be uploaded and processed, and queuing of data input.

Appendix E: System Validation Test Plan

<Include system acceptance procedures to be performed after the system has been recovered and prior to putting the system into full operation for users. The system validation test plan may include data testing and regression, or functionality testing conducted prior to implementation of a system upgrade or change.
An example of a system validation test plan:>

Once the system has been recovered, the following steps will be performed to validate system data and functionality:

Procedure	Expected Results	Actual Results	OK?	Tester
At the command prompt, type in system name	System Log-in Screen appears			
Log in as user "testuser", using password "testpass"	Initial Screen with Main Menu shows			
From Menu - select `5- Generate Report`	Report Generation Screen shows			
- Select `Current Date Report` - Select `Weekly`	Report is generated on screen with last successful transaction included			

Procedure	Expected Results	Actual Results	OK?	Tester
- Select `To Screen`				
- Select `Close`	Report Generation Screen Shows			
- Select `Return to Main Menu`	Initial Screen with Main Menu shows			
- Select `Log-Off`	Log-in Screen appears			

Appendix F: Primary, Alternate Storage, Site, Travel Directions/Maps and Telecommunications

<Alternative storage, site, and telecommunications information is required for high-impact systems. Refer to NIST SP 800-53 for required control specifics. Information that should be provided for each area includes:

Alternate Storage

- City and state of alternative storage facility, and distance from primary facility
- Whether the alternative storage facility is owned by the organization or is a third-party storage provider
- Name and points of contact for the alternate storage facility
- Delivery schedule and procedures for packaging media to go to alternate storage facility
- Procedures for retrieving media from the alternative storage facility
- Names and contact information for those persons authorized to retrieve media
- Alternative storage configuration features that facilitate recovery operations (such as keyed or card reader access for authorized retrieval personnel)
- Any potential problems with access to the alternative storage site in the event of a widespread disruption or disaster
- Mitigation for potential access problems at alternative storage site in the event of a widespread disruption or disaster
- Types of data located at the alternative storage site, including databases, application software, operating systems, and other critical information system software
- Other information as appropriate

Primary Location	
FACILITY NAME:	
STREET ADDRESS:	FLOOR:
CITY/STATE/ZIP:	
CONTACT PERSON: ALTERNATE CONTACT:	PHONE NO: 24 HOUR NO: FAX NO: OTHER NO.:
SECURITY CONSIDERATIONS:	

Alternate Processing Site

- Location (city and state) of alternative processing site, and distance from primary facility
- Whether the alternative processing site is owned by the organization or is provided by another organization
- Name and contact information for the alternative processing site
- Procedures for accessing and using the alternative processing site
- Access security features of alternate processing site
- Names and contact information for those persons authorized to go to alternate processing site
- Type of alternate processing site, and equipment available there
- Alternate processing site configuration information such as available power, floor space, office space, telecommunications availability, etc.
- Potential accessibility problems at the alternate processing site in the event of a widespread disruption or disaster
- Mitigation for access problems at the alternative processing site in the event of a widespread disruption or disaster
- SLAs or other agreements for use of the alternative processing site, available office space, setup times, etc.
- Other information as appropriate

Alternate Location	
FACILITY NAME:	
STREET ADDRESS:	FLOOR:
CITY/STATE/ZIP:	
CONTACT PERSON: ALTERNATE CONTACT:	PHONE NO: 24 HOUR NO: FAX NO: OTHER NO.:
SECURITY CONSIDERATIONS:	

Alternative Telecommunications:

- Name and contact information of alternate telecommunications vendors;
- Geographic locations of alternate telecommunications vendors facilities (such as central offices, switch centers, etc.);
- Contracted capacity of alternate telecommunications;
- SLAs or other agreements for implementation of alternate telecommunications capacity;
- Information on alternate telecommunications vendor contingency plans;
- Names and contact information for those persons authorized to implement or use alternate telecommunications capacity
- Other information as appropriate. >

Appendix G: System and Input-Output Diagrams

<Information for this appendix should be available from the system's system Security Plan (SP). The appropriate information can be copied from the SP, or the appendix can be attached as part of this appendix and reference made here to the appropriate SP section. Language or references should include any system architecture, input/output, or other technical or logical diagrams that may be useful in recovering the system.>

Appendix H: Hardware and Software Inventory

< Inventory information should include type of system server or hardware, including processors and memory requirements, storage requirements, and any other pertinent information. The software inventory should identify the operating system (including version and service pack levels, and any applications (such as database software), needed to operate the system.>

Manufacturer	Model	Specifications	Quantity	Comments

<In the "Specifications" column, include all information needed to adequately define the item.>

Appendix I: Interconnections Table

<Information for this appendix should be available from the system's system Security Plan (SP). The appropriate information can be copied from the SP, or the appendix can be attached as part of this appendix and reference made here to the appropriate SP section. Include information on all other systems that directly interconnect or exchange information with the system. Include the type of connection, information transferred, and contact person for that system.

If the system does not have any direct interconnections, so state.>

Appendix J: Test and Maintenance Schedule

<All CPs should be reviewed and tested at the frequency specified by the organization (at least annually) or whenever there is a significant system change. In this appendix, provide a schedule for the testing of the system. For low-impact systems, a yearly tabletop exercise is sufficient. The tabletop exercise should include all CP Points of Contact and should be conducted by an outside or impartial observer. A formal test plan should be developed prior to the tabletop exercise, and the exercise and questions developed to include key sections of the CP including a walk-through of the following:

- Notification procedures
- System recovery on an alternate platform from backup media
- Internal and external connectivity
- Reconstitution procedures

Results of the test are documented in an After-Action Report, and Lessons Learned are developed for updating the CP.
The following is a sample annual test and maintenance schedule for a low-impact system:>

Step	Due Date	Responsible Party	Date Scheduled	Date Completed
Identify tabletop facilitator.		Contingency Management Team Leader		
Develop tabletop test plan.		Tabletop Facilitator		
Invite participants.		Tabletop Facilitator		
Conduct tabletop test.		Tabletop Facilitator, Contingency Management Team Leader, POCs		
Finalize after action report and lessons learned.		Contingency Management Team Leader		
Update CP based on lessons learned.		CP Coordinator		
Approve and distribute updated version of CP.		CP Director, CP Coordinator		

Appendix J: Associated Plans, Processes, and Procedures

<Information for this appendix should be available from the system's system Security Plan (SP). The appropriate information can be copied from the SP, or the appendix can be attached as part of this appendix and reference made here to the appropriate SP section. Identify CPs for any other systems that either interconnect or provide support. Identify the current version of the CP, its location, and the primary POC.

Appendix K: Business Impact Analysis

<Include Business Impact Analysis results in this appendix.>