NIH Data Center
Disaster Recovery Plan

November 2007

November 16, 2007

FOREWARD

This Disaster Recovery Plan describes the strategy and procedures for recovering Data Center processing of applications should a disaster substantially disrupt operations.

The plan is organized into three parts: the main body provides a general description of the disaster recovery strategy and program, the appendices provide detailed information for conducting the recovery, and the attachments provide supplemental information. The main body is public information and may be freely distributed; the appendices and attachments contain sensitive information that is restricted to the individuals responsible for recovering Data Center operations. The appendices and attachments must be destroyed when updated versions are received.

The plan is frequently updated to reflect current hardware, software, procedures, applications, and staffing. Revisions are distributed to the disaster recovery team members at least twice a year following the disaster recovery tests.

When copies of the plan are no longer required, please return them to the Disaster Recovery (DR) Coordinator. All corrections are welcome at any time and should be directed to the DR Coordinator.

Adrienne Yang
Disaster Recovery Coordinator

TABLE OF CONTENTS

APPENDICES

ATTACHMENTS

1 Introduction

The Center for Information Technology (CIT) at the National Institutes of Health (NIH) provides information processing services to NIH research and management programs, as well to Department of Health and Human Services (DHHS) and other government agency management programs. CIT also provides networking and telecommunications services to NIH. The information technology equipment supporting these services is housed in the NIH Data Center (the *Data Center*) which is operated by the Division of Computer System Services (DCSS), a component of CIT.

In March 1992 a formal Business Impact Analysis (BIA) of the Data Center’s major applications was completed. The resulting disaster recovery plan to mitigate extended interruptions focused on the mainframe, since the major applications were hosted on that platform. Over time, major applications were being hosted on Unix systems and the disaster recovery plan was expanded to include those systems.

As an information technology service provider, DCSS now offers the Disaster Recovery Program as a service to the general customer base. Participation in the disaster recovery program is completely voluntary and is provided on a cost-recovery basis.

1.1 Purpose

This Disaster Recovery Plan documents CIT’s Disaster Recovery Program for recovering limited Data Center operations after a disaster. The plan describes the preparation and actions required to effectively respond to a disaster, assigns responsibilities, and describes the procedures for testing and maintaining the plan.

1.2 Scope

The Disaster Recovery Plan is focused only on DCSS-owned and managed computer systems, currently the z/OS mainframe system, Titan, and the Unix platforms comprising the EOS system. This plan addresses all preparation and steps necessary to restore processing on those systems so that the participating applications can continue processing after a disaster has rendered any or all of the systems inoperable.

Many functions and facilities that would be needed in a disaster involving physical devastation are outside the current scope of this plan. These include, but are not limited to:

- care for affected CIT personnel and their families;
- communications equipment supporting the NIH network (NIHnet) and the equipment supporting the NIH electronic mail services;
- computing equipment owned by other entities that is housed in the Data Center;
- voice communications internal to CIT;

- ongoing communications protocol between the CIT and NIH officials outside of CIT;
- the role of non-CIT NIH officials following a disaster;
- handling inquiries from the Press;
- implementation of controls to prevent disasters; and
- other aspects of contingency planning such as responses to various localized system outages.

1.3 Disaster Recovery Strategy

Should the Data Center encounter a disaster that prevents it from functioning, DCSS is prepared to provide adequate computational, data storage, and data communications services and facilities at an off-site disaster recovery resource for the participating applications. The off-site disaster recovery resource is a fully operational data center that is prepared to host the NIH systems and participating applications; it is referred to as the *hot site*.

Customers are responsible for disaster recovery preparedness for their applications in the event of a disaster. There is no mandatory requirement that customers use the Data Center's disaster recovery services and facilities. Application owners are free to make other disaster recovery arrangements.

DCSS has assigned a Disaster Recovery Coordinator to oversee the Disaster Recovery Program. The Disaster Recovery Coordinator is responsible for:

- organizing regularly-scheduled, periodic tests of the disaster recovery procedures;
- maintaining and updating the Disaster Recovery Plan based on changes in customer requirements, personnel, hardware and software configurations, and the results of disaster recovery tests and plan reviews; and
- orchestrating the execution of the Disaster Recovery Plan when a disaster has been declared.

DCSS has also designated a Disaster Recovery Technical Support Coordinator for each of the processing systems covered by this Disaster Recovery Program. The coordinators are responsible for:

- assisting the participating application customers in preparing for the disaster recovery test events;
- serving as liaisons for the participating application customers during the disaster recovery tests (by assisting customers in resolving errors in jobs, reporting communications problems to the DCSS disaster recovery team, and answering disaster recovery testing questions in general); and
- assisting the participating application customers in preparing their applications to run successfully at the hot site in the event of a disaster.

DCSS is ready to work with application program managers and technical leaders to further the disaster recovery capabilities of the participating applications. However, it is important that managers of the applications pro-actively prepare their applications for a disaster. This includes participating in the periodic hot site tests and communicating with the Data Center's Disaster Recovery Coordinator regarding significant changes or developments in their applications.

1.4 Disaster Definition

For the purposes of this plan, a disaster is any unplanned event that prevents the Data Center from providing services needed by the participating applications for a period of 72 hours or longer. Conditions that could be declared a disaster include, but are not limited to, extended electrical power outage to the computer room, and extensive fire, smoke, water, or explosion damage to computing equipment.

In the event of a disaster, the Damage Assessment Team (reference Section 3.1) will evaluate the damage to the physical assets and functional capability of the Data Center, and report its findings to the Executive Team (reference Section 3.2). The Executive Team will consider the findings together with other available information to make a decision regarding a formal disaster declaration. Only the Executive Team has the authority to declare a disaster.

1.5 Assumptions

The Disaster Recovery Plan has been developed under the following assumptions:

- Only the Data Center is damaged; other buildings on the NIH campus are unaffected.

- Only those applications (listed in Appendix A) that are currently participating in the Disaster Recovery Program will be supported.

- A disaster will result in real losses, both for the Data Center itself, and for many of the applications that it supports. At a minimum, time, money, and operational capability will be lost. A physical disaster (hurricane, flood, bomb, etc.) would lead to the loss of at least some data and software.

1.6 Area-Wide Disasters

If the NIH Data Center is adversely affected in an area-wide disaster, the first priority is the well-being of staff members and their families. After the first 24 to 48 hours, the Executive Team (reference Section 3.1) will meet to determine if and when the disaster recovery plan is to be activated. The decision will be coordinated with the NIH Continuity of Operations Plan management team and with owners of the applications participating the the Disaster Recovery Program.

1.7 Contractual Arrangement For Recovery Services

CIT has an Inter-Agency Agreement with the General Services Agency (GSA) for hot site services to accommodate recovery of participating applications for the Titan and EOS systems.

2 Disaster Recovery Action Plan

2.1 Backup and Off-Site Storage Procedures

Titan:

All disks are dumped to tape on weekly cycles. These weekly dumps are written simultaneously to two separate automated tape libraries (ATLs), one located in the Data Center and the second located in the NIH Consolidated Co-location Site (NCCS). The latter set of tapes are referred to as the *off-site backup tapes*. Both backups are cycled through six sets of tapes so that six successive weeks worth of backups are always maintained.

Incremental backups of all changed data sets are taken daily for public and systems disk storage. Up to five unique backup versions per data set name are maintained. The incremental backups are written simultaneously to the two ATLs. In a disaster situation, all usable tapes will be sent to the hot site.

EOS:

EOS system disks are dumped to tape on weekly cycles and the tapes are rotated to a secure off-site storage facility. The off-site backup tapes are cycled through six sets of tapes. Customer files and data are included in the dumps for those customers who have requested off-site disaster data storage.

Incremental backups of all changed files are taken nightly. The following day the incremental backups are copied to a second tape library located in the NCCS. In a disaster situation, all usable tapes will be sent to the hot site.

2.2 Off-Site Storage Services

CIT has contracted with a commercial vendor to provide lockable space (referred to as the NCCS) in a secure, environmentally controlled facility. The facility is located in Northern Virginia and authorized CIT staff have 24x7 access.

CIT has contracted with a commercial vendor to provide secure off-site tape storage services. The vendor’s facility and procedures meet Department of Defense standards for secure storage. The following services are provided under CIT’s contract:

- Delivery of the backup tapes between the storage facility and the Data Center on a weekly schedule;
- Delivery of backup tapes (both those stored at the storage facility and at the NIH campus) to the hot site upon request and as directed by the Data Center (both for disaster recovery tests and for an actual disaster); and
- Delivery of the backup tapes from the hot site back to NIH.

In general, the vendor can respond within two hours notice, twenty-four hours per day, three hundred sixty-five days per year.

2.3 Disaster Response

In the event of a disaster, DCSS will take the following actions; responsible teams are indicated:

- Assess the damage to the Data Center to determine if a disaster should be declared. (Damage Assessment Team)

- Make the decision to formally declare a disaster. (Executive Team)

- Establish a Disaster Command Post, if necessary, in another building on the NIH campus having appropriate communications and support equipment. (Executive Team)

- Notify the off-site storage facility, the hot site, key NIH executives, and the participating application sponsors of the disaster declaration. (Executive Team)

- Work with the hot site staff to restore the NIH operating systems and applications at the hot site and establish the communications link to the hot site in preparation for operating at the hot site for the duration of the emergency. (Restoration Team, Operations Team, and Customer Support Team)

- Reconstruct the Data Center. (Salvage/Reclamation Team)

- Conduct operations at the hot site until the Data Center is ready to resume operations. (Operations Team, Restoration Team, and Customer Support Team)

- Conduct preparations to leave the hot site and to resume operations at the Data Center. (Operations Team and Restoration Team)

Reference Section 3, Functional Teams and Responsibilities, for details regarding the responsibilities of the disaster recovery teams and the actions required to accomplish the above listed tasks.

2.4 Hot Site Hardware and Software Configurations

The Data Center's standard disaster recovery configuration at the hot site includes a mainframe system, Unix systems, data communications support to the mainframe and Unix systems, and a work area recovery center.

The following are the major hardware components of the standard mainframe configuration:

- IBM processor with sufficient MIPS and memory capacity,
- two logical partitions (LPARs),
- sufficient quantity of tape drives (STK 9840, 3490E, and 3480),
- sufficient disk storage (3390-3 DASD), and
- sufficient printer capacity (IBM 3825-1 page printer, IBM 4245/4248 impact line printer, OCE 372 pagestream with MICR (compatible with IBM 3900), and OCE PS 75 printer (compatible with IBM 3825, 3827)).

The following system software and subsystems will be loaded into the hot site mainframe LPARS as appropriate:

- z/OS operating system,
- Resource Access Control Facility (RACF),
- TSO/ISPF,
- Wylbur under TSO,
- Customer Information Control System (CICS),
- Job Control Language (JCL),
- MODEL 204,
- Limited DB2,
- SPF,
- Transport Control Protocol/Internet Protocol (TCP/IP – TN3270),
- File Transfer Protocol (FTP),
- SAS,
- IMS,
- VISION:Builder and VISION:Report, and
- Connect:Direct.

The following are the major hardware components of the standard Unix configuration:

- AlphaServer 8400 5/625 with sufficient memory capacity,
- sufficient internal and external disk storage,
- CD ROM drive,
- sufficient quantity of tape drives,
- Laser Jet printer, and
- network connectivity.

- SunFire V880 UltraSPARC III server with sufficient memory capacity,
- sufficient internal and external disk storage,
- CD ROM drive,
- tape drive, and
- network connectivity.

The following system software will be loaded onto the hot site AlphaServer:

- Tru64 Operating System,
- Oracle relational database management system,
- Connect:Direct, and
- ADSM.

The following system software will be loaded onto the hot site UltraSPARC server:

- Solaris Operating System, and

- Oracle relational database management system.

Note that at the hot site, the functions of multiple AlphaServers and multiple UltraSparc servers are consolidated into one machine, respectively.

The following are provided to support data communications to the hot site:

- Network Control Center for communication support to the mainframe and Unix computers,
- remote console support for the Unix computers,
- dedicated T1 line with appropriate routers, switches, and firewalls for IP communication between Washington, D.C., and the mainframe and Unix computers, and
- Web redirect services, for Internet connectivity to provide alternate connectivity should the T1 line be inoperable.

The following are the provisions at the work area recovery center, located within driving distance of the Washington, D.C. metropolitan area:

- enough work space to accommodate thirty-two (32) individuals,
- twenty-five work stations,
- twenty-five phone sets,
- twenty-five work stations with 3270 emulation,
- remote consoles for the Unix computers,
- Ethernet connection to the hot site, and
- one facsimile machine and one copier.

DCSS will contract for additional emergency hot site support to meet individual customer's special needs.

2.5 Resuming Normal Operations

While recovery operations are ongoing at the hot site, the Salvage/Reclamation Team will be managing the restoration or rebuilding of the Data Center.

2.6 Security

While operating at the hot site, information security will be assured by firewall restrictions and the security controls on the hot site host systems which will be configured in accordance with the policies and procedures governing the security of the production Titan and EOS systems. As processing continues at the hot site, the hot site host systems will be closely monitored to ensure the systems are not compromised.

3 Functional Teams and Responsibilities

The following subsections describe each functional team's role as well as its responsibilities in preparing for and responding to a disaster. The responsibility for planning, coordinating, and managing this program is assigned to the Disaster Recovery Coordinator with assistance from technical advisors.

The appendices and attachments provide supplemental information and instructions to assist the teams in fulfilling their functions.

3.1 Damage Assessment Team

The Damage Assessment Team assesses the extent of the damage to the Data Center, reports to the Executive Team, and makes a recommendation on declaring a disaster.

The major pre-disaster responsibility is to determine appropriate considerations/criteria for identifying the extent of the damage and the estimated duration of the outage.

The disaster responsibilities and actions are:

- Receive the first alert regarding the disaster.
- Ensure that the NIH police/fire departments have been notified.
- Coordinate with the police and/or fire department to provide for safety, security, and access to the damaged facility.
- Notify the DCSS Director or alternate regarding the potential disaster.
- Assess the damage to each area of the computer facility.
- Brief the Director or alternate, communicating the recommendation(s).

3.2 Executive Team

The Executive Team officially declares that a disaster has occurred, authorizes the execution of the Disaster Recovery Plan, and oversees the execution of the plan during the emergency.

The pre-disaster responsibilities are:

- Approve the DCSS Disaster Recovery Plan and all major or material modifications to the plan.
- Establish primary and alternate disaster command posts, ensuring that the posts are adequately prepared for a disaster.

The disaster responsibilities and actions are:

- Notify the hot site and the off-site storage facility of a possible disaster.
- Review the report of the Damage Assessment Team.
- Declare a disaster:
    a) establish the command post and communications,
    b) activate the Functional Teams,

c) inform the hot site of the disaster declaration, and
d) initiate the shipment of the backup materials to the hot site.

- Notify the Key Executives (listed in Appendix C).
- Monitor the performance of the Disaster Recovery Teams and the execution and effectiveness of the Disaster Recovery Plan.
- Keep senior CIT management and the designated Information Officer/alternate informed of material/sensitive matters.

3.3 Restoration Team

The Restoration Team brings the hot site systems to operational mode by managing the relocation of services to the hot site, initiating and managing the recovery procedures at the hot site, and responding to operational problems at the hot site. The Restoration Team also manages the relocation of services back to the Data Center.

The pre-disaster responsibilities are:

- Establish and maintain the recovery procedures for the hot site systems.
- Manage and maintain the backup procedures.
- Establish and maintain the disaster recovery data communications link.
- Plan and conduct regular hot site tests.

The disaster responsibilities and actions are:

- Coordinate recovery procedures with hot site personnel.
- Restore the operating systems environments on the hot site host systems.
- Establish the data communications link to the hot site.
- Verify the operating systems and all other system and communication software are working properly.
- Restore the application files.
- Support the operations at the hot site by resolving problems and monitoring and maintaining the data communications link to the hot site.
- Manage the backup tapes that were sent to the hot site.
- Ensure all required backups of the entire system are completed in preparation for leaving the hot site.
- Coordinate the return of the DCSS/customer media to the Data Center.
- Install all NIH system software at the Data Center.

3.4 Operations Team

The Operations Team assists in the recovery operations and manages the operations of the computer systems at the hot site.

The pre-disaster responsibilities are:

- Ensure that appropriate backups are made on the prescribed, rotating basis and are ready to be taken off-site.

- Maintain current, up-to-date systems operations documentation, ensuring that this documentation is suitably stored off-site.

The disaster responsibilities and actions are:

- Provide assistance to the Restoration Team in the restoration of the system software and customer files, as required.
- Run system and operation jobs, as required.
- Implement and maintain a problem log.
- Provide information to the Customer Support Team regarding the status of the system, operations, and the customer jobs.
- Effect the transfer of media and print output from the hot site to suitable customer pickup location(s).
- Coordinate the shutdown of the hot site operations and the transfer back to the Data Center.

3.5 Customer Support Team

The Customer Support team provides assistance to customers during the disaster from the time the disaster is declared until operations resume at the Data Center.

The pre-disaster responsibilities are:

- Advise and consult with application customers regarding their disaster recovery requirements.
- Assist application customers during disaster recovery tests.

The disaster responsibilities and actions are:

- Notify participating application customers that a disaster has been declared.
- Advise customers of the disaster recovery system status, availability, and accessibility.
- Provide problem diagnosis and resolution guidance/assistance to application owners and their customers.

3.6 Salvage/Reclamation Team

The Salvage/Reclamation Team manages the restoration or rebuilding of the Data Center.

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

The disaster responsibilities and actions are:

- After the Restoration Team has implemented recovery operations at the hot site, assess the damage to the Data Center and report the damage, with recommendations, to the Executive Team.

- Organize the recovery of salvageable equipment, supplies and the physical plant.
- Initiate, coordinate, and expedite construction and work requests to prepare the NIH facility to receive equipment, supplies, tools, machinery, and utilities (electrical power, telephones, network connectivity, air conditioning, plumbing, water, gas, and HVAC).
- Order and expedite replacements for unusable IT equipment.
- Monitor the construction of the new/repaired facility, and the installation of all utilities and other essentials.
- Monitor the installation of computers, 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 by the participating applications and by other customers.

3.7 Administrative Support Team

The Administrative Support Team provides logistical and organizational support for all the other teams.

The major pre-disaster responsibility is to prepare up-to-date property management lists, inventory lists, and other pertinent documentation on the physical assets of the Data Center, ensuring current copies of this documentation are in the doc box.

The disaster responsibilities and actions are:

- Prepare travel orders and other documents to facilitate the Restore Team activities.
- Provide general administrative support to the Executive Team and to all other DCSS Functional Teams, as necessary.

4 Testing the Disaster Recovery Plan

Testing and exercising the Disaster Recovery Plan helps to verify that the recovery procedures work as intended and that the supporting documentation is accurate and current. Testing also provides an opportunity to identify any omissions in recovery procedures or documentation and to determine whether personnel are adequately prepared to perform their assigned duties. Therefore, DCSS regularly schedules exercises of its Disaster Recovery Plan at the vendor hot site, referred to as hot site tests (HSTs).

4.1 Hot Site Test Procedures

DCSS schedules two hot site tests per year with sufficient time to test the operating system and customer application recovery procedures. The initial hours are dedicated to exercising the system recovery procedures and establishing the communications link. The remaining hours are dedicated to testing the recovery of participating applications. The hot site tests are managed and conducted by members of the Restoration Team, the Operations Team, and the Customer Support Team, referred to collectively as the *HST Team*.

Prior to the HSTs, the HST Team determines which backup tapes will be used for the tests; establishes a test plan which outlines the HST Team goals and activities for the given test; conducts the necessary preparations for the test; and assists customers in their preparations for the HST. (Customers set their own HST objectives.) During the tests, in addition to providing customer assistance, the HST Team participants maintain a running log of the test activities to assist in the post-test review.

After every test, the HST Team participants meet to discuss the tests in order to improve the recovery procedures and the plan documentation. The HST Team also schedules a meeting with the customers to gain their input and suggestions for improvements.

4.2 Hot Site Test Planning

To ensure a successful hot site test, the HST team will:

- Confirm with the hot site vendor that the hot site mainframe, Unix computer, and data communications configurations will meet the HST needs, and that the hot site will be ready for the test. (Two to three months prior to the scheduled test)

- Set the HST Team objectives for the test and establish action items for the team in preparation for the test. (At least two months prior to the scheduled test)

- Disseminate information to the user community regarding the test. (Six to eight weeks prior to the scheduled test)

- Confirm that preparatory tasks are being completed and review the schedule of events for the days of the HST. (Four to six weeks prior to the scheduled test)

- Discuss the final test preparations with the hot site vendor to confirm the hot site configurations, to obtain the information required for the mainframe backups, and to reconfirm the hot site will be ready. (Two to three days before the scheduled backups for the test will be taken)

- Send the backup tapes and tape lists to the hot site. (One week prior to the scheduled test)

Reference Appendix J for complete guidelines and instructions for preparing and testing applications during a hot site test. This guideline is distributed to the user community well in advance of the HST.

4.3 Application Testing Support

The HST Team offers user support during a hot site test to assist the application owners/participants in successfully running their applications at the alternate site. The assistance includes help with test preparations, on-call support during the duration of the test, resolving reported problems, and serving as the liaison between the user and the HST Team.

Test preparation support includes:

- Ensuring the users have made all appropriate preparations for their data to be available for the HST,
- Ensuring the users are ready for the HST and have no further questions, and
- Ensuring users have the necessary contact phone numbers for user support during the HST.

Hot site test support includes:

- Notifying those users who have not logged on that the disaster system is up and ready for user testing,
- Responding to general user questions and to user problem reports, ensuring they are resolved, and
- Recording all problem reports and general notes to a system status database that is made available to users to read.

4.4 Post-Test Wrap-Up

Two debriefings are schedule on the days immediately following the hot site test. One is for the HST Team participants to assess the systems software recovery procedures. The second is for the user community who participated in the HST.

These meetings are general discussions to address:

- Areas where the exercise was successful,
- Problems that were encountered, and
- Suggestions for improvements.

Based on the conclusions, an “action list” of improvements to be made prior to the next test is developed and responsibility for implementing them is assigned.

4.5 Hot Site Test Schedule

The bi-yearly tests are scheduled approximately six months apart. To date, twenty-five tests have been conducted. The next scheduled tests are:

- HST26: December 2 - 4, 2007
- HST27: July 13 - 15, 2008

The following are the dates of the previous tests for the indicated systems:

HST1:	May 3, 1994 – NIH mainframe
HST2:	March 21, 1995 – NIH mainframe
HST3:	September 12, 1995 – NIH mainframe
HST4:	March 14, 1996 – NIH mainframe
HST5:	October 22,1996 – NIH mainframe
HST6:	May 13, 1997 – NIH mainframe
HST7:	December 12, 1997 – NIH mainframe
HST8:	July 21, 1998 – North and South (consolidation of NIH and HHS mainframes onto two LPARS at NIH)
HST9:	January 22, 1999 – North and South
HST10A:	June 7, 1999 – EOS
HST10:	August 30-31, 1999 – North, South, and EOS
HST11:	February 22-23, 2000 – North, South, and EOS
HST12:	August 14-15, 2000 – North, South, and EOS
HST13:	March 26 - 27, 2001 – North, South, Titan, and EOS
HST14:	November 01 –02, 2001 – Titan (standardized system to replace North and South; hosting North applications at the time of the test), South, and EOS
HST15:	March 26 – 27, 2002 – Titan, South, and EOS
HST16:	November 12 – 13, 2002 – Titan, South, and EOS
HST17:	July 21 – 22, 2003 – Titan, South, and EOS
HST18:	December 8 – 9, 2003 – Titan and EOS
HST19:	July 19 - 20, 2004 - Titan and EOS
HST20:	December 6 - 7, 2004 - Titan and EOS
HST21:	July 18 - 19, 2005 - Titan and EOS
HST22:	December 5 - 6, 2005 - Titan and EOS
HST23:	July 17 - 18, 2006 - Titan and EOS
HST24:	December 4 - 5, 2006 - Titan and EOS
HST25:	July 15 - 17, 2007 - Titan and EOS

4.6 Training

In addition to regular testing, team members and managers receive annual refresher training regarding the emergency alert procedures covered in Appendix C and the SunGard notification procedures covered in Appendix D. The following are the completed training sessions:

Date	**Training**
10/23/06	Manager training regarding emergency alert and SunGard notification procedures
11/2/06	Team member training regarding emergency alert procedures

5 Maintaining the Plan

The Disaster Recovery Coordinator of the Data Center is responsible for the maintenance of this document. The plan is updated as needed:

- in response to events such as office moves, telephone number changes, new personnel joining DCSS, retirements, duty changes, and additions or deletions of participating applications;
- after each hot site test to reflect the recommendations resulting from the post-test wrap-up debriefings; and
- after a periodic review of the plan.

As sections of the plan are updated, the revised sections are posted to the internal DCSS web site to ensure the most current information is available to DR team members. DR participants are notified of the changes and are encouraged to produce printouts for their copies of the disaster recovery plan.

Additionally, the plan will be updated in the event an actual disaster occurs. The plan will be reviewed and updated at a convenient point after the initial responses to the disaster have been completed.

Revision History:

Revision Date	**Summary of Changes**
November, 2000:	The *Disaster Recovery Plan*, covering the mainframe systems and the *Compaq Digital AlphaServer Disaster Recovery Plan* were revised following the August, 2000 disaster recovery tests.
July, 2001:	Major restructuring and revision of the disaster recovery plan was completed. The prior two plans are now combined into one plan.
October, 2001	Revised Appendices B, C, D, G, and J due to changes in communications support and the Comdisco contract, and in preparation for the November, 2001 disaster recovery test.
November/December, 2001	Revised main body and Appendices A, C and F following the November, 2001 disaster recovery test.
March, 2002	Revised Appendix J for distribution to customers prior to March, 2002 disaster recovery test.
May 2002	Revised main body and Appendices A, B, C, D, F, G, H, J, K, and L due to contractual changes, customer responses to application surveys, and

results of the March, 2002 disaster recovery test.

June, 2002 Revised Attachments list in table of contents to include Department of the Treasury instructions, and Appendices A, C, D, and, I due to further responses to application surveys, contact information changes, and reviews of procedures.

October, 2002 Revised sections 1, 2, and 4 to reflect contractual changes; Appendix A to reflect changes in applications participating in the Disaster Recovery Program; Appendices B and D to reflect the new work area recovery location; Appendix C to change format and update contact telephone numbers; Appendix F to reflect updates to recovery procedures based upon further reviews; Appendix J in preparation for the November hot site test; and Appendix I to reflect the new location of the Information Security and Awareness Office.

August, 2003 Revised section 1 to clarify user responsibilities; section 4 to record recent test dates; Appendix A to reflect changes to applications supported; Appendix C to reflect personnel changes and to update telephone numbers; Appendix D to reflect changes in vendor support personnel and to update notification procedures; Appendix F to reflect changes to recovery procedures; Appendix G to reflect new IP addresses and update information regarding the T1 line; and Appendix J in preparation for the July hot site test.

April, 2004 Revised sections 1 and 2 to eliminate references to South which was decommissioned January 12, 2004; section 3 to reflect updates to team responsibilities; section 4 to record recent test dates and to describe plan review process and employee training; section 5 to indicate plan approvals; Appendix A to reflect changes to applications supported; Appendix C to reflect personnel changes and updates to alert procedures; Appendix D to reflect changes in vendor support personnel; Appendix F to reflect changes to recovery procedures; Appendix G to reflect changes to IP addresses and pending relocation of the T-1 line; Appendix J in preparation for the December hot site test. Eliminated Appendix L, Hot Site JCL (South) due to the decommissioning of South.

July, 2004 Revised Appendix J and Appendix F in preparation for the July hot site test.

February, 2005 Revised section 2 to update the backup procedures; section 4 to record current test dates; Appendix A to reflect changes to applications supported; Appendix C to reflect personnel changes; Appendix D to reflect changes in vendor support personnel; Appendix E to reflect personnel changes; Appendix F to reflect changes to recovery procedures; Appendix G to reflect changes to IP addresses and T-1 line relocation; Appendix H to reflect changes in products and vendor contacts; Appendix J to reflect changes to test instructions prior to the December test.

November, 2005 Revised Section 2 to reflect hot site hardware changes; section 4 to record current test dates; Appendix A to reflect changes to applications supported; Appendices C, D, and E to reflect personnel changes; Appendix F to reflect changes to recovery procedures based on July test results; Appendix G to reflect changes to communications architecture; Appendix H to reflect changes to vendor contact information; Appendix J to reflect changes to test instructions prior to the December test; replaced Attachment 4 (3172 Configuration Controls) with Communication Architecture and Configuration detailing the disaster recovery network (the 3172 is no longer used for communications connectivity on the mainframe).

June, 2006 Revised Appendix J in preparation for the July 17 - 18, 2006 DR test.

July, 2006 Revised Section 1 to clarify the Disaster Recovery Program is provided as a paid service open to any Titan or EOS customer; Section 2 to update the mainframe configuration; Section 4 to record the most current tests; and Section 5 to describe the procedures for publishing plan updates on the DCSS internal web site and to indicate recent revisions.
Revised Appendix D to reflect changes to SunGard contact information and DCSS authorized disaster declarers.
Revised Appendix F1 to reflect changes to Titan recovery procedures based on July test results.
Revised Appendix K to describe Titan communications used for DR testing. This replaces the previous Appendix K, VTAM Telecommunications.

September, 2006 Revised Appendix C to describe mitigation actions to potential accessibility problems to the alternate processing sites, revised team memberships based on personnel changes and updated contact information.
Revised Appendix E to indicate the off-site tape backup storage facility is not susceptible to the same hazards affecting the Data Center and to reflect changes in personnel authorized to request tape deliveries and/or manage backup tape storage procedures.

October, 2006 Updated Section 4.5 to include the dates for the July 2007 test.
Updated Appendix B to include alternate routes to the work area recovery center.
Revised Section 4.6 to include the list of specific training activities and

frequency.

November, 2006
Updated Appendix C to record personnel and contact changes.
Updated Appendix J in preparation for the December DR test.
Updated Appendix F1 to reflect changes to the recovery procedures and removal of the ADABAS product.

January, 2007
Updated Section 2.1 to reflect the relocation of the off-site ATL.
Updated Section 2.4 to reflect the removal of the ADABAS product.
Updated Section 4.1 to remove references to a specific test duration and section 4.5 to reflect completion of hot site test 24 and the date of the 25th hot site test.
Updated Section 4.6 to record completed training sessions.

March, 2007
Updated Appendix H to reflect changes to list of supported software.

May, 2007
Updated Appendix A to reflect responses to application surveys.

June, 2007
Updated Appendix D to reflect changes to SunGard support personnel.
Updated Appendix J in preparation for July test.

October, 2007
Added Section 1.6 to address area-wide disasters.
Updated Section 4.5 to record the most recently completed test and to record the date for the future scheduled test.
Updated Appendix C, the description of Accessibility to the Hot Site Locations to be consistent with Section 1.6.
Updated Appendix F2 to reflect the changes to the recovery procedures based on the July, 2007 test.
Updated Appendix J in preparation for the December DR test.

November, 2007
Updated Section 2.2 to include a description of the NIH Consolidated Co-location Site.
Updated Appendix C, to reflect personnel changes and contact information changes.
Updated Appendix E to include the location, contact number, list of DCSS staff having access to the NCCS, and directions.
Updated Appendix F1 in preparation for the December DR test.

Plan Approval:

Revision	**Signed, Director DCSS**	**Date**
April, 2004	/s/ John Dickson	4/12/04
November, 2007		