Disaster Recovery Plan (DRP)

for the

SCG Secure Cloud System

Version 1.7

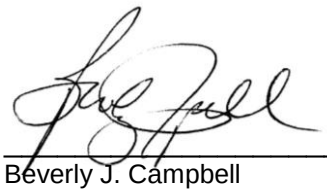
May 19, 2016

The Scientific Consulting Group, Inc.
656 Quince Orchard Road
Suite 210
Gaithersburg, MD *20878*

Disaster Recovery Plan Approval

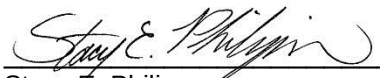
The Disaster Recovery Plan (DRP) for the SCG Secure Cloud system must be approved by the SCG President, Vice President of Administration, and Information Technology (IT) Director. We hereby certify that the SCGSC Disaster Recovery Plan is complete and that the information contained in this DRP provides an accurate representation of the application, its hardware, software, and telecommunication components. We further certify that this document identifies the criticality of the system as it relates to the mission of SCG and our client, the National Institute of Diabetes and Digestive and Kidney Diseases (NIDDK), and that the recovery strategies identified will provide the ability to recover the system functionality in the most expedient and cost-beneficial method in keeping with its level of criticality.

We further attest that this SCGSC DRP will be tested at annually. This plan will be first tested on or about May 29, 2015, after the SCG Secure Cloud system is fully functional, and will be tested annually thereafter. The testing, training, and exercise materials associated with this test will be developed and subsequently filed in the SCG Secure Cloud repository. The DRP will be reviewed annually by the SCG President and IT Director and modified as changes occur and will remain under version control. Any changes to the DRP will be coordinated with and approved by the undersigned or their designated representatives.



Beverly J. Campbell
President

5/19/16
DATE



Stacy E. Philipson
Vice President of Administration

5/19/16
DATE

Chuck C. Lee
IT Director

5/19/16
DATE

Document Information and Revision History

Document Owners	
SCG President	
Name	Beverly J. Campbell
Contact Number	301-670-4990 (W); 301-461-1109 (C)
E-mail Address	bcampbell@scgcorp.com
SCG Vice President of Administration	
Name	Stacy Philipson
Contact Number	301-670-4990 (W); 301-742-5954 (C)
E-mail Address	bcampbell@scgcorp.com
SCG Information Technology Director	
Name	Chuck Lee, Information Technology Director
Contact Number	301-670-4990 (W); 301-366-3273 (C)
E-mail Address	clee@scgcorp.com

Document Revision and History			
Revision	**Date**	**Author**	**Comments**
1.0	2/12/15	C. Lee	Initial Draft
1.1	2/13/15	B. Campbell	Revised Draft
1.2	2/20/15	C. Berry	Document reviewed; minor comments/ modifcations entered
1.3	2/21/15	B. Campbell	Document reviewed; minor modifications entered
1.4	2/25/15	B. Campbell	Minor revisions on p.7
1.5	2/26/15	B. Campbell	Minor revisions on numerous pages
1.6	3/28/16	B. Campbell	Revisions on numerous pages, tables, and figures
1.7	5/19/16	B. Campbell	Minor edits throughout document

This record shall be maintained throughout the life of the document. Each published update shall be recorded. Revisions are a complete re-issue of the entire document. The version number's decimal (minor) portion here and on the cover page is updated for each revision. The version number's integer (major) portion will be updated at each time a full Security Assessment and Authorization is performed.

DRP Distribution

Distribution of the DRP should be restricted to personnel involved in the activities for the continued operations of SCG Secure Cloud system. This table identifies the key personnel who are required to receive and maintain access to a copy of this plan, as well as plan updates when they are issued.

Name and Title	Phone Numbers	Email Address
Chuck Lee, IT Director	301-670-4990 (W) 301-366-3273 (C) 301-637-4355 (H)	chuck@scgcorp.com
Kenny Ying Lee, IT Systems Specialist	301-670-4990 (W) 315-956-7796 (C)	ylee@scgcorp.com
John Bernheimer, IT Systems Specialist	301-670-4990 (W) 410-428-1330 (C)	jbernheimer@scgcorp.com
Ric Blackman, Web Development Director	301-670-4990 (W) 301-529-0760 (C)	rblackman@scgcorp.com
Stacy Philipson, Vice President of Administration	301-670-4990 (W) 301-742-5954 (C) 301-363-5707 (H)	sphilipson@scgcorp.com
Beverly Campbell, President	301-670-4990 (W) 301-461-1109 (C) 540-887-9829 (H)	bcampbell@scgcorp.com
Susie Warner, Program Manager	301-670-4990 (W) 301-366-3217 (C) 301-355-4388 (H)	swarner@scgcorp.com

Table of Contents

List of Figures

List of Tables

1. Introduction

Information systems (IS) are a vital aspect of SCG's business processes and the clients we support. Therefore, it is critical that services provided by the SCG Secure Cloud (SCGSC) system are able to operate effectively without excessive interruption. This Disaster Recovery Plan (DRP) establishes comprehensive procedures to recover SCGSC quickly and effectively following a service disruption that requires the mobilization of personnel and operations to an alternate location. The DRP is one plan within a suite of site business continuity of operations plans.

SCG requires a robust information technology (IT) contingency planning process that includes IT contingency plans (ITCPs) and DRPs that are fully compliant with:

- Federal Information Security Management Act of 2002
- Office of Management and Budget Circular A-130, Management of Federal Information Resources, Appendix III, November 2000
- Federal Continuity Directive 1, Federal Executive Branch National Continuity Program and Requirements, February 2008
- National Security Presidential Directive-51/Homeland Security
- Homeland Security Presidential Directive 20, National Continuity Policy, May 2007
- National Continuity Policy Implementation Plan, August 2007
- National Response Framework, March 22, 2008
- National Institute of Standards and Technology (NIST) Special Publication (SP) 800-34, Revision 1, *Contingency Planning Guide for Information Technology Systems*, May 2010
- NIST SP 800-53, Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations, April 2013
- NIST SP 800-84, Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities, September 2006

1.1 Objective

The purpose of the SCGSC DRP is to provide a documented information system focused plan designed to address the restoration of operations of IS services, either systems or applications, at an alternate site after an emergency has occurred. The DRP may be supported by several ITCPs, which together may recover one entire system once the alternate site has been established. The DRP is one plan within the suite of site business continuity of operations plans that address federal guidance requirements for the continued operations of IS services that support critical business processes.

1.2 Scope

This SCGSC DRP has been developed for the purpose of increasing the site's resilience posture in the face of an emergency that jeopardizes IS operations. It was written in accordance with federal guidance. Procedures and instructions in this DRP are for a system rated "Moderate" after the Information System Contingency Planning

Assessment (ISCPA) and are designed to recover SCGSC within 7 calendar days following a catastrophic disaster. This DRP plan does not address disruptions that can be resolved at the primary site; instead, it addresses disruptions that require either the electronic transfer of data to an alternate location or the delivery of backups to a different processing location. Also not within scope of this plan is the replacement or purchase of new equipment and short-term disruptions or loss of data at the onsite facility or at the user-desktop levels.

ITCPs are referenced in the DRP in order to assist in the full restoration of critical systems or transfer of critical systems data to the alternate site.

1.3 DRP Assumptions and Constraints

The following *assumptions* were considered when developing this DRP:

- Personnel well versed in day-to-day operating procedures are available to operate at the alternate site.
- Staff is prepared to deal with emergency procedures without the need to reference detailed written steps.
- Management personnel will be available to make decisions.
- System and supporting component restoration priorities have been established.
- Alternate processing procedures have been established by business/service lines.
- Current backups of the system software and data are intact and available at the offsite data storage facility in Frederick, Maryland.
- The SCGSC is inoperable at the primary site and its operation cannot be restored at that site within 48 hours.
- Hardware resources are available.
- Internet Service Provider (ISP) is available and functioning.

This plan does not apply to disruptions deemed recoverable at the primary site or the following situations:

- Emergency evacuation of personnel, which is addressed by the occupant evacuation plan.
- Overall recovery of business operations, which should be addressed in a separate business recovery plan.

1.4 Document Ownership

The contents of this document are the responsibility of SCG. The IT Director will serve as the DRP Director and has been assigned responsibility of the DRP content, modifications, currency, and distribution to stakeholders.

1.5 Plan Review and Maintenance

To ensure currency, this document will be reviewed annually and when the SCG Secure Cloud system incurs significant modifications.

1.6 Document Distribution

A copy of the SCG Secure Cloud DRP will be:

- Provided to system stakeholders who have an interest or responsibility for the development, modification, or testing of this plan.
- Held electronically or in hard copy or both by every member of the Recovery Teams where it is easily accessible in an emergency.
- Stored in an off-site location in both soft and hard copy format for ease of use under a wide range of circumstances.

2. Concept of Operations

The Concept of Operations section provides details about SCGSC; an overview of DRP Activation and Notification, Recovery, and Reconstitution phases; and a description of roles and responsibilities of SCG's personnel during a disaster recovery activation.

DRP phases are similar to the phases of the ITCP; however, the DRP must consider the existing capabilities of the alternate location. For sites that are "cold" or "warm" requiring setup of equipment or infrastructure to support operations, the DRP must include any activities necessary to prepare the alternate site to support the systems or data relocated or electronically transferred to the site.

2.1 System Description for SCGSC

2.1.1 System Architecture

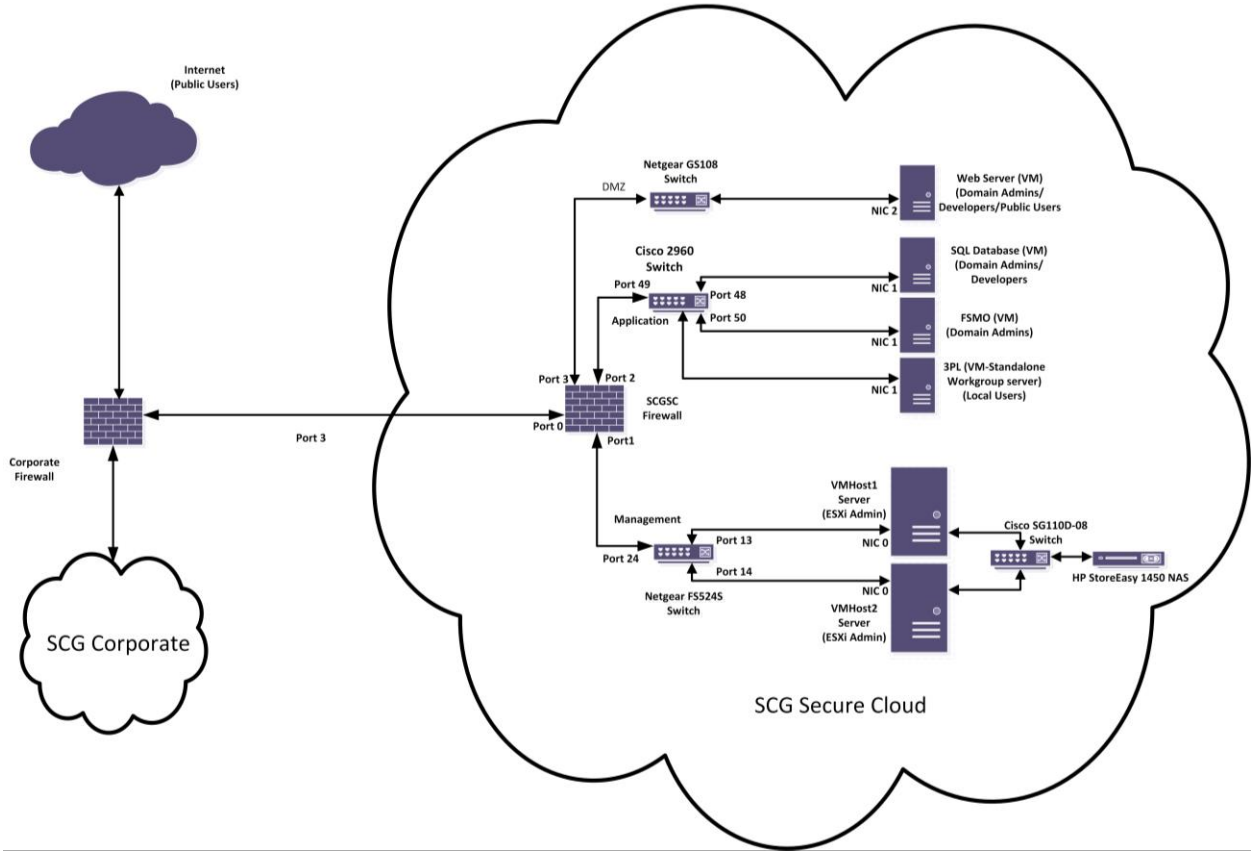
This section provides a general description of the system architecture and functionality, as well as all relevant SCGSC architectural diagrams (system architecture, input/output) that will be useful in recovering the system (see Figure 1). These diagrams also are available in the most recent version of SCGSC's System Security Plan. A description of the operating environment, physical location, and general location of users follows:

- Operating environment for SCGSC – The system operates under normal room temperature (i.e., 60-80 degrees F). The temperature is kept constant by SCG's Mitsubishi 2-ton mini split dedicated HVAC system. The Esensors environment monitoring device checks temperature and humidity in the secure room where the SCGSC equipment is located. The humidity is maintained between 30% and 50%. If the temperature exceeds 95 degrees F or the humidity is outside of the normal range, an e-mail notification is automatically sent to the IT Director.
- Physical location of the system (production) – The SCGSC is located on the 7th floor of the building at 656 Quince Orchard Road, Gaithersburg, Maryland. It is

located in a secured server room in a locked server cabinet. The server room door is locked and access is managed and monitored with Brivo security swipe.

- General location of users (operating locations) – Users access SCGSC through a SSL port on the firewall. Domain Administrators and Developers access SCGSC through a secure management port on the firewall.

Figure 1. SCG Secure Cloud System Architecture Diagram



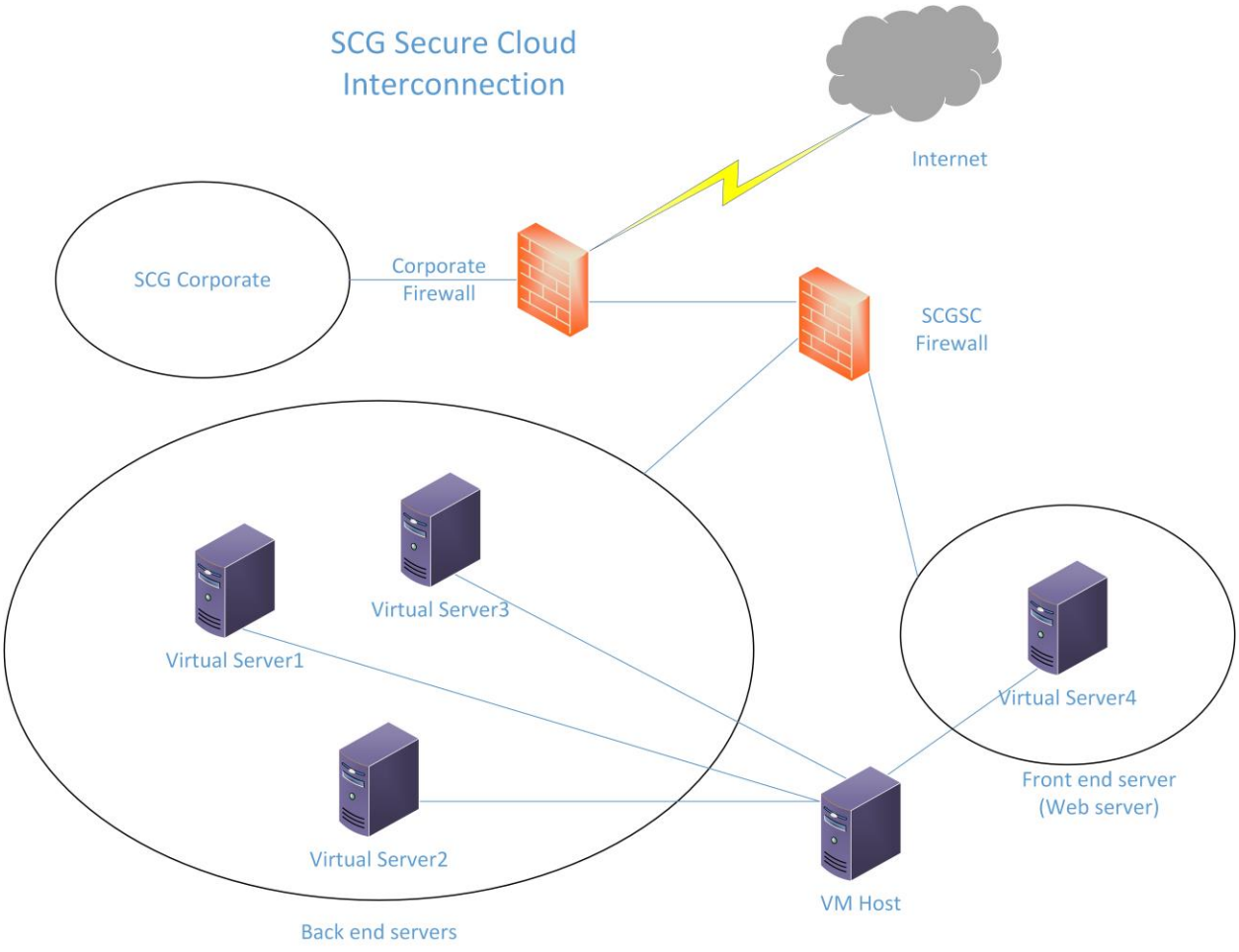
2.1.2 System Interconnections and Associated Plans

SCG Secure Cloud connects to the Internet through a SSL port on the firewall. The connections for SCGSC to operate are listed in Table 1 and depicted in Figure 2-2. The SCGSC does not directly connect with any other systems. Symantec Endpoint Protection, BackupExec, Microsoft Dynamics NAV, and VSphere communication is controlled through a firewall rule that allows services to operate.

Table 1. Information Systems that Connect to SCGSC

Information System	Information Transferred or Support Provided	POC	POC Contact Data
Internet Service Provider	SSL Web access	Level 3 Communications	(877) 453-8353

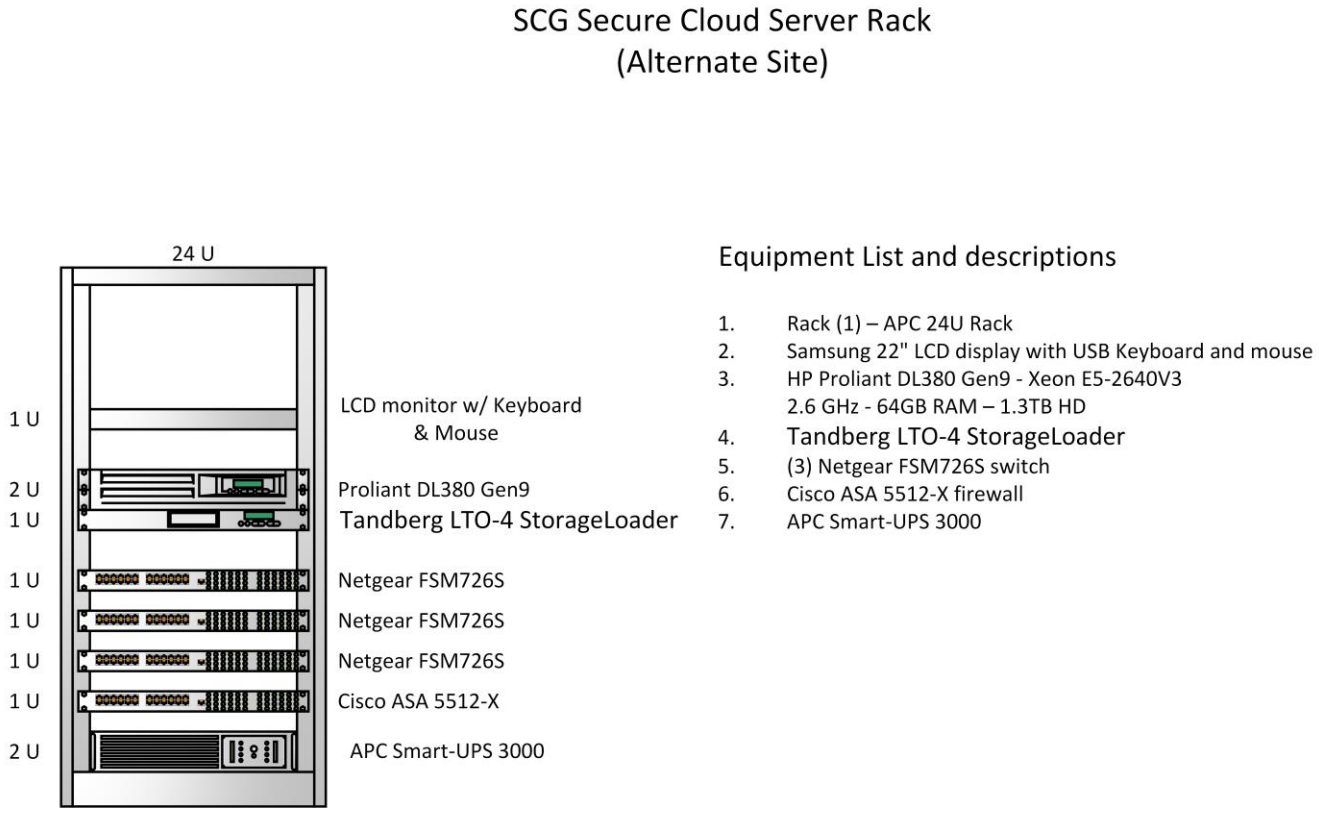
Figure 2. SCG Secure Cloud Connections



2.1.3 Alternate Site Inventory

The hardware and software inventory to support the operations of the SCGSC at the alternate location are listed in Figure 3. This inventory includes information on the type of equipment required to house, store, run, and backup the system.

Figure 3. Alternate Site Inventory for SCGSC



2.1.4 SCGSC System and Component Inventory

This section identifies the hardware and software inventory for the SCGSC. The inventory information includes the type of server on which the system runs, processors and memory requirements, storage requirements, and any other pertinent details. The software inventory identifies the OS, including service pack or version levels, and any other applications necessary to operate the system, such as database software.

The SCGSC components at the alternate site are identified in Table 2.

Table 2. SCGSC System and Component Inventory

Configuration Item Name	Item Description	Type	Function	Software/Version
SCGSCRACKCONV	Startech LCD Serial #: E071X4B40040	Hardware	Display, keyboard, mouse	NA
VHOST1	HP ProLiant DL380 Gen9 – Xeon E5-2640V3 2.6 GHz, 64 GB RAM, 1.3 TB HD, RAID 5 Serial #: MXQ52705DT	Hardware	Server	VMware VSphere ESXi 6.0 update 2
SCSQL-PROD (VM 1*)	Virtual Machine Serial #: NA	Software	Database Server	Windows 2008 R2 Enterprise (x64) SP1 SQL Server 2012 Standard (x64) SP2 Symantec Protection Suite Enterprise 2015 DNS (secondary)
SCCOLDSHARE-PROD (VM 2*)	Virtual Machine Serial #: NA	Software	Web Server	Windows 2008 R2 Enterprise (x64) Microsoft IIS 7.0 ColdFusion 9 SharePoint Foundation 2010 Symantec Protection Suite Enterprise 2015
SCFSMO (VM 3*)	Virtual Machine Serial #: NA	Software	Domain Controller	Windows 2008 R2 Enterprise (x64) DNS (primary) Active Directory Kiwi Syslog Symantec Protection Suite Enterprise 2015
3PL (VM 4*)	Virtual Machine Serial #: NA	Software	Webserver	Windows 2008 R2 Enterprise (x64) MS Dynamics NAV Symantec Protection Suite Enterprise 2015
SCGSCTandberg (Tape Backup)	Tandberg StorageLoader LTO-4 Tape Autoloader, LTO Ultrium – SAS-2 Serial #: PW0833AMJ50041	Hardware	Automated Backup of VM1, VM2, VM3, VM4	BackupExec 2015 Enterprise

Configuration Item Name	Item Description	Type	Function	Software/Version
SCGSCSW01 (Unmanaged Switch)	Netgear FSM726S 24-Port Switch Serial #: FM76339DB026365	Hardware	Routes traffic to non-privileged user network (internet to apps)	NA
SCGSCSW02 (Unmanaged Switch)	Netgear FSM726S 24-Port Switch Serial #: FM76339DB026372	Hardware	Routes traffic to management network	NA
SCGSCSW03 (Unmanaged Switch)	Netgear FSM726S 24-Port Switch Serial #: FM76339DB026373	Hardware	Routes traffic to the DMZ network	NA
SCGSCFW02	Cisco ASA 5512-X Model: ASA 5512v3 Serial #: FCH2012J2LN	Hardware	Filters traffic and maps internal network to external	Cisco Firewall ASA 9.5.2
SCGSCUPS	APC Smart-UPS 3000VA Serial #: AS135013348400C0B78682CD	Hardware	Uninterruptable Power Supply	NA

* VM 1, VM 2, VM 3, and VM 4 are virtual machines that are an emulation of a particular computer system that resides in the memory of the physical host.

2.2 DRP Roles and Responsibilities

Table 3 includes responsibilities that describe the roles and responsibilities of each individual or team for executing or supporting and coordinating system recovery at an alternate site. Primary site personnel responsible for assisting in the coordination of the transition of data or full operations of the system to an alternate processing location are referenced below. Recovery points of contact at the primary site and the alternate site are documented in this plan.

The leadership role is the responsibility of the DRP Director. SCG's Director of IT will serve in this role. The DRP Director has overall management responsibility for the plan and is responsible for overseeing recovery effort progress, initiating any needed escalations or awareness communications, and establishing coordination with other recovery teams as appropriate.

Table 3. DRP Roles and Responsibility

DRP Role	Name and Title	Responsibilities
DRP Director, Disaster Recovery Team Leader	Chuck Lee, Director of IT	• Overall responsibility for the development, execution, and maintenance of the DRP. • Ensures that the DRP is developed with the cooperation of managers associated with the business processes supported by the system. • Confirms expected duration of the system disruption with the DR Team, Program Manager, and SCG President based on the outage assessment. • Oversees activation of the DRP. • Determines if interim/secondary processing procedures activities should be initiated to maintain current business operations or if operations should be temporarily suspended until the system has been recovered. • Responsible for the testing, maintenance, and distribution of the DRP, which may be delegated to other personnel. • Authorizes all changes to the DRP. • Monitors Recovery Team activities until the system is fully recovered at the alternate site. • Ensures that recovery operations are being performed consistent with service level agreements/service level requirements. • Provides periodic status updates to the Program Manager and SCG President. • Files an After Action Report upon resumption of normal operations. • Oversees testing, maintenance, and distribution of the DRP.
SCG President	Beverly Campbell, SCG President	• Activates the DRP based on the assessment of the damage reported by the DRP Director.
Business/ Service Line POC(s)	Stacy Philipson, Vice President of Administration Susie Warner, Program Manager	• Represents the recovery and restoration interests of affected business/service line.
Disaster Recovery Team Members	Chuck Lee, IT Director Kenny Ying Lee, IT Systems Specialist	• Determines the expected duration of the failover to the alternate site. • Prioritizes the sequence of resource recovery.

DRP Role	Name and Title	Responsibilities
	John Bernheimer, IT Systems Specialist Justin Gray, Information Center Manager Ric Blackman, Web Development Director Adam Mann, Web Developer Susie Warner, Program Manager	• Performs all system recovery and resumption activities. • Powers systems on/off. • Retrieves backup tapes. • Configures systems. • Ensures voice and data communications are functioning. • Provides IP numbers and network routing information. • Includes validation testing teams or personnel.
Alternate DRP Director, Alternate Disaster Recovery Team Leader	Ric Blackman/Web Development Director	• Assumes responsibilities for the DRP Director when the DRP Director is unavailable
Alternate Disaster Recovery Team Members	Justin Kaufman, Web Developer Stacy Philipson, Vice President of Administration Denise Hoffman, Project Manager Rick Casazza, Distribution Center Manager	• Same responsibilities as the primary Disaster Recovery Team • Activated when one or more members of the primary is/are unavailable • Coordinate with Primary Site Recovery Team
Primary Site Recovery Team	Chuck Lee, Director of IT Kenny Ying Lee, IT Systems Specialist John Bernheimer, IT Systems Specialist Ric Blackman, Web Development Director Adam Mann, Web Developer Susie Warner, Program Manager	• Responsible for coordinating recovery activities with the Alternate Site Recovery Team

3. Activation and Notification

The Activation and Notification Phase defines initial actions taken once a disruption has been detected and appears to be imminent. The DRP Activation and Notification phase defines the activities required to activate the DRP and notify supporting recovery personnel. For sites that require mobilization, these phases include preparing for deployment of support personnel to the specified alternate site or coordinating activities between the primary site and the site where data or operations will be temporarily processed.

NOTE: *In an emergency, SCG's top priority is to preserve the health and safety of its staff before proceeding to the Notification and Activation procedures.*

3.1 Activation Criteria and Procedures

The SCGSC DRP may be activated if one or more of the following criteria are met:

1. The facility housing SCGSC is rendered unusable and may not be available within 48 hours as set forth in the Information Technology Contingency Plan (ITCP).
2. The nature of the disaster is such that SCGSC will be down for more than 48 hours[1].

The following persons may activate the DRP if one or more of the above criteria are met:

- Chuck Lee, Director of IT
- Beverly Campbell, SCG President
- Stacy Philipson, Vice President of Administration
- Susie Warner, Program Manager
- Ric Blackman, Web Development Director

3.2 Notification Procedures

The first step upon activation of the SCGSC DRP is notification of appropriate business personnel, users, and system support personnel that operations will be transferred to the alternate site. To facilitate the contact to key personnel and others, contact tables are provided in Sections 3.2.3 and 3.2.4.

Once the DRP has been activated by one of the individuals listed above, that person notifies the others (i.e., IT Director, SCG President, Vice President of Administration, Web Development Director, Program Manager) using the sequence established in the call tree (defined in the SCGSC Contingency Plan) if they are not present and involved in the decision to activate the DRP. The DRP Director notifies the members of the DR

[1] *All RTOs in this document are derived from the system ITCP.*

Team of the event and if relocation is required; the Vice President of Administration (Business Continuity Plan Team Leader) notifies members of the Business Continuity Plan Team; and the SCG President (Contingency Planning Team Leader) notifies the members of the Contingency Plan Team. Team members are to be informed of all applicable information and prepared to respond and relocate if necessary. The Vice President of Administration also notifies other key personnel, vendors, and users.

The IT Director is to notify the alternate site that the DRP has been activated and request that personnel prepare the facility for the arrival of the recovery teams.

The Vice President of Administration is to notify remaining personnel (via notification procedures) on the general status of the incident.

3.2.1 Notification Procedures

Following activation of the DRP, the notification procedures in the event of a disaster are as follows:

- The DRP Director will contact each member of the Disaster Recovery Team, which includes the Program Manager for the SCGSC.
- The Vice President of Administration and Program Manager will notify the NIDDK client.
- The DRP Director will contact the alternate site and request personnel to prepare the site for the DR Team arrival.

When contacting the members of their teams, the Team Leaders will ensure that notification is done as quickly and efficiently as possible using available technology (e.g., e-mail blast, smart phone calls and voice and text messages, and home phone calls and voice messages). If a team member cannot be reached directly by the Team Leader, a text message, voicemail (on mobile and home phones), and e-mail message will be left and the Team Leader will continue contacting the remaining team members. The notification should include the following:

- Approximate date and time SCGSC was impacted.
- Who discovered the outage.
- The extent of the damage.
- Whether the SCGSC can be recovered at the primary facility or must be recovered at an alternate site.
- Time and place to report for recovery operations.
- Estimated time to recover.

The call tree will be used to notify other relevant personnel and users. If the first individual is contacted and is reached, that individual will contact the next person on the list. If the next person is not reachable, the caller will continue to call down the tree until an individuals on the list is reached. Once an individual is reached, that individual will be

responsible for contacting the next person on the list, as well as those above them. Each of the individuals listed in the call tree have cell phones by which to reach other key personnel after hours.

3.2.2 Alternate Site Access

SCG maintains an alternate processing facility for SCGSC at 7315-A Grove Road, Frederick, Maryland. This facility provides a location to resume system operations in the event of a catastrophic event that disables or destroys the primary facility. The Frederick facility has the appropriate security and environment to accommodate SCGSC.

Members of the DR Team have keys to gain entry to the building in Frederick as well as keys to access the server room at that facility. All SCG staff members are authorized to enter the Frederick facility. The Information Center Manager, Justin Gray, will serve as the point of contact for the Frederick facility. He will be contacted by the DRP Director to prepare the Frederick facility for the arrival of the DR Team.

The Frederick site already contains a server room with a server rack and all of the hardware and software necessary to rebuild the SCGSC. The facility also has appropriate work space (300 square feet) to accommodate the DR Team working to recover the SCGSC system. The facility is secure and has power, water, telephones, computers, printers, copiers, fax machine, and 100 Mbps fiber optic Internet service. Tape backup of SCGSC also is maintained at the Frederick facility. If the disaster is so widespread that both the Gaithersburg and Frederick facilities are impacted, the DR Team has identified an appropriate alternate site (i.e., the Staunton, Virginia office) that could be used to recover the SCGSC system. Tape backup of the SCGSC also is stored at the Staunton location.

3.2.3 DRP Personnel Contact Information

Contact information for each person who has a role or responsibility for the activation or implementation of the DRP or coordination with the DR Team is provided in Tables 4, 5, 6, and 7.

Table 4. Key Personnel with DRP Activation Authority Contact Information

Title	Name	Contact Information	Emergency Role
IT Director	Chuck Lee	301-670-4990 (W) 301-366-3273 (C) 301-637-4355 (H) clee@scgcorp.com	Damage Assessment DRP Activation DRP Director Disaster Recovery Team Leader
SCG President	Beverly Campbell	301-670-4990 (W) 301-461-1109 (C) 540-887-9829 (H) bcampbell@scgcorp.com	Damage Assessment DRP Activation Contingency Planning Team Leader

Title	Name	Contact Information	Emergency Role
Vice President of Administration	Stacy Philipson	301-670-4990 (W) 301-742-5954 (C) 301-363-5707 (H) sphilipson@scgcorp.com	Damage Assessment SCG Facilities Management Business Continuity Plan Team Leader Disaster Recovery Team Alternate
Web Development Director	Ric Blackman	301-670-4990 (W) 301-529-0760 (C) rblackman@scgcorp.com	Damage Assessment DRP Director Alternate Disaster Recovery Team Member
Program Director	Susie Warner	301-670-4990 (W) 301-366-3217 (C) 301-355-4388 (H) swarner@scgcorp.com	Damage Assessment DRP Activation Disaster Recovery Team Member
Note: If the incident/disaster occurs when staff members are not in the facility, call cell phone numbers before trying home numbers.			

Table 5. Disaster Recovery Team Contact Information

Title	Name	Contact Information	Emergency Role
IT Director	Chuck Lee	301-670-4990 (W) 301-366-3273 (C) 301-637-4355 (H) clee@scgcorp.com	DRP Director Disaster Recovery Team Leader
Web Development Director	Ric Blackman	301-670-4990 (W) 301-529-0760 (C) 301-529-0760 (H) rblackman@scgcorp.com	Alternate DRP Director Alternate Disaster Recovery Team Leader Disaster Recovery Team Member
IT Systems Specialist	Kenny Ying Lee	301-670-4990 (W) 315-956-7796 (C) ylee@scgcorp.com	Disaster Recovery Team Member
IT Systems Specialist	John Bernheimer	301-670-4990 (W) 410-428-1330 (C) jbernheimer@scgcorp.com	Disaster Recovery Team Member
Web and Applications Developer	Adam Mann	301-670-4990 (W) 301-717-3273 (C) amann@scgcorp.com	Disaster Recovery Team Member
Program Manager	Susie Warner	301-670-4990 (W) 301-366-3217 (C) 301-355-4388 (H) swarner@scgcorp.com	Disaster Recovery Team Member

Title	Name	Contact Information	Emergency Role
Information Center Manager	Justin Gray	240-629-3238 (W) 301-524-2986 (C) jgray@scgcorp.com	Incident Response/Disaster Recovery Team Member Frederick Facility POC
Note: If the incident/disaster occurs when staff members are not in the facility, call cell phone numbers before trying home numbers.			

Table 6. Alternate Disaster Recovery Team Contact Information

Title	Name	Contact Information	Emergency Role
Web and Applications Developer	Justin Kaufman	301-670-4990 (W) 240-351-4522 (C) jkaufman@scgcorp.com	Disaster Recovery Team Alternate
Vice President of Administration	Stacy Philipson	301-670-4990 (W) 301-742-5954 (C) 301-363-5707 (H) sphilipson@scgcorp.com	Disaster Recovery Team Alternate
Project Manager	Denise Hoffman	301-670-4990 (W) 240-426-2566 (C) dhoffman@scgcorp.com	Disaster Recovery Team Alternate
Distribution Manager	Rick Casazza	240-629-3232 (W) 301-514-7283 (C) rcasazza@scgcorp.com	Disaster Recovery Team Alternate
Note: If the incident/disaster occurs when staff members are not in the facility, call cell phone numbers before trying home numbers.			

Table 7. Primary Site Recovery Team Contact Information

Title	Name	Contact Information	Emergency Role
IT Director	Chuck Lee	301-670-4990 (W) 301-366-3273 (C) 301-637-4355 (H) clee@scgcorp.com	DRP Director Disaster Recovery Team Leader
Web Development Director	Ric Blackman	301-670-4990 (W) 301-529-0760 (C) 301-529-0760 (H) rblackman@scgcorp.com	Alternate DRP Director Alternate Disaster Recovery Team Leader Disaster Recovery Team Member
IT Systems Specialist	Kenny Ying Lee	301-670-4990 (W) 315-956-7796 (C) 315-956-7796 (H) ylee@scgcorp.com	Disaster Recovery Team Member

Title	Name	Contact Information	Emergency Role
IT Systems Specialist	John Bernheimer	301-670-4990 (W) 410-428-1330 (C) jbernheimer@scgcorp.com	Disaster Recovery Team Member
Web and Applications Developer	Adam Mann	301-670-4990 (W) 301-717-3273 (C) amann@scgcorp.com	Disaster Recovery Team Member
Program Manager	Susie Warner	301-670-4990 (W) 301-366-3217 (C) 301-355-4388 (H) swarner@scgcorp.com	Disaster Recovery Team Member
Note: If the incident/disaster occurs when staff members are not in the facility, call cell phone numbers before trying home numbers.			

3.2.4 Call Tree Activation

A call tree is a commonly used notification method when information must be communicated to a group of people in a relatively short time. Call trees are an effective means of conveying the communication sequence in which leadership, recovery personnel, and facility points of contact should be alerted. To be effective, the call tree must be defined and the needed contact information gathered and disseminated prior to an incident occurrence. Also, it is very important to keep the contact information current.

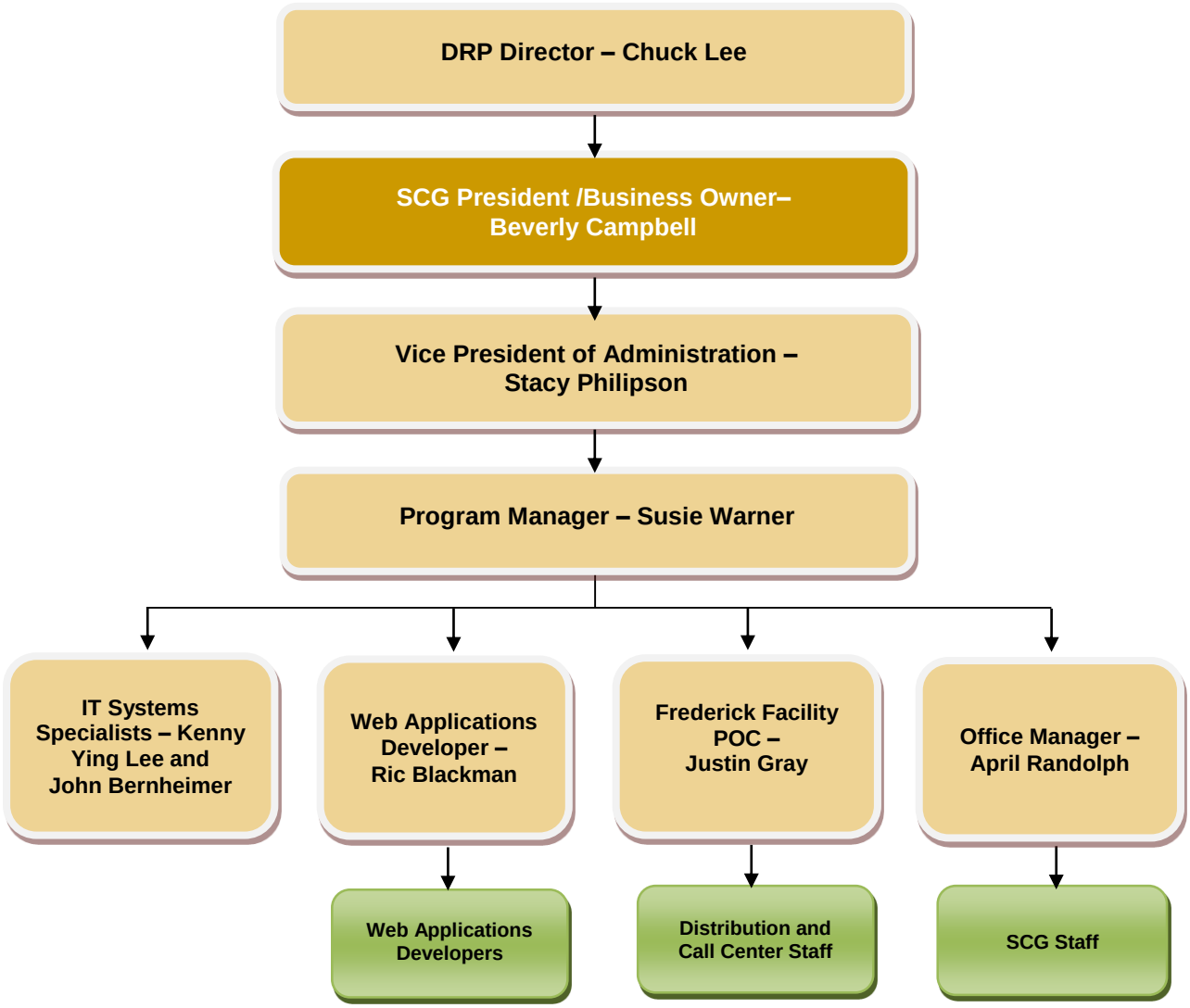
If the call tree is activated for a disaster impacting the SCGSC system, the following key individuals will be contacted first and in the order listed:

- Chuck Lee, IT Director
- Beverly Campbell, SCG President/Business Owner
- Stacy Philipson, Vice President of Administration
- Susie Warner, Program Manager
- Kenny Ying Lee, IT Systems Specialist
- John Bernheimer, IT Systems Specialist
- Ric Blackman, Web Development Director
- Justin Gray, Frederick Facility POC/Information Center Manager
- April Randolph, Office Manager

If the first individual is contacted and reached, that individual will contact the next person on the list. If the next person is not reachable, the caller will continue to call down the tree until an individual on the list is reached. Once an individual is reached, that individual will be responsible for contacting the next person on the list, as well as those above them. Each of the individuals listed above have cell phones that they monitor after business hours to ensure they can be reached in an emergency.

The call tree will be used to notify additional SCG personnel about the disaster. A call tree for the alert/notification of SCGSC leadership, recovery personnel, and any facility points of contact who are to be alerted of the DRP activation is presented in Figure 4.

Figure 4. DRP Call Tree for SCGSC System Recovery



3.2.5 Alternate Site Vendors

Table 8 identifies the vendors that may be needed to recover the SCGSC system at the Frederick facility.

Table 8. Alternate Site Vendor Contact Information

VENDOR CONTACT DATA			
Vendor Number	1	**Vendor Type***	ISP
Vendor Name	Comcast Enterprise Business		
Address	20 W. Gude Drive		
City-State-Zip Code	Rockville, MD 20850		
Product	Internet Service Provider (100 Mbps fiber optic circuit)		
Model/Serial No.			
Contract No.			
Vendor Type Code	Internet Service Provider		
Last Updated	5-19-2016		
Primary Contact Name	Bettel Mussie		
Office Phone #	(240) 762-8962	**Emergency Phone #**	(240) 762-8962
Secondary Contact Name	Kathy Lowe		
Office Phone #	(856) 792-3272	**Emergency Phone #**	(856) 207-0243
Special Instructions			

VENDOR CONTACT DATA			
Vendor Number	2	**Vendor Type***	Hardware/Software
Vendor Name	Zones, Inc.		
Address	1102 15th St SW, Suite 102		
City-State-Zip Code	Auburn, WA 98001-6509		
Product	Hardware/Software		
Model/Serial No.			
Contract No.			
Vendor Type Code	Hardware/Software		
Last Updated	5-19-2016		
Primary Contact Name	Daniel Turgeon		
Office Phone #	(800) 258-0882 Ext. 56257	**Emergency Phone #**	
Secondary Contact Name	Zones, Inc.		
Office Phone #	(253) 205-3000	**Emergency Phone #**	
Special Instructions			

VENDOR CONTACT DATA			
Vendor Number	3	**Vendor Type***	ISP
Vendor Name	Nextiva		
Address	8800 E. Chaparral Road, Suite 300		
City-State-Zip Code	Scottsdale, AZ 85250		
Product	Internet Service Provider and VOIP		
Model/Serial No.			
Contract No.			
Vendor Type Code	Internet Service Provider/VOIP		
Last Updated	5-19-2016		
Primary Contact Name	Thomasina Cady		
Office Phone #	(480) 725-9628	**Emergency Phone #**	
Secondary Contact Name	Nextiva		
Office Phone #	(800) 375-5325	**Emergency Phone #**	
Special Instructions			

4. Recovery

The Recovery Phase provides formal recovery operations that begin after the DRP has been activated, outage assessments have been completed (if possible), personnel have been notified, and in some situations appropriate teams have been mobilized.

Recovery Phase activities focus on implementing recovery strategies to restore the system and data capabilities through the restoration of the facility or alternate processing location, failover of IS processes, IS components, repair of damage, and resumption of operational capabilities at the original or new permanent location. At the completion of the Recovery Phase, SCGSC will be operational and capable of performing all necessary functions. Specific instructions at the key stroke level are provided in Appendix D.

4.1 System Recovery at Alternate Site

The DRP Director will coordinate recovery activities at the alternate site in Frederick, Maryland. He will confirm with the Frederick facility POC that the building's power, communications, climate control system, security system, and Internet services are functioning. Once the DRP Director confirms the functionality of these services, the DR Team will meet at the Frederick facility to begin SCGSC system recovery efforts.

4.2 Sequence of System or Data Recovery Activities

The following high level activities occur during the recovery of the SCGSC system:

- Retrieve most recent backup tape (from the previous evening backup).
- Rebuild all necessary items listed in Figure 3 (System and Component Inventory).
- Restore the system data from the backup tapes. The restore sequence is as follows:
  - Firewall configuration
  - Switch configuration
  - VMWare configuration
  - Virtual Machines
  - Modify public DNS at Network Solutions to reflect new ISP
  - Server configuration
- Conduct functional system testing and validation:
  - Test SQL databases
    - ✓ Use SQL Management Studio to connect to SQL server
    - ✓ Query data and verify data are correct (date of tape)
  - Test Web Applications
    - ✓ Use Visual Studio to connect to .Net applications and verify content
  - Test Website access and functionality
    - ✓ Use Internet browsers (Internet Explorer, Google Chrome, and Firefox) to connect to websites and verify functionality.
  - Test MS Dynamics NAV
    - ✓ Connect to 3PL CRM and verify functionality.

4.3 Escalation Procedures

SCG's normal business hours are from 7:00 a.m. to 6:00 p.m. Eastern, Monday through Friday. SCG's non-business hours are Monday through Friday from 6:00 p.m. until 7:00 a.m. Eastern, and all day Saturday and Sunday. If an event occurs during normal business hours, the Vice President of Administration will activate the DRP and communicate with SCG staff to initiate orderly evacuation procedures. The emergency exits in the building are well marked and SCG conducts periodic drills to ensure timely, safe evacuation. Once outside the building, supervisors will verify their staff members are present and report to the Vice President of Administration to ensure everyone has exited the building. The Vice President of Administration then will provide instructions to evacuated staff and activate the call tree to update staff who were not in the office, and inform them of the situation.

If a disaster occurs during non-business hours, and SCG employees have not already been contacted with instructions, they are instructed to take the following steps:

- **Staff Members.** Staff members have been instructed to contact their immediate supervisor for further instructions. If their immediate supervisor is not available, then staff members have been instructed to escalate the matter with their supervisor's supervisor. If that supervisor is not available, then the staff members have been instructed to contact a member of the DR Team and to continue trying until he/she reaches any member of SCG's senior management or DR Team member.
- **Senior Managers (Directors, Program Managers, Project Managers, and Team Leads).** SCG's senior managers have been instructed to escalate the matter to a member of the Executive Management Team.
- **Executive Management Team.** The President and Vice President of Administration will be contacted to authorize the initiation of the DRP.

5. Reconstitution

Reconstitution is the process by which a recovered system is tested to validate system capability and functionality. During Reconstitution, recovery activities are completed, normal system operations are resumed, and operations are transitioned back to the primary site.

The DRP Director will ensure that there are no remaining after effects of the disaster and that no threats have remained unaddressed. If the original facility is "unrecoverable," the activities in this phase are applied to transferring the SCGSC system to a new permanent site or preparing the alternate site as the new permanent location to support system processing requirements. This phase consists of two major activities: (1) validating successful recovery, and (2) deactivation of the DRP.

5.1 Concurrent Processing

SCGSC does not have concurrent processing as part of validation. Once the system has been tested and validated, it will be placed into normal operations.

5.2 Validation Data Testing

Validation data testing is the process of testing and validating recovered data to ensure that data files or databases have been recovered completely. After current data are restored, the data are verified with SQL database to ensure that the recovered data are complete and current to the last available backup. The detailed procedure is described in Appendix E.

5.3 Validation of Functionality

The DPR Director will validate the functionality of the firewall, VMWare host, virtual machine, virtual machine applications, and database.

- The firewall will be validated by browsing the Internet and using commandline tools (ping, tracert, and nslookup).
- VMWare host will be validated by using host client software, VSphere Client.

- The Virtual Machine (VM) will be validated using VSphere client's "Power On Virtual Machine."
- VM applications will be validated as follows:
    - Symantec Endpoint Protection Suite will be validated by logging VMs and checking updates.
    - Coldfusion 9 will be validated using Coldfusion Administration and Management Console.
    - SharePoint Foundation 2010 will be validated using SharePoint Administration and Management Console.
    - DNS will be validated using Windows "Command Prompt" and pinging network names and IPs.
    - Kiwi Syslog will be validated using Management Console and running reports.
- Database will be validated using front end interface (Web browser) to write information to the database and then using SQL Management Studio to run a query for specific fields to see if the information was saved.

Detailed functionality test procedures are provided in Appendix E.

5.4 Recovery Declaration

Upon successfully completing the testing and validation of the SCGSC system, the DRP Director will formally declare recovery efforts complete, and that SCGSC is in normal operations. The DR Team, Vice President, President, Program Manager, and SCG staff will be notified of the declaration by the DRP Director.

5.5 Notifications (Users)

Upon return to normal system operations, NIDDK and all SCGSC users will be notified by the Program Manager via e-mail that SCGSC has returned to normal operations.

5.6 Cleanup

Cleanup is the process of cleaning up or dismantling any temporary recovery locations, restocking supplies used, returning manuals or other documentation to their original locations, and readying the site for a possible future contingency event.

All backup tapes, documents, software, media, and manuals will be returned to their designated permanent storage locations at the Gaithersburg and Frederick facilities.

5.7 Offsite Data Storage

It is important that all backup and installation media used during recovery be returned to the offsite data storage location so that they are available for future use. All backup tapes and software originals and backup copies will be returned to offsite storage at SCG's Frederick location.

5.8 Data Backup

As soon as reasonable following recovery, the system should be fully backed up and a new copy of the current operational system stored for future recovery efforts. This full backup is stored securely with other system backups and marked appropriately. Within 48 hours after recovery status, the IT Director will prepare a full backup of the current system for permanent storage. One backup will be stored at the Gaithersburg facility and a second at the offsite storage facility in Frederick.

5.9 Event Documentation

It is important that all recovery events throughout the transition of operations to the alternate site and back to the primary site be well-documented, including actions taken and problems encountered during the recovery effort, and lessons learned for inclusion and update to the DRP. It is the responsibility of each member of the DR Team to document his/her actions during the recovery effort, and to provide that documentation to the DRP Director. Alternatively, one of the DR Team members may be appointed the task of tracking and documenting the events in the event log.

All key events that occur during the disaster recovery phase must be recorded. An event log (see Table 9) will be maintained by the DR Team Leader. The Disaster Recovery Event Log should include all recovery steps performed and by whom, the time the steps were initiated and completed, and any problems or concerns encountered while executing activities).

This event log should be started at the commencement of the emergency and a copy of the log submitted to the Vice President of Administration and President once the initial dangers have been controlled and the system recovered at the alternate site. The DR Team Leader will continue to record actions in the event log until the recovery efforts are complete. The final event log will be submitted to the Vice President of Administration and the President. It will be used to update the DRP and Contingency Plan for SCGSC.

Table 9. Disaster Recovery Event Log

Description of Disaster:					
Commencement Date:					
Date/Time DR Team Mobilized:					
Activities Undertaken by the DR Team	**Date & Time Initiated**	**Date & Time Completed**	**DR Team Member Responsible**	**Problems Encountered, Resolution, & Outcome**	**Follow-on Action Required**

In addition to the Disaster Recovery Event Log, the following types of documentation should be generated and collected after a contingency activation:

- Functionality and data testing results.
- Description of problems encountered and the solutions employed to overcome them.
- Lessons learned and suggestions for improving the recovery process.
- After Action Report (AAR).

The AAR should include a description of the disaster, the participants involved in the recovery and their roles, the activities taken in the recovery, who executed the activity, problems that were encountered, solutions implemented to overcome problems, an assessment of how well the participants performed and the effectiveness of the DRP and Contingency Plan, and next steps or follow-up actions.

An important part of the AAR is next steps, which may include recommendations to: (1) improve the DRP and Contingency Plan, (2) modify an operational process to improve its recoverability, (3) identify recovery steps that may be in the wrong sequence, (4) identify changes to the system or technology that will improve its recoverability, or (5) implement changes to the recovery process.

The information in the AAR will be used as a tool for improving SCG's overall disaster recovery capabilities. It also provides an important audit tool, documenting what happened in the recovery process, what worked/didn't work, and what can be done to improve the recovery process.

5.10 Deactivation

Once all recovery activities have been completed and documentation has been updated, the IT Director will formally deactivate the DRP recovery effort. Notification of this declaration will be provided to all business and technical POCs.

Appendix A: Alternate Storage Site

This appendix provides alternate storage site information and procedures for SCGSC. Alternate storage site information is a required control for systems with one or more high and moderate critical exposure values after the ISCPA.

- The alternate site is located at 7315-A Grove Road, Frederick, Maryland, approximately 30 miles from SCG's primary facility at 656 Quince Orchard Road, Gaithersburg, Maryland.
- The alternate site is leased by The Scientific Consulting Group, Inc. (SCG).
- Tape backups of the SCGSC are run daily for the SCGSC system and stored in a locked fireproof safe. As is done in Gaithersburg, at the end of every month, the daily tapes will be removed and the monthly backup tape will be stored indefinitely in the fireproof safe at the Frederick site.
- Justin Gray, Frederick Facility POC, will authorize retrieval of media or documents from the alternate storage facility.
- All members (and alternate members) of the DR Team are authorized to retrieve media or documents from the alternate storage facility.
- Access to the media and documents stored at the alternate storage facility is controlled by security card and key.
- There is adequate secure storage space available at the Frederick facility to accommodate SCGSC recovery.
- In the event of a widespread disruption or disaster that impacts both the Gaithersburg location and the alternate storage site in Frederick, the DR Team will retrieve backups from the Staunton, Virginia, office, located approximately 185 miles from the Gaithersburg facility.

Appendix B: Telecommunications

- Data line for Gaithersburg is leased from Level 3 Communications, Broomfield, CO 80021, 1-877-253-8353
- Data line for Frederick is leased from Comcast Enterprise, Philadelphia, PA, 1-800-741-4141.
- VoIP Phone system lines and alternate Internet Service service are provided by Nextiva, Scottsdale, AZ 85250, 1-800-285-7995
- Cellular communication service is provided by Sprint, Carol Stream, IL 60197, 1-800-777-4681 and Verizon Wireless, Wallingford, CT 06492, 203-639-9097.

Appendix C: Alternate Processing Procedures

One of the key functions of the SCGSC is the online catalog that allows users to order publications from the NIDDK clearinghouses. In the event that the SCGSC system is down and the catalog is unavailable, users can still order the desired publications through the Call Center operated by SCG at the Frederick facility as long as the phone lines are functioning.

Appendix D: Detailed Recovery Procedures

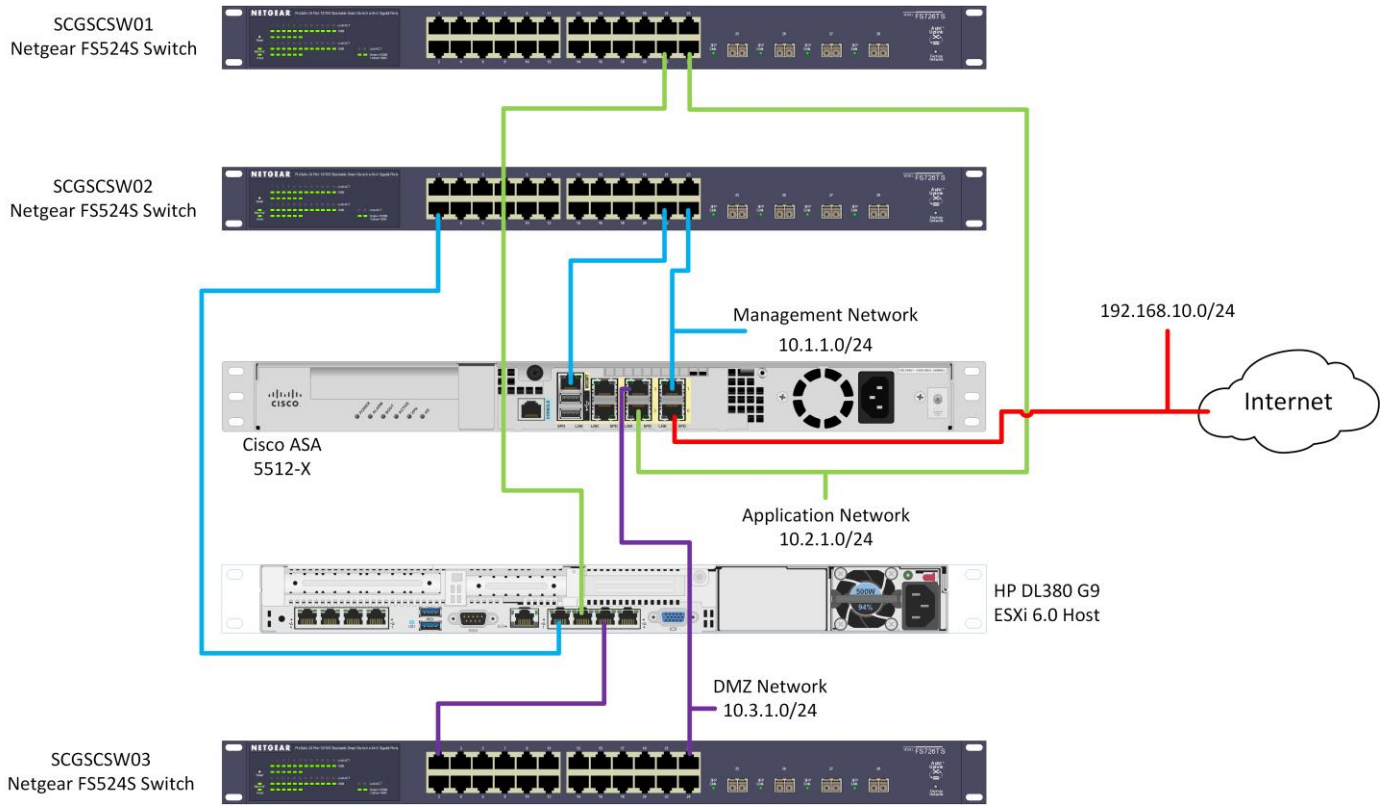
This appendix contains detailed recovery procedures for each SCGSC system component in the order in which each component is recovered (recovery priority). Recovery procedures are keyed to the specific requirements of the alternate site.

Failover Site: SCG, Frederick, MD	
Primary Site: Gaithersburg, Maryland	
Responsible Person and Emergency Contact Data:	Chuck Lee 301-366-3273 (C)
Alternate Responsible Person and Emergency Contact Data:	John Bernheimer 410-428-1330 (C)
Alternate Site: Frederick, Maryland	
Responsible Person and Emergency Contact Data:	Justin Gray 301-524-2986 (C)
Alternate Site: Alternate Responsible Person and Emergency Contact Data:	Ric Blackman 301-529-0760 (C)
Keystroke-Level Failover Steps	
Shutting Down the System (Primary Site)	
Virtual Machines (VMs)	1. Connect to VMWare host using VSphere Client software 2. Open VM's Console 3. Press Ctl+Alt+Ins 4. Log in as Administrator 5. Click <Start>, then choose <Shutdown>
VMWare ESXi Host	1. Connect to VMWare host using VSphere Client software 2. Right-Click on VHost and choose <Shutdown>
Network Devices (switches and firewall)	1. Manually power devices down by pressing the "OFF" button 2. Unplug power plug

Turning the System On (Alternate Site)	
Network Devices (switches, firewall, and VMWare ESXi Host)	1. Plug devices to network 2. Plug power cords into devices 3. Manually power devices up by pressing the “ON” button
VMWare ESXi Host	1. Assure all power connections s are connected to host server 2. Press the Power On button in front of the computer
Virtual Machines (VMs)	1. Connect to VMWare Host using VSphere Client software 2. Open VM’s Console 3. Click <Power On Virtual Machine>

Recovery Priority 1: Firewall	
Responsible Person and Emergency Contact Data:	Chuck Lee 301-366-3273 (C)
Alternate Responsible Person and Emergency Contact Data:	John Bernheimer 410-428-1330 (C)
Keystroke-Level Recovery Steps	
1. Copy firewall configuration from backup to local drive 2. Connect to Cisco firewall using ASDM software 3. Ensure IP address is accurate 4. Click Tools\Restore Configuration 5. Browse configuration file and click next; accept warning 6. Save new configuration and reboot firewall	

Recovery Priority 2: Connectivity	
Responsible Person and Emergency Contact Data:	Chuck Lee 301-366-3273 (C)
Alternate Responsible Person and Emergency Contact Data:	John Bernheimer 410-428-1330 (C)
Recovery Steps	
Connect the alternate site inventory devices as shown in Figure below using patch cables.	



Recovery Priority 3: VMWare ESXi Host*	
Responsible Person and Emergency Contact Data:	Chuck Lee 301-366-3273 (C)

Recovery Priority : Virtual Machines (VMs)*	
Responsible Person and Emergency Contact Data:	Chuck Lee 301-366-3273 (C)
Alternate Responsible Person and Emergency Contact Data:	John Bernheimer 410-428-1330 (C)

Keystroke-Level Recovery Steps

1. On computer connected to the network, run an internet browser and type in the IP of the ESXi host
2. Click File\New Virtual Machine\Typical
    a. Give new VM a name (e.g., SCGSQL, ColdShare-Prod)
    b. Select datashore1 for destination
    c. Select Windows and Windows 2008 R2 (64Bit) and click Next
    d. Ensure VM Network, Nic = 1, and Adapter = E1000 and click Next
    e. Virtual Disk size = 250 GB and click Next
    f. Click Finish
3. Right-click new VM and select Open Console
4. Insert Windows installation CD into DVD/CD drive
5. Click Power On button
6. Install Windows Server as usual

* These steps likely are not going to be necessary as a virtual machine restore will restore the entire server and operating system.

Recovery Priority 5: Applications	
Responsible Person and Emergency Contact Data:	Chuck Lee 301-366-3273 (C)
Alternate Responsible Person and Emergency Contact Data:	John Bernheimer 410-428-1330 (C)

Keystroke-Level Recovery Steps

1. Run Symantec BackupExec Enterprise from dedicated backup server at the Frederick location.
    a. Insert backup tape into drive
    b. In Symantec BackupExec, click Storage
    c. Right-click on Tape drive 0001 and choose Catalog
    d. Click the Backup and Restore Tab and right click the vCenter server (192.168.0.17) and click Restore
    e. Select latest backups of 3PL, SCCOLDSHARE-PROD, SCSQL-PROD, and SCFSMO
    f. Select to restore the data to a different vCenter or ESX server, enter IP of ESXi host (192.168.0.40), enter credentials, and provide the appropriate Virtual Machine name
    g. Click Next to the end of the Restore Wizard and then click Finish

Appendix E: System Validation Test Plans

This appendix identifies system acceptance procedures performed after the system has been recovered and prior to putting the system into full operation.

SCGSC Component Tested	Test Plan
Firewall	1. Validate by browsing the Internet - Validate www.google.com site - Validate www.msn.com site - Validate www.scgcorp.com 2. Use commandline tools (ping, tracert, and nslookup) - Ping firewall and Internet site (www.google.com) - Tracert to firewall and Internet site (www.google.com)
VMWare Host	Validate Host by using host client software, VSphere Client
Virtual Machine (VM)	Validate VM using VSphere client's "Power On Virtual Machine"
VM Applications	Symantec Endpoint Protection Suite – Validate by logging VMs and checking updates Active Directory – Test by logging on as a different user on the console of VM (SCFSMO). Validate login success. Coldfusion 9 – Validate using Coldfusion Administration and Management Console SharePoint Foundation 2010 – Validate using SharePoint Administration and Management Console IIS 7.0 – Validate using IIS Manager. Ensure websites can be viewed externally DNS – Validate using Windows "Command Prompt" and ping network names and IPs Kiwi Syslog – Run application on server and check log collection (date and time stamp) MS SQL Server 2012 – Validate using SQL Management Studio and run queries on databases

SCGSC Component Tested	Test Plan
	MS Dynamics NAV – Validate using credentials software credentials (administrator) and test functionality 3PL Server – Use MS Dynamics NAV client to connect to 3PL. Validate connection to server.

Database Validation Test Plan	
Procedure	**Expected Results**
Log into the database server being tested using SA credentials	Successful login, then presented with available databases on the server
Select a database for testing, expand modules, open query window and perform select statements on each table	Expect to receive results from each query showing all records in each table
Log off system as SA, then log in as webuser to confirm webuser account access	Successful login demonstrates SQL users are not corrupt
Perform select, update, insert, delete test statements with webuser	If records are returned then the users rights are intact
Log off and exit database server	By stepping back to login screen we know the server is functioning normally

Appendix F: DRP Testing

This appendix describes strategies and procedures for DRP Test, Training and Exercises (TT&E). Strategies and procedures for incident response (refer to the Incident Response Plan) will be tested in conjunction with DRP TT&E. Refer to NIST SP 800-53 Rev 4 CP-4 for details on control specifics.

Test, Training, and Exercise

Persons or teams assigned DRP roles must be trained to respond to a contingency event affecting the SCGSC system efficiently and correctly. SCG has developed a TT&E program to support the following objectives:

- Ensure that SCG's personnel are familiar with the DRP and its associated activation, recovery, and reconstitution procedures.
- Validate DRP policies and procedures.
- Exercise procedures through the use of tabletop and functional exercises, as appropriate.
- Ensure that hardware, software, backup data, and records required to support recovery at an alternate site are available.

SCG's testing program is conducted to ensure that SCG leadership and personnel have familiarity with contingency plans and DRP procedures. SCG validates contingency capabilities through regular tests, training, and exercises. TT&E also can identify issues or deficiencies for remediation. Exercises and tests offer different ways of ensuring that Contingency Plans and DRPs provide viable and actionable procedures to recover or restore the SCGSC system and applications to their original state in the event of a disruption. Training exercises and tests also provide valuable information for updating the DRP, IRP, and CP to ensure SCG personnel are well equipped to perform their roles and responsibilities in managing incidents and disasters. SCG also plans to conduct integrated training and testing for the SCGSC DRP, IRP, and CP activities.

Refer to NIST SP 800-84, *Test, Training, and Exercise (TT&E) Program for IT Plans and Capabilities*, for guidance on establishing an effective DRP testing program and the various methods and approaches for conducting tabletop exercise activities.

All tests and exercises shall include some kind of determination of the effects on SCG's operations and provide for a mechanism to update and improve the plan as a result.

The depth and rigor of DRP testing activities increase with the FIPS 199 availability security objective. (Refer to the FIPS 199 low, moderate, high in NIST SP 800-34 for details for conducting testing activities appropriate to their respective impact level.)

In most cases, for low-impact systems, a tabletop exercise is sufficient on an annual basis. The tabletop should follow a scenario that simulates a disruption, include points of contact whose roles appear in the DRP, be attended by the business and/or system owners or responsible authority, and be facilitated by the DRP personnel.

For moderate-impact systems, a functional exercise shall be conducted annually. The functional exercise should include an element of system recovery from backup media and is performed by the DR Team personnel.

Exercises

An exercise is a simulation of an emergency designed to validate the viability of one or more aspects of a Contingency Plan or DRP. Personnel with roles and responsibilities in a particular CP or DRP meet to validate the content of a plan through discussion of their roles and responses to emergency situations, execution of responses in a simulated operational environment, or other means of validating responses that do not include using the actual operational environment. Exercises are scenario-driven, such as a power failure at SCG's primary computing center or a fire causing certain systems to be damaged, with additional situations often being presented during the course of an exercise. Exercises help to identify gaps and inconsistencies within CPs and DRPs and procedures, as well as cases where personnel need additional training or when training needs to be changed. The deficiencies identified in exercises are documented as part of the exercise process.

Tabletop exercises are discussion-based exercises only and do not involve deploying or recovering systems, equipment, or other resources. Personnel meet to discuss their roles during an emergency and their responses to a particular emergency situation. During the tabletop exercise, participants also identify information or procedures in the plan that are outdated and need to be updated and corrected. The objectives of any tabletop exercise are to validate the content of the CP and DRP and related policies and procedures, validate participants' roles and responsibilities as documented in the plan, and validate the interdependencies documented in the plan.

Functional exercises allow personnel to validate their operational readiness for emergencies by performing their duties in a simulated operational environment. A functional exercise is designed to exercise the roles and responsibilities of specific team members, procedures, and assets involved in one or more functional aspects of a plan (e.g., backup procedures, communications, emergency notifications, information system equipment setup). Functional exercises vary in complexity and scope, from validating specific aspects of a plan (e.g., backup retrieval, reading backup data, and validation of offsite storage) to exercising all plan elements in a simulation. Functional exercises allow staff to execute their roles and responsibilities as they would in an actual emergency situation, but in a simulated manner.

DR Testing

DR testing is the method used to evaluate SCG's readiness and ability to recover a system from varying degrees of non-functioning to its original functional state by following authorized DRP keystroke procedures.

Tests are used to measure the effectiveness and suitability of the processes and procedures contained in the CP and DRP for the SCGSC system being tested and to evaluate compliance with an information system contingency. In the event of a disaster or disruption the goal is to be able to use tested CP and DRP to ensure that following

documented operational procedures and plans will result in successful recovery of the SCGSC system.

The scope of tests can range from individual system components or the entire system. Examples of tests are:

- Component tests - Restoring a system by retrieving backup data from offsite storage and loading the data to test the usability of the data.
- System tests - Restoring multiple components such as the operating system, database, and system software by using data stored offsite.

A test is conducted in as close to an operational environment as possible, testing components, or systems used to conduct daily operations. If feasible, an actual test of the components or system used to conduct daily operations can be used to comply with the CP testing program's annual requirements.

The SCGSC CP/DRP should be maintained routinely and exercised/tested at least annually. Contingency procedures must be tested periodically to ensure the effectiveness of the plan. The scope, objective, and measurement criteria of each exercise will be determined and coordinated by the DR Team Leader on a "per event" basis. The purpose of exercising and testing the plan is to continually refine resumption and recovery procedures to reduce the potential for failure.

There are two categories of testing: announced and unannounced. In an announced test, personnel are instructed when testing will occur, what the objectives of the test are, and what the scenario will be for the test. Announced testing is helpful for the initial test of procedures. It gives teams the time to prepare for the test and allows them to practice their skills. Once the team has had an opportunity to run through the procedures, practice, and coordinate their skills, unannounced testing may be used to test the completeness of the procedures and sharpen the team's abilities. Unannounced testing consists of testing without prior notification. The use of unannounced testing is extremely helpful in preparing a team for disaster preparation because it focuses on the adequacy of in-place procedures and the readiness of the team. Unannounced testing, combined with closely monitored restrictions, will help to create a simulated scenario that might exist in a disaster. This more closely measures the teams' ability to function under the pressure and limitations of a disaster. Once it has been determined whether a test will be announced or unannounced, the actual objective(s) of the test must be determined. There are several different types of tests that are useful for measuring different objectives.

A recommended schedule for testing is as follows:

- Desktop testing on a quarterly basis
- One structured walk-through per year
- One integrated business operations/information systems exercise per year

The DRP Director, and Contingency Plan Team Leaders, together with the SCG President and Vice President of Administration, will determine end-user participation.

Tests that result in components or a system malfunctioning or becoming inoperable could indicate problems in personnel training or in the DRP and procedures. Each system component shall be tested to confirm the accuracy of individual recovery procedures. The test plan shall include a schedule detailing the timeframes for each test and test participants. The test plan shall clearly delineate scope, scenario, and logistics. The scenario chosen may be a worst-case incident or an incident most likely to occur. It should mimic reality as closely as possible.

Training

Training refers to informing personnel of their roles and responsibilities within the SCGSC system plan and teaching them skills related to those roles and responsibilities, thereby preparing them for participation in exercises, tests, and actual emergency situations related to the SCGSC system plan.

The scheduling of training sessions will be coordinated closely with the schedules for CP/DRP tabletop exercises, functional exercises, and DR tests.

Training sessions will emphasize studying and understanding the following documents in preparation for participating in each test or exercise:

- SCGSC CP – Participants will be able to answer questions about the purpose of the plan, system recovery procedures, specific application processes, recovery roles and responsibilities, notification procedures, and all appendices included in the plan.
- SCGSC DRP – Participants will be able to answer questions about the purpose of the plan, system recovery procedures, specific application processes, recovery roles and responsibilities, notification procedures, and all appendices included in the plan.
- FISMA Contingency Plan Computer Controls – Participants will gain knowledge of the Contingency Plan family of security controls (NIST 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems and Organizations*) and how exercising and testing of plans will address deficiencies in compliance with those controls.

Recovery personnel shall be trained on the following plan elements:

- Purpose of the plan
- Cross-team coordination and communication
- Reporting procedures
- Security requirements
- Team-specific processes (Activation and Notification, Recovery, and Reconstitution Phases)
- Individual responsibilities (Activation and Notification, Recovery, and Reconstitution Phases)

The TT&E calendar for the SCGSC system is presented in the following table.

Activity	Frequency
Tests	
Test SCGSC CP notification/activation procedures	**Quarterly**
Test SCGSC CP communications	**Quarterly**
Test Alert, Notification, and Activation Procedures for DRP personnel	**Quarterly**
Test recovery of vital records, critical information systems, services, and data	**Semi-Annually**
Test primary and backup infrastructure systems and services at alternate operating facility	**Annually**
Test continuity facility logistics and physical security capabilities at alternate facility	**Annually**
Document and report testing results	**Annually**
Training	
NIH Security and Privacy classes (Information Security and Privacy Awareness, Information Security Awareness, and Privacy Awareness).	**Annually**
SCGSC CP/DRP Training	**Annually**

The results of training and testing will be documented in reports that describe the training/testing conducted, the date conducted, and the names of the individuals trained/tested.

Appendix G: NIDDK Contacts

NIDDK System Owner: Dana Sheets, Digital Engagement Lead, Office of Communications and Public Liaison (OCPL), NIDDK/NIH, 301-496-7059, sheetsdm@mail.nih.gov

NIDDK Information System Security Officer (ISSO) Contact: Warren Herder, Information System Security Officer, Computer Technology Branch, NIDDK/NIH, 301-443-9292, herderjw@niddk.nih.gov

NIDDK Authorizing Official/Designated Approving Authority Contact (AO/DAA): Chandan Sastry, IT Director and CIO, Computer Technology Branch, NIDDK/NIH, 301-496-9555, sastrych@mail.nih.gov

NIDDK Privacy Officer: Kelly Yager, Management Analyst, Office of Management and Policy Analysis, NIDDK/NIH, 301-594-3056, kelly.yager@nih.gov.

Appendix H: Glossary

Alternate Processing Procedures—Procedures that can be initiated in lieu of the application to maintain business operations during an outage.

Alternate Site—A location, other than the primary location, used to continue operational capabilities during a significant system disruption.

Business Impact Analysis (BIA)—An analysis of an information system's requirements, processes, and interdependencies used to characterize system contingency requirements and priorities in the event of a significant disruption.

Critical Business Process (CBP)—The operational and/or business support functions that could not be interrupted or unavailable for more than a mandated or predetermined timeframe without significantly jeopardizing the organization.

Data—A representation of facts, concepts, or instructions in a formalized manner suitable for communication, interpretation, or processing by humans or by automatic means.

Disruption—An unplanned event that causes an information system to be inoperable for an unacceptable length of time (e.g., minor or extended power outage, extended unavailable network, or equipment or facility damage or destruction).

Disaster Recovery Plan (DRP)—A written plan for recovering one or more information systems at an alternate facility in response to a major hardware or software failure or destruction of facilities.

Hardware—The mechanical, magnetic, electrical, and electronic devices or components of an information system.

Information System (IS)—An assembly of computer hardware, software, or firmware configured to collect, create, communicate, compute, disseminate, process, store, and control data or information. An information system will consist of automated data processing system hardware, operating system and application software, peripheral devices, and associated data communications equipment.

Information Technology Contingency Plan (ITCP)—OMB Circular A-130, Appendix III, requires the development and maintenance of continuity of support plans for general support systems and contingency plans for major applications. Because an IT contingency plan should be developed for each major application and general support system, multiple contingency plans may be maintained within the organization's business continuity plan**.**

Information System Contingency Planning—Information system contingency planning refers to the dynamic development of a coordinated recovery strategy for information systems, operations, and data after a disruption.

Information System Contingency Plan Assessment (ITCPA) Process—The four step process (BIA, IS Services Analysis, Threat Assessment, and Vulnerability Assessment,) that is the precursor for contingency planning.

Maximum Tolerable Downtime (MTD) —The MTD represents the total amount of time leaders/managers are willing to accept for a business process outage or disruption and includes all impact considerations. Determining MTD is important because it could leave continuity planners with imprecise direction on (1) selection of an appropriate recovery method, and (2) the depth of detail which will be required when developing recovery procedures, including their scope and content.

Operating System (OS)—An organized collection of techniques, procedures, programs, or routines for operating an information system, usually supplied by the system hardware vendor.

RTO (Recovery Time Objective)—The maximum amount of time that a system resource can remain unavailable before there is an unacceptable impact on other system resources, supported business processes, and the MTD. Determining the information system resource RTO is important for selecting appropriate technologies that are best suited for meeting the MTD.

System—A generic term used for briefness to mean either a major application or a general support system.

Test—An evaluation tool that uses quantifiable metrics to validate the operability of a system or system component in an operational environment specified in ITCPs and DRPs**.**

Test Plan—A document that outlines the specific steps that will be performed for a particular test, including the required logistical items and expected outcome or response for each step.

User—A person who accesses information systems to use programs or applications in order to perform an organizational task.

Appendix I: Acronyms

AAR	After Action Report
BIA	Business Impact Assessment
CBP	Critical Business Process
CP	Contingency Plan
DR	Disaster Recovery
DRP	Disaster Recovery Plan
IS	Information System
ISCPA	Information System Contingency Planning Assessment
ISP	Internet Service Provider
ISSO	Information System Security Officer
IT	Information Technology
ITCP	Information Technology Contingency Plan
LAN	Local Area Network
MTD	Maximum Tolerable Downtime
NIDDK	National Institute of Diabetes and Digestive and Kidney Diseases
NIST	National Institute of Standards and Technology
OI&T	Office of Information and Technology
OS	Operating System
POC	Point of Contact
RTO	Recovery Time Objective
SA	System Administrator
SCG	The Scientific Consulting Group, Inc.
SCGSC	SCG Secure Cloud
SOP	Standard Operating Procedure
SP	Special Publication
TT&E	Tests, Training, and Exercises
IP	Internet Protocol
UPS	Uninterruptible Power Supply
VM	Virtual Machine