|  |
| --- |
|                               NIH Cover Page Logo'     **Contingency Plan****for****[System Name] ([System Acronym])**Security Categorization: [High, Moderate, or Low]**[IC Name] ([IC Acronym])**      **Version [Revision]**  **[Date]**   **Prepared by**Click or tap here to enter text.**FOR OFFICIAL USE ONLY** |

**Document Revision History**

This [System Name] Contingency Plan (CP) is a living document that is changed as required to reflect system, operational, or organizational changes.  Modifications made to this document are recorded in the version history matrix below.

At a minimum, this document will be reviewed and assessed annually. Reviews made as part of the assessment process shall also be recorded below.

This document history shall be maintained throughout the life of the document and the associated system.

| **Date** | **Description** | **Version** | **Author** |
| --- | --- | --- | --- |
| March 2017 | Document Publication | 1.0 | NIH Information Security Program |
|  November 2017 | Formatting, Added Appendix C/D for CP Testing | 1.1 | NIH Information Security Program |
| October 2018  |  Review and Update | 1.2 | NIH Information Security Program |
|   |   |   |   |
|   |   |   |   |
|   |   |   |   |
|   |   |   |   |
|   |   |   |   |
|   |   |   |   |
|   |   |   |   |

 **Contingency Plan Approval Signatures**

I have reviewed the [System Name] Contingency Plan and agree with the information presented within this document. Changes to this Contingency Plan will be coordinated with, and approved by, the undersigned, or their designated representatives.

|  |
| --- |
| Instruction: If the System Owner and Contingency Plan Coordinator are the same person remove the System Owner signature block.Please delete these instructions before finalizing this document. |

|  |  |
| --- | --- |
|   |   |
|   |   |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | \_\_\_\_\_\_\_\_\_\_ |
| [System Owner] | Date |
| System Owner |   |
|   |   |
|   |   |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | \_\_\_\_\_\_\_\_\_\_ |
| [Contingency Plan Coordinator] | Date |
| Contingency Plan Coordinator |   |
|   |   |
|   |   |
|   |   |
|   |   |
|   |   |

**Table of Contents**

[1 Overview 5](#_Toc532999980)

[1.1 Purpose 5](#_Toc532999981)

[1.2 Authorities and Other Requirements 5](#_Toc532999982)

[1.3 Applicability 7](#_Toc532999983)

[1.4 Scope 7](#_Toc532999984)

[1.4.1 Planning Principles 7](#_Toc532999985)

[1.4.2 Assumptions 7](#_Toc532999986)

[2 Concept of Operations 9](#_Toc532999987)

[2.1 System Description 9](#_Toc532999988)

[2.2 Line of Succession 9](#_Toc532999989)

[2.3 Contact List 9](#_Toc532999990)

[2.4 Responsibilities 9](#_Toc532999991)

[2.4.1 [IC Acronym] Restoration/Operations Team 9](#_Toc532999992)

[2.4.2 [IC Acronym] User Liaison Support Team 10](#_Toc532999993)

[2.4.3 [IC Acronym] Salvage/Reclamation Team 11](#_Toc532999994)

[2.5 Plan Testing, Training, & Exercises (TT&E) 11](#_Toc532999995)

[2.6 Testing 11](#_Toc532999996)

[2.6.1 Training 11](#_Toc532999997)

[2.6.2 Exercises 12](#_Toc532999998)

[3 Notification & Activation Phase 13](#_Toc532999999)

[4 Recovery Operations 13](#_Toc533000000)

[4.1 Recovery Goal – Identify Recoverable/Stable Inventory & Update Inventory List 13](#_Toc533000001)

[5 Return to Normal Operations 14](#_Toc533000002)

[5.1 Concurrent Processing 14](#_Toc533000003)

[5.2 Plan Deactivation 14](#_Toc533000004)

[Appendix A: [IC Acronym] Key Personnel 15](#_Toc533000005)

[Appendix B: NIH Senior Executive Management 16](#_Toc533000006)

[Appendix C: Example After-Action Report 17](#_Toc533000007)

[Appendix D: Example Test Participant Evaluation Form 19](#_Toc533000008)

# Overview

## Purpose

This [System Name] Contingency Plan (CP) establishes procedures to recover the [System Name] following a disruption. The following objectives have been established for this plan:

* Identify [System Name] priorities and resources by conducting a Business Impact Analysis (BIA).
* Maximize the effectiveness of contingency operations through an established plan that consists of the following phases:
	+ **Notification/Activation Phase** to detect and assess damage and to activate the plan;
	+ **Recovery Phase** to restore temporary IT operations and recover damage done to the original system; and
	+ **Reconstitution Phase** to restore IT system processing capabilities to normal operations.
* Identify the activities, resources, and procedures needed to carry out [System Name] processing requirements during prolonged interruptions to normal operations.
* Assign responsibilities to designated NIH/[IC Acronym] personnel and provide guidance for recovering [System Name] during prolonged periods of interruption to normal operations.
* Ensure coordination with other NIH staff who will participate in the contingency planning strategies.
* Ensure coordination with external points of contact and vendors who will participate in the contingency planning strategies.

## Authorities and Other Requirements

This [System Name] Contingency Plan has been developed as in accordance with the Office of Management and Budget (OMB) Circular A-130, Managing Information as a Strategic Resource, July 2016, and Department of Health and Human Services (HHS) Information Systems Security and Privacy Policy, July 30, 2014, which requires the establishment and implementation of procedures for responding to events that damage systems containing electronic protected health information.

This [System Name] Contingency Plan is promulgated under the legislative requirements set forth in the Federal Information Security Modernization Act (FISMA) of 2014 and the guidelines established by the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-34, titled "Contingency Planning Guide for Information Technology Systems.”

The [System Name] Contingency Plan also complies with the following federal and departmental policies:

* Office of Management and Budget (OMB) Circular A-130, Managing Information as a Strategic Resource, July 2016
* Health and Human Services (HHS) Information Systems Security and Privacy Policy (IS2P), July 2014
* National Institutes of Health (NIH) Information Security Policy Handbook 4.0, May 2018
* Federal Preparedness Circular (FPC) 65, Federal Executive Branch Continuity of Operations
* Presidential Decision Directive (PDD) 63, Critical Infrastructure Protection, May 1998
* Defense Authorization Act (Public Law 106-398), Title X, Subtitle G, “Government Information Security Reform,” October 30, 2000
* Federal Information Security Modernization Act (FISMA) (Public Law 113-283), December 2014
* Department of Homeland Security (DHS), National Response Plan, May 2006
* Homeland Security Presidential Directive (HSPD) 7, Critical Infrastructure Identification, Prioritization, and Protection, December 2003
* National Institute of Standards and Technology (NIST) Special Publication (SP) 800-34 Rev 1, Contingency Planning Guide for Information Technology Systems, Current Version
* National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Rev 4, Recommended Security Controls for Federal Information Systems, Current Version
* National Institute of Standards and Technology (NIST) Special Publication (SP) 800-84, Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities, Current Version

## Applicability

The [System Name] Contingency Plan applies to the functions, operations, and resources necessary to restore and resume [System Name] operations as it is installed at the following locations:

| **Common Name/Reference** | **Physical Address** |
| --- | --- |
|  |  |
|  |  |

The [System Name] tools and applications at these locations are managed by [Enter details about the CP and any supporting CPs that exist within NIH or the IC, (example: Data Center CP, etc.)]

## Scope

### Planning Principles

Various scenarios were considered to form a basis for the plan, and multiple assumptions were made. The applicability of the plan is predicated on the following key principles.

* *Example:* NIH facilities in Bethesda, MD are inaccessible; therefore, IC is unable to perform Example GSS processing for the IC.
* *Example:* Example GSS does not use or deploy an alternate recovery site.

### Assumptions

Based on these principles, the following assumptions were used when developing the [System Name] Contingency Plan. *(examples provide below; modify/add/delete as appropriate for this System)*

* The [System Name] (hardware, software, virtual, infrastructure, etc.) is inoperable or unavailable at some or all of its NIH locations and cannot be recovered within 48 hours.
* Key [System Name] personnel have been identified and trained in their emergency response and recovery roles; they are available to activate the [System Name] Contingency Plan.
* Preventive controls (e.g., generators, environmental controls, waterproof tarps, sprinkler systems, fire extinguishers, and fire department assistance) are fully operational at the time of the disaster.
* Data center equipment, including components supporting [System Name] are connected to an uninterruptible power supply (UPS) that provides 45 minutes to 1 hour of electricity during a power failure.
* Current backups of the tools and application software and data are intact and available.
* Service agreements are maintained with [System Name] hardware, software, and communications providers to support the emergency system recovery.

The [System Name] Contingency Plan does not apply to the following situations: *(examples provide below; modify/add/delete as appropriate for this System)*

* Emergency evacuation of personnel. The occupant evacuation plan (OEP) will cover personnel evacuation is a section in the Business Continuity Plan and Procedures (BCP).
* Overall recovery of business operations. These will be covered by the BCP.
* Relocation of personnel and equipment as this should be covered by the NIH Data Center’s Disaster Recovery Plan (DRP), as applicable.

# Concept of Operations

## System Description

[System Description]

## Line of Succession

| **POC Name** | **Role** |
| --- | --- |
|  |  |
|  |  |
|  |  |

## Contact List

| **POC Name** | **Role** | **Contact Information** |
| --- | --- | --- |
|  |  |  |
|  |  |  |
|  |  |  |

## Responsibilities

The following teams have been developed and trained to respond to a contingency event affecting the IT system.

[IC Acronym] Disaster Recovery Coordinator

[IC Acronym] Disaster Recovery Technical Support Coordinator

[IC Acronym] Damage Assessment Team

[IC Acronym] Executive Team

The pre-disaster responsibilities are:

(*Example*: Approve the [System Name] Contingency Plan and all major or material modifications to the plan)

(*Example*: Establish primary and alternate disaster command posts, ensuring that the posts are adequately prepared for a contingency event.)

The disaster responsibilities and actions are:

(*Example*: Review the report of the Damage Assessment Team)

(*Example*: Declare a disaster)

Establish the command post and communications,

Notify and activate the disaster recovery teams, and identify a disaster recover coordinator.

Notify the NIH Senior Executive Management (listed in Appendix B) that [IC Acronym] is executing their Contingency Plan.

(*Example*: Keep NIH Senior Executive Management and other enterprise COOP/Disaster Recovery teams updated as required)

### [IC Acronym] Restoration/Operations Team

The pre-disaster responsibilities are (*examples*:)

* Establish and maintain the recovery procedures.
* Manage and maintain the backup procedures.
* Plan, conduct, and document regular Contingency Plan tests.
* Ensure that appropriate backups are made on the prescribed basis
* Maintain up-to-date systems operations documentation, ensuring that this documentation is in the doc box, and, as needed, is stored in a suitable location.

The disaster responsibilities and actions are (*examples*):

* Verify the operating systems and all other system and communication software are working properly.
* Restore service of the designated tools and applications in accordance with the priorities detailed in the BIA.
* Support the operations by resolving problems.
* Implement and maintain a problem log.
* Provide information to [IC Acronym] User Liaison Support Team regarding the status of the tools/applications and operations.
* Keep the Damage Assessment Team and the Executive Team informed of operation status.

The post disaster responsibilities are:

* Ensure all required backups of the entire system are completed in preparation for recovery at the primary location.

### [IC Acronym] User Liaison Support Team

The User Liaison Support Team aids users during the contingency event from the time the disaster is declared until operations resume at the primary location.

*(Examples:)*

The pre-disaster responsibilities are:

* Advise and consult with tool and application users regarding their disaster recovery requirements.
* Assist tool and application users during Contingency Plan tests.

The disaster responsibilities and actions are:

* Provide guidance to the NIH IT Service Desk during the contingency event
* Notify the tool and application users that a contingency event has been declared.
* Advise users of the disaster recovery system status, availability, and accessibility.
* Provide problem diagnosis and resolution guidance/assistance to tool/application owners and their users.

### [IC Acronym] Salvage/Reclamation Team

The Salvage/Reclamation Team manages the restoration of services at the primary location

The pre-disaster responsibility is to maintain current copies of equipment inventory lists, physical plant layout/diagrams (floor plans), and other pertinent documentation describing the [System Name] production hardware configuration in a documentation box.

The disaster responsibilities and actions are (*Examples*):

* After the Restoration Team has implemented recovery operations, the Salvage\Reclamation Team assess the damage at the primary location and reports the damage, with recommendations, to the Executive Team.
* Organize the recovery of salvageable equipment.
* Order and expedite replacements for unusable IT equipment.
* Monitor and verify construction progress of the new/repaired facility, and the installation of all utilities (electrical power, telephones, network connectivity, air conditioning, plumbing, water, gas, and HVAC), and other essentials such as security.
* Monitor the installation of servers, peripherals, and other IT equipment.
* Advise the Executive Team regarding status, progress, and schedules, and any problems associated with the construction/reconstruction and installation.
* Inform the Executive Team when the new/restored facility is ready for use.

## Plan Testing, Training, & Exercises (TT&E)

The [System Name] Contingency Plan must be maintained and made ready, which includes having (*examples*):

* personnel trained to fulfill their roles and responsibilities within the plan;
* plans exercised to validate content; and
* systems and system components tested to ensure their operability as specified in the [System Name] Contingency Plan.

[IC Acronym] recognizes that it should conduct TT&E events periodically, following organizational or system changes, or the issuance of new TT&E guidance.

## Testing

[System Name] Contingency Plan testing is a critical element of a viable contingency capability. Testing enables plan deficiencies to be identified and addressed by validating one or more of the system components and the operability of the plan. The Contingency Plan Exercise will include the following areas:

* Notification procedures;
* System recovery from backup media;
* Internal and external connectivity;
* System performance;
* Restoration of normal operations; and
* Other plan testing (where coordination is identified, i.e., NIH ORS, NIH CIT).

### Training

Training for personnel with contingency plan responsibilities will focus on familiarizing them with their [System Name] Contingency Plan roles and teaching skills necessary to accomplish those roles. In some cases, the Contingency Plan Exercise may be used to for training.

### Exercises

NIST 800-84, “Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities,” identifies the following types of exercises that are widely used to evaluate Contingency Plans:

* **Tabletop Exercises.** Tabletop exercises are discussion-based exercises where personnel meet in a classroom setting or in breakout groups to discuss their roles during an emergency and their responses to a particular emergency. A facilitator presents a scenario and asks the exercise participants questions related to the scenario, which initiates a discussion among the participants of roles, responsibilities, coordination, and decision making. A tabletop exercise is discussion-based only and does not involve deploying equipment or other resources.
* **Functional Exercises.** Functional exercises allow personnel to validate their operational readiness for emergencies by performing their duties in a simulated operational environment. Functional exercises are designed to exercise the roles and responsibilities of specific team members, procedures, and assets involved in one or more functional aspects of a plan (e.g., communications, emergency notifications, system equipment setup). Functional exercises vary in complexity and scope, from validating specific aspects of a plan to full-scale exercises that address all plan elements. Functional exercises allow staff to execute their roles and responsibilities as they would in an actual emergency, but in a simulated manner.

According to NIST 800-34, Revision 1, “Contingency Planning Guide for Federal Information Systems,”

* **For low-impact systems, a tabletop exercise at an organization-defined frequency is sufficient.** The tabletop should simulate a disruption, include all main Information System Contingency Plan (ISCP) points of contact, and be conducted by the system owner or responsible authority.
* **For moderate-impact systems, a functional exercise at an organization-defined frequency should be conducted.** The functional exercise should include all ISCP points of contact and be facilitated by the system owner or responsible authority. Exercise procedures should be developed to include an element of system recovery from backup media.
* **For high-impact systems, a full-scale functional exercise at an organization-defined frequency should be conducted.** The full-scale functional exercise should include a system failover to the alternate location. This could include additional activities such as full notification and response of key personnel to the recovery location, recovery of a server or database from backup media or setup, and processing from a server at an alternate location. The test should also include a full recovery and reconstitution of the information system to a known state.

The [System Name] is a FISMA [Low/Moderate/High] system. NIH should conduct a functional exercise that includes all [System Name] Contingency Plan points of contact and be facilitated by the [System Name] System Owner or responsible authority. The exercise procedures should be developed to include an element of system recovery from backup media.

In accordance with HHS and NIH policies and guidance, [IC Acronym] will conduct a [System Name] Contingency Plan Functional Exercise annually (within 365 days) and produce an After Action Report. An example can be found in Appendix C.

# Notification & Activation Phase

This phase addresses the initial actions taken to detect and assess damage inflicted by a disruption to [System Name]. Based on the assessment of the event, the plan may be activated by the Disaster Recovery (DR) Coordinator. In an emergency, [IC Acronym]’s top priority is to preserve the health and safety of its staff before proceeding to the Notification and Activation procedures.

Contact information for key personnel is located in [Appendix A](#_Appendix_A:_NHLBI/DIR). The notification sequence is listed below:

# Recovery Operations

This section provides procedures for recovering services/applications, whereas other efforts are directed to repair damage to the original system and capabilities.

The following procedures are for recovering the [System Name]. Procedures are outlined for each team that is required. Each procedure should be executed in the sequence it is presented to maintain efficient operations.

## Recovery Goal – Identify Recoverable/Stable Inventory & Update Inventory List

These are the steps for recovering stable and salvageable resources in the event of a catastrophic disruption of service impacting a [System Name] facility.

* Salvage/Reclamation Team
	+ Task 1: Coordinate with CIT, ORS, or responsible entity to gain access to the impacted building
	+ Task 2: Use the current [System Name] inventory to identify and locate damaged and salvageable resources
	+ Task 3: Mark inventory to flag:
		- Undamaged, reusable resources
		- Damaged, repairable/salvageable resources
		- Unsalvageable resources
	+ Task 4: Undamaged, reusable resources
		- Secure resources to mitigate of damage from downstream events and activities
		- Determine criticality and priority of the resource
		- Coordinate with Restoration/Operations Team to determine if additional resources from NIH CIT are required to sustain operations
	+ Task 5: Assess damaged, repairable/salvageable resources
		- Locate and review applicable warranties
		- Determine criticality, priority and feasibility of repair
		- Decide on whether to repair or throw-away
	+ Task 6: Assess unsalvageable resources
		- Locate and review applicable warranties
		- Determine criticality, priority and feasibility of replacing resource
		- Decide on whether to replace, upgrade, or discontinue using the resource

# Return to Normal Operations

This section discusses activities necessary for restoring [System Name] operations at the original or new site. When the data center at the original site has been restored or a new site is designated as the Primary location, [System Name] operations must be resumed. The goal is to provide a quick restoration of operations.

* Disaster Recovery Coordinator
	+ Task 1: Notify the Executive Team and obtain approval and set the date/time to restore operations
	+ Task 2: Inform the Restoration/Operations and User Liaison Support Teams when the restoration will occur
	+ Task 3: Coordinate with CIT and manage the Restoration/Operations Team activities throughout the restoration
* Restoration/Operations Team
	+ Task 1: Confirm site is ready for operations
	+ Task 2: Inspect and test all resources
	+ Task 3: Execute storage fallback to Production
* User Liaison Support Team
	+ Task 1: Provide transition guidance to the NIH IT Service Desk
	+ Task 2: Prepare user community communication and coordinate language and release approval from the Executive Team
	+ Task 3: Send transition communication to user community

## Concurrent Processing

This section is not applicable. There will be no current processing on [System Name] resources.

## Plan Deactivation

Plan deactivation will be coordinated by the Disaster Recovery Coordinator and Disaster Recovery Technical Support Coordinator at the direction of the Executive Team. The Executive Team may coordinate with the NIH Emergency Coordinators to determine when and how to deactivate the plan.

# Appendix A: [IC Acronym] Key Personnel

**Disaster Recovery Coordinator**

| **#** | **Name** | **Office Phone** | **Cell Phone** | **Email** |
| --- | --- | --- | --- | --- |
| 1 |  |  |  |  |

**Disaster Recovery Technical Support Coordinator**

| **#** | **Name** | **Office Phone** | **Cell Phone** | **Email** |
| --- | --- | --- | --- | --- |
| 1 |  |  |  |  |

**Damage Assessment Team**

| **#** | **Name** | **Office Phone** | **Cell Phone** | **Email** |
| --- | --- | --- | --- | --- |
| 1 |  |  |  |  |
| 2 |  |  |  |  |

**Executive Team**

| **#** | **Name** | **Office Phone** | **Cell Phone** | **Email** |
| --- | --- | --- | --- | --- |
| 1 |  |  |  |  |
| 2 |  |  |  |  |
| 3 |  |  |  |  |

**Restoration/Operations Team**

| **#** | **Name** | **Office Phone** | **Cell Phone** | **Email** |
| --- | --- | --- | --- | --- |
| 1 |  |  |  |  |
| 2 |  |  |  |  |

**User Liaison Support Team**

| **#** | **Name** | **Office Phone** | **Cell Phone** | **Email** |
| --- | --- | --- | --- | --- |
| 1 |  |  |  |  |
| 2 |  |  |  |  |

**Salvage/Reclamation Team**

| **#** | **Name** | **Office Phone** | **Cell Phone** | **Email** |
| --- | --- | --- | --- | --- |
| 1 |  |  |  |  |
| 2 |  |  |  |  |

# Appendix B: NIH Senior Executive Management

| **#** | **Name/Title** | **Office Phone** | **Cell Phone** | **Email** |
| --- | --- | --- | --- | --- |
| 1 |  |  |  |  |
| 2 |  |  |  |  |
| 3 |  |  |  |  |

# Appendix C: Example After-Action Report

|  |  |
| --- | --- |
| Type of Event | ***[Tabletop Exercise/Functional Exercise/Live Recovery]*** |
| Name of System | ***[IC Acronym] [System Name]*** |
| Date of Test/Live Recovery | ***[Date of Exercise/Recovery]*** |
| Testing/Live Recovery Point of Contact | ***[Insert Name and Title]*** |
| Purpose, Type of Test, and Scope or Disruption Description (describe the events that led to contingency plan implementation): |
| To validate the [IC Acronym] [System Name] contingency plan, [IC Acronym] will conduct a [Tabletop Exercise/Functional Exercise/Live Recovery] to examine processes and procedures associated with the implementation of the contingency plan. The exercise is designed to facilitate communication among select personnel regarding the implementation of recovery operations at [IC Acronym] following an event causing the outage of mission critical systems that are housed in the [insert facility name]. This exercise is designed to improve the readiness of the [IC Acronym] [System Name] and help validate existing contingency plan procedures. |
| Activities and Results (action, expected results, actual results): |
| The exercise objectives are as follows:* ­Validate the team’s ability to recover IT operations at alternate facility
* ­Validate the accuracy of recovery procedures documented in the [insert plan name]
* ­Identify areas of the contingency plan that need to be revised.

At [insert time] on [insert date], an electrical fire in the [insert facility name] caused extensive damage and the termination of operations in the data center. The [insert plan name] was fully activated in response to this incident, and operations will be conducted at the [insert alternate facility name] for the foreseeable future. [Insert organization name] employees will be displaced from the building until smoke, water, and other health hazards are removed. Despite the problem at the [insert facility name], Directors and Administrators show no sign of altering their agendas and expect a seamless transition of IT operations to the [insert alternate facility name].The [insert exercise name] provided information on [insert relevant information]. An important benefit of the exercise was the opportunity for participants to raise important questions, concerns, and issues. At the conclusion of the exercise, participants were asked to complete an evaluation form regarding the information provided, additional information needed, and their thoughts on the event and topics, to be included in the after-action report. A sample evaluation form can be found in Appendix D.The exercise provided an excellent opportunity for participants to [insert relevant information]. As a result of the exercise, participants left with a heightened awareness of [insert relevant information]. Following the [insert functional exercise name], participants were given an evaluation form on which to record their impressions of the exercise. These forms allowed participants to rate presentations on a numerical scale and to provide additional comments for consideration in the after-action report. The questions covered whether participants thought additional issues should have been raised; whether participants thought the exercise was beneficial; what participants gained from the exercise; and what can be done to improve future exercises. [Insert percentage] of the participants completed the evaluation. In response to the question regarding whether participants thought additional issues should have been raised, nearly [insert percentage] of those who completed the evaluation indicated that all relevant issues were addressed. Other comments were [insert relevant information].In response to the question regarding whether participants thought the exercise was beneficial, [insert percentage] of those who completed the evaluation indicated that the exercise was beneficial. Comments ranged from [insert relevant information (i.e., "good start" to "extremely beneficial.")].In response to the question about what participants gained from the exercise, nearly [insert percentage] of those who completed the evaluation form remarked [insert relevant information]. |
| Actual Duration of System Outage: |
| This exercise will be a [insert number of hours]-hour event that will begin at [insert start time] and will last until [insert end time]. |
| Lessons Learned/Action Item Assessment: |
| The following questions are designed to obtain input into the after action report from participants.* ­Are there any other issues you would like to discuss that were not raised?
* ­What are the strengths of the contingency plan? What areas require closer examination?
* ­Was the exercise beneficial? Did it help prepare you for follow-on testing?
* ­What did you gain from the exercise?
* ­How can we improve future exercises and tests?

Specific observations made during the exercise, and recommendations for enhancement of the plan, are asfollows:**Observation 1.** [Insert general topic area][Insert observation]Recommendations[Insert recommendations]**Observation 2.** [Insert general topic area][Insert observation]Recommendations[Insert recommendations] |

# Appendix D: Example Test Participant Evaluation Form

|  |
| --- |
| INSERT NAME OF EVENTExercise Evaluation FormINSERT DATEPlease take a few moments to answer the following questions about the exercise.NAME: 1) Did you have available to you all the information and resources needed to fulfill your responsibilities?2) Did you feel that there was an adequate level of training to support the response effort at the relocation site?3) Was the structure of the exercise realistic?4) Please provide comments regarding what you believe worked and didn't work during the exercise.5) Do you believe you are sufficiently prepared to conduct extended emergency operations from the relocation facility? Please Circle OneNot Prepared Slightly Prepared Prepared Extremely Prepared6) Please rate the overall exercise. Please Circle OneNeeds Improvement Fair Good Very Good |

**END OF DOCUMENT**