|  |
| --- |
| **{COMMAND}** |
| **{SYSTEM NAME} {ACRONYM}** |
| **System Version: {VERSION}****eMASS# {EMASS#}****Confidentiality: {CONFIDENTIALITY}****Integrity: {INTEGRITY}****Availability: {AVAILABILITY}** |
| **Department of the {SERVICE}** |
| **{LOGO}** |
|  |
| **Information Systems Contingency Plan****Document Version: 1.0.0****{DATE}** |
| Prepared by: {ORGANIZATION}**DISTRIBUTION IS LIMITED TO U.S. GOVERNMENT AGENCIES AND THEIR CONTRACTORS.****OTHER REQUESTS FOR THIS DOCUMENT MUST BE REFERRED TO: {ORGANIZATION}** |

**Change Record**

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Version | Author | Changes Made / Section(s) |
| {DATE} | 1.0.0 | {ORGANIZATION} | Initial Document |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Amplifying Guidance**

1. NIST Special Publication 800-34 Rev. 1, "Contingency Planning Guide for Federal Information Systems" 

**Table** **of Contents**

[1.0 OVERVIEW 1](#_Toc432762844)

[2.0 INTRODUCTION 2](#_Toc432762845)

[2.1 Background 2](#_Toc432762846)

[2.2 Scope 2](#_Toc432762847)

[2.3 Assumptions 2](#_Toc432762848)

[3.0 CONCEPT OF OPERATIONS 3](#_Toc432762849)

[3.1 System Description 3](#_Toc432762850)

[3.1.1 Essential Mission 3](#_Toc432762851)

[3.1.2 Essential Business Function 3](#_Toc432762852)

[3.2 Overview of Three Phases 3](#_Toc432762853)

[3.3 Roles and Responsibilities 4](#_Toc432762854)

[3.3.1 System Owner 4](#_Toc432762855)

[3.3.2 ISCP Coordinator 5](#_Toc432762856)

[3.3.2 Technical Recovery Lead 5](#_Toc432762857)

[4.0 ACTIVATION AND NOTIFICATION 6](#_Toc432762858)

[4.1 Activation Criteria and Procedure 6](#_Toc432762859)

[4.2 Notification 6](#_Toc432762860)

[4.3 Outage Assessment 6](#_Toc432762861)

[5.0 RECOVERY 7](#_Toc432762862)

[5.1 Sequence of Recovery Activities 7](#_Toc432762863)

[5.2 Recovery Procedures 7](#_Toc432762864)

[5.2.1 Recovery After a Disruption 7](#_Toc432762865)

[5.2.2 Recovery After a Compromise 7](#_Toc432762866)

[5.2.3 Recovery After a Failure 7](#_Toc432762867)

[5.2.4 Transaction Recovery 7](#_Toc432762868)

[5.3 Recovery Escalation Notices/Awareness 8](#_Toc432762869)

[6.0 RECONSTITUTION 8](#_Toc432762870)

[6.1 Validation Testing 8](#_Toc432762871)

[6.2 Recovery Declaration 8](#_Toc432762872)

[6.3 Notifications (Users) 8](#_Toc432762873)

[6.5 Data Backup 8](#_Toc432762874)

[6.6 Event Documentation 8](#_Toc432762875)

[6.8 Deactivation 9](#_Toc432762876)

[APPENDIX A – PERSONNEL CONTACT LIST 10](#_Toc432762877)

[APPENDIX B – VENDOR CONTACT LIST 12](#_Toc432762878)

[APPENDIX C – DETAILED BACKUP AND RECOVERY PROCEDURES 14](#_Toc432762879)

[C.1.0 Built-in Windows Backup/Restore 15](#_Toc432762880)

[C.1.1 Windows Backup 15](#_Toc432762881)

[C.1.2 Windows Restore 15](#_Toc432762882)

[APPENDIX D – ALTERNATE PROCESSING PROCEDURES 17](#_Toc432762883)

[APPENDIX E – SYSTEM VALIDATION TEST PLAN 20](#_Toc432762884)

[APPENDIX F – TEST AND MAINTENANCE SCHEDULE 22](#_Toc432762885)

[APPENDIX G – LESSONS LEARNED / AFTER ACTION REPORTS 24](#_Toc432762886)

[G.1.0 LESSONS LEARNED 25](#_Toc432762887)

[G.2.0 AFTER ACTIONS REPORTS 25](#_Toc432762888)

[G.3.0 METRICS 26](#_Toc432762889)

[APPENDIX H – BUSINESS IMPACT ANALYSIS 28](#_Toc432762890)

[APPENDIX I – DETAILED COMPLIANCE MATRIX 30](#_Toc432762891)

[ENCLOSURE 1 – CONTINGENCY PLAN TEST REPORT TEMPLATE 67](#_Toc432762892)

[ENCLOSURE 2 – AFTER ACTIONS REPORT TEMPLATE 69](#_Toc432762893)

[ENCLOSURE 3 – TRAINING RESOURCES 71](#_Toc432762894)

[Figure 1 - Three Phases 4](#_Toc432677062)

[Table 1 - SP-800-53v4 Compliance Matrix 2](#_Toc432762897)

[Table 2 - Key Personnel List 11](#_Toc432762898)

[Table 3 - Vendor Contact List 13](#_Toc432762899)

[Table 4 - System Validation Procedures 21](#_Toc432762900)

[Table 5 - Test and Maintenance Schedule 23](#_Toc432762901)

[Table 6 - Metrics 27](#_Toc432762902)

# **OVERVIEW**

Information systems are vital elements in most mission/business processes. Because information system resources are so essential to an organization’s success, it is critical that identified services provided by these systems are able to operate effectively without excessive interruption. Contingency planning supports this requirement by establishing thorough plans, procedures, and technical measures that can enable a system to be recovered as quickly and effectively as possible following a service disruption. Contingency planning is unique to each system, providing preventive measures, recovery strategies, and technical considerations appropriate to the system’s information confidentiality, integrity, and availability requirements and the system impact level.

This document does not address facility-level information system planning (commonly referred to as a disaster recovery plan) or organizational mission continuity (commonly referred to as a continuity of operations [COOP] plan) except where it is required to restore information systems and their processing capabilities. Nor does this document address continuity of mission/business processes

Information system contingency planning refers to a coordinated strategy involving plans, procedures, and technical measures that enable the recovery of information systems, operations, and data after a disruption. Contingency planning generally includes one or more of the following approaches to restore disrupted services:

1. Restoring information systems using alternate equipment;
2. Performing some or all of the affected business processes using alternate processing (manual) means (typically acceptable for only short-term disruptions);
3. Recovering information systems operations at an alternate location (typically acceptable for only long–term disruptions or those physically impacting the facility); and
4. Implementing of appropriate contingency planning controls based on the information system’s security impact level.

This document complies with the following requirements from NIST Special Publication 800-53 Revision 4, "Security and Privacy Controls for Federal Information Systems and Organizations". A detailed compliance matrix can be found in [Appendix I, “Detailed Compliance Matrix”](#_APPENDIX_I_–).

| CNTL NO. | CONTROL NAME | PRIORITY | LOW | MOD | HIGH |
| --- | --- | --- | --- | --- | --- |
| [CP-1](#CP1) | Contingency Planning Policy and Procedures | P1 | CP-1 | CP-1 | CP-1 |
| [CP-2](#CP2) | Contingency Plan | P1 | CP-2 | CP-2 (1) (3) (8) | CP-2 (1) (2) (3) (4) (5) (8) |
| [CP-3](#CP3) | Contingency Training | P2 | CP-3 | CP-3 | CP-3 (1) |
| [CP-4](#CP4) | Contingency Plan Testing | P2 | CP-4 | CP-4 (1) | CP-4 (1) (2) |
| CP-5 | Contingency Plan Update | N/A | Not Selected  | Not Selected  | Not Selected  |
| [CP-6](#CP6) | Alternate Storage Site | P1 | Not Selected  | CP-6 (1) (3) | CP-6 (1) (2) (3) |
| [CP-7](#CP7) | Alternate Processing Site | P1 | Not Selected  | CP-7 (1) (2) (3) | CP-7 (1) (2) (3) (4) |
| [CP-8](#CP8) | Telecommunications Services | P1 | Not Selected  | CP-8 (1) (2) | CP-8 (1) (2) (3) (4) |
| [CP-9](#CP9) | Information System Backup | P1 | CP-9 | CP-9 (1) | CP-9 (1) (2) (3) (5) |
| [CP-10](#CP10) | Information System Recovery and Reconstitution | P1 | CP-10 | CP-10 (2) | CP-10 (2) (4) |
| [CP-11](#CP11) | Alternate Communications Protocols | P0 | Not Selected  | Not Selected  | Not Selected  |
| [CP-12](#CP12) | Safe Mode | P0 | Not Selected  | Not Selected  | Not Selected  |
| [CP-13](#CP13) | Alternative Security Mechanisms | P0 | Not Selected | CP-1 | CP-1 |

Table 1 - SP-800-53v4 Compliance Matrix

# **INTRODUCTION**

Information assets are vital to {ACRONYM}’s mission/business processes; therefore, it is critical that services provided by {ACRONYM} are able to operate effectively without excessive interruption. This Information System Contingency Plan (ISCP) establishes comprehensive procedures to recover {ACRONYM} quickly and effectively following a service disruption.

## **2.1 Background**

This {ACRONYM} ISCP establishes procedures to recover {ACRONYM} following a disruption. The following recovery plan objectives have been established:

1. Maximize the effectiveness of contingency operations through an established plan that consists of the following phases:
	1. Activation and Notification phase to activate the plan and determine the extent of damage;
	2. Recovery phase to restore {ACRONYM} operations; and
	3. Reconstitution phase to ensure that {ACRONYM} is validated through testing and that normal operations are resumed.
2. Identify the activities, resources, and procedures to carry out {ACRONYM} processing requirements during prolonged interruptions to normal operations.
3. Assign responsibilities to designated {ACRONYM} personnel and provide guidance for recovering {ACRONYM} during prolonged periods of interruption to normal operations.
4. Ensure coordination with other personnel responsible for {ACRONYM} contingency planning strategies. Ensure coordination with external points of contact and vendors associated with {ACRONYM} and execution of this plan.

## **2.2 Scope**

This ISCP has been developed for {ACRONYM}, which is classified as an **Availability = LOW** impact system, in accordance with Federal Information Processing Standards (FIPS) 199 – Standards for Security Categorization of Federal Information and Information Systems. Procedures in this ISCP are for Low- Impact systems and designed to recover {ACRONYM} within {RTO DAYS}. This plan does not address replacement or purchase of new equipment, short-term disruptions lasting less than {RTO DAYS}; or loss of data at the onsite facility or at the user-desktop levels. As {ACRONYM} is a low-impact system, alternate data storage and alternate site processing are not required.

## **2.3 Assumptions**

The following assumptions were used when developing this ISCP:

* {ACRONYM} has been established as a low-impact system for Availability purposes, in accordance with FIPS 199.
* Alternate processing sites and offsite storage are not required for this system.
* The {ACRONYM} is inoperable and cannot be recovered within {RTO DAYS}.
* Key {ACRONYM} personnel have been identified and trained in their emergency response and recovery roles; they are available to activate the {ACRONYM} Contingency Plan.

The {ACRONYM}ISCP does not apply to 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 mission/business operations.
* Emergency evacuation of personnel.The Occupant Emergency Plan (OEP) addresses employee evacuation

# **CONCEPT OF OPERATIONS**

The Concept of Operations section provides details about {ACRONYM}, an overview of the three phases of the ISCP (Activation and Notification, Recovery, and Reconstitution), and a description of roles and responsibilities of {ACRONYM}’s personnel during a contingency activation

## **3.1 System Description**

{SYSTEM DESCRIPTION}

The {ACRONYM}’s hardware, software, architecture and diagrams can be found in the System Security Plan (SSP), which is available within eMASS.

### **3.1.1 Essential Mission**

{ESSENTIAL MISSION}

### **3.1.2 Essential Business Function**

{ESSENTIAL BUSINESS FUNCTION}

## **3.2 Overview of Three Phases**

This ISCP has been developed to recover and reconstitute the {ACRONYM} using a three-phased approach. This approach ensures that system recovery and reconstitution efforts are performed in a methodical sequence to maximize the effectiveness of the recovery and reconstitution efforts and minimize system outage time due to errors and omissions. The three system recovery phases are:



Figure 1 - Three Phases

**Activation and Notification Phase.** Activation of the ISCP occurs after a disruption or outage that may reasonably extend beyond the RTO established for a system. The outage event may result in severe damage to the facility that houses the system, severe damage or loss of equipment, or other damage that typically results in long-term loss.

Once the ISCP is activated, system owners and users are notified of a possible long-term outage, and a thorough outage assessment is performed for the system. Information from the outage assessment is presented to system owners and may be used to modify recovery procedures specific to the cause of the outage.

**Recovery Phase.** The Recovery phase details the activities and procedures for recovery of the affected system. Activities and procedures are written at a level that an appropriately skilled technician can recover the system without intimate system knowledge. This phase includes notification and awareness escalation procedures for communication of recovery status to system owners and users.

**Reconstitution Phase.** The Reconstitution phase defines the actions taken to test and validate system capability and functionality at the original or new permanent location. This phase consists of two major activities: validating successful reconstitution and deactivation of the plan.

During validation, the system is tested and validated as operational prior to returning operation to its normal state. Validation procedures may include functionality or regression testing, concurrent processing, and/or data validation. The system is declared recovered and operational by system owners upon successful completion of validation testing.

Deactivation includes activities to notify users of system operational status. This phase also addresses recovery effort documentation, activity log finalization, incorporation of lessons learned into plan updates, and readying resources for any future events.

## **3.3 Roles and Responsibilities**

The ISCP establishes several roles for {ACRONYM} recovery and reconstitution support. Persons or teams assigned ISCP roles have been trained to respond to a contingency event affecting {ACRONYM}.

### **3.3.1 System Owner**

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. Following are their responsibilities:

* Pre-event
	+ Approve the plan
	+ Ensure the plan is maintained
	+ Ensure training is conducted
	+ Authorize periodic plan testing exercises
	+ Support the Technical Recovery Lead 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
	+ Manage and monitor the overall recovery process
	+ Periodically advise senior staff, customers, and media relations personnel of the status
	+ Support the ISCP Coordinator and all other participants during debilitating conditions/situations

### **3.3.2 ISCP Coordinator**

This individual is responsible for managing the total recovery effort; for ensuring that other personnel perform all checklist items and for coordination and overall communications. Following are their responsibilities:

* 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
	+ Assist in damage assessment
	+ Coordinate activities of recovery team members
	+ Periodically report to the System Owner the status of recovery efforts and details as required

### **3.3.2 Technical Recovery Lead**

This individual has a full understanding of the technical aspects of the system. Following are their responsibilities:

* Pre-event
	+ Assist the ISCP Coordinator as directed
	+ Participate in contingency exercises
	+ Understand all CP roles and responsibilities
* Post-event
	+ Perform restoration functions
	+ Maintain a record of all communications

# **4.0 ACTIVATION AND NOTIFICATION**

The Activation and Notification Phase defines initial actions taken once a {ACRONYM}disruption has been detected or appears to be imminent. This phase includes activities to notify recovery personnel, conduct an outage assessment, and activate the ISCP. At the completion of the Activation and Notification Phase, {ACRONYM}ISCP staff will be prepared to perform recovery measures.

## **4.1 Activation Criteria and Procedure**

The {ACRONYM} ISCP may be activated if one or more of the following criteria are met:

1. The type of outage indicates {ACRONYM} will be down for more than {RTO DAYS};
2. The facility housing {ACRONYM} is damaged and may not be available within {RTO DAYS}; and

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

* System Owner
* ISCP Coordinator
* Technical Recovery Lead

## **4.2 Notification**

The first step upon activation of the {ACRONYM} ISCP is notification of appropriate mission/business and system support personnel. Contact information for appropriate POCs is included in [Appendix A, “Personnel Contact List”](#_APPENDIX_A_–).

For {ACRONYM}, the following method and procedure for notifications can be used:

* Phone Call
* Email
* In-person

As stated previously, any role within the process can execute initial notification.

## **4.3 Outage Assessment**

Following notification, a thorough outage assessment is necessary to determine the extent of the disruption, any damage, and expected recovery time. Assessment results are provided to the ISCP Coordinator to assist in the coordination of the recovery of {ACRONYM}.

The following procedures will be followed:

* Determines if there has been loss of life or injuries
* Assesses the extent of damage to the facilities and the information systems
* Estimates the time to recover operations
* Determines accessibility to facility, building, offices, and work areas
* Assess the need for and adequacy of physical security/guards
* Advises the ISCP Coordinator that physical security/guards are required
* Identify salvageable hardware
* Maintain a log/record of all salvageable equipment
* Estimates levels of outside assistance required
* Report updates, status, and recommendations to the ISCP Coordinator

# **5.0 RECOVERY**

The Recovery Phase provides formal recovery operations that begin after the ISCP has been activated, outage assessments have been completed (if possible), personnel have been notified, and appropriate teams have been mobilized. The following Recovery Objectives have been identified:

1. restore system capabilities
2. repair damage
3. resume operational capabilities at the original location

At the completion of the Recovery Phase, {ACRONYM} will be functional and capable of performing the functions identified in Section 3.1 of this plan.

## **5.1 Sequence of Recovery Activities**

The following activities occur during recovery of {ACRONYM}:

1. Identify recovery location (if not at original location);
2. Identify required resources to perform recovery procedures;
3. Retrieve backup and system installation media;
4. Recover hardware and operating system (if required); and
5. Recover system from backup and system installation media.

## **5.2 Recovery Procedures**

Recovery procedures are outlined in [Appendix C, “Detailed Backup and Recovery Procedures”](#_APPENDIX_C_–) and will be executed in the sequence presented to maintain an efficient recovery effort.

### **5.2.1 Recovery After a Disruption**

Recovery procedures are outlined in [Appendix C, “Detailed Backup and Recovery Procedures”](#_APPENDIX_C_–). In the event of a disruption, the System Owner will execute the following:

* [System Validation Test Plan](#_APPENDIX_E_–)
* Create [Lessons Learned and After Actions Reports](#_APPENDIX_G_–_1)
* Update the [Test and Maintenance Schedule](#_APPENDIX_F_–) to reflect the real-world event

### **5.2.2 Recovery After a Compromise**

Recovery procedures are outlined in [Appendix C, “Detailed Backup and Recovery Procedures”](#_APPENDIX_C_–). In the event of a security incident or compromise, the Incident Response Plan (IRP) will be followed and the IRP and Contingency Planning teams will coordinate recovery objectives and requirements together.

### **5.2.3 Recovery After a Failure**

Recovery procedures are outlined in [Appendix C, “Detailed Backup and Recovery Procedures”](#_APPENDIX_C_–). In the event of a failure that requires the purchase of new and/or additional equipment, the System Owner will start the purchase request process.

### **5.2.4 Transaction Recovery**

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. This requirement is only applicable to the above system types.

Is the system transaction based or contain a database management system?

|  |
| --- |
|[x]  No |
|[ ]  Yes**{Delete, or describe how transactions are recovered}** |

## **5.3 Recovery Escalation Notices/Awareness**

During the Recovery Process, it is extremely important to keep both senior management and the general user population aware of all activities and status. The ISCP Coordinator is responsible for communicating status through either phone, email or in-person to the general user population. If the outage escalates and potentially causes outages to other systems or networks, the ISCP Coordinator will up-channel reporting to the CIO so that other teams are notified.

# **6.0 RECONSTITUTION**

Reconstitution is the process by which recovery activities are completed and normal system operations are resumed. If the original facility is unrecoverable, the activities in this phase can also be applied to preparing a new permanent location to support system processing requirements. A determination must be made on 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 plan.

## **6.1 Validation Testing**

Validation data testing is the process of testing and validating data to ensure that data files have been recovered completely at the permanent location and the system is ready to return to normal operations. Procedures are located in [Appendix E, “System Validation Test Plan”](#_APPENDIX_E_–).

## **6.2 Recovery Declaration**

Upon successfully completing testing and validation, the {ACRONYM} will formally declare recovery efforts complete, and that {ACRONYM} is in normal operations. {ACRONYM} business and technical POCs will be notified of the declaration by the ISCP Coordinator.

## **6.3 Notifications (Users)**

Upon return to normal system operations, {ACRONYM} users will be notified by the System Owner or ISCP Coordinator using predetermined notification procedures (e.g., email, phone calls, etc.).

## **6.5 Data Backup**

As soon as reasonable following recovery, the system should 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 located in [Appendix C, “Detailed Backup and Recovery Procedures”](#_APPENDIX_C_–).

## **6.6 Event Documentation**

It is important that all recovery events be well-documented, including actions taken and problems encountered during the recovery and reconstitution effort, and lessons learned for inclusion and update to this ISCP. It is the responsibility of each ISCP team or person to document their actions during the recovery and reconstitution effort, and to provide that documentation to the ISCP Coordinator. The process contained within [Appendix G, “Lessons Learned and After Action Reports”](#_APPENDIX_G_–_1) will be followed.

## **6.8 Deactivation**

Once all activities have been completed and documentation has been updated, the {ACRONYM} will formally deactivate the ISCP recovery and reconstitution effort. Notification of this declaration will be provided to all business and technical POCs.

# **APPENDIX A – PERSONNEL CONTACT LIST**

|  |
| --- |
| ISCP Key Personnel |
| Key Personnel | Contact Information |
| System Owner | Work | *Insert number* |
| *Insert Name and Title* | Home | *Insert number* |
| *Insert Street Address* | Cellular | *Insert number* |
| *Insert City, State, and Zip Code* | Email | *Insert email address* |
| ISCP Coordinator | Work | *Insert number* |
| *Insert Name and Title* | Home | *Insert number* |
| *Insert Street Address* | Cellular | *Insert number* |
| *Insert City, State, and Zip Code* | Email | *Insert email address* |
| Technical Recovery Lead | Work | *Insert number* |
| *Insert Name and Title* | Home | *Insert number* |
| *Insert Street Address* | Cellular | *Insert number* |
| *Insert City, State, and Zip Code* | Email | *Insert email address* |

Table 2 - Key Personnel List

# **APPENDIX B – VENDOR CONTACT LIST**

|  |  |  |
| --- | --- | --- |
| Vendor Name | Phone Number | Contract Number |
| Symantec NetBackup | 1-888-358-7658 |  |
| Red Hat | 1-888-467-3342 |  |
| Microsoft Support | 1-800-936-4900 |  |
| Dell Support | 1-800-945-3355 |  |

Table 3 - Vendor Contact List

# **APPENDIX C – DETAILED BACKUP AND RECOVERY PROCEDURES**

# **C.1.0 Built-in Windows Backup/Restore**

## **C.1.1 Windows Backup**

Windows Backup uses the built-in Microsoft tools.

1. Open Backup and Restore by navigating to Control Panel, clicking System and Maintenance, and then clicking Backup and Restore.
2. Do one of the following:
	* If you've never used Windows Backup before, click Set up backup, and then follow the steps in the wizard.
	* If you've created a backup before, you can wait for your regularly scheduled backup to occur, or you can manually create a new backup by clicking Back up now.

**To create a new, full backup**

After you create your first backup, Windows Backup will add new or changed information to your subsequent backups. If you're saving your backups on a hard drive or network location, Windows Backup will create a new, full backup for you automatically when needed. If you're saving your backups on CDs or DVDs and can't find an existing backup disc, or if you want to create a new backup of all of the files on your computer, you can create a full backup. Here's how to create a full backup:

1. Open Backup and Restore by navigating to Control Panel, clicking System and Maintenance, and then clicking Backup and Restore.
2. In the left pane, click Create new, full backup.

## **C.1.2 Windows Restore**

Windows Restore uses the built-in Microsoft tools.

You can restore backed-up versions of files that are lost, damaged, or changed accidentally. You also restore individual files, groups of files, or all of the files that you've backed up.

1. Open Backup and Restore by navigating to Control Panel, clicking System and Maintenance, and then clicking Backup and Restore.
2. Do one of the following:
	* To restore your files, click Restore my files.
	* To restore the files of all users, click Restore all users' files.
3. Do one of the following:
	* To browse the contents of the backup, click Browse for files or Browse for folders.

When you're browsing for folders, you won't be able to see the individual files in a folder. To view individual files, use the Browse for files option.

* + To search the contents of the backup, click Search, type all or part of a file name, and then click Search.

**To restore a backup made on another computer**

You can restore files from a backup that was created on another computer running Windows.

1. Open Backup and Restore by navigating to **Control Panel**, clicking **System and Maintenance**, and then clicking **Backup and Restore**.
2. Click **Select another backup to restore files from**, and then follow the steps in the wizard.

**To find files that were restored from a backup made on another computer**

If you're restoring files from a backup that was made on another computer, the files will be restored in a folder under the user name that was used to create the backup. If the user names are different, you'll need to navigate to the folder where the files are restored. For example, if your user name was **Molly** on the computer that the backup was made on but your user name is **MollyC** on the computer that the backup is being restored on, the restored files will be saved in a folder labelled **Molly**. You can find the restored files by following these steps:

1. Open Computer by clicking clicking **Computer**.
2. Double-click the icon of the drive that the files are saved on, for example C:\.
3. Double-click the **Users** folder.

You will see a folder for each user account.

1. Double-click the folder for the user name that was used to create the backup.

The restored files will be in the various folders based on where they were located originally.

**To restore files from a file backup after restoring your computer from a system image backup**

After you restore your computer from a system image backup, there might be newer versions of some of your files in a file backup that you want to restore. Because you've reverted your computer to the state that it was in at the time the system image backup was created, Windows Backup won't show any file backups in the Restore Files wizard that were created after the system image backup was created. To restore files from a file backup that was created after the system image backup was created, follow these steps:

1. Open Backup and Restore by navigating to Control Panel, clicking System and Maintenance, and then clicking Backup and Restore.
2. Click Select another backup to restore files from.
3. In the Backup Period, select the date range of the backup that contains the files that you want to restore, and then follow the steps in the wizard

# **APPENDIX D – ALTERNATE PROCESSING PROCEDURES**

This section identifies alternate manual or technical processing procedures available that allow the business unit to continue some processing of information that would normally be done by the affected system.

**Information System Disruption**

Maintaining Essential Mission. {ACRONYM} is not considered Mission Essential. During a Contingency Event, unaffected assets will continue work as before. For affected assets, if they are a higher priority than the currently operational assets then operational assets will be re-purposed to prioritize continuing mission. In the event the full system is impacted for more than {RTO DAYS}, the System Owner will contact the Program sponsor to activate the overarching Business Continuity Plan, which is outside the scope of this document.

Maintaining Business Functions. During a Contingency Event, unaffected assets will continue work as before. For affected assets, if they are a higher priority than the currently operational assets then operational assets will be re-purposed to prioritize continuing mission. In the event the full system is impacted for more than {RTO DAYS}, the System Owner will contact the Program sponsor to activate the overarching Business Continuity Plan, which is outside the scope of this document. All documentation, meetings and face-to-face communications will continue to occur.

**Information System Compromise**

Maintaining Essential Mission. {ACRONYM} is not considered Mission Essential. During a Contingency Event, unaffected assets will continue work as before. For affected assets, if they are a higher priority than the currently operational assets then operational assets will be re-purposed to prioritize continuing mission. In the event the full system is impacted for more than {RTO DAYS}, the System Owner will contact the Program sponsor to activate the overarching Business Continuity Plan, which is outside the scope of this document.

Maintaining Business Functions. During a Contingency Event, unaffected assets will continue work as before. For affected assets, if they are a higher priority than the currently operational assets then operational assets will be re-purposed to prioritize continuing mission. In the event the full system is impacted for more than {RTO DAYS}, the System Owner will contact the Program sponsor to activate the overarching Business Continuity Plan, which is outside the scope of this document. All documentation, meetings and face-to-face communications will continue to occur.

**Information System Failure**

Maintaining Essential Mission. {ACRONYM} is not considered Mission Essential. During a Contingency Event, unaffected assets will continue work as before. For affected assets, if they are a higher priority than the currently operational assets then operational assets will be re-purposed to prioritize continuing mission. In the event the full system is impacted for more than {RTO DAYS}, the System Owner will contact the Program sponsor to activate the overarching Business Continuity Plan, which is outside the scope of this document.

Maintaining Business Functions. During a Contingency Event, unaffected assets will continue work as before. For affected assets, if they are a higher priority than the currently operational assets then operational assets will be re-purposed to prioritize continuing mission. In the event the full system is impacted for more than {RTO DAYS}, the System Owner will contact the Program sponsor to activate the overarching Business Continuity Plan, which is outside the scope of this document. All documentation, meetings and face-to-face communications will continue to occur.

# **APPENDIX E – SYSTEM VALIDATION TEST PLAN**

This appendix includes system acceptance procedures that are performed after the system has been recovered and prior to putting the system into full operation and returned to users.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Procedure | Expected Result | Actual Result | Successful? | Performed By |
| Apply power | System boots through POST and user is presented with logon screen. |  |  |  |
| Perform Logon | Administrator gains access to the system |  |  |  |
| Restore system | Backup files/image/media applied to system |  |  |  |
| Perform connectivity checks | System has required network connectivity. Initial verification through PING |  |  |  |
| Perform functional checks | General users have system access and do not report access or work-related Helpdesk tickets. |  |  |  |
| Perform ACAS Scan | Credentialed scans performed that verify the current system compliance level with the POA&M |  |  |  |
| Perform SCAP Scan | Credentialed scans performed that verify the current system compliance level with the POA&M |  |  |  |

Table 4 - System Validation Procedures

# **APPENDIX F – TEST AND MAINTENANCE SCHEDULE**

The ISCP will be reviewed and tested yearly or whenever there is a significant change to the system. For low-impact systems, a yearly tabletop exercise is sufficient. The following table details the review and testing.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Step | Date Due by | Responsible Party | Date Scheduled | Date Held |
| Identify tabletop facilitator. |  | System Owner |  |  |
| Develop tabletop test plan. |  | ISCP Coordinator |  |  |
| Invite participants. |  | ISCP Coordinator |  |  |
| Conduct tabletop test. |  | ISCP, POCs |  |  |
| Finalize after action report and lessons learned. |  | ISCP Coordinator |  |  |
| Update ISCP based on lessons learned. |  | ISCP Coordinator |  |  |
| Approve and distribute updated version of ISCP. |  | System Owner |  |  |

Table 5 - Test and Maintenance Schedule

# **APPENDIX G – LESSONS LEARNED / AFTER ACTION REPORTS**

# **G.1.0 LESSONS LEARNED**

One of the most important parts of contingency planning is also the most often omitted: learning and improving. The {ACRONYM} contingency planning team will evolve to reflect new threats, improved technology, and lessons learned. Holding a “lessons learned” meeting with all involved parties after a major contingency, and optionally periodically after lesser contingencies as resources permit, can be extremely helpful in improving security measures and the contingency planning process itself. Multiple contingencies can be covered in a single lessons learned meeting. This meeting provides a chance to achieve closure with respect to a contingency by reviewing what occurred, what was done to intervene, and how well intervention worked. The meeting should be held within several days of the end of the contingency. Questions to be answered in the meeting include:

1. Exactly what happened, and at what times?
2. How well did staff and management perform in dealing with the contingency? Were the documented procedures followed? Were they adequate?
3. What information was needed sooner?
4. Were any steps or actions taken that might have inhibited the recovery?
5. What would the staff and management do differently the next time a similar contingency occurs?
6. How could information sharing with other organizations have been improved?
7. What corrective actions can prevent similar contingency in the future?
8. What precursors or indicators should be watched for in the future to detect similar contingencies?
9. What additional tools or resources are needed to detect, analyze, and mitigate future contingencies?

Small contingencies s need limited post- contingency analysis, with the exception of contingencies s performed through new attack methods that are of widespread concern and interest. After serious attacks have occurred, it is usually worthwhile to hold post-mortem meetings that cross team and organizational boundaries to provide a mechanism for information sharing. The primary consideration in holding such meetings is ensuring that the right people are involved. Not only is it important to invite people who have been involved in the contingency that is being analyzed, but also it is wise to consider who should be invited for the purpose of facilitating future cooperation.

The success of such meetings also depends on the agenda. Collecting input about expectations and needs (including suggested topics to cover) from participants before the meeting increases the likelihood that the participants’ needs will be met. In addition, establishing rules of order before or during the start of a meeting can minimize confusion and discord. Having one or more moderators who are skilled in group facilitation can yield a high payoff. Finally, it is also important to document the major points of agreement and action items and to communicate them to parties who could not attend the meeting.

Because of the changing nature of information technology and changes in personnel, the contingency planning team will review all related documentation and procedures for handling contingencies s at designated intervals.

# **G.2.0 AFTER ACTIONS REPORTS**

The After Actions Report (AAR) provides evaluation criteria based on the exercise objectives and a means to evaluate how well exercise objectives were met, and identify areas where additional exercises might be necessary. Evaluating the exercise is a critical step to ensuring success of the contingency response program. After the test or exercise is complete, the participants will conduct a debriefing to discuss observations for things that worked well and things that could be improved. The comments that surface during the debriefing, along with lessons learned documented during the exercise, will be captured in the AAR. The AAR will also document observations made throughout the exercise and participants during the exercise and recommendations for enhancing the IR plan that was exercised.

The template used to document the AAR can be found in [Enclosure 2, “After Actions Report Template”](#_ENCLOSURE_2_–_1).

# **G.3.0 METRICS**

The {ACRONYM} contingency planning team will collect the below data, which will be used to measure the success of the contingency team:

| Data | Description |
| --- | --- |
| Number of contingencies Handled | Handling more contingencies is not necessarily better—for example, the number of contingencies handled may decrease because of better network and host security controls, not because of negligence by the contingency planning team. The number of contingencies handled is best taken as a measure of the relative amount of work that the contingency planning team had to perform, not as a measure of the quality of the team, unless it is considered in the context of other measures that collectively give an indication of work quality. It is more effective to produce separate contingency counts for each contingency category. Subcategories also can be used to provide more information.  |
| Time per Contingency | For each contingency, time can be measured in several ways:1. Total amount of labor spent working on the contingency
2. Elapsed time from the beginning of the contingency to contingency discovery, to the initial impact assessment, and to each stage of the contingency handling process (e.g., containment, recovery)
3. How long it took the contingency planning team to respond to the initial report of the contingency
4. How long it took to report the contingency to management and, if necessary, appropriate external entities (e.g., Tier-2).
 |
| Objective Assessment of each Contingency | The response to a contingency that has been resolved can be analyzed to determine how effective it was. The following are examples of performing an objective assessment of a contingency:1. Reviewing logs, forms, reports, and other contingency documentation for adherence to established contingency planning policies and procedures
2. Identifying which precursors and indicators of the contingency were recorded to determine how effectively the contingency was logged and identified
3. Determining if the contingency caused damage before it was detected
4. Determining if the actual cause of the contingency was identified
5. Determining if the contingency is a recurrence of a previous contingency
6. Calculating the estimated monetary damage from the contingency
7. Measuring the difference between the initial impact assessment and the final impact assessment
8. Identifying which measures, if any, could have prevented the contingency.
 |
| Subjective Assessment of each Contingency | Contingency Planning team members may be asked to assess their own performance, as well as that of other team members and of the entire team. Another valuable source of input is the owner of a resource that was attacked, in order to determine if the owner thinks the contingency was handled efficiently and if the outcome was satisfactory. |

Table 6 - Metrics

# **APPENDIX H – BUSINESS IMPACT ANALYSIS**

.

|  |
| --- |
| **Business Impact Analysis (BIA)** |
| **Organization:** {ACRONYM} | **Date BIA Completed:** {DATE} |
| **System Name:** {ACRONYM} | **BIA POC:** {POC} |
| **System Manager POC:** {POC} |
| ***System Description:*** {SYSTEM DESCRIPTION} |
| 1. **Identify System POCs**
 | **Role** |
| ***Internal {Identify the individuals, positions, or offices within your organization that depend on or support the system; also specify their relationship to the system}***  |
| {PERSONNEL} | {ROLE} |
| **B. Identify System Resources *{Identify the specific hardware, software, and other resources that comprise the system; include quantity and type}***  |
| **Hardware:** | Listed in SSP |
| **Software:** | Listed in SSP |
| **C. Identify critical roles *{List the roles identified in Section A that are deemed critical}***  |
| **Critical Role:**System OwnerISCP CoordinatorTechnical Recovery Lead | **Critical Resource:**{POC}{POC}{POC} |
| **E. Identify outage impacts and allowable outage times *{Characterize the impact on critical roles if a critical resource is unavailable; also, identify the maximum acceptable period that the resource could be unavailable before unacceptable impacts resulted}***  |
| **Resource** | **Outage Impact** | **Allowable Outage Time** |
| {RESOURCE] | {IMPACT} | {RTO DAYS} |
| **F. Prioritize resource recovery *{List the priority associated with recovering a specific resource, based on the outage impacts and allowable outage times provided in Section E. Use quantitative or qualitative scale (e.g., high/medium/low, 1-5, A/B/C)}***  |
| **Resource** | **Recovery Priority** |
| {RESOURCE] | {PRIORITY} |

# **APPENDIX I – DETAILED COMPLIANCE MATRIX**

The following table provides traceability between this document and the Assessment Procedures contained within NIST Special Publication 800-53A Revision 4, "Assessing Security and Privacy Controls in Federal Information Systems and Organizations".

| Control Number | Assessment Number | CCI | Confidentiality | Integrity | Availability | Assessment Procedures | Reference |
| --- | --- | --- | --- | --- | --- | --- | --- |
| CP-1 | CP-1 (a) (1) | CCI-002825 | HighModerateLow | HighModerateLow | HighModerateLow | The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the personnel or roles as all stakeholders identified in the contingency plan. | Automatically compliant with this CCI because they are covered at the DoD level |
| CP-1 | CP-1 (a) (1) | CCI-000438 | HighModerateLow | HighModerateLow | HighModerateLow | DoDI 8500.01 and NIST SP 800-34 meet the DoD requirements for contingency planning policy and procedures. DoD Components are automatically compliant with this control because they are covered by the DoD level policy, DoDI 8500.01 and NIST SP 800-34. | Automatically compliant with this CCI because they are covered at the DoD level |
| CP-1 | CP-1 (a) (1) | CCI-000439 | HighModerateLow | HighModerateLow | HighModerateLow | DoD Components are automatically compliant with this control because they are covered by the DoD level policy, DoDI 8500.01 and NIST SP 800-34. | Automatically compliant with this CCI because they are covered at the DoD level |
| CP-1 | CP-1 (a) (2) | CCI-002826 | HighModerateLow | HighModerateLow | HighModerateLow | The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the personnel or roles as all stakeholders identified in the contingency plan. | Automatically compliant with this CCI because they are covered at the DoD level |
| CP-1 | CP-1 (a) (2) | CCI-000441 | HighModerateLow | HighModerateLow | HighModerateLow | DoDI 8500.01 and NIST SP 800-34 meet the DoD requirements for contingency planning policy and procedures. DoD Components are automatically compliant with this control because they are covered by the DoD level policy, DoDI 8500.01 and NIST SP 800-34. | Automatically compliant with this CCI because they are covered at the DoD level |
| CP-1 | CP-1 (a) (2) | CCI-001597 | HighModerateLow | HighModerateLow | HighModerateLow | DoD Components are automatically compliant with this control because they are covered by the DoD level policy, DoDI 8500.01 and NIST SP 800-34. | Automatically compliant with this CCI because they are covered at the DoD level |
| CP-1 | CP-1 (b) (1) | CCI-000437 | HighModerateLow | HighModerateLow | HighModerateLow | The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as every 5 years. | Automatically compliant with this CCI because they are covered at the DoD level |
| CP-1 | CP-1 (b) (1) | CCI-000440 | HighModerateLow | HighModerateLow | HighModerateLow | DoDI 8500.01 and NIST SP 800-34 meet the DoD requirements for contingency planning policy and procedures. DoD Components are automatically compliant with this control because they are covered by the DoD level policy, DoDI 8500.01 and NIST SP 800-34. | Automatically compliant with this CCI because they are covered at the DoD level |
| CP-1 | CP-1 (b) (2) | CCI-001596 | HighModerateLow | HighModerateLow | HighModerateLow | The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as annually. | Automatically compliant with this CCI because they are covered at the DoD level |
| CP-1 | CP-1 (b) (2) | CCI-001598 | HighModerateLow | HighModerateLow | HighModerateLow | DoDI 8500.01 and NIST SP 800-34 meet the DoD requirements for contingency planning policy and procedures. DoD Components are automatically compliant with this control because they are covered by the DoD level policy, DoDI 8500.01 and NIST SP 800-34. | Automatically compliant with this CCI because they are covered at the DoD level |
| CP-10 | CP-10 | CCI-000550 |   |   | HighModerateLow | The organization conducting the inspection/assessment obtains and examines the contingency plan to ensure it identifies the recovery and reconstitution method for its information system to a known state after a disruption. | [Section 5.2.1](#_5.2.1_Recovery_After) |
| CP-10 | CP-10 | CCI-000551 |   |   | HighModerateLow | The organization conducting the inspection/assessment obtains and examines the contingency plan to ensure it identifies the recovery and reconstitution method for its information system to a known state after a compromise. | [Section 5.2.2](#_5.2.2_Recovery_After) |
| CP-10 | CP-10 | CCI-000552 |   |   | HighModerateLow | The organization conducting the inspection/assessment obtains and examines the contingency plan to ensure it identifies the recovery and reconstitution method for its information system to a known state after a failure. | [Section 5.2.3](#_5.2.3_Recovery_After) |
| CP-10 (2) | CP-10 (2) | CCI-000553 |   | HighModerate | HighModerate | The organization conducting the inspection/assessment obtains and examines the contingency plan test results to verify transaction recovery. | [Section 5.2.4](#_5.2.4_Transaction_Recovery) |
| CP-10 (4) | CP-10 (4) | CCI-000557 |   | High | High | The organization conducting the inspection/assessment obtains and examines contingency plan test results to verify the organization exercises the capability to restore information system components from configuration-controlled and integrity-protected information representing a secure, operational state for the components, and that restoration occurred within the defined time period:1 hour (Availability High )24 hours (Availability Moderate)1 - 5 days (Availability Low) as defined in the contingency plan. | The system is not considered a HIGH level. Therefore, this AP is not applicable. |
| CP-10 (4) | CP-10 (4) | CCI-000556 |   | High | High | The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the time period as 1 hour (Availability High ) 24 hours (Availability Moderate) 1 - 5 days (Availability Low) as defined in the contingency plan. | Automatically compliant with this CCI because they are covered at the DoD level |
| CP-10 (6) | CP-10 (6) | CCI-000560 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines documentation of protection measures to ensure the organization is actively protecting backup and restoration hardware. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| CP-10 (6) | CP-10 (6) | CCI-000561 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines documentation of protection measures to ensure the organization is actively protecting backup and restoration firmware. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| CP-10 (6) | CP-10 (6) | CCI-000562 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines documentation of protection measures to ensure the organization is actively protecting backup and restoration software. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| CP-11 | CP-11 | CCI-002854 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented alternative communications protocols to ensure the organization being inspected/assessed defines the alternative communications protocols the information systems must be capable of providing in support of maintaining continuity of operations. DoD has determined the alternative communications protocols are not appropriate to define at the Enterprise level. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| CP-11 | CP-11 | CCI-002853 | blank | blank | blank | The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to provide the capability to employ alternative communications protocols defined in CP-11, CCI 2854 in support of maintaining continuity of operations. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 2853. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| CP-12 | CP-12 | CCI-002856 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented conditions to ensure the organization being inspected/assessed defines the conditions, that when detected, the information system enters a safe mode of operation with organization-defined restrictions of safe mode of operation.  DoD has determined the conditions are not appropriate to define at the Enterprise level. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| CP-12 | CP-12 | CCI-002857 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented restrictions to ensure the organization being inspected/assessed defines the restrictions of safe mode of operation that the information system will enter when organization-defined conditions are detected. DoD has determined the restrictions on safe mode of operation are not appropriate to define at the Enterprise level. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| CP-12 | CP-12 | CCI-002855 | blank | blank | blank | The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to enter a safe mode of operation with restrictions of safe mode of operation defined in CP-12, CCI 2857 when conditions defined in CP-12, CCI 2856 are detected. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 2855. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| CP-13 | CP-13 | CCI-002858 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed employs alternative or supplemental security mechanisms defined in CP-13, CCI 2859 for satisfying security functions defined in CP-13, CCI 2860 when the primary means of implementing the security function is unavailable or compromised. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| CP-13 | CP-13 | CCI-002859 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented alternative or supplemental security mechanisms to ensure the organization being inspected/assessed defines the alternative or supplemental security mechanisms that will be employed for satisfying organization-defined security functions when the primary means of implementing the security function is unavailable or compromised. DoD has determined the alternative or supplemental security mechanisms are not appropriate to define at the Enterprise level. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| CP-13 | CP-13 | CCI-002860 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented security functions to ensure the organization being inspected/assessed defines the security functions that must be satisfied when the primary means of implementing the security function is unavailable or compromised. DoD has determined the security functions are not appropriate to define at the Enterprise level. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| CP-2 (1) | CP-2 (1) | CCI-000469 |   |   | HighModerate | The organization conducting the inspection/assessment obtains and examines documentation of agreements with entities responsible for the contingency or related plans to ensure there is evidence of coordination of those plans. | The system is not considered a MODERATE or HIGH level for Availability. |
| CP-2 (2) | CP-2 (2) | CCI-000470 |   |   | High | The organization conducting the inspection/assessment obtains and examines the documented capacity planning to ensure that the organization has performed capacity planning. | The system is not considered a HIGH level. Therefore, this AP is not applicable. |
| CP-2 (2) | CP-2 (2) | CCI-000471 |   |   | High | The organization conducting the inspection/assessment obtains and examines the documented capacity planning to ensure that the organization has performed capacity planning. | The system is not considered a HIGH level. Therefore, this AP is not applicable. |
| CP-2 (2) | CP-2 (2) | CCI-000472 |   |   | High | The organization conducting the inspection/assessment obtains and examines the documented capacity planning to ensure that the organization has performed capacity planning. | The system is not considered a HIGH level. Therefore, this AP is not applicable. |
| CP-2 (3) | CP-2 (3) | CCI-000475 |   |   | HighModerate | The organization conducting the inspection/assessment obtains the contingency plan to ensure it contains procedures for resumption of essential missions within 1 hour (Availability High) 12 hours (Availability Moderate) as defined in the contingency plan. | The system is not considered a MODERATE or HIGH level for Availability. |
| CP-2 (3) | CP-2 (3) | CCI-000476 |   |   | HighModerate | The organization conducting the inspection/assessment obtains the contingency plan to ensure it contains procedures for resumption of essential business functions within 1 hour (Availability High) 12 hours (Availability Moderate) as defined in the contingency plan. | The system is not considered a MODERATE or HIGH level for Availability. |
| CP-2 (3) | CP-2 (3) | CCI-000473 |   |   | HighModerate | The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the time period as 1 hour (Availability High ) 12 hours (Availability Moderate) as defined in the contingency plan. | Automatically compliant with this CCI because they are covered at the DoD level |
| CP-2 (3) | CP-2 (3) | CCI-000474 |   |   | HighModerate | The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the time period as 1 hour (Availability High) 12 hours (Availability Moderate) as defined in the contingency plan. | Automatically compliant with this CCI because they are covered at the DoD level |
| CP-2 (4) | CP-2 (4) | CCI-000479 |   |   | High | The organization conducting the inspection/assessment obtains the contingency plan to ensure it contains procedures for full resumption of affected missions within 1 hour (Availability High ) 1-5 days (Availability Moderate) 5-30 days (Availability Low) as defined in the contingency plan. | The system is not considered a HIGH level. Therefore, this AP is not applicable. |
| CP-2 (4) | CP-2 (4) | CCI-000480 |   |   | High | The organization conducting the inspection/assessment obtains the contingency plan to ensure it contains procedures for full resumption of affected business functions within 1 hour (Availability High) 1-5 days (Availability Moderate) 5-30 days (Availability Low) as defined in the contingency plan. | The system is not considered a HIGH level. Therefore, this AP is not applicable. |
| CP-2 (4) | CP-2 (4) | CCI-000477 |   |   | High | The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the time period as 1 hour (Availability High ) 1-5 days (Availability Moderate) 5-30 days (Availability Low) as defined in the contingency plan. | Automatically compliant with this CCI because they are covered at the DoD level |
| CP-2 (4) | CP-2 (4) | CCI-000478 |   |   | High | The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the time period as 1 hour (Availability High ) 1-5 days (Availability Moderate) 5-30 days (Availability Low) as defined in the contingency plan. | Automatically compliant with this CCI because they are covered at the DoD level |
| CP-2 (5) | CP-2 (5) | CCI-000481 |   |   | High | The organization conducting the inspection/assessment obtains and examines the contingency plan to ensure it clearly and accurately documents maintaining essential missions despite an information system disruption for its information system(s). | The system is not considered a HIGH level. Therefore, this AP is not applicable. |
| CP-2 (5) | CP-2 (5) | CCI-000482 |   |   | High | The organization conducting the inspection/assessment obtains and examines the contingency plan to ensure it clearly and accurately documents maintaining essential business functions despite an information system disruption for its information system(s). | The system is not considered a HIGH level. Therefore, this AP is not applicable. |
| CP-2 (5) | CP-2 (5) | CCI-001599 |   |   | High | The organization conducting the inspection/assessment obtains and examines the contingency plan to ensure it documents procedures to sustain operational continuity of essential missions until full information system restoration at primary processing and/or storage sites. | The system is not considered a HIGH level. Therefore, this AP is not applicable. |
| CP-2 (5) | CP-2 (5) | CCI-001600 |   |   | High | The organization conducting the inspection/assessment obtains and examines the contingency plan to ensure it documents procedures to sustain operational continuity of essential business functions until full information system restoration at primary processing and/or storage sites. | The system is not considered a HIGH level. Therefore, this AP is not applicable. |
| CP-2 (6) | CP-2 (6) | CCI-000483 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the continuity plan to ensure the organization being inspected/assessed documents a process to transfer essential missions to alternate processing and/or storage sites with little or no loss of operational continuity. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| CP-2 (6) | CP-2 (6) | CCI-000484 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the continuity plan to ensure the organization being inspected/assessed documents a process to transfer essential business functions to alternate processing and/or storage sites with little or no loss of operational continuity. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| CP-2 (6) | CP-2 (6) | CCI-001601 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the continuity plan to ensure the organization being inspected/assessed documents a process for continuation of essential missions at alternate processing and/or storage sites until information system restoration at primary processing and/or storage sites. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| CP-2 (6) | CP-2 (6) | CCI-001602 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the continuity plan to ensure the organization being inspected/assessed documents a process for continuation of essential business functions at alternate processing and/or storage sites until information system restoration at primary processing and/or storage sites. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| CP-2 (7) | CP-2 (7) | CCI-002827 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines service level agreements and/or memorandums of agreement with external service providers to ensure the organization being inspected/assessed coordinates with those providers. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| CP-2 (8) | CP-2 (8) | CCI-002828 |   |   | HighModerate | The organization conducting the inspection/assessment obtains and examines the documented list of critical information system assets supporting essential missions to ensure the organization being inspected/assessed identifies those assets. | The system is not considered a MODERATE or HIGH level for Availability. |
| CP-2 (8) | CP-2 (8) | CCI-002829 |   |   | HighModerate | The organization conducting the inspection/assessment obtains and examines the documented list of critical information system assets supporting essential business functions to ensure the organization being inspected/assessed identifies those assets. | The system is not considered a MODERATE or HIGH level for Availability. |
| CP-2 | CP-2 (a) (1) | CCI-000443 |   |   | HighModerateLow | The organization conducting the inspection/assessment obtains and examines the contingency plan to ensure it clearly and accurately documents essential missions for its information system(s). | [Section 3.1.1](#_3.1.1_Essential_Mission) |
| CP-2 | CP-2 (a) (1) | CCI-000444 |   |   | HighModerateLow | The organization conducting the inspection/assessment obtains and examines the contingency plan to ensure it clearly and accurately documents essential business functions for its information system(s). | [Section 3.1.2](#_3.1.2_Essential_Business) |
| CP-2 | CP-2 (a) (1) | CCI-000445 |   |   | HighModerateLow | The organization conducting the inspection/assessment obtains and examines the contingency plan to ensure it clearly and accurately documents associated contingency requirements for its information system(s). | This document |
| CP-2 | CP-2 (a) (2) | CCI-000446 |   |   | HighModerateLow | The organization conducting the inspection/assessment obtains and examines the contingency plan to ensure it clearly and accurately documents recovery objectives for its information system(s). | [Section 5](#_5.0_RECOVERY) |
| CP-2 | CP-2 (a) (2) | CCI-000447 |   |   | HighModerateLow | The organization conducting the inspection/assessment obtains and examines the contingency plan to ensure it clearly and accurately documents restoration priorities for its information system(s). | [Appendix H](#_APPENDIX_H_–_1) |
| CP-2 | CP-2 (a) (2) | CCI-000448 |   |   | HighModerateLow | The organization conducting the inspection/assessment obtains and examines the contingency plan to ensure it clearly and accurately documents metrics for its information system(s). | [Appendix G.3.0](#_G.3.0_METRICS) |
| CP-2 | CP-2 (a) (3) | CCI-000449 |   |   | HighModerateLow | The organization conducting the inspection/assessment obtains and examines the contingency plan to ensure it clearly and accurately documents contingency roles, responsibilities, assigned individuals with contact information for its information system(s). | [Section 3.3](#_3.3_Roles_and)[Appendix A](#_APPENDIX_A_–) |
| CP-2 | CP-2 (a) (4) | CCI-000450 |   |   | HighModerateLow | The organization conducting the inspection/assessment obtains and examines the contingency plan to ensure it clearly and accurately documents maintaining essential missions despite an information system disruption for its information system(s). | [Appendix D](#_APPENDIX_D_–) |
| CP-2 | CP-2 (a) (4) | CCI-000451 |   |   | HighModerateLow | The organization conducting the inspection/assessment obtains and examines the contingency plan to ensure it clearly and accurately documents maintaining business functions despite an information system disruption for its information system(s). | [Appendix D](#_APPENDIX_D_–) |
| CP-2 | CP-2 (a) (4) | CCI-000452 |   |   | HighModerateLow | The organization conducting the inspection/assessment obtains and examines the contingency plan to ensure it clearly and accurately documents maintaining essential missions despite an information system compromise for its information system(s). | [Appendix D](#_APPENDIX_D_–) |
| CP-2 | CP-2 (a) (4) | CCI-000453 |   |   | HighModerateLow | The organization conducting the inspection/assessment obtains and examines the contingency plan to ensure it clearly and accurately documents maintaining business functions despite an information system compromise for its information system(s). | [Appendix D](#_APPENDIX_D_–) |
| CP-2 | CP-2 (a) (4) | CCI-000454 |   |   | HighModerateLow | The organization conducting the inspection/assessment obtains and examines the contingency plan to ensure it clearly and accurately documents maintaining essential missions despite an information system failure for its information system(s). | [Appendix D](#_APPENDIX_D_–) |
| CP-2 | CP-2 (a) (4) | CCI-000455 |   |   | HighModerateLow | The organization conducting the inspection/assessment obtains and examines the contingency plan to ensure it clearly and accurately documents maintaining business functions despite an information system failure for its information system(s). | [Appendix D](#_APPENDIX_D_–) |
| CP-2 | CP-2 (a) (5) | CCI-000456 |   |   | HighModerateLow | The organization conducting the inspection/assessment obtains and examines the contingency plan to ensure it clearly and accurately documents eventual, full information system restoration without deterioration of the security safeguards originally planned and implemented for its information system(s). | [Appendix C](#_APPENDIX_C_–) |
| CP-2 | CP-2 (a) (6) | CCI-000457 |   |   | HighModerateLow | The organization conducting the inspection/assessment obtains and examines the audit trail to ensure the contingency plan has been reviewed and approved by at a minimum, the ISSM and ISSO. DoD has defined the personnel or roles as at a minimum, the ISSM and ISSO. | [Signatures](#Signatures) |
| CP-2 | CP-2 (a) (6) | CCI-002830 |   |   | HighModerateLow | The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the personnel or roles as at a minimum, the ISSM and ISSO. | Automatically compliant with this CCI because they are covered at the DoD level |
| CP-2 | CP-2 (b) | CCI-000459 |   |   | HighModerateLow | The organization conducting the inspection/assessment obtains and examines the contingency plan via the inspected organization's information sharing capability (e.g. portal, intranet, email, etc.) to ensure it has been disseminated. | Internal Web Portal (external link) |
| CP-2 | CP-2 (b) | CCI-000458 |   |   | HighModerateLow | The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the list as all stakeholders identified in the contingency plan. | Automatically compliant with this CCI because they are covered at the DoD level |
| CP-2 | CP-2 (c) | CCI-000460 |   |   | HighModerateLow | The organization conducting the inspection/assessment obtains and examines the contingency plan and the incident response plan (IR-8) to ensure theydo not contradict each other's objectives or result in duplicate efforts/activities. | IRP (external artifact) |
| CP-2 | CP-2 (d) | CCI-000462 |   |   | HighModerateLow | The organization conducting the inspection/assessment obtains and examines the audit trail to ensure the contingency plan is reviewed annually. | [Appendix F](#_APPENDIX_F_–) |
| CP-2 | CP-2 (d) | CCI-000461 |   |   | HighModerateLow | The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as annually. | Automatically compliant with this CCI because they are covered at the DoD level |
| CP-2 | CP-2 (e) | CCI-000463 |   |   | HighModerateLow | The organization conducting the inspection/assessment obtains and examines the contingency plan and audit trail to ensure the organization clearly and accurately updates the contingency plan to address organizational changes. | [Change Record](#ChangeRecord) |
| CP-2 | CP-2 (e) | CCI-000464 |   |   | HighModerateLow | The organization conducting the inspection/assessment obtains and examines the contingency plan and audit trail to ensure the organization clearly and accurately updates the contingency plan to address information system changes. | [Change Record](#ChangeRecord) |
| CP-2 | CP-2 (e) | CCI-000465 |   |   | HighModerateLow | The organization conducting the inspection/assessment obtains and examines the contingency plan and audit trail to ensure the organization clearly and accurately revises the contingency plan to address changes to the environment of operation. | [Change Record](#ChangeRecord) |
| CP-2 | CP-2 (e) | CCI-000466 |   |   | HighModerateLow | The organization conducting the inspection/assessment obtains and examines the contingency plan and audit trail to ensure the organization clearly and accurately revises the contingency plan to address problems encountered during contingency plan implementation, execution, or testing. | [Change Record](#ChangeRecord)[Appendix G](#_APPENDIX_G_–_1) |
| CP-2 | CP-2 (f) | CCI-000468 |   |   | HighModerateLow | The organization conducting the inspection/assessment examines the contingency plan via the inspected organization's information sharing capability (e.g. portal, intranet, email, etc.) to ensure the most current version has been communicated. | Internal Web Portal (external link) |
| CP-2 | CP-2 (f) | CCI-002831 |   |   | HighModerateLow | The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the list as all stakeholders identified in the contingency plan | Automatically compliant with this CCI because they are covered at the DoD level |
| CP-2 | CP-2 (g) | CCI-002832 |   |   | HighModerateLow | The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed protects the contingency plan from unauthorized disclosure and modification. | CM in place. Plan stored in eMASS |
| CP-3 (1) | CP-3 (1) | CCI-000488 |   |   | High | The organization conducting the inspection/assessment obtains and examines contingency training materials to ensure that simulated events have been included. | The system is not considered a HIGH level. Therefore, this AP is not applicable. |
| CP-3 (2) | CP-3 (2) | CCI-000489 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the automated mechanism such as scenario-based interactive online training/CBT to verify that it provides a realistic contingency training environment. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| CP-3 | CP-3 (a) | CCI-000486 |   |   | HighModerateLow | The organization conducting the inspection/assessment obtains and examines the list of contingency personnel and documentation of initial contingency training for the purpose of ensuring that all personnel with contingency roles and responsibilities have received initial contingency training at a maximum, 10 working days of assuming a contingency role or responsibility. DoD has defined the time period as at a maximum, 10 working days.  | [Attachment A](#_APPENDIX_A_–)[Enclosure 3](#_ENCLOSURE_3_–) |
| CP-3 | CP-3 (a) | CCI-002833 |   |   | HighModerateLow | The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the time period as at a maximum, 10 working days.  | Automatically compliant with this CCI because they are covered at the DoD level |
| CP-3 | CP-3 (b) | CCI-002834 |   |   | HighModerateLow | The organization conducting the inspection/assessment obtains and examines training materials and documentation of training activities to determine whether the materials are accurate in consideration of the state of the information system and content of the contingency plan. The organization ensures that training is provided to users consistent with assigned roles and responsibilities. | [Section 3.3](#_3.3_Roles_and)[Enclosure 3](#_ENCLOSURE_2_–) |
| CP-3 | CP-3 (c ) | CCI-000487 |   |   | HighModerateLow | The organization conducting the inspection/assessment obtains and examines the list of contingency personnel and documentation of refresher contingency training for the purpose of ensuring that all personnel with contingency roles and responsibilities have received refresher contingency training at least annually. DoD has defined the frequency as at least annually. | [Enclosure 3](#_ENCLOSURE_2_–) |
| CP-3 | CP-3 (c ) | CCI-000485 |   |   | HighModerateLow | The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as at least annually | Automatically compliant with this CCI because they are covered at the DoD level |
| CP-4 (1) | CP-4 (1) | CCI-000498 |   |   | HighModerate | The organization conducting the inspection/assessment obtains and examines documentation of agreements with entities responsible for the contingency or related plans to ensure there is evidence of coordination of those tests. | The system is not considered a MODERATE or HIGH level for Availability. |
| CP-4 (2) | CP-4 (2) (a) | CCI-000500 |   |   | High | The organization conducting the inspection/assessment obtains and examines the record of personnel who participated in the contingency plan testing at the alternate site to ensure the organization being inspected/assessed tests the contingency plan at the alternate processing site to familiarize personnel expected to implement the contingency plan at the alternate site with the facility and available resources. | The system is not considered a HIGH level. Therefore, this AP is not applicable. |
| CP-4 (2) | CP-4 (2) (b) | CCI-002835 |   |   | High | The organization conducting the inspection/assessment obtains and examines the test results to ensure the organization being inspected/assessed tests the contingency plan at the alternate processing site to evaluate the capabilities of the alternate processing site to support contingency operations. | The system is not considered a HIGH level. Therefore, this AP is not applicable. |
| CP-4 (3) | CP-4 (3) | CCI-000502 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the identified automated mechanisms in use to thoroughly test the contingency plan. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| CP-4 (4) | CP-4 (4) | CCI-000504 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the full recovery and reconstitution procedures and contingency plan testing results to ensure all tests were performed IAW CP-2, CCIs 446 and 447. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| CP-4 | CP-4 (a) | CCI-000494 |   |   | HighModerateLow | The organization conducting the inspection/assessment obtains and examines the record of test results to ensure the organization being inspected/assessed conduct tests defined in CP-4, 492 at least annually to determine the effectiveness of the plan and the organizational readiness to execute the plan. DoD has defined the frequency as at least annually. | [Appendix F](#_APPENDIX_F_–) |
| CP-4 | CP-4 (a) | CCI-000492 |   |   | HighModerateLow | The organization conducting the inspection/assessment obtains and examines the documented contingency plan tests to ensure the organization being inspected/assessed defines contingency plan tests to be conducted for the information system. DoD has determined the contingency plan tests are not appropriate to define at the Enterprise level. | [Enclosure 1](#_Enclosure_1_–) |
| CP-4 | CP-4 (a) | CCI-000490 |   |   | HighModerateLow | The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as at least annually. | Automatically compliant with this CCI because they are covered at the DoD level |
| CP-4 | CP-4 (b) | CCI-000496 |   |   | HighModerateLow | The organization conducting the inspection/assessment obtains and examines the audit trail of issues identified during the reviews of the contingency plan test results to ensure the organization being inspected/assessed reviews the contingency plan test results. | [Appendix G](#_APPENDIX_G_–_1) |
| CP-4 | CP-4 (c ) | CCI-000497 |   |   | HighModerateLow | The organization conducting the inspection/assessment obtains and examines the contingency plan test results as well as any documented corrective actions required and ensures the corrective actions are being implemented and tracked within the POA&M. | [Appendix G](#_APPENDIX_G_–_1) |
| CP-6 (1) | CP-6 (1) | CCI-000507 |   |   | HighModerate | The organization conducting the inspection/assessment obtains and examines the risk management strategy and the contingency plan to ensure the organization identifies an alternate storage site that is separated from the primary storage site so as not to be susceptible to the same threats identified at the primary site. | The system is not considered a MODERATE or HIGH level for Availability. |
| CP-6 (2) | CP-6 (2) | CCI-000508 |   |   | High | The organization conducting the inspection/assessment obtains and examines the contingency plan and conducts a walk-through of the alternate storage site to ensure the organization's documented recovery time and recovery point objectives have been met. | The system is not considered a HIGH level. Therefore, this AP is not applicable. |
| CP-6 (3) | CP-6 (3) | CCI-000509 |   |   | HighModerate | The organization conducting the inspection/assessment obtains and examines the contingency plan to ensure the organization has documented potential accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster. | The system is not considered a MODERATE or HIGH level for Availability. |
| CP-6 (3) | CP-6 (3) | CCI-001604 |   |   | HighModerate | The organization conducting the inspection/assessment obtains and examines the contingency plan to ensure the organization has documented explicit mitigation actions for accessibility problems identified in CP-6 (3), CCI 509 to the alternate storage site in the event of an area-wide disruption or disaster. | The system is not considered a MODERATE or HIGH level for Availability. |
| CP-6 | CP-6 (a) | CCI-000505 |   |   | HighModerate | The organization conducting the inspection/assessment obtains and examines the contingency plan to confirm the organization has established an alternate storage site. | The system is not considered a MODERATE or HIGH level for Availability. |
| CP-6 | CP-6 (b) | CCI-002836 |   |   | HighModerate | The organization conducting the inspection/assessment obtains and examines the documentation of the primary/alternate site information security safeguards that are in place as well as evidence that the alternate site was approved based on an assessment that security is equivalent at the alternate site. | The system is not considered a MODERATE or HIGH level for Availability. |
| CP-7 (1) | CP-7 (1) | CCI-000516 |   |   | HighModerate | The organization conducting the inspection/assessment obtains and examines the risk management strategy and the contingency plan to ensure the organization identifies an alternate processing site that is separated from the primary processing site so as not to be susceptible to the same threats identified at the primary site. | The system is not considered a MODERATE or HIGH level for Availability. |
| CP-7 (2) | CP-7 (2) | CCI-000517 |   |   | HighModerate | The organization conducting the inspection/assessment obtains and examines the contingency plan to ensure the organization has documented potential accessibility problems to the alternate processing site in the event of an area-wide disruption or disaster. | The system is not considered a MODERATE or HIGH level for Availability. |
| CP-7 (2) | CP-7 (2) | CCI-001606 |   |   | HighModerate | The organization conducting the inspection/assessment obtains and examines the contingency plan to ensure the organization has documented explicit mitigation actions for accessibility problems identified in CP-7 (2), CCI 517 to the alternate processing site in the event of an area-wide disruption or disaster. | The system is not considered a MODERATE or HIGH level for Availability. |
| CP-7 (3) | CP-7 (3) | CCI-000518 |   |   | HighModerate | The organization conducting the inspection/assessment obtains and examines the approved alternate processing site agreements to ensure they contain priority-of-service provisions in accordance with CP-2, CCI 447 for alternate processing site support (including recovery time objectives). | The system is not considered a MODERATE or HIGH level for Availability. |
| CP-7 (4) | CP-7 (4) | CCI-000519 |   |   | High | The organization conducting the inspection/assessment obtains and examines the contingency plan and conducts a walk-through of the alternate processing site to ensure it is ready to be used as the operational site supporting essential missions. | The system is not considered a HIGH level. Therefore, this AP is not applicable. |
| CP-7 (4) | CP-7 (4) | CCI-000520 |   |   | High | The organization conducting the inspection/assessment obtains and examines the contingency plan and conducts a walk-through of the alternate processing site to ensure it is ready to be used as the operational site supporting business functions. | The system is not considered a HIGH level. Therefore, this AP is not applicable. |
| CP-7 (6) | CP-7 (6) | CCI-002837 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed plans for circumstances that preclude returning to the primary processing site. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| CP-7 (6) | CP-7 (6) | CCI-002838 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines system resource lists or agreements with external support providers to ensure the organization being inspected/assessed prepares for circumstances that preclude returning to the primary processing site. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| CP-7 | CP-7 (a) | CCI-000513 | HighModerate | HighModerate | HighModerate | The organization conducting the inspection/assessment obtains and examines the approved alternate processing site agreements to ensure the organization has alternate processing site support that will permit the transfer and resumption of information system operations for essential missions within 1 hour (Availability High ) 12 hours (Availability Moderate) as defined in the contingency plan. | The system is not considered a MODERATE or HIGH level for Availability. |
| CP-7 | CP-7 (a) | CCI-000514 | HighModerate | HighModerate | HighModerate | The organization conducting the inspection/assessment obtains and examines the approved alternate processing site agreements to ensure the organization has alternate processing site support that will permit the transfer and resumption of information system operations for business functions within 1 hour (Availability High ) 12 hours (Availability Moderate) as defined in the contingency plan. | The system is not considered a MODERATE or HIGH level for Availability. |
| CP-7 | CP-7 (a) | CCI-002839 | HighModerate | HighModerate | HighModerate | The organization conducting the inspection/assessment obtains and examines the documented information system operations to ensure the organization being inspected/assessed defines information system operations that are permitted to transfer and resume at an alternate processing sites for essential missions/business functions when the primary processing capabilities are unavailable. DoD has determined the information system operations are not appropriate to define at the Enterprise level. | The system is not considered a MODERATE or HIGH level for Availability. |
| CP-7 | CP-7 (a) | CCI-000510 | HighModerate | HighModerate | HighModerate | The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the time period as 1 hour (Availability High ) 12 hours (Availability Moderate) as defined in the contingency plan | Automatically compliant with this CCI because they are covered at the DoD level |
| CP-7 | CP-7 (b) | CCI-000515 | HighModerate | HighModerate | HighModerate | The organization conducting the inspection/assessment obtains and examines:1. Inventory of equipment and supplies or,2. Contract documentationto ensure the organization has the equipment and supply resources necessary, or provisions to obtain the resources to transfer and resume operations at the alternate processing site within 1 hour (Availability High ) 12 hours (Availability Moderate) as defined in the contingency plan. | The system is not considered a MODERATE or HIGH level for Availability. |
| CP-7 | CP-7 (c ) | CCI-000521 | HighModerate | HighModerate | HighModerate | The organization conducting the inspection/assessment obtains and examines the documentation of the primary/alternate site information security safeguards that are in place as well as evidence that the alternate site was approved based on an assessment that security is equivalent at the alternate site. | The system is not considered a MODERATE or HIGH level for Availability. |
| CP-8 | CP-8 | CCI-000524 |   |   | HighModerate | The organization conducting the inspection/assessment obtains and examines the approved alternate telecommunications service agreements to ensure they permit the resumption of telecommunications services for essential mission IAW DoDI 8100.04. DoD has defined the time period as 1 hour (Availability High ) 12 hours (Availability Moderate) as defined in the contingency plan. | The system is not considered a MODERATE or HIGH level for Availability. |
| CP-8 | CP-8 | CCI-000525 |   |   | HighModerate | The organization conducting the inspection/assessment obtains and examines the approved alternate telecommunications service agreements to ensure they permit the resumption of telecommunications services for business functions IAW DoDI 8100.04. DoD has defined the time period as 1 hour (Availability High ) 12 hours (Availability Moderate) as defined in the contingency plan. | The system is not considered a MODERATE or HIGH level for Availability. |
| CP-8 | CP-8 | CCI-002840 |   |   | HighModerate | The organization conducting the inspection/assessment obtains and examines the documented information system operations to ensure the organization being inspected/assessed defines the information system operations to be resumed for essential missions within the organization-defined time period when the primary telecommunications capabilities are unavailable at either the primary or alternate processing or storage sites.  DoD has determined the information system operations are not appropriate to define at the Enterprise level. | The system is not considered a MODERATE or HIGH level for Availability. |
| CP-8 | CP-8 | CCI-002841 |   |   | HighModerate | The organization conducting the inspection/assessment obtains and examines the documented information system operations to ensure the organization being inspected/assessed defines the information system operations to be resumed for essential business functions within the organization-defined time period when the primary telecommunications capabilities are unavailable at either the primary or alternate processing or storage sites.   DoD has determined the information system operations are not appropriate to define at the Enterprise level. | The system is not considered a MODERATE or HIGH level for Availability. |
| CP-8 | CP-8 | CCI-000522 |   |   | HighModerate | The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the time period as 1 hour (Availability High ) 12 hours (Availability Moderate) as defined in the contingency plan. | Automatically compliant with this CCI because they are covered at the DoD level |
| CP-8 | CP-8 | CCI-000523 |   |   | HighModerate | The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the time period as 1 hour (Availability High ) 12 hours (Availability Moderate) as defined in the contingency plan. | Automatically compliant with this CCI because they are covered at the DoD level |
| CP-8 (1) | CP-8 (1) (a) | CCI-000526 |   |   | HighModerate | The organization conducting the inspection/assessment obtains and examines the approved primary telecommunications service agreements to ensure they contain priority-of-service provisions IAW DoDI 8100.04 (including recovery time objectives). | The system is not considered a MODERATE or HIGH level for Availability. |
| CP-8 (1) | CP-8 (1) (a) | CCI-000527 |   |   | HighModerate | The organization conducting the inspection/assessment obtains and examines the approved alternate telecommunications service agreements to ensure they contain priority-of-service provisions IAW DoDI 8100.04 (including recovery time objectives). | The system is not considered a MODERATE or HIGH level for Availability. |
| CP-8 (1) | CP-8 (1) (b) | CCI-000528 |   |   | HighModerate | The organization conducting the inspection/assessment obtains and examines the contingency plan, the telecommunication service agreement, and any existing formal requests for Telecommunications Service Priority. The purpose of the review is to ensure the organization or the mid-tier provider has requested Telecommunications Service Priority for all telecommunications services used for national security emergency preparedness where the primary telecommunications services are provided by a common carrier. | The system is not considered a MODERATE or HIGH level for Availability. |
| CP-8 (1) | CP-8 (1) (b) | CCI-000529 |   |   | HighModerate | The organization conducting the inspection/assessment obtains and examines the contingency plan, the telecommunication service agreement, and any existing formal requests for Telecommunications Service Priority. The purpose of the review is to ensure the organization has requested Telecommunications Service Priority for all telecommunications services used for national security emergency preparedness in the event the alternate telecommunications services are provided by a common carrier. | The system is not considered a MODERATE or HIGH level for Availability. |
| CP-8 (2) | CP-8 (2) | CCI-000530 |   |   | HighModerate | The organization conducting the inspection/assessment obtains and examines agreements with their service providers to ensure that a single point of failure is not shared. | The system is not considered a MODERATE or HIGH level for Availability. |
| CP-8 (3) | CP-8 (3) | CCI-000531 |   |   | High | The organization conducting the inspection/assessment obtains and examines agreements with alternate service providers to ensure they are not susceptible to the same hazards as the primary service provider. | The system is not considered a HIGH level. Therefore, this AP is not applicable. |
| CP-8 (4) | CP-8 (4) (a) | CCI-000532 |   |   | High | The organization conducting the inspection/assessment obtains and examines the primary telecommunications service provider agreements to ensure the organization requires the primary service provider to have contingency plans. | The system is not considered a HIGH level. Therefore, this AP is not applicable. |
| CP-8 (4) | CP-8 (4) (a) | CCI-000533 |   |   | High | The organization conducting the inspection/assessment obtains and examines the alternate telecommunications service provider agreements to ensure the organization requires the alternate service provider to have contingency plans. | The system is not considered a HIGH level. Therefore, this AP is not applicable. |
| CP-8 (4) | CP-8 (4) (b) | CCI-002842 |   |   | High | The organization conducting the inspection/assessment obtains and examines the audit trail of reviews to ensure the organization being inspected/assessed reviews provider contingency plans to ensure that the plans meet organizational contingency requirements. | The system is not considered a HIGH level. Therefore, this AP is not applicable. |
| CP-8 (4) | CP-8 (4) (c ) | CCI-002845 |   |   | High | The organization conducting the inspection/assessment obtains and examines the evidence of contingency testing to ensure that the organization being inspected/assessed obtains evidence that contingency testing is conducted by providers at least annually.  DoD has defined the frequency as at least annually. | The system is not considered a HIGH level. Therefore, this AP is not applicable. |
| CP-8 (4) | CP-8 (4) (c ) | CCI-002846 |   |   | High | The organization conducting the inspection/assessment obtains and examines the evidence of contingency training to ensure that the organization being inspected/assessed obtains evidence that contingency training is conducted by providers at least annually.  DoD has defined the frequency as at least annually. | The system is not considered a HIGH level. Therefore, this AP is not applicable. |
| CP-8 (4) | CP-8 (4) (c ) | CCI-002843 |   |   | High | The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as at least annually. | Automatically compliant with this CCI because they are covered at the DoD level |
| CP-8 (4) | CP-8 (4) (c ) | CCI-002844 |   |   | High | The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as at least annually. | Automatically compliant with this CCI because they are covered at the DoD level |
| CP-8 (5) | CP-8 (5) | CCI-002848 |   |   | High | The organization conducting the inspection/assessment obtains and examines the documented process as well as the record of tests to ensure the organization being inspected/assessed tests alternate telecommunication services at least annually. DoD has defined the frequency as at least annually. | The system is not considered a HIGH level. Therefore, this AP is not applicable. |
| CP-8 (5) | CP-8 (5) | CCI-002847 |   |   | High | The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level DoD has defined the frequency as at least annually. | Automatically compliant with this CCI because they are covered at the DoD level |
| CP-9 (1) | CP-9 (1) | CCI-000542 |   | HighModerate | HighModerate | The organization conducting the inspection/assessment obtains and examines the backup plan and verifies that the organization has tested and logged backup information. | The system is not considered a MODERATE or HIGH level for Availability. |
| CP-9 (1) | CP-9 (1) | CCI-000541 |   | HighModerate | HighModerate | The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as at least monthly in accordance with contingency plan. | Automatically compliant with this CCI because they are covered at the DoD level |
| CP-9 (2) | CP-9 (2) | CCI-000543 |   |   | High | The organization conducting the inspection/assessment obtains and examines the contingency plan test results to verify that the sample of backup information was restored as part of the restoration of selected information system functions. | The system is not considered a HIGH level. Therefore, this AP is not applicable. |
| CP-9 (3) | CP-9 (3) | CCI-002849 |   |   | High | The organization conducting the inspection/assessment obtains and examines the documented critical information system software and other security-related information to ensure the organization being inspected/assessed defines critical information system software and other security-related information which backup copies must be stored in a separate facility or in a fire-rated container. DoD has determined the critical information system software and other security-related information is not appropriate to define at the Enterprise level. | The system is not considered a HIGH level. Therefore, this AP is not applicable. |
| CP-9 (3) | CP-9 (3) | CCI-002850 |   |   | High | The organization conducting the inspection/assessment obtains and examines the record of where software is stored to ensure the organization being inspected/assessed stores backup copies of critical information system software and other security-related information defined in CP-9 (3), CCI 2849 in a separate facility or in a fire-rated container that is not collocated with the operational system. | The system is not considered a HIGH level. Therefore, this AP is not applicable. |
| CP-9 (5) | CP-9 (5) | CCI-000548 |   |   | HighModerate | The organization conducting the inspection/assessment obtains and examines the contingency plan and related logs to ensure the organization transfers information system backup information to the alternate site Continuously (Availability High) 24 hours (Availability Moderate) 7 days (Availability Low) as defined in the contingency plan. | The system is not considered a MODERATE or HIGH level for Availability. |
| CP-9 (5) | CP-9 (5) | CCI-000547 |   |   | HighModerate | The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the time period as Continuously (Availability High ) 24 hours (Availability Moderate) 7 days (Availability Low) as defined in the contingency plan. | Automatically compliant with this CCI because they are covered at the DoD level |
| CP-9 (6) | CP-9 (6) | CCI-000549 | blank | blank | blank | The organization conducting the inspection/assessment determines if the organization is maintaining a redundant, secondary backup system that is not co-located with the primary system. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| CP-9 (6) | CP-9 (6) | CCI-001609 | blank | blank | blank | The organization conducting the inspection/assessment determines if the organization has established a service level agreement for a redundant secondary system support that is not co-located with the primary system, and has configured the system so it can be activated to accomplish system backups without a loss of information or operational disruption. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| CP-9 (7) | CP-9 (7) | CCI-002851 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented backup information to ensure the organization being inspected/assessed defines the backup information that requires dual authorization for deletion or destruction. DoD has determined the backup information is not appropriate to define at the Enterprise level. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| CP-9 (7) | CP-9 (7) | CCI-002852 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented process and record of deletion and destruction to ensure the organization being inspected/assessed enforces dual authorization for the deletion or destruction of backup information defined in CP-9 (7), CCI 2851. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| CP-9 | CP-9 (a) | CCI-000535 | HighModerateLow | HighModerateLow | HighModerateLow | The organization conducting the inspection/assessment obtains and reviews the backup strategy, and examines a sample of systems to ensure they are configured to perform backups at least weekly as defined in the contingency plan. | [Appendix C](#_APPENDIX_C_–) |
| CP-9 | CP-9 (a) | CCI-000534 | HighModerateLow | HighModerateLow | HighModerateLow | The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as at least weekly as defined in the contingency plan. | Automatically compliant with this CCI because they are covered at the DoD level |
| CP-9 | CP-9 (b) | CCI-000537 | HighModerateLow | HighModerateLow | HighModerateLow | The organization conducting the inspection/assessment obtains and reviews the backup strategy, and examines a sample of systems to ensure they are configured to perform back ups at least weekly and as required by system baseline configuration changes in accordance with the contingency plan. | [Appendix C](#_APPENDIX_C_–) |
| CP-9 | CP-9 (b) | CCI-000536 | HighModerateLow | HighModerateLow | HighModerateLow | The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as at least weekly and as required by system baseline configuration changes in accordance with the contingency plan. | Automatically compliant with this CCI because they are covered at the DoD level |
| CP-9 | CP-9 (c) | CCI-000539 | HighModerateLow | HighModerateLow | HighModerateLow | The organization conducting the inspection/assessment obtains and examines the latest version of the information system documentation including security-related documentation to verify it is the same version as contained in backups. | This document |
| CP-9 | CP-9 (c) | CCI-000538 | HighModerateLow | HighModerateLow | HighModerateLow | The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as when created or received, when updated, and as required by system baseline configuration changes in accordance with the contingency plan. | Automatically compliant with this CCI because they are covered at the DoD level |
| CP-9 | CP-9 (d) | CCI-000540 | HighModerateLow | HighModerateLow | HighModerateLow | The organization conducting the inspection/assessment obtains and examines the system security plan and ensures backup information at the storage location is protected IAW the system security plan. | SSP (external artifact) |

# **ENCLOSURE 1 – CONTINGENCY PLAN TEST REPORT TEMPLATE**

|  |  |
| --- | --- |
| Test Information | Description |
| Name of Test |  |
| System Name |  |
| Date of Test |  |
| Team Test Lead and Point of Contact |  |
| Location Where Conducted |  |
| Participants |  |
| Components |  |
| Assumptions |  |
| Objectives | Assess effectiveness of coordination among recovery personnelAssess effectiveness of proceduresAssess effectiveness of notification procedures |
| Methodology |  |
| Activities and Results (Action, Expected Results, Actual Results) |  |
| Post Test Action Items |  |
| Recommended Changes to Contingency Plan Based on Test Outcomes |  |

# **ENCLOSURE 2 – AFTER ACTIONS REPORT TEMPLATE**

**After Actions Report**

**1.0 Introduction**

On {DATE}, {ACRONYM} participated in a tabletop exercise designed to validate their understanding of the {ACRONYM} Information Systems Contingency Plan.

**2.0 Objectives**

The exercise objectives are as follows:

* Validate the team’s ability to respond to contingencies
* Validate the accuracy of procedures documented in the {ACRONYM} Information Systems Contingency Plan
* Identify areas of the {ACRONYM} Information Systems Contingency Plan that need to be revised.

**3.0 Agenda**

|  |  |
| --- | --- |
| Date | {DATE} |
| Location | {LOCATION} |
| Exercise Name | {EXERCISE NAME} |
| {TIME} | Welcoming Remarks and Introductions |
| {TIME} | Exercise Briefing (Objectives, Rules of Engagement, etc.) |
| {TIME} | Scenario Discussion |
| {TIME} | Debrief/Hotwash |

**4.0 Discussion of Findings**

The {EXERCISE NAME} provided information on the {ACRONYM} Information Systems Contingency Plan. An important benefit of the exercise was the opportunity for participants to raise important questions, concerns, and issues. The discussion findings from the exercise along with any necessary recommended actions are as follows:

|  |  |  |  |
| --- | --- | --- | --- |
|  | Subject | Observation | Recommendations |
| 1 |  |  |  |
| 2 |  |  |  |
| 3 |  |  |  |
| 4 |  |  |  |
| 5 |  |  |  |
| 6 |  |  |  |
| 7 |  |  |  |
| 8 |  |  |  |
| 9 |  |  |  |
| 10 |  |  |  |

# **ENCLOSURE 3 – TRAINING RESOURCES**

Contingency training to information system users, other than general users, consistent with assigned roles and responsibilities is a key principle to ensure a successful ISCP implementation.

For general users, DoD components are automatically compliant with the requirement based on DoDD 8570.01 requirements for IA awareness training.

The below resources have been compiled to assist with ISCP training requirements. Additional, commercial-based training, may be used to supplement in-house DoD provided training.