State of Maryland

Sample Disaster Recovery Report

March 18, 2004

Prepared by:
Amanda Gossett, DRP Task Leader
Shawn Taylor, Senior Security Engineer

SAIC Science Applications International Corporation
An Employee-Owned Company

13921 Park Center Road, Suite 300
Herndon, VA 20171

SAIC-6099-2002-131 (A)

Prepared for:
Maryland Department of Budget & Management
Carmella Thompson, Assistant Director of Security
Office of Information Technology
45 Calvert Street
Annapolis, MD 21401

CONTENTS

INDEX OF FIGURES

INDEX OF TABLES

INDEX OF APPENDICES

1. INTRODUCTION

1.1. DRP Purpose

This System Disaster Recovery Plan (DRP) is designed to mitigate the risk of system and service unavailability by providing written and cost-effective contingency solutions for the prompt and effective continuation or resumption of mission-critical services in the event of a disaster. In addition, this DRP has a preventive component that fulfills Presidential Decision Directive 63 (PDD#63) requiring federal agencies to identify mission-critical infrastructure components and develop a plan to protect them.

Throughout the recovery effort, this DRP establishes action steps and clear lines of responsibility for recovery efforts. The DRP consists of the following phases:

Notification and Activation—The Disaster Recovery Team (DRT) members are notified and the Disaster Recovery Coordinator (DRC) activates the team.

Assessment and Reporting—DRT members report to the scene, evaluate conditions, and develop a formal recommendation on whether or not to declare a disaster for presentation to the Disaster Recovery Manager (DRM).

Continuity of IT Services and Initial Recovery—If directed by the DRM, then the DRT takes action to quickly recover and continue providing IT services to the best extent allowed by conditions and, if necessary, at a degraded level until normal operations can be restored. If conditions warrant, the DRT will relocate and recover IT operations at the alternate site.

Full Recovery and Reconstitution of Normal Operations—As conditions stabilize, actions will be taken by the DRT to reestablish IT operations at the permanent location. Depending on the damage that occurred, facilities will be repaired, damaged equipment will be replaced, platforms will be returned to operation, applications will be reloaded, network connectivity will be restored, and normal computer operations and associated procedures will be fully restored.

1.2. Applicability

This document applies to two distinct conditions, described as follows:

1. **Component-Level Disruption**—Individual component failures with contingency actions to address each component-level failure and provide for continuity of support and eventual recovery and reconstitution of the failed components.

2. **Facility-Level Disruption**—An event that renders the system facility (*give location*) as inoperable. This catastrophic scenario requires the availability of information technology resources needed to restore IT services at an alternate site.

This DRP applies to the continuity, recovery, and reconstitution of th*e IT services* provided by a particular system and not the specific *business functions* performed by the various system divisions. The business functions are the responsibility of the divisions, who develop and execute business continuity/continuity of operations plans and business recovery plans (BRP). The Occupant Evacuation Plan (OEP) covers facility-related procedures to follow in a disaster event and is appended to this plan.

1.3. Scope

The scope of this DRP focuses on the recovery and continued operation of system components that support mission-critical systems and mission-essential services in the event of a disaster.

For the purposes of this DRP, a disaster is defined as:

> *A major incident that seriously disrupts, or is expected to disrupt, operations for 12 or more hours, requiring: the reassignment of personnel to disaster recovery activities, the use of additional vendor/contractor support to accomplish recovery requirements, and/or the acquisition of special funding to support equipment replacement and other recovery-related costs that are outside of the scope of normal day-to-day operations.*

If the level of effort (LOE) required to accomplish these requirements falls within the scope of a disaster, as defined above, then a disaster declaration should be made, and DRP processes and procedures should be initiated. If not, then the recovery actions should be conducted as part of day-to-day operations.

1.3.1. Assumptions

The following assumptions were made concerning the operational capabilities that will be available to execute this DRP:

- Senior management will provide the support needed to implement this DRP and provide for its effective execution as needed.

- The Chief Technical Officer (CTO) for the system will be provided the resources needed to implement and execute the DRP.

- Organizations and offices outside of the system CTO and CIO will provide any support required to successfully implement the DRP (see Section 2.3.5 of this DRP).

- A system DRT will be established, trained, and tested to the degree necessary to effectively execute provisions of this DRP.

- The DRP will effectively provide for the level of IT support that is needed to recover mission-critical systems and mission-essential services.

- This IT System DRP does not address business resumption or continuity of operations procedures.

- The Occupant Evacuation Plan for (*insert address where system resides*) can be found in Attachment B of this DRP.

1.4. References and Requirements

Table 1-1 contains the reference and requirement documents used to develop this DRP.

Table 1-1: References and Requirements

Reference	Basic Security Requirements
Computer Security Act of 1987	Established uniform standards and guidelines to protect information in Federal computer Systems.
Paperwork Reduction Act of 1995	Charged NIST with development of computer security standards and guidelines for Sensitive But Unclassified IT, while National Security Agency retained authority for classified IT.
Clinger-Cohen Act of 1996	Establishes agency responsibility to manage IT, including procurement, lifecycle management, etc. Made the agency head responsible for ensuring that adequate information security policies, procedures, and practices are in place and enforced. Created a CIO position within each agency.
Government Information Security Reform Act, October 2000	Primarily addresses the program management and evaluation aspects of security. Requires the following for both unclassified and national security programs: • Annual agency program reviews • Annual Inspector General (IG) evaluations • Agency reporting to OMB on the results of IG evaluations for unclassified Systems and audits of IG evaluations for national security programs • An annual OMB report to Congress summarizing the materials received from agencies
OMB Circular A-130, Management of Federal Resources, February 1996	Revision to December 1985 edition. Implemented Clinger-Cohen Act requirement for greater Office of Management and Budget involvement in Federal computer-security issues. Appendix III specifically addresses Security of Federal Automated Information Resources.
Executive Order 12656, Assignment of Emergency Preparedness	Established the functions, roles, and responsibilities of each Federal department/agency in response to a national emergency. Required

Reference	Basic Security Requirements
Responsibilities, November 1988	each Federal department/agency to accomplish continuity of operations planning.
Executive Order 13010, CIP, July 1996	Established the national Critical Infrastructure Protection (CIP) Program.
PDD#63, CIP, May 1998	Established roles, responsibilities, and requirements for Federal department/agency implementation of CIP.
PDD#67, Enduring Constitutional Government and Continuity of Government Operations, October 1998	Required all Federal departments and agencies to prepare and implement continuity of operation plans by October 1999. Established requirements for ensuring the continuity of the Federal government in all national emergencies.
FPC 65, Federal Executive Branch Continuity of Support Planning; July 1999	Requires that Federal agencies develop and implement Continuity of Support Plans. Requires that these plans: ● Must be maintained at a high level of readiness ● Must be capable of implementation both with and without warning ● Must be operational no later than 12 hours after activation ● Must maintain sustained operations for up to 30 days ● Should take maximum advantage of existing agency field infrastructures
National Plan for Information Systems Protection Version 1.0, January 2000	Implements PDD#63 at a national-level. Established the basic approach for protecting national, cyber-based critical infrastructures.
Practices For Securing Critical Information Assets, January 2000	Prepared by the National Critical Infrastructure Assurance Office. Provides guidance to Federal departments/agencies in establishing security policy, identifying critical infrastructure assets, performing vulnerability assessments, using tools and implementing practices to improve security, and implementing an incident response capability.
NIST Special Publication 800-12, An Introduction to Computer Security: The NIST Handbook, March 1995	Provides computer security guidelines and practices for implementation by Federal departments/agencies.
NIST SP 800-14, Generally Accepted Principles and Practices for Securing Information Technology Systems, 1996	Expands on NIST SP 800-12, and focuses on security of information Systems.

Reference	Basic Security Requirements
NIST Special Publication 800-16, Information Technology Security Training Requirements: A Role- and Performance-Based Model	Establishes a three-tier approach to training based on the position and security responsibilities of trainees.
NIST SP 800-18, Guide for Developing Security Plans for Information technology Systems, 1998	Provides guidelines for the development of comprehensive System security plans. Used as the basis for structuring and developing of this DRP.
NIST Special Publication 800-34 Contingency Planning Guide for Information Technology Systems, December 2001	Provides guidelines to Federal agencies covering the development and implementation of contingency plans of varying types.
General Accounting Office (GAO) Federal Information System Controls Audit Manual, January 1999	Provides approach and procedures for assessing Federal information Systems.
U.S. Agency, Information Technology Continuity Of Operations Planning Program Guidance, November 5, 1999	Provides Department-level guidance for the preparation of Continuity of Support Plans.

1.5. Record of Changes

A history of all changes will be recorded in the *Record of Changes* table immediately following the Table of Contents in the front of this DRP.

1.5.1. Change Drivers

Ongoing changes in systems, software, applications, communications, and operations necessitate modifications and updates to the DRP in order for it to be in a constant state of readiness. Scheduled desk reviews and DRP testing should review the DRP for needed changes. Information that may require plan modifications include the following:

- Organizational and staffing changes
- New safety requirements
- New applications
- Configuration changes
- New vendor agreements

- Changes in resources and responsibilities obtained from other governmental organizations

Also, necessary changes identified during testing should be carefully noted and a modification made to the DRP immediately following the test exercise.

1.5.2. Maintenance of the DRP

The Disaster Recovery Team Security Coordinator (DRT-SC) for the system is responsible for reviewing the DRP, keeping it up to date, ensuring that copies are distributed, and that current versions available in the (*insert server room location*) server room and at the alternate site. Specifically, the DRT-SC is responsible for the following:

- Developing a schedule to review all parts of the DRP and assign responsibility for each portion

- Publishing the DRP review schedule and distributing it to personnel responsible for reviewing and updating the DRP

- Conducting annual DRP tests, documenting results, and improving the DRP to reflect lessons learned during the testing activities

- Monitoring scheduled review actions for timely review and update

- Distributing plan updates and revisions

- Ensuring plans maintained at the *(insert server room location)* as well as at the alternate site are up-to-date at all times

1.5.3. Maintenance of Technical Data

The System Administrators (SAs) are responsible for maintaining the currency of the following technical data contained in this DRP:

- System Network Architecture (Figure 2-1)

- System Component Inventory and Business Functions Supported (Table 2-1)

- System IT Hardware Inventory (Tables 2-2 and 2-3)

- Servers with Automatic Take Over or Fail-over Functionality Upon Component Failure (Table 4-8)

- Servers With No Automatic Take Over or Fail-over Capability (Table 4-9)

- Production/Development Server Configuration Information (Table 4-10)
- Tape Backup/Retrieval Information (Table 4-11)

The data for each of the exhibits and attachments noted will be maintained in electronic files. The electronic files will be current and available to the DRT-SC for incorporation in the next available update of the DRP. The SAs will forward change files to the DRT-SC at least monthly on the last workday or the month (or more frequently if there has been a major change in network components, configuration, or connectivity). For the purposes of this DRP, a "major change" is considered to be any change in the network or its component hardware or software that could result in significant problems or a serious delay in system recovery. Any major changes should be made available to the team if the DRT did not have the revised information available to them in the DRP. Examples of major changes would include, but not be limited to server re-assignments, revision to identified fail-over actions, modifications to configuration and connectivity guidance, and changes in the major components or routing information. For the attachments, examples of a major change would be the addition of a major vendor that supports critical IT resources or the change in contact information for someone on the Emergency Contact List.

1.5.4. Distribution of Changes

When changes are made to this document, only those pages with modifications will be printed and distributed via a transmittal letter with instructions for substituting the changed pages for the originals.

2. CONCEPT OF OPERATIONS

2.1. System Description and Architecture

System Name:

Address:

Provide system description: hardware, telecommunication infrastructure, operating system, and security components. For example: Include the following diagrams or exhibits:

System uses network infrastructure provided by ____, and is on an ATM circuit, which provides access to the Internet. The system Web site infrastructure consists of -#- Microsoft Windows 2000 servers, ## Microsoft NT 4 Servers, and ### F5 Networks BigIP Load Balancing servers. In addition to the servers there is also a Cisco 5500 Catalyst switch and a Cisco 2600 series router. The entire system infrastructure is in a Demilitarized Zone (DMZ) that is isolated from the internal user network (Windows network). The DMZ was established to isolate the system infrastructure since many of its servers are accessible from the Internet. This isolation is a security control taken to protect the larger network infrastructure (see Figure 2-1) from vulnerability. Table 2-1 provides a detailed description of the individual components of the system infrastructure, and Tables 2-2 and 2-3 are lists of IT inventory for the system.

The system LAN includes a Storage Area Network (SAN) and redundant fiber-optic connectivity between servers and storage Systems. The LAN connects to outside contractors and suppliers via Microsoft Point-to-Point Tunneling Protocol (PPTP).

Figure 2-1: Insert architectural diagram inclusive of network infrastructure

Table 2-1: System Component Inventory and Business Functions Supported

SAMPLE FORMAT

Component Name	Business Functions	Software Components	Public IP Address	Private Backend IP Address
Xxxxxxxxxxx	**Production Web Server. Provides access to the following web sites:**	**Sun Solaris 2.7** **HIS 1.3.12** **IBM WebSphere 3.5.3**	**xxx.xxx.xxx.xx**	**xxx.xxx.xxx.xx**

Table 2-2: System IT Hardware Inventory—Servers

SAMPLE FORMAT

Server	Vendor	Model	CPU	RAM	Integ. Storage	RAID (IS)	SAN Conn.	NIC	Barcode	Location

Table 2-3: System IT Hardware Inventory—Components

SAMPLE FORMAT

Component Name	Vendor	Model	NIC	Barcode	Location
SAN/Backups					
	Compaq/Brocade	SAN Switch 16-EL	1x 10/100	N/A	Rack 5
	Compaq/Brocade	SAN Switch 16-EL	1x 10/100	N/A	Rack 4
	Compaq/Brocade	SAN Switch 16-EL	1x 10/100	N/A	Rack 4
-	Compaq	Modular Data Router	-	N/A	Rack 5
-	Compaq	TL891 Mini-library	-	xxx	Rack 5
-	Compaq	TL891 Mini-library	-	xxx	Rack 5
-	Compaq	TL891 Mini-library	-	xxx	Rack 5
-	Compaq	HSG80/MA8000	-	xxx	Rack 5
-	Compaq	HSG80/MA8000	-	xxx	Rack 6
-	Compaq	Fibre Channel Tape Controller	-	xxx	Rack 2
-	Compaq	DLT Tape Library	-	xxx	Rack 2
Networking					
K-9Z-A	Cisco	Catalyst 5500	-	8623	Aux. Rack 2
-	Cisco	Catalyst 5509	-	E01	Aux. Rack 2, offline
-	Cisco	2600	-	381035	Aux. Rack 1

Component Name	Vendor	Model	NIC	Barcode	Location
Monitors					
-	Matsushita	Generic	-	D242735	SYSTEM13
-	Compaq	V55	-	324661	Rack 2
-	Dell	Generic	-	10575	Rack 3
-	Compaq	TFT5000	-	N/A	Rack 4
-	NEC	MultiSync 3V	-	8122	UPS01
-	Compaq	Qvision 172	-	48234	Rm. 9007
-	CD Writer	Generic	-	50035	SYSTEM13
Other					
-	Compaq	KVM Switch 8-port	-	N/A	Rack 2
-	Compaq	KVM Switch 8-port	-	N/A	Rack 3
-	Compaq	KVM Switch 8-port	-	N/A	Rack 4
-	Compaq	KVM Switch 8-port	-	N/A	Rack 4

2.1.1. System Web Site Infrastructure

Two of the Windows 2000 servers currently act as the Primary Domain Controller (PDC) and a Backup Domain Controller (BDC) for the system Domain. A third Windows server is currently the VPN server, which is running Microsoft's PPTP and IPSEC. This server allows developers and administrators to log into the INETSYSTEM domain using a secure connection across the Internet. A Windows NT4 server is currently being used as the backup server for the development servers and other servers used for administrative tasks.

The # Windows 2000 servers handle a variety of functions. The production and development Web sites consist of Windows 2000 servers running IIS5 and SQL 2000. Other Windows 2000 servers run Microsoft Site Server, IPCheck, Norton AV/Symantec System Center, Liebert MultiLink, and Veritas NetBackup. The servers supporting the production and development environments are depicted in Exhibit 5 and 6.

The F5 BigIP servers handle load balancing but also separate the private IP subnet from the public IP addresses using Network Address Translation (NAT). There is only one server that is publicly accessible without using the BigIP servers: the VPN server. All other servers that can be accessed from the outside world are accessed through BigIP. This provides an additional layer of security.

## of the Windows 2000 servers are connected to a SAN, which has a total of five terabytes of storage space. These servers also have Compaq Remote Insight Boards that are used for remote administrative purposes.

2.1.2. Security Software

The router supporting the system infrastructure is running Inter-Network Operating System Firewall to isolate system from (*the network provider*). All system servers are running Norton Anti-Virus. The system site server (*name of server*) is running Symantec System Center, as is the Primary server (*server name*).

2.1.3. System Backup Procedures

Incremental backups are performed on all servers Monday through Thursday. On Fridays, a full backup is performed. There is an eight-week tape rotation schedule for general backup tapes and monthly archive tapes are kept indefinitely. Monthly archive tapes are made the last Friday of every month.

Backup tapes are kept on-site in the DLT Library and then sent off-site to the offsite data storage facility. Every weekday morning between the hours of 10 a.m. to12 p.m., the offsite storage vendor collects the backup tapes and delivers the next tape in the rotational set. All of this transaction is recorded on a form provided by the offsite vendor. The information is entered in the offsite vendor's database when their Service Representative arrives back at the storage facility. More information on backup procedures and off-site storage can be found in Tables 4-11 through 4-14 and in Appendix C.

2.2. Line of Succession

The line of succession for critical DRT members is presented in this section.

2.2.1. Disaster Recovery Manager

If the DRM is not available the order of succession for this role is as follows:

- Disaster Recovery Coordinator
- DRP Security Coordinator

The person succeeding the DRM would also perform their regularly assigned DRT roles and responsibilities. They may delegate their duties to the System Administrators as appropriate and as needed to facilitate recovery.

2.2.2. Disaster Recovery Coordinator

If the DRC is not available the line of succession for this role is as follows:

1. DRP Security Coordinator
2. Disaster Recovery Manager

The person succeeding the DRM would also perform their regularly assigned DRT roles and responsibilities. They may delegate their duties to the System Administrators as appropriate and as needed to facilitate recovery.

2.2.3. DRP Security Coordinator

If the DRT-SC is not available the line of succession for this role is as follows:

1. Disaster Recovery Coordinator
2. Disaster Recovery Manager

The person succeeding the DRT-SC will also perform their regularly assigned DRT roles and responsibilities. They may delegate their duties to the System Administrators as appropriate and as needed to facilitate recovery.

2.2.4. System Administrators

If one or both System administrators are not available, then follow the steps documented in Appendix A.

2.3. Responsibilities

Within the system, a DRT has been established to respond effectively, function in an efficient manner, allow independent tasks to proceed simultaneously, and maintain overall control of the recovery and reconstitution process. The system DRT has been established, briefed, and trained to respond to the contingency events covered in this DRP. This team is responsible for recovery of the system computer environment and applications housed at (system address), 9th floor server room,(city). Members of this team include those personnel responsible for the daily operations and maintenance of the (system name). Because of their familiarity with the System, the DRT membership will consist of persons currently assigned to system IT operations. The objectives of the DRT are to successfully provide the following:

Incident response—Assemble the people and resources needed to respond to an incident and evaluate conditions.

Continuity of IT services and initial recovery—Assessing the status of operations, recommending courses of action, and implementing whatever intermediate measures available to continue IT services, even if at degraded level, until conditions permit the full restoration of normal levels of support.

Full reconstitution of IT operations—Applying the materials acquired and resources available to fully reconstitute normal operations and levels of support at the original or a new permanent location.

2.3.1. DRT Positions and Assigned Roles and Responsibilities

The System DRT consists of the positions shown in Table 2-3.

Table 2-4: DRT Roles and Responsibilities

DRT Position	Roles and Responsibilities
Disaster Recovery Manager (DRM)	This position will normally be filled by the System CTO. Responsibilities include the following: ● Directing and overseeing the effective accomplishment of disaster recovery planning ● Directing and supporting the establishment, staffing, training, and preparation of a System DRT ● Officially declaring a disaster situation and authorizing the initiation of the DRP ● Providing high-level management and oversight during disaster recovery efforts ● Obtaining the funding and resources needed to accomplish disaster recovery planning, establish and train a DRT, and provide whatever is needed to successfully execute the plan ● Ensuring annual testing of the DRP and incorporating any required changes ● Ensuring required agreements are prepared for any local support required in a disaster ● Keeping the Department's CIO informed of status throughout a disaster ● Notifying and providing updates to the Department's senior management and Chief of Public Affairs as appropriate
Disaster Recovery Coordinator (DRC)	The SystemWebmaster functions as the DRC. Responsibilities include the following: ● Determining the extent and seriousness of a disaster ● Notifying the DRM of a disaster immediately upon notification ● Assembling and presenting assessment data to the DRM for a disaster declaration decision ● Managing and overseeing all DRT actions and activities ● Issuing disaster recovery directives

DRT Position	Roles and Responsibilities
	● Keeping the DRM informed of DRT activities and recovery progress ● If necessary, directing and managing the relocation to alternate site operations ● Ensuring the proper recovery and reconstitution of all platforms and applications and the full restoration of network operations ● Maintaining appropriate recovery documentation in magnetic and paper form ● Serving as liaison between the CIO personnel and system staff
DRT Security Coordinator (DRT-SC)	The SystemComputer Security Officer will normally fill this position. Responsibilities include the following: ● Performing as deputy to the DRC ● Monitoring recovery and reconstitution activities to ensure that security measures are reestablished and maintained ● Obtaining necessary clearances for vendor personnel brought in to support recovery activities ● Conducting risk assessments during the course of the recovery to ensure actions taken do not put the System at further risk or, if risks are noted, that viable risk mitigation actions are identified and implemented ● Ensuring backup procedures are reconstituted ● Participating in other recovery activities as directed by the DRC
DRT SAs (System SAs)	The SAs will provide technical support to the DRT (for the system environment, the SAs will fill the role of DRT Technical Members). Their responsibilities include the following: ● Assisting the DRC with the damage assessment and providing recommendations concerning recovery and reconstitution efforts ● Functioning as technical leads for all recovery and reconstitution activities ● Maintaining file and System backups in all recovery media (tape, disk or optical) ● Participating in the move to, and recovery of IT services at, the RTSC alternate site

DRT Position	Roles and Responsibilities
	● Accomplishing whatever technical actions are necessary to recover and fully reconstitute platforms, applications and network operations ● Ensuring connectivity with appropriate clients ● Establishing the required connectivity to the effected end-users' sites using the predetermined communications infrastructure ● Providing other technical support and general assistance required by the DRC

2.3.2. Disaster Recovery Response Phases

The disaster recovery response process will be accomplished in the following phases:

Notification and Activation Phase—detect and assess damage and to activate the plan (Section 3.0)

Recovery Phase—restore temporary IT operations and recover damage done to the original System at the current site or an alternate site (Section 4.0)

Reconstitution Phase—restore IT System processing capabilities to normal operations (Section 5.0)

Following these phases will ensure that effective management and controls exist throughout the recovery and rebuilding of system IT operations.

2.3.3. System DRT Emergency Operations Center

The Emergency Operations Center (EOC) is the location identified for the assembly of the DRT immediately following declaration of a disaster. It is also the location from which the DRT Coordinator (DRC) will manage and coordinate recovery and reconstitution activities, and where DRT members will meet to report the status of their actions. If the (*system name*) facility is accessible, then the EOC will be the 9th floor server room. If the (*system name*) facility is not accessible, then the server room on the 4th floor of (*service provider address*) located at (*address*), (city), will be the designated alternate EOC. If the alternate site is activated, then the EOC will be in the (*service provider address*) location to facilitate communication and coordination with (*service provider*) and the alternate site.

2.3.4. Training, Testing, and Exercising the DRT

New DRT members will be trained in standard disaster recovery processes and procedures. The DRT-SC will ensure that members are provided with up-to-date copies of this DRP. The DRT-SC will also periodically test DRT members on aspects of DRP policies, processes, and procedures that are unique to system operations and essential to recovery and reconstitution. A test strategy will be developed and used to conduct formal tests and exercises of the team. The DRP Evaluation Form, Table 3-2, will be prepared following each test or exercise, and the DRC will use the information to make any necessary modifications to plan processes and procedures.

2.3.5. Other Supporting Agencies

The Agency CIO and (*other organizations/agencies as appropriate*) will support and coordinate with the DRC. Points-of-contact for each of these organizations is provided in Appendix A, Emergency Contact List.

3. NOTIFICATION AND ACTIVATION PHASE

This phase addresses the initial actions taken to detect and assess damage inflicted by a disruption to the *(insert name)* system. Based on the assessment of the event, the DRP may be activated by the DRM. Notification procedures are documented in Section 3.1 and Appendix A. The primary objectives of the Notification and Activation Phase are as follows:

- Advising the DRM of an emergency condition or disaster situation.
- Documenting events, issues, and activities through the course of the incident
- Contacting and recalling the DRT members to respond to the contingency
- Assembling the DRT at the designated EOC
- Alerting vendors of the contingency and the potential need for their support.
- Briefing the DRT on known facts about the contingency
- Assigning DRT members specific inspection and evaluation assignments
- Establishing reassembly time and location for DRT evaluation reports

3.1. Notification Procedures

Table 3-1 provides a step-by-step summary of Notification and Activation Phase activities. Appendix A contains emergency contact information.

Table 3-1: Notification and Activation Phase Activities

Task Description	When to Begin Task	Responsible Party(ies)
1. Notify the DRC, or other member of the DRT, of the event in as much detail as known.	As soon as first responder is knowledgeable of the event.	First Responder: The first person to detect that the disaster has occurred.
A. Notify the DRM of the event and provide briefing of the situation. B. Contact the DRT SAs, inform them of the event, and advise them to begin assessment procedures. Determine target time for assessment to be complete and for the assessors to report back. C. Initiate Disaster Log Form (Table 3-4) and begin journaling all activities. D. Perform Facility/Site Damage Assessment, using the Facility/Site Evaluation Checklist (Table 3-5)	Upon notification from the First Responder	DRC (if the DRC is not available any member of the DRT is responsible for this activity)
2. Perform damage assessment using the following assessment checklists: Platform Damage and Operability Checklist (Table 3-6) Application Status Checklist (Table 3-7) Network Operations Checklist (Table 3-8)	Upon notification by the DRC	SAs
3. Contact the DRT-SC to communicate the situation and activate him/her to one of the EOCs for deployment and a briefing: *(system address)* if accessible (*EOC)* server room if (*system address*) is not accessible	Upon notification by the DRC	DRM

Task Description	When to Begin Task	Responsible Party(ies)
4. Provide damage assessment results and recommendations to the DRT.	As soon as assessments are complete	SAs DRC
5. Conduct Security Assessment using Table 3-9, Security Evaluation Checklist based on the assessment reports. Specifically: Document existing security controls Identify and document any recommendations for improving security Document any potential vulnerabilities and risks	As soon as assessments referenced above are available.	DRT-SC
6. Make determination on how to recover (choose one): Implement appropriate Continuity of Support solution Activate the DRP that calls for reconstituting services at the alternate site Terminate DRT operations	At DRT briefing once assessments are available.	DRM

3.2. Damage Assessment Procedures

The DRC will ensure that each DRT member understands, and is prepared to perform specified, pre-assigned areas of evaluation that will provide an overall picture of (*name of system*) ability to recover and sustain IT operations. Areas evaluated will include the following:

Facility/Site Damage—The DRC and the DRT-SC will normally perform Facility/Site Damage Evaluation (Table 3-5)—Depending on conditions and the discretion of the DRC, and the facility/site evaluation. The degree of damage done to the facility will be determined, initially focusing on the ability to both gain access to the building and occupy it. If the building is accessible and can be utilized, the evaluation will then focus on the operational capability the 9th floor server site. In addition to assessing the extent of physical damage sustained, the electrical, environmental, and communications capabilities of the site must be assessed. Included in this evaluation would be the operational status of fire retardant systems, environmental/cooling systems, and electronic physical security systems. Overall, this evaluation must determine whether a safe and adequate physical operating environment can be established and maintained to support IT operations. Based on conditions, it would also determine the need to relocate to the alternate site.

Platform Damage and Operability—The platform evaluation (Table 3-6) will normally be assigned to the DRT SAs. The condition of all servers must be evaluated. Physical condition will be determined, as well as the status of all operating systems. Also, the ability of each server to function properly and to sustain a normal-level of operations must be determined. The condition of each server will be documented and an assessment made as to its ability to fulfill its primary assigned function. If a portion of the platform inventory is inoperable, recommendations for reassigning operable servers must be developed. The evaluation must determine the overall server operational capability and provide an assessment of the level of operations that can be recovered and maintained. This could range from none to full operational capability. The level of disruption could necessitate the temporary cessation of development activities and reassigning platforms to support production at either a full or reduced level of operations. Overall, the assessment must determine the condition of system platforms and the type and level of operations they can support. If there is an inability to support an acceptable level of production operations, or if there will be an unacceptably long outage of development operations, a determination as to the need to relocate to the (*alternate site*) will be made. The final assessment must include a list of replacement equipment needed to recover and eventually reconstitute operations at the *(system address)* facility.

Application Status—The DRT SAs must assess the availability and recoverability of system applications (Table 3-7). This includes the quality of data stored on-site, and the potential need to retrieve backup media to recover operations. Overall, conditions must be documented and a determination made as to whether or not full program support can be recovered. If not, what level of reduced support can be made available and for how long? If facility, platform, or network conditions warrant, the ability to relocate and recover applications at the *(alternate site)* will be assessed. The final evaluation will include ability to effectively recover applications and the quality of information stored and recoverable in the SAN.

Network Capabilities—The DRT SAs will evaluate the condition of routers, switches and data communication lines and their ability to reconnect, reestablish and support network operations (Table

3-8). An assessment will be made as to the networks ability to support either full or reduced operations. Considerations will be given to the ability to support the production environment, if development activities are suspended. Overall, the assessment must determine the condition of the system network and the type and level of operations it can support. If there is an inability to support an acceptable level of production operations, or if there will be an unacceptably long outage of development operations, a determination as to the need to relocate to the (*alternate site*) will be made. The final assessment must include a list of replacement equipment needed to recover and eventually reconstitute the network.

Security Evaluation—The DRT-SC will assess the results of the above evaluations and determine the level and quality of security controls and safeguards that can be recovered and maintained at the (*system address*) server site (Table 3-9). An overall assessment as to the quality and acceptability of security measures must be made and documented, along with any recommendations for improving security. If security cannot be established and maintained at a satisfactory level, potential impacts should be addressed to assist in an assessment on the need to relocate to the alternate site.

3.2.1 DRT Report/Recommendations for the DRM

The DRT reassembles following the completion of the above evaluations and proceeds with the collection of information and the development of an overall assessment report for the DRM. The report will include recommendations for appropriate action that could include declaration of a disaster and execution of the DRP, or some other approach to recovering and reconstituting operations. The DRC will obtain a verbal report from the DRT members responsible for each of the evaluation areas outlined in Section 3.2 above. The DRC should discuss potential courses of action for recovering/reconstituting IT operations with the DRT Members, obtaining their recommendations on the approach to recommend to the DRM.

3.3. Activation Decision

The final decision on actions to be taken rest with the DRM. Upon receipt of the initial DRT assessment of conditions and capabilities following an incident, the DRM must make a decision on the approach that will be used to recover from its impacts and reinstate critical IT service support.

Table 3-3 provides guidelines to aid the DRM and DRC in making the disaster recovery decision. After reviewing the assessments and conferring with DRT, the DRM must decide to take one of the following actions:

1. Activate the appropriate procedures from the Continuity of Support Plan (Section 4 of this DRP).

2. Activate the DRP section of this plan requiring reconstitution of operations at the alternate site (Section 5 of this DRP).

3. Terminate the DRT and handle situation using standard operating procedures.

Table 3-2: DRP Evaluation Form

Purpose*:* The purpose of this report is to capture information on problems encountered during execution of the *system* DRP, and to identify necessary changes in DRP policies, processes and procedures to prevent reoccurrence.

Please prepare a separate form for each problem/issue noted. If more space is needed, continue on the reverse or attach additional pages.

Reported By:	**Office/Phone #:**	**Date:**

Problem/Issue: *(Define the problem or issue. Be as specific as possible. Describe events leading up to and following its occurrence)*

Disaster Recovery Phase: *(Identify the phase of the recovery process in which the problem/issue arose)* Notification and Activation Recovery Reconstitution	**Source of Problem/Issue:** *(Identify the basic cause of the problem/issue, if known)* Event Not Covered in DRP Insufficient Training/Preparation Weakness in Normal Operations Other (Explain):_______________________________

Impact of the Problem/Issue: *(Define the specific impacts of the problem/issue on the DRT's ability to execute the DRP)*

Recommendations: *(Provide recommendations for changes in DRP policies, processes andr procedures that would help to prevent the reoccurrence of the problem/issue)*

Table 3-3: Disaster Recovery Decision Guidelines

If….	Then…
The situation fits one or more scenario found in the Continuity of Support Plan (Section 4) and onsite recovery is possible… NOTE: It has been established that a minimum of 3 servers must be operational in order to maintain mission-essential services (production environment only).	Activate the appropriate recovery scenarios from Section 4. Distribute DRP Evaluation Forms (Exhibit 13) and instruct all DRT members to record any problems encountered or gaps in procedures identified throughout the DR process.
It is anticipated that the (*system name*) system will be unavailable for more than 48 hours and/or the facility is damaged and is expected to be unavailable for more than 24 hours…	Activate the DRP found in Section 5 of this document. Distribute DRT Evaluation Forms and instruct all DRT members to record any problems encountered or gaps in procedures identified throughout the DR process.
Relocation is not indicated and the situation can be handled by existing operating procedures…	Disband the DRT and instruct DRT SAs to invoke the appropriate standard operating procedures.

Table 3-4: Disaster Log Form

<table>
<tr><td colspan="4"><b>Page____ of ____</b>
<b>System Disaster Log</b></td></tr>
<tr><td><b>Date/Time
(a.m. or p.m.)</b></td><td><b>Event
<i>(Recorded By)</i></b></td><td><b>Comments</b></td><td><b>Action Taken
<i>(If Any)</i></b></td></tr>
<tr><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td></tr>
</table>

Table 3-5: Facility/Site Evaluation Checklist

Note: To be completed by the DRC or designated back up.

Areas of Evaluation	**Comments**
Assess the following in relation to the facility's/site's availability and usability:	
Identify extent of damage to the facility.	
Determine condition of equipment.	
Determine condition of environmental systems.	
Determine condition of physical security controls.	
Describe salvagability of supplies.	
Assess operational capability.	
Define restoration requirements.	
Determine minimum level of recovery that needs to be accomplished to make site usable and available to support continuity of IT services.	
Work with building management and disaster response agency, if applicable, to schedule salvage and restoration.	
Monitor salvage and restoration operations and report progress to coordinate on overall recovery and reconstitution of IT operations.	
Advise the DRC and DRT of status and progress.	
Develop a detailed accounting of damages for DRM review/decision process.	
Prepare a detailed written description of facility/site damages, specifically identifying: ● Items undamaged and operational ● Damaged items that can be recovered/repaired ● Destroyed items (i.e., unsalvageable) needing to be replaced.	
Note any identifiable costs associated with return site to a usable condition.	

Areas of Evaluation	**Comments**		
Summary of Findings:			
Facility/Site Conditions:			
Damage Assessments:	**Unusable**	**Extensive**	**Minor**
Overall Facility	o	o	o
Server Site	o	o	o
Structural	o	o	o
Equipment	o	o	o
Environmental Systems	o	o	o
Physical Security Controls Supplies	o	o	o

Comments:

Recommendations:

Assessor Signature: **Date:**

Table 3-6: Platform Damage and Operability Checklist

Instructions: To be completed by an SA. Assess the status of system servers using the following checklist.

Areas of Evaluation			
Platform Operability			
Damage Assessments	Undamaged/ Usable	Recoverable/ Repairable	Destroyed/ Unsalvageable
xxxxxxWEB01	o	o	o
xxxxxxWEB02	o	o	o
xxxxxxWEB03	o	o	o
xxxxxxWEB04	o	o	o
XxxxxxWEB05	o	o	o
xxxxxxWEB06	o	o	o
xxxxxxWEB07	o	o	o
xxxxxxWEB08	o	o	o
xxxxxxWEB21	o	o	o
xxxxxxSQL05	o	o	o
xxxxxxSQL06	o	o	o
xxxxxxSQL07	o	o	o
xxxxxxSQL08	o	o	o
xxxxxxSQL21	o	o	o
SYSTEM02	o	o	o
SYSTEM03	o	o	o
SYSTEM00	o	o	o
Xxxxxxxx01	o	o	o
SYSTEM05/13	o	o	o
SYSTEM130	o	o	o

Areas of Evaluation			
Platform Operability			
Damage Assessments	Undamaged/ Usable	Recoverable/ Repairable	Destroyed/ Unsalvageable
xxxxxxSS01	o	o	o
xxxxxxUPS01	o	o	o
xxxxxxBIP01	o	o	o
xxxxxxB1P02	o	o	o
xxxxxxVPN01	o	o	o
xxxxxxCON01	o	o	o
xxxxxxVPN01	o	o	o
xxxxxxSQL01	o	o	o
xxxxxxSQL02	o	o	o
xxxxxxSQL03	o	o	o
xxxxxxSQL04	o	o	o
Comments: (Define the overall extent of damage to hardware, the type and approximate cost of repairs required, the ability to reconfigure the infrastructure to use surviving equipment, the time needed to reconfigure, and the level of support that reconfiguration will be able to provide).			
Define the level of service that can be provided with the amount of equipment operational (e.g., reduced production support, production but no development support, production and development support at some level).			
Determine the availability and usability of all operating systems.			
Develop a list of components to be purchased and their specifications for forwarding, through the DRC, to Procurement.			
Review the recovery steps documented in this DRP and make any changes necessary to fit the situations present at the moment.			

Areas of Evaluation			
Platform Operability			
Damage Assessments	Undamaged/ Usable	Recoverable/ Repairable	Destroyed/ Unsalvageable
Identify support required to reconfigure surviving servers to provide for continuity of IT services.			
Prepare a detailed written description of platform damages, specifically identifying: ● Servers undamaged and operational ● Damaged servers that can be recovered/repaired ● Destroyed servers (i.e., unsalvageable) that must be replaced			
Note any identifiable costs.			

Summary of Findings:

Recommendations:

Assessor Signature: **Date:**

Table 3-7: Application Status Checklist

Instructions: To be completed by an SA

Areas of Evaluation	Comments
Assess the status of system applications:	
Determine recoverability of applications.	
Identify backup versions required for application recovery.	
Initiate emergency production schedule for critical applications processing.	
Analyze the need for additional recovery activities such as data base restores or individual file restores	
Identify and document actions that must be taken to provide for continuity of IT services based on operational capabilities reported for the system servers and network operations.	
Determine ability to support the production environment.	
Determine ability to support the development environment.	
Determine ability to support the data entry/collection functions.	
Prepare a detailed written description of application status, specifically identifying: ● Applications operational ● Inoperable applications that can be recovered ● Lost applications that must be replaced	
Note any identifiable costs.	

Summary of Findings:

____

____

____

____

Recommendations:

____

____

____

Assessor Signature: ______________________ **Date:** ______________________

Table 3-8: Network Operations Checklist

Instructions: To be completed by an SA. Assess the status of network operations using the following checklist.

Damage Assessments	Undamaged/ Usable	Recoverable/ Repairable	Destroyed/ Unsalvageable
Data Communication Lines	o	o	o
ATMs	o	o	o
Switches	o	o	o
Routers	o	o	o
Firewall	o	o	o
Intranet	o	o	o
Internet	o	o	o
Comments: (Define the level of damage done to the communications network and the level of work needed to repair. Provide estimate of downtime)			

Actions	Comments
Coordinate restoration of operations with CIO and applicable vendors.	
Determine what will be required to recover network operations to the extent possible to provide for continuity of IT services.	
Work with CIO to determine what will be required to restore voice, data, and video communications links between users and the computer, regardless of location.	
Determine the availability, and the ability to restore necessary telephone service.	
Prepare a detailed written description of the damage to network operations, specifically identifying: • Equipment/software undamaged and operational • Damaged equipment/software that can be recovered/repaired • Destroyed equipment/software (i.e., unsalvageable) that must be replaced	
Note any identifiable costs.	

Summary of Findings:

Recommendations:

Assessor Signature: **Date:**

Table 3-9: Security Evaluation Checklist

The DRT Security Coordinator completes this checklist. They will assess the physical and IT security capabilities.

Areas of Evaluation	Comments
Review the applications and platform assessment forms to determine the availability of the proper back-up software, applications software, applications data and documentation required to provide for the continuity of IT services.	
Review assessment form and coordinate with the facility reviewer to assess the status of physical security controls.	
Use assessment forms and coordinate with the platform and network operations reviewers to assess the status of IT security measures.	

Summary of Findings:

____

____

____

____

Recommendations:

____

____

____

Assessor Signature: **Date:**

______________________________ ______________________________

4. RECOVERY PHASE

This section provides procedures to recover and provide service sufficient to meet the minimal needs of users of the system, as required by OMB Circular No. A-130, Appendix III. This Circular acknowledges that service disruptions are inevitable in an automated system. Given this, procedures must be developed to ensure recovery of the critical IT services in order to support continuity of mission-essential functions.

Sections 4.2 through 4.7 provide recovery procedures in table format for the disaster scenarios identified as most likely to occur based on the residual risks identified in the system Risk Assessment that would impact the ability to perform identified mission-essential functions in the system environment as identified in the BIA interviews. Recovery procedures are documented as step-by-step instructions for ease of use. The recovery actions were developed to provide the appropriate level of recovery while balancing the importance of the service with the cost to recover per OMB A-130 guidance.

The contingency plan information is presented in table format organized by critical element:

- Section 4.1 contains a table of contingency scenarios and recovery actions for targeted hardware failures.
- Section 4.2 contains a table of contingency scenarios and recovery actions for security-related failures.
- Section 4.3 contains a table of contingency scenarios and recovery actions for mass storage and backup-related failures.
- Section 4.4 contains a table of contingency scenarios and recovery actions for network-related failures.
- Section 4.5 contains a table of contingency scenarios and recovery actions for targeted environmental failures.
- Section 4.6 contains a table of contingency scenarios and recovery actions for people/resource failures.
- Section 4.7 contains a table of recovery actions for a failure or disruption requiring reconstitution of services at an alternate location.
- Section 4.8 contains exhibits relevant to, and supportive of, sections 4.1 through 4.6.

4.1. Critical Element: Hardware Contingency Scenarios

This section contains a table listing contingency scenarios and recovery procedures for hardware failures recoverable at the *(system address)* facility. They are arranged from the scenarios that affect the most critical equipment and are the most likely to occur to those who would have a minimal impact and whose likelihood of occurrence is very low.

Table 4-1: Hardware Contingency Scenarios

Failure Scenario	When to Begin Recovery Activity	Recovery Activities	Responsible Party(ies)
Disruption or Failure of F5 Big IP Server	Immediately upon detection or notification of failure	**EXAMPLE OF SCENARIO AND RECOVERY ACTIVITIES** If either server fails, the other automatically assumes all load balancing responsibilities. 1. Reboot the failed server. If this fails, troubleshoot the problem and attempt to resolve. If this fails proceed to step 3. 2. Rebuild the server. Apply current service packs and hot fixes from www.microsoft.com. Note: Repair/replace the faulty server as quickly as possible. As long as the system is running on a single F5 Big IP server, there is a single point of failure that, if experienced, would result in a major disruption of production operations. 3. Bring the server back on line.	Fail-over occurs automatically; however, system SAs monitor performance. SAs
		(Insert scenarios and recovery activities specific to system)	

4.2. Critical Component: Security Scenarios

This section contains security-related contingency scenarios and recovery procedures. The scenarios are presented in the order of the greatest impact and most likely to occur to the least impact/least likely to occur.

Table 4-2: Contingency Scenarios and Recovery Actions For Security-Related Failures

Failure Scenarios	When to Begin Recovery Activity	Continuity/Recovery Activity(ies)	Responsible Party(ies)*
Virus Detected in System	Immediately	**EXAMPLE OF SCENARIO AND ACTIVITIES** 1. Report incident to the DRT-SC. 2. Identify infected system(s). 3. Disconnect compromised systems from the network. 4. Analyze and evaluate the infection and identify the extent of the damage. 5. Eradicate the virus. 6. For a program infector virus, use write-protected or manufacturer disks to overwrite the infected files and restore the original copy of the programs 7. For a boot-sector virus, copy all data from the disk onto a clean disk, reformat the original disk, and copy the data back to the original disk. 8. After the infection has been removed, clean and replace all suspect diskettes using the same methods detailed above. 9. If data was lost or corrupted restore files by retrieving the last good (uninfected) backup tape using the procedures found in Exhibit 24. 10. Reconnect to the network and monitor for signs of re-infection from a missed file, etc. 11. Review audit logs. Provide all relevant information to the DRT-SC. 12. Keep the DRM and Security Officer apprised of the situation, document lessons learned, and update Security Policy if needed to address this instance.	1-11. SAs 12. DRT-SC

Failure Scenarios	When to Begin Recovery Activity	Continuity/Recovery Activity(ies)	Responsible Party(ies)*
		(Insert scenarios and recovery activities specific to system)	

4.3. Critical Component: Mass Storage/Backup

This section contains contingency scenarios and recovery procedures for possible mass storage and backup failures.

Table 4-3: Contingency Scenarios and Recovery Actions for Mass Storage and Backup-Related Failures

Failure Scenarios	When to Begin Recovery Activity	Continuity/Recovery Activity(ies)	Responsible Party(ies)*
		(Insert scenarios and recovery activities specific to system)	

4.4. Critical Component: Network Connectivity

This section contains contingency scenarios and recovery procedures for identified network connectivity failures.

Table 4-4: Contingency Scenarios and Recovery Procedures For Identified Network Connectivity Failures

Failure Scenarios	When to Begin Recovery Activity	Continuity/Recovery Activity(ies)	Responsible Party(ies)*
		(Insert scenarios and recovery activities specific to system)	

4.5. Critical Component: Environmental Controls

This section contains contingency scenarios and recovery procedures for possible environmental failures.

Table 4-5: Contingency Scenarios And Recovery Procedures For Possible Environmental Failures

Failure Scenarios	**When to Begin Recovery Activity**	**Continuity/Recovery Activity(ies)**	**Responsible Party(ies)***
Power Outage	Immediately	**EXAMPLE SCENARIO AND RECOVERY ACTIONS** 1. UPS should automatically cut on as soon as power is lost. 2. Contact building management to determine the anticipated duration of the outage. 3. If the outage is expected to last loner than the lifespan of the UPS then begin an orderly shutdown following procedures found in Exhibit 26.	Automatic fail-over 2-3 SAs
		(Insert scenarios and recovery activities specific to system)	

4.6. Critical Element: People

This section contains contingency scenarios and recovery procedures people-related risks.

Table 4-6: Contingency Scenarios And Recovery Procedures People-Related Risks

Failure Scenarios	When to Begin Recovery Activity	Continuity/Recovery Activity(ies)	Responsible Party(ies)*
		(Insert scenarios and recovery activities specific to system)	

4.7. Relocation Scenario

This section contains information to be followed in the event that a system failure or disruption necessitates recovery of operations at an alternate processing site. The alternate site for the (*system name*) system is a dedicated warm site located near (*location*) owned and operated by the Agency CIO. The Memorandum of Agreement (MOA) and Interconnecting System Agreement (ISA) for this service is located in the appendix section of this document.

The production environment only will be reconstituted. Remote developers will not have access to the reconstituted system. The servers are configured to allow remote access by *(insert system name)* SAs.

Table 4-7: Recovery Actions for A Failure or Disruption Requiring Reconstitution Of Services At An Alternate Location

Failure Scenarios	When to Begin Recovery Activity	Continuity/Recovery Activity(ies)	Responsible Party(ies)*
Event occurs that renders existing production site inoperable for at least 12 hours	As soon as the DRM invokes the DRP and advises the DRT to begin reconstitution procedures.	*(Insert recovery activities specific to the system)* *(These should be consistent with the MOA and ISA)*	

4.8. Recovery Phase Exhibits

This section contains the following exhibits that support the procedures documented in the recovery tables found in Sections 4.1 through 4.6:

- Table 4-8: Servers With Automatic Take Over or Fail-over Functionality Upon Component Failure
- Table 4-9: Servers With No Automatic Take Over or Fail-over Capability
- Table 4-10: Production/Development Server Configuration Information
- Table 4-11: Tape Backup/Retrieval Information
- Table 4-12: Offsite Tape Retrieval Contact List
- Table 4-13: Critical Backup and Reporting Tasks
- Table 4-14: Database Backup Schedule
- Table 4-15: SAN Shutdown/Power-up Steps
- Table 4-16: SAN Requirements

Table 4-8: Servers with Automatic Take Over or Fail-over Functionality Upon Component Failure

SAMPLE FORMAT

Component Failure	Server Business Function	Business Function Effects	Technical Interdependencies	Actions
XXXXXXWEB01	Production Web Server	Possible loss of access to the following production Web sites on this server. -X -X -X	Uses XXXXXXSQL05 as database backend. Load-balanced with XXXXXXWEB02.	XXXXXXWEB02 automatically assumes full load without manual intervention or loss of functionality or accessibility

Table 4-9: Servers With No Automatic Take Over or Fail-over Capability

SAMPLE FORMAT

Component Failure	Server Business Function	Business Function Effects	Technical Interdependencies
XXXXXXWEB07	Development Web Server	Loss of access to Web development for system surveys.	Uses XXXXXXSQL08 as database backend.

Table 4-10: Production/Development Server Configuration Information

SAMPLE FORMAT

Servers	**Server Configuration Data**
Production Servers	All system Web servers are configured as follows: *(system specific information)*
Database Servers	*(system specific information)*
Site Servers	**EXAMPLE** The Site Server is configured as follows: **Server Manager:** **1 Log Data Source** 3 Servers 3 Sites (1/server) **Log Data Source:** Name: LDS Type: Auto Detect

Servers	Server Configuration Data
	Servers: Type: World Wide Web Index Files: index.asp, index.html, index.htm, default.asp, welcome.asp Timezone: GMT 00:00 Monrovia, Casablanca **Sites:** Excludes: *.gif *.jpg *.jpeg *.cdf *.png *.exe *.txt *.inc *.css Visit Algorithm: A visit ends after: 30 minutes. Multiple users use the same username: checked **Options:** **Import:** Drop database indexes before import: checked Adjust request timestamps to: GMT –05:00 Eastern Time Start day of week: Monday After import, look up unknown HTML file titles: checked **Crawler list:** spider bot worm rover Scooter slurp Architext InfoSeek Lycos Netscape-Catalog IBM_Planetwide crawl inktomi googlebot Following are the locations of critical files on the site server. Report Templates = D:\infra

Servers	Server Configuration Data
	Finished Reports = D:\ssreports Batch Files = C:\ Log Files = D:\logfiles **Batch File Modifications for Reporting Tasks:** All batch files on the site server except for autossca.bat require variables passing the month and year for the reporting tasks to work properly. These are passed as follows (substitute correct month/year): copylogs.bat Feb2002 copylogs_cs.bat Feb02_cs copylogs_re.bat Feb02_re copyreports.bat Feb2002 Upon completion of the site server reports and successful copying to the live site, the reporting period must be modified by doing the following: In \\xxxxxxWEB01\e$\ixxxpub\Systemmembers\ssreports\Feb2002\inc change the following line as appropriate: Session ("curmonth")="February 2002” In \\xxxxxxWEB01\e$\ixxxxxx\Systemmembers\ssreports\index.asp change all occurrencessystem of the following variables as appropriate: TheGMonth = 2 (indicating February) TheGYear = 2002
Authentication Server	*(system specific)*

Table 4-11: Tape Backup/Retrieval Information

Offsite Tape Retrieval

System receives services from (*service provider*). Tapes can be retrieved 24x7x365. Server administrators are authorized to request and receive tapes on a non-emergency basis for receipt the next business day. Table 4-12 denotes contacts authorized to request tapes on an emergency basis. Emergency tapes are provided within 2 hours of request per contractual agreement.

Backup Archive Information

(system specific)

SAN Backup Requirements

(system specific)

Table 4-12: Offsite Tape Retrieval Contact List

<table>
<tr><th colspan="11">Data Backup Support Vendor</th></tr>
<tr><td colspan="8"><i>Service provider name and address</i></td><td colspan="3">Phone:
Fax:</td></tr>
<tr><th colspan="11">Access Authorization Listing</th></tr>
<tr><th rowspan="2">First Name</th><th rowspan="2">Last Name</th><th rowspan="2">Position</th><th colspan="5">Authorization Level</th><th rowspan="2">Work Phone</th><th rowspan="2">Home Phone</th><th rowspan="2">Cell Phone</th></tr>
<tr><th>A</th><th>B</th><th>C</th><th>D</th><th>E</th></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
</table>

Legend: Authorized to: A = Release Data, B = Receive Data, C = Request Access to Facility, D = Request Emergency Service To/From Customer Site, E = Make Changes to the Authorization List.

Critical Backup and Reporting Tasks

Table 4-13 lists critical backup and reporting tasks that must be performed by the site server.

Table 4-13: Critical Backup and Reporting Tasks

Task	Host Server	Frequency/ Run Time	Exec/Software Performing Task	Generated Data Location

Database Backup Schedule

Database and transaction log backups are backed up to tape as part of the nightly general backup schedule. Database and transaction log backups are kept on the database servers for 24 hours. The SQL Agent has been configured to generate backups shown in Table 4-14.

Table 4-14: Database Backup Schedule

Task	Frequency/ Run Time	Exec/Software Performing Task	Generated Data Location

Table 4-15: SAN Shutdown/Power-Up Steps

EXAMPLE

Shutdown Procedure	Power Up Procedure
1. Shut down all attached servers. 2. Shut down all fiber switches by unplugging the power cable, beginning with the second switches in each fabric. 3. Shut down the arrays starting with the “other” controller in the pair as follows: 4. Start a terminal session and issue the following separate commands in the sequence presented: shutdown other, shutdown this. Repeat for each array. 5. Unplug the power cord. 6. Unplug power from each disk shelf.	1. Plug in power cables to all disk shelves. 2. Plug in power to array controllers. 3. Plug in power to the fiber switches starting with the first switch in each fabric. 4. Boot all servers.

Table 4-16: SAN Requirements (system specific)

SAN Elements

The elements of the SAN and the connectivity between them are as follows:

(system specific)

SAN Connectivity Requirements

Following is the connectivity information for the SAN:

(system specific)

SAN Redundancy Requirements

(system specific)

Other SAN Documentation

All standard procedures pertaining to the operation and maintenance of the SAN as well as its supporting devices can be found in the following hardcopy literature located in the server room:

- XXXX

5. RECONSTITUTION PHASE

The goal of this final phase is to provide for the smooth and orderly transition from the alternate site processing to normal operations. The objectives of the Reconstitution Phase are as follows:

- Assess existing site conditions and contribute to the decision as to whether to restore the current site or acquire a new permanent operating location.
- Effectively prepare the restored or newly acquired permanent operating location to fully recover and reconstitute normal operations, and ensure that procedures required to support and backup operations are properly reinstated.
- Support the orderly phase out and transition of system IT operations from the RTSC alternate site to the permanent operating location.
- Ensure that the transition does not affect the availability of the system to users.
- Implement standard operating procedures.

5.1. Concurrent Processing Procedures

Once the continuity of IT services has been ensured through the successful transition of operations to the alternate site, actions must be started to prepare for the full recovery and reconstitution of IT support back to the/a permanent site. This means assessing the physical and technological condition of the system permanent site and taking whatever actions necessary to ensure its return to a safe, effective, and fully functional IT operation. Specific actions taken during this phase will depend on the nature and scope of the incident that resulted in the disruption and loss of the primary site. The sections that follow will provide procedures to assist the DRC in assessing permanent site conditions for the scenarios covered in this DRP. The DRC should use experienced vendors in accomplishing the assessments discussed below. Attachment C provides the system vendor contact list.

The return of IT operations to the permanent site should be a well-planned and coordinated exercise. Planning meetings, with system, CIO and alternate site representatives attending, should be held in advance of the action, and all parties should coordinate on and concur with the actions planned.

Planning should provide a seamless transition for users (i.e., they should not experience any impact on operations as a result of the transfer). Therefore, the relocation should be planned for night hours and on weekends when usage is low and any problems experienced can be properly fixed without affecting users.

The alternate and reconstituting systems should be run concurrently until it can be confirmed that the reconstituted system is stabilized.

5.1.1. Physical Damage

If the disruption and loss was caused by a physical source (e.g., fire, hurricane, broken water line, biological agent, etc), then several components of site operations must be assessed:

Structural stability—An assessment of structural stability must be accomplished by qualified personnel. Therefore, the DRC must rely on the assessments made by building engineers and emergency personnel (e.g., fire department officials). The DRC will coordinate directly with building management and appropriate officials as they assess the condition of the K Street facility. The DRC will assist in the evaluation in any way possible, such as arranging for the movement and relocation of equipment to allow better access for personnel performing structural assessments. Determinations made concerning the facility's structural stability and soundness are key factors in the recovery and reconstitution process. If the facility is unstable, or must undergo extensive renovation for repair, then the identification of, and relocation to, a new facility will be a necessity. The DRC will obtain copies of any written reports concerning the stability of the K Street facility and make a recommendation to the DRM as to whether to remain at K Street or to plan on relocating. Based on the DRC's recommendation, the DRM will make a decision and request the assistance of senior system management in either expediting needed repairs at K Street or in locating new working space.

Safety—While structural stability plays a major part in the safety of the work environment, there are other factors that must be considered as well. For example, a major water leak or water used to extinguish a fire could foster the development of mold in equipment, furniture, floor, and wall coverings and inside walls and ventilating systems. The inhalation of mold is a serious health hazard that can result in physical problems and possibly even death. Therefore, the DRC must ensure that a health inspection of the facility is performed and that the results are provided to system for review. In a situation where there has been the release of a biological agent in the facility, the DRC must obtain an evaluation of conditions from city health officials and their official clearance to reoccupy the facility. Further, the DRC should ensure that all system equipment has been inspected and, if necessary, decontaminated. Other safety factors that must be considered and evaluated, in coordination with building management, include the following:

- Use of repair materials and electrical supplies that are of the proper specifications and meet or exceed applicable building codes

- Proper installation and operability of fire alarm and suppression systems

- Unhampered emergency exits

- Operational restrooms

Safety is another key factor that will determine whether existing or new facilities will be used to fully recover and reconstitute operations.

Power—The DRC will ensure that any repairs or changes to the electrical system are appropriate and will satisfy the needs of the IT site. Problems will be brought to the attention of building management, and the DRC will follow up to ensure that appropriate changes are accomplished.

Hardware—The system IT hardware must be carefully examined and tested to ensure it is operational. If necessary, the DRC will arrange to relocate the equipment to ROB3 to perform inspections to identify any physical damage and to run the hardware diagnostics to validate operability. An inventory of all equipment should be prepared and the exact condition of each piece documented. Any actions required (i.e., repair or replacement) should also be recorded.

Communications—The DRC will also ensure that any damaged voice or data communication lines have been repaired and meet the specifications contained in the MOA and ISA agreements with the CIO.

5.1.2. Technological Damage

If the disruption and loss of IT operations was caused by a technological problem or failure (e.g., virus or faulty equipment), then the DRC must accomplish hardware inspections and assessments to ensure that the site will be in a technologically sound condition to operate. Hardware diagnostics should be used to assess and validate the technical capabilities of each piece of equipment. If problems are noted, action should be taken to repair or replace any faulty equipment.

5.1.3. Facility Preparation

Once the facility is ready for occupancy, actions must be taken to ready it for full recovery and reconstitution of IT operations. The following actions should be taken by the DRT:

- Inspect and test electrical system and communication lines
- Remove damaged and inoperable equipment (if using original site)
- Install repaired and replacement equipment
- Properly configure equipment
- Assign equipment dependencies to allow for adequate take over or fail-over functionality for critical servers.
- Install operating systems and test
- Install virus protection and IDS systems and test.

- Load system with test data and perform structured testing

- Ensure tape backup and retrieval procedures are in place and test

When all equipment and software has been properly installed, configured, and tested and procedures have been reviewed and coordinated, the operation is ready to recover and reconstitute the system from the alternate site to the permanent site. The first step is to bring up the reconstituted site and run it concurrently with the alternate site until it is determined viable.

5.2. Plan Deactivation

The disaster recovery process does not end with the full recovery and reconstitution of IT operations. Formal closure needs to be included in the procedures to ensure that nothing important is overlooked. Further, the experience must be examined, analyzed and assessed, in an effort to do the following:

- Pinpoint weaknesses in established IT policies, processes and procedures that may have caused or permitted the disaster to occur and/or contributed to accentuating its impacts on operations

- Note problems encountered and develop procedures that will prevent them from reoccurring or minimize their impact

- Streamline and modify procedures to provide for smoother execution of the plan in the future

- Identify weaknesses in execution that required better team training, preparation, and testing

- Apply post-disaster knowledge and insight to normal, day-to-day operations in an effort to improve the way we do business

5.2.1. Approach for Plan Deactivation

The system approach to plan deactivation will consist of two basic actions:

1. Conducting a Post-Disaster "Lessons Learned" briefing

2. Establishing and implementing corrective actions based on lessons learned

5.2.2. Post-Disaster DRT Debrief

Immediately following the successful completion of the Reconstitution Phase, the DRC conducts a post-disaster meeting of the DRT for the following reasons:

- Costs associated with maintaining continuity of IT services, relocating and recovering IT operations are identified, collected, and reported (accomplished by the DRT-SC)

- Any remaining post-disaster tasks (e.g., returning rented or borrowed equipment, terminating vendor services, certifying vendor invoices, disposing of damaged equipment, updating software licenses, etc) are identified and assigned to team members to complete.

A debriefing is held to identify what things worked well and where improvement is needed. The Disaster Log Form (Table 3-4) using all DRP phases should be used during this discussion. Corrective actions to improve current procedures may include the following:

- Modifications to the DRP

- Creation of new test scripts to strengthen areas and improve execution where plan execution was weak

- Modifications to standard operating procedures to prevent weaknesses in operations that may have provided an opportunity for the disaster to occur or resulted in impacts of a greater magnitude than should have been experienced

- Revision to the system Risk Management and Security Plan to mitigate newly identified security vulnerabilities (either by risk mitigation or security controls)

5.2.3. DRT Deactivation

The final item on the DRT follow-on meeting agenda is the formal deactivation of the DRT. As with plan activation, the plan can only be deactivated by the DRM or designee.

Appendix A: DRT Emergency Contact List

Appendix B: Vendor Contact Information

Appendix C: Off-site Storage Contact and Escalation List

Appendix D: System Recovery Checklists and Configuration Information

Appendix E: System Inventory (Hardware, Software, Firmware, etc)

Appendix F: MOA and ISA for Alternate Site

Appendix G: Map to Alternate Site

Appendix H: BIA and Risk Assessment for (*insert system name*)

Appendix I: Occupant Evacuation Plan for the (*insert system location*) building

Appendix J: DRP Test Plan and Schedule