



**The Scientific Consulting Group, Inc.**

# **Contingency Planning Policy and Contingency Plan**

**for the**

## **SCG Secure Cloud System**

***Version 1.6***

***June 13, 2016***

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

## Contingency Planning Policy and Contingency Plan Approval

The Contingency Planning Policy and Contingency Plan must be approved by the SCG President, Information Technology (IT) Director, and Vice President of Administration. If the National Institute of Diabetes and Digestive and Kidney Diseases (NIDDK) deems it necessary, other signatures may be added. The undersigned acknowledge that they have reviewed the SCG Secure Cloud Contingency Planning Policy and Contingency Plan and agree with the information presented in this document. The SCG President and IT Director will review this Contingency Planning Policy and Contingency Plan annually and revise the plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing. Any changes to the Contingency Planning Policy and Contingency Plan will be coordinated with, and approved by, the undersigned or their designated representatives.



Beverly J. Campbell  
President

6/13/16

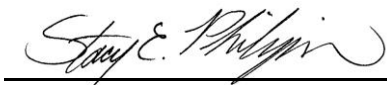
DATE



Chuck C. Lee  
IT Director

6/13/16

DATE



Stacy E. Philipson  
Vice President of Administration

6/13/16

DATE

## Document Information and Revision History

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

Document Revision and History			
Revision	Date	Author	Comments
1.0	1/27/15	K. Martinez	Template for SCG Secure Cloud CP
1.1	2/4/15	B. Campbell/C. Lee	Draft CP for SCG Secure Cloud
1.2	2/17/15	K. Martinez/C. Berry	Minor modifications throughout document
1.3	2/25/15	B. Campbell	Minor changes on p. 6 and 27
1.4	2/26/15	B. Campbell	Minor change on p. 14
1.5	5/19/16	B. Campbell	Edits throughout document
1.6	6/13/16	B. Campbell	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.

## Table of Contents

<b>1. Overview .....</b>	<b>1</b>
1.1 Purpose .....	1
1.2 Exceptions .....	2
1.3 Scope .....	2
1.4 Consequences of Non-Compliance .....	2
1.5 Maintenance .....	2
<b>2. Contingency Planning Policy .....</b>	<b>3</b>
2.1 Contingency Plan .....	3
2.2 Contingency Training and Testing .....	3
2.3 Alternate Storage/Processing Sites .....	4
2.4 Telecommunications.....	5
2.5 Backups and Information System Recovery .....	5
2.6 Audience.....	6
2.7 Responsibilities.....	6
<b>3. Contingency Plan .....</b>	<b>6</b>
3.1 Planning Principles .....	6
3.2 Operational Contingency Status .....	7
3.3 Special Circumstances .....	8
3.4 References/Requirements .....	8
3.5 Concept of Operations.....	9
3.5.1 System Information and Architecture .....	9
3.5.2 Interfaces/Dependencies.....	10
3.5.3 Location of the SCGSC System .....	10
3.5.4 Backups – Data and System .....	10
3.5.5 Line of Succession .....	11
3.5.6 Recovery Responsibilities .....	12
3.6 Notification and Activation Phase .....	13
3.6.1 Overview .....	13
3.6.2 Call Tree.....	13
3.6.3 Damage Assessment .....	14
3.6.4 Access to Damaged Facility .....	15
3.6.5 Salvage and Offsite Storage.....	15
3.7 Recovery Operations.....	16
3.7.1 Recovery Time Objective (RTO) .....	16

3.7.2	Recovery Point Objective (RPO) .....	16
3.7.3	Recovery Procedures .....	16
3.8	Return to Normal Operations.....	16
3.8.1	Original or New Site Restoration .....	17
3.8.2	Concurrent Processing .....	17
3.8.3	Plan Deactivation .....	17
<b>4.</b>	<b>Testing, Training, and Exercise (TT&amp;E).....</b>	<b>17</b>
4.1	Tabletop Testing .....	17
4.2	Technical Testing .....	18
4.3	Contingency Plan Testing Communication Procedures.....	18
<b>5.</b>	<b>Contingency Plan Maintenance .....</b>	<b>18</b>
5.1	Review and Update .....	18
5.2	Distribution/Access List .....	18
	<b>Appendix A: Subordinate Contingency Plan List and NIDDK Contacts.....</b>	<b>20</b>
A.1	NIDDK Contacts .....	20
A.2	Facility DRP Director Contact.....	20
A.3	Facility Disaster Recovery Plans .....	20
	<b>Appendix B: Key Personnel Contact List .....</b>	<b>21</b>
	<b>Appendix C: Vendor Contact List.....</b>	<b>22</b>
	<b>Appendix D: Hierarchical Recovery Team Diagram.....</b>	<b>23</b>
	<b>Appendix E: Vital Records and Instructions for Restoring Operations .....</b>	<b>24</b>
	<b>Appendix F: Recovery Checklist .....</b>	<b>25</b>
	<b>Appendix G: Reconstitution Checklist.....</b>	<b>28</b>
	<b>Appendix H: System Hardware and Software Inventory .....</b>	<b>30</b>
	<b>Appendix I: Acronyms .....</b>	<b>32</b>

## List of Figures

Figure 1.	SCG Secure Cloud System Architecture Diagram.....	11
Figure 2.	SCG Contingency Plan Communication Call Tree.....	19

## List of Tables

Table 1. Line of Succession .....	11
Table 2. Call Tree Activation .....	14

## 1. Overview

### 1.1 Purpose

This document represents the Contingency Planning Policy and Contingency Plan for the SCG Secure Cloud (SCGSC) system. Its purpose is to define the Contingency Planning Policy and the Contingency Plan for the SCGSC. Its purpose is to provide the policy to define the contingency planning requirements and mechanisms to be implemented as well as define the information technology (IT) recovery information and procedures to recover the SCG Secure Cloud system following a disruption. The contingency planning policy and It is essential the policy, information, procedures, and action plans in this document remain viable and be maintained in a state of currency to ensure the accuracy of their contents. Every individual who has a role and/or responsibility for any of the information or materials discussed in this document is responsible for ensuring the information is correct and current. The designated SCG team leader, program manager, or system manager, in coordination with the IT Director, has the responsibility for updating this document in accordance with the documented Plan change management procedures.

The following objectives have been established for the Contingency Plan:

- Maximize the effectiveness of contingency operations through an established plan that consists of the following phases:
  - **Notification/Activation Phase** – to detect and assess damage and to activate the plan.
  - **Recovery Phase** – to restore temporary IT operations and repair damage to the original system.
  - **Reconstitution Phase** – to restore IT system processing capabilities to normal operations.
- Identify activities, resources, and procedures needed to carry out SCG Secure Cloud processing requirements during prolonged interruptions to normal operations.
- Assign responsibilities to designated SCG personnel and provide guidance for recovering SCG Secure Cloud during prolonged periods of interruption to normal operations.
- Ensure coordination with other SCG staff who will participate in the contingency planning strategies, and with external points of contact and vendors who will participate in the contingency planning strategies.

This SCGSecureCloud Contingency Planning Policy and Contingency Plan has been developed as required under the Office of Management and Budget (OMB) Circular A-130, Management of Federal Information Resources, Appendix III, November 2000.

This SCGSC Contingency Planning Policy and Contingency Plan is promulgated under the legislative requirements set forth in the Federal Information Security Management

Act (FISMA) of 2002 and the guidelines established by the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-34, titled "Contingency Planning Guide for Information Technology Systems," dated June 2002. The contingency planning policy and contingency plan have been developed in accordance with compliance requirements.

## **1.2 Exceptions**

Exceptions to the Contingency Planning Policy must be formally documented with a valid business justification and submitted to the Contingency Planning Team for review. All requests will have their potential business and security risks, identified, analyzed, and determined to be either acceptable or unacceptable. When the Contingency Planning Team determines the risks are acceptable, the Contingency Planning Team may approve the request and document the exception in an appendix to this document.

## **1.3 Scope**

This policy and plan applies to the SCG Secure Cloud environment.

## **1.4 Consequences of Non-Compliance**

Subject to applicable laws and regulations, all applicable entities found in violation of this policy are subject to further actions/discussions by SCG's Human Resources Department.

## **1.5 Maintenance**

The SCG President and IT Director are responsible for updating this policy and all supporting documents, procedures, standards, and guidelines at least annually and after any significant change to the SCGSC, including:

- Policy or rules change
- Approver or policy owner leaves the company or changes roles
- Significant change to the definitions
- Introduction of new systems/hardware
- Identification and remediation of security vulnerabilities
- Regulatory changes
- Changes to the risk profile

The change management process and weekly team meetings should be monitored to identify significant changes that would require a policy update.

Updating and maintaining the Contingency Planning and Contingency Plan document will be the responsibility of the Contingency Management Team, led by SCG's President.

The responsible party for this document is listed in the Responsibilities section.



## 2. Contingency Planning Policy

The following Contingency Planning requirements, mechanisms, and provisions are to be applied within the SCG Secure Cloud system:

### 2.1 Contingency Plan

- A formal contingency plan must be developed for the SCGSC system. The contingency plan must:
  - Identify the essential missions and business functions and associated contingency requirements;
  - Provide recovery objectives, restoration priorities, and metrics;
  - Address contingency roles, responsibilities, and assigned individuals with contact information;
  - Address maintaining essential missions and business functions despite an information system disruption, compromise, or failure;
  - Address eventual, full information system restoration without deterioration of the security measures originally planned and implemented; and
  - Be reviewed and approved by the SCG President, IT Director, and Vice President of Administration. **(CP-2.1)**
- The IT Director must distribute copies of the contingency plan to key personnel and organizational elements, including FISMA personnel. **(CP-2.1)**
- A process to coordinate contingency planning activities with incident handling activities must be established. **(CP-2.1)**
- The SCG President and IT Director must review the contingency plan for the SCGSC at least annually and revise the contingency plan to address any changes to the SCGSC, its information system, or environment of operation and problems encountered during contingency plan implementation, execution, or testing. **(CP-2.1)**
- Changes to the contingency plan must be communicated to key personnel and organizational elements, including FISMA personnel. **(CP-2.1)**
- As part of the contingency planning process, the Contingency Planning Team must coordinate the information system's contingency plan development with organizational elements responsible for related plans. **(CP-2.1.1)**
- The contingency plan must conduct capacity planning in order for information processing, telecommunications, and environmental support exists during contingency operations. **(CP-2.2.1)**

### 2.2 Contingency Training and Testing

- The IT Director must train key personnel of contingency roles and responsibilities for the information system. Training must be conducted at least annually for refresh purposes. **(CP-3.1)**

- The Contingency Plan for the SCGSC system must be tested or exercised on an annual basis through functional exercises. **(CP-4.1)**
- It is the responsibility of the IT Director to develop test plans that align with NIST SP 800-34 and to provide those plans to FISMA personnel prior to initiating the test for review and approval. **(CP-4.1)**
- The IT Director must review the Contingency Plan test/exercise results and initiate any corrective actions. **(CP-4.1)**
- Contingency plan testing or exercises must be coordinated with organizational elements responsible for related plans. **(CP-4.1.1)**

## **2.3 Alternate Storage/Processing Sites**

- An alternate site must be established, including necessary agreements to permit the storage and recovery information system backup information. The current alternate site location is at SCG's facility in Frederick, Maryland. **(CP-6.1)**
- The current alternate site must be separated from the primary site to prevent susceptibility of the same hazards. **(CP-6.1.1)**
- A process to identify potential accessibility problems to the alternate site must be established in the event of an area-wide disruption or disaster. Explicit mitigation actions must be defined to those potential accessibility problems. **(CP-6.3.1)**
- An alternate processing site must be established, including necessary agreements to permit the resumption of information system operations for essential mission and business functions within defined time periods when primary processing capabilities become unavailable. The current alternate processing site location is SCG's facility in Frederick, Maryland. **(CP-7.1)**
- It is the responsibility of the IT Director to develop a Contingency Plan that is consistent with the recovery time objectives and business impact analysis for submission to the Contingency Planning Team for review and approval. **(CP-7.1)**
- A process to ensure that equipment and supplies required for the resumption of operations at the alternate processing site (or contracts to support delivery to the site that support the time period for the resumption of business operations) must be in place. **(CP-7.1)**
- The current alternate processing site must be separated from the primary processing site to prevent susceptibility of the same hazards. **(CP-7.1.1)**
- A process to identify potential accessibility problems to the alternate processing site must be established in the event of an area-wide disruption or disaster. Explicit mitigation actions must be defined to those potential accessibility problems. **(CP-7.2.1)**
- Priority-of-service provisions must be developed within alternate processing site agreements. **(CP-7.3.1)**

- Alternate processing sites must include security measures that are equivalent to the primary processing site. **(CP-7.5.1)**

## **2.4 Telecommunications**

- Alternate telecommunication services must be established to permit the resumption of information system operations for essential mission and business functions when the primary telecommunications capabilities become unavailable. A time period for alternate telecommunication services must be defined, documented, and reviewed by the Contingency Planning Team. **(CP-8.1)**
- Priority-of-service provisions must be established for primary and alternate telecommunications service agreements. **(CP-8.1.1)**
- A process to request Telecommunications Service Priority for all telecommunications services used for national security emergency preparedness in the event that the primary or alternate telecommunication services are provided by a common carrier. **(CP-8.1.1)**
- SCG must obtain alternate telecommunication services that reduce the likelihood for the sharing of a single point of failure with primary telecommunication services. **(CP-8.2.1)**

## **2.5 Backups and Information System Recovery**

- Mechanisms must be in place to conduct backups of user-level information, system-level information, and information system documentation. **(CP-9.1)**
- Backups are to be done in daily differential and at least weekly for full backups. **(CP-9.1)**
- At least three (3) backups must be maintained, with at least one backup copy available at the primary site, the alternate site, and a third site. **(CP-9.1)**
- Backup storage capabilities must be defined. It is the responsibility of the IT Director to provide the backup storage capabilities to the Contingency Planning Team for review and approval. **(CP-9.1)**
- All backup information must be protected at the defined storage locations in order to preserve confidentiality and integrity. **(CP-9.1)**
- Backup information is to be tested on an annual basis in order to verify its reliability and integrity. **(CP-9.1.1)**
- Backup copies relating to the operating system, other critical information system software, and copies of the information system inventory (including hardware, software, and firmware components) must be stored in a separate facility or in a fire-rated container that is not co-located with the operational SCGSC system. **(CP-9.3.1)**
- Mechanisms and processes must be in place to recover and reconstitute the SCGSC to a known state following a disruption, compromise, or failure. **(CP-10.1)**

- For systems that are transaction-based, mechanisms must be in place to for transaction recovery. **(CP-10.2.1)**
- Any circumstances that could inhibit recovery and reconstitution for the information system to a known state must be identified and documented. **(CP-10.3.1)**

## 2.6 Audience

SCG employees who have responsibility for managing and maintaining the SCGSC system.

## 2.7 Responsibilities

The following table identifies who within SCG is responsible for developing, implementing, and approving the contingency planning policy. The following definitions apply:

- **Responsible Parties** – the persons responsible for the identified responsibilities.
- **Responsibilities** – the tasks performed by the responsible parties
- **Approver** – the person(s) required to approve the final policy implementation or amendment.

Policy	Responsible Parties	Responsibilities	Approver
Contingency Planning Policy	IT Director, Program Manager, System Owner, and ISSO	Support and approve the policy	SCG President, IT Director, and Vice President of Administration
	Contingency Planning Team	Develop, implement, and maintain the policy at least annually	SCG President, IT Director, and Vice President of Administration
	IT Director	Enforces the policy and communicates any changes	SCG President
	SCG Employees	Acknowledge and comply with policy	IT Director and Program Manager

## 3. Contingency Plan

### 3.1 Planning Principles

Planning principles are based on the Federal Information Processing Standard Publication (FIPS Pub) 199, *Standards for Security Categorization of Federal Information and Information Systems* security categorization (High, Moderate, or Low impact) of the system the SCGSC Contingency Plan represents.

For Low impact systems, the applicability of the Contingency Plan is predicated on the following key principles:

- The SCGSC is inoperable and must be within the recovery time objective of 48 hours.
- Key personnel have been identified and trained in their emergency response and recovery roles; they are available to activate the SCGSC Contingency Plan.

For Moderate and High impact systems, the applicability of the Contingency Plan is predicated on the following key principles:

- The system's primary processing facility in Gaithersburg, Maryland, is inaccessible; therefore, SCG is unable to perform SCGSC processing for the National Institute of Diabetes and Digestive and Kidney Diseases (NIDDK).
- Key personnel have been identified and trained in their emergency response and recovery roles; they are available to activate the SCGSC Contingency Plan.
- SCG's Frederick, Maryland, facility is designated as the SCGSC alternate operating facility.
- SCG will use the alternate site building and IT resources to recover SCGSC functionality during an emergency situation that prevents access to the Gaithersburg facility, until the return to normal operations.
- The designated computer system at the alternate site has been configured to begin processing SCGSC information according to its recovery time objective (RTO).

### **3.2 Operational Contingency Status**

- Preventive controls (e.g., generators, environmental controls, waterproof tarps, sprinkler systems, fire extinguishers, and fire department assistance) are fully operational at the time of the disaster.
- Computer center equipment, including supporting components, are connected to an uninterruptible power supply (UPS) that provides an alternative source of electricity during a power failure for a limited timeframe.
- Current backups of the application software and data are intact and available at the Frederick facility as well as at another secure offsite location.
- The equipment, connections, and capabilities required to operate are available at the alternate site.
- Service agreements are maintained with hardware, software, and communications providers to support the emergency system recovery.

The SCGSC Contingency Plan does not apply to the following situations:

- Overall recovery and continuity of business operations.
- Emergency evacuation of personnel.

### 3.3 Special Circumstances

There are special circumstances that can result in the system being left in an unknown state. An unknown state is one where it is questionable whether the system is functioning correctly, whether the data in the system are accurate and/or correct, or whether the data in the system are traceable back to a known backup. These special circumstances are not things that can be planned, but care can be taken to minimize their effect or minimize the probability of their occurrence.

Examples of special circumstances include: backup tape corruption, incomplete backups, corrupt or improperly patched/updated operating system, database corruption, network/Domain Name System (DNS) error, or unavailable system administrators. There may be other conditions, but these are the more common causes of the system to be in an unknown state. Even with the best planning, any of these events can wreak havoc and cause additional system downtime. Actions used to compensate for the above listed conditions include:

- Routinely replacing backup tapes with new ones.
- Routinely and thoroughly testing backup tapes.
- Ensuring all parties are aware of any special operating system requirements for the system.
- Documenting and testing installation instructions, operating procedures, special precautions, and special handling instructions.
- Documenting and functionally testing contingency plans.
- Ensuring there is always more than one trained administrator for the system.

### 3.4 References/Requirements

This plan complies with the following Federal and Departmental policies:

- Federal Continuity Directive 1 (FCD 1), *Federal Executive Branch National Continuity Program and Requirements*, February 2008
- Federal Information Security Management Act (FISMA), P.L. 107-347, Title III, December 2002
- Homeland Security Presidential Directive (HSPD) 7, *Critical Infrastructure Identification, Prioritization, and Protection*, December 17, 2003
- National Institute of Standards and Technology (NIST) Special Publication (SP) 800-34 (Revision 1), *Contingency Planning Guide for Federal Information Systems*, May 2010
- NIST SP 800-53 (Revision 3), *Recommended Security Controls for Federal Information Systems*, August 2009 (Errata as of May 1, 2010)

- Office of Management and Budget (OMB), Circular A-130, Appendix III, Transmittal Memorandum #4, *Management of Federal Information Resources*, November 2000
- HHS requirement: The organization shall develop a contingency planning capability to meet the needs of critical supporting operations in the event of a disruption extending beyond 48 hours. The procedures for execution of such a capability shall be documented in a formal contingency plan and shall be reviewed at least once every year and updated as necessary. Personnel responsible for target systems shall be trained to execute contingency procedures. The plan, recovery capabilities, and personnel shall be tested to identify weaknesses of the capability at least annually.

### **3.5 Concept of Operations**

#### *3.5.1 System Information and Architecture*

The SCGSC system supports the development and communication of health information that improves public health and quality of life. It was created to support the 3-year contract awarded to SCG to provide Support for National Information Clearinghouses and Campaign-Focused Programs for the NIDDK Office of Communications and Public Liaison, in Bethesda, Maryland. This contract enables NIDDK to ensure that the science-based knowledge gained from NIDDK-funded research is imparted to NIDDK target audiences, including health care providers and the public for the direct benefit of patients and their families.

The main Statement of Work areas for this contract are:

- Support for the Information Requests for NIDDK Clearinghouses and Several Campaign-Focused Programs and Exhibit Support;
- Support for Content Development and Maintenance for Multiple Health Information Products; Support for Printing, Print on Demand Services;
- Support for Materials Receipt, Storage, and Dissemination, Integrated Tracking System;
- Support Services for NIDDK's Digital Channels Including Website Development and Website Usability Testing;
- Campaign Support for numerous NIDDK Health Campaigns including: NKDEP, Weight-Control Information Network's Sisters Together Campaign, Celiac Disease Awareness and Bowel Control Awareness Campaigns, and NDEP; Conference/Exhibit Logistics and Meeting Support;
- Market Research and Evaluation Services for OCPL Programs; and
- Message Promotion Services.

NIDDK supports a wide range of medical research through grants to universities and other medical research institutions across the country. The Institute also supports government scientists who conduct basic, translational, and clinical research across a broad spectrum of topics and serious, chronic diseases and conditions related to the

Institute's mission. In addition, the NIDDK supports research training for students and scientists at various stages of their careers and a range of education and outreach programs to bring science-based information to patients and their families, health care professionals, and the public.

The SCGSC system is housed in a secure office building in Gaithersburg, Maryland. SCG has the entire second floor of the building as well as a suite on the seventh floor. The SCGSC system is located in SCG's suite on the seventh floor. There is controlled access to SCG's offices and the server is located in a locked room with fob-controlled electronic security that logs the name, date, and time when an individual enters the room.

The SCGSC system has two host servers consisting of two HP ProLiant DL360 Gen9 – Xeon E5-2620V3 2.4 GHz, 80 GB RAM, 900 GB HD, RAID 5 running VMWare VSphere ESXi 6.0 update 2. Within this host environment, the system is running four virtual machines: VM 1 (SCSQL-PROD), VM 2 (SCCOLDSHARE-PROD), VM 3 (3PL), and VM 4 (SCFSMO). The operating system for all VMs is Windows 2008 R2 Enterprise (x64). VM 1 has SQL Server 2012 Standard (x64), a local DNS Server. VM 2 has Coldfusion 9 and SharePoint Foundation 2010. VM 3 has Microsoft Dynamics NAV CRM. VM 4 has Active Directory and a local DNS server. All VMs are running Symantec Protection Suite Enterprise 2015. SCGSC has four switches—Cisco 2960 Manageable Switch, Netgear FS524S Unmanaged Switch, Netgear GS108 Unmanaged Switch, and Cisco SG110D-08 Unmanaged Switch. There is one firewall—Cisco ASA 5512-X and backups are conducted externally from the SCG corporate network using the Tandberg StorageLoader LTO-6 Tape Autoloader with LTO Ultrium and SAS-2 running BackupExec 2015 Enterprise. There is an additional tape backup device in Frederick (Tandberg StorageLoader LTO-4 Tape Autoloader with LTO Ultrium and SAS-2 running BackupExec 2015 Enterprise). The external IP address for VM 2 is 206.130.148.40. The SCGSC architecture diagram is presented in Figure 1.

All users are required to be authenticated with user ID and password before access is granted to the system. Additionally, up-to-date antivirus software is installed on each user's desktop and laptop computer.

### *3.5.2 Interfaces/Dependencies*

There are no system interfaces/dependencies identified for the SCGSC system.

### *3.5.3 Location of the SCGSC System*

The SCGSC system is located in a locked, access controlled room within SCG's offices located on the 7<sup>th</sup> floor at 656 Quince Orchard Road, Gaithersburg, Maryland.

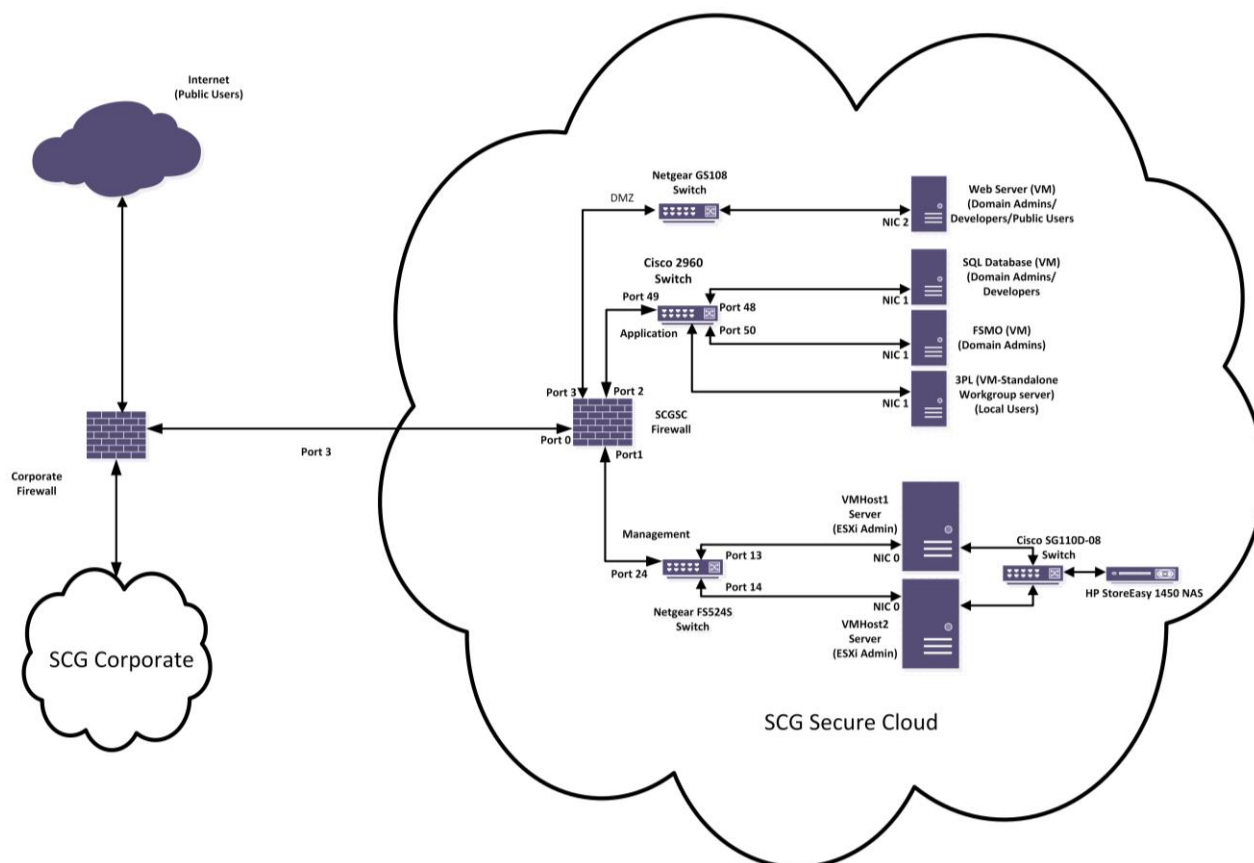
### *3.5.4 Backups – Data and System*

The SCGSC is automatically backed up externally from the corporate network in Gaithersburg on a daily basis using the Tandberg StorageLoader LTO-6 Tape Autoloader, LTO Ultrium - SAS-2 running BackupExec 2015 Enterprise and in Frederick using the Tandberg StorageLoader LTO-4 Tape Autoloader, LTO Ultrium - SAS-2 running BackupExec 2015 Enterprise. Data and system backups occur daily. Backup



tapes are archived weekly and monthly in both locations, and monthly backup tapes are retained indefinitely. Tape backups are stored in a locked fire safe in the IT Director's office at the Gaithersburg facility and in a locked firesafe at the Frederick facility. In addition, monthly duplicate backup tapes are stored in Staunton, Virginia, as specified in the SCGSC System Security Plan (SSP).

**Figure 1. SCG Secure Cloud System Architecture Diagram**



### 3.5.5 Line of Succession

SCG sets forth an order of succession to ensure decision-making authority for the SCGSC Contingency Plan is uninterrupted. The IT Director is responsible for ensuring the safety of IT personnel and the execution of procedures documented within this plan. If the IT Director is unable to function as the overall authority or chooses to delegate this responsibility to a successor, the successor shall function as that authority. The Line of Succession is shown in Table 1.

**Table 1. Line of Succession**

Name	Title	Role	Responsibility
Chuck Lee	IT Director	Leadership role and overall responsibility for SCGSC continuity/recovery	Executing procedures documented in the CP

Name	Title	Role	Responsibility
Ric Blackman	Web Development Director	Successor leadership role and overall responsibility for SCGSC continuity/recovery	Executing procedures documented in the CP
Kenny Ying Lee	IT Systems Specialist	Successor leadership role and overall responsibility for SCGSC continuity/recovery	Executing procedures documented in the CP
John Bernheimer	IT Systems Specialist	Successor leadership role and overall responsibility for SCGSC continuity/recovery	Executing procedures documented in the CP

### 3.5.6 Recovery Responsibilities

The following three teams are involved in contingency planning and contingency operations:

- The **Contingency Planning Team** is responsible for the overall planning for unexpected events. This team positions SCG to prepare for, detect, react to, and recover from events that threaten the security of information resources and assets, such as the SCGSC system. The team is responsible for preparing, reviewing, and updating the Incident Response Plan, the Disaster Recovery Plan, the Contingency Plan, and the Business Continuity Plan. The SCG President directs the Contingency Planning Team.
- The **Incident/Disaster Recovery Team** is responsible for leading recovery from an incident or disaster. In the event of an incident or disaster, this team will restore the SCGSC computer environment and all applications. Members of the team include personnel who also are responsible for the daily operations and maintenance of the system. SCG's IT Director is responsible for leading the Incident/Disaster Recovery Team.
- The **Business Continuity Plan Team** ensures that critical business functions can continue if a disaster occurs. This team facilitates the establishment of operations at an alternate site until SCG is able to either resume operations at its primary site or select a new primary location. The Vice President of Administration directs the Business Continuity Plan Team for SCG and the Program Manager for the NIDDK contract coordinates restoration of the SCGSC system with NIDDK.

The names of the team members and the team leaders are listed in Appendix B: Key Personnel Contact List.

A hierarchical Recovery Team Diagram is depicted in Appendix D. This diagram shows the team names and leaders.

The responsibilities for each team were identified above. The teams are aware of their responsibilities and have been trained to respond to a contingency event affecting the SCGSC system.

## 3.6 Notification and Activation Phase

### 3.6.1 Overview

The Notification and Activation Phase addresses the initial actions taken to detect and assess damage inflicted by a disruption to the SCGSC system. Based on the assessment of the damage, the Contingency Plan may be activated by the SCG President, Vice President of Administration, IT Director, or Web Development Director.

**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.*

Contact information for key personnel is located in Appendix B: Key Personnel Contact List. The notification sequence is listed below:

- If the Contingency Plan is to be activated, the SCG President notifies the Vice President of Administration. The Vice President of Administration then notifies all Team Leaders and informs them of the details of the event and if relocation is required.
- Upon notification from the Vice President of Administration, Team Leaders are to notify their respective teams. Team members are to be informed of all applicable information and prepared to respond and relocate if necessary.
- The IT Director is to notify the alternate site that a contingency event has been declared and to 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.

This plan will be executed if any of the following conditions exist:

- The system is inoperable for more than 48 hours.
- The space where the system is located is damaged and will not be available for more than 48 hours.

### 3.6.2 Call Tree

Call down exercises are a part of SCG's emergency planning and the SCGSC system Contingency Plan is designed to be exercised in nearly the same fashion. The significant difference is the purpose—the Contingency Plan is designed to mitigate IT disasters, which may or may not be part of a larger event, thus the scope of the Contingency Plan focuses on IT assets and personnel needed for SCG to recover and accomplish its mission.

A call tree is a commonly used notification method when information must be communicated to a group of people in a relatively short time. 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, the individuals in Table 2 will be contacted in the order identified. 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 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 that were not reached. Each of the individuals listed in the call tree have mobile phones to facilitate contact with key personnel after regular business hours.

**Table 2. Call Tree Activation**

Title	Name	Contact Information	Emergency Role
IT Director	Chuck Lee	301-670-4990 (W) 301-366-3273 (C) 301-637-4355 (H)	Damage Assessment, Incident/Disaster Recovery Team Leader
SCG President	Beverly Campbell	301-670-4990 (W) 301-461-1109 (C) 540-887-9829 (H)	Damage Assessment, CP Activation Decision, and Business Continuity Plan Team Leader
Vice President of Administration	Stacy Philipson	301-670-4990 (W) 301-742-5954 (C) 301-363-5707 (H)	SCG Facilities Management, Damage Assessment, Incident Response/ Disaster Recovery Team Member
Program Manager	Susie Warner	301-670-4990 (W) 301-366-3217 (C) 301-355-4388 (H)	SCGSC Contract Management, Incident Response/Disaster Recovery Team Member
IT Systems Specialist	Kenny Ying Lee	301-670-4990 (W) 315-956-7796 (C)	Incident Response/Disaster Recovery Team Member
IT Systems Specialist	John Bernheimer	301-670-4990 (W) 410-428-1330 (C)	Incident Response/Disaster Recovery Team Member
Web Development Director	Ric Blackman	301-670-4990 (W) 301-529-0760 (C)	Applications and Web Development, Incident Response/Disaster Recovery Team Member
Information Center Manager	Justin Gray	301-670-4990 (W) 301-524-2986 (C) jgray@scgcorp.com	Incident Response/Disaster Recovery Team Member Frederick Facility POC
Office Manager	April Randolph	301-670-4990 (W) 240-848-6803 (C) arandolph@scgcorp.com	Incident Response/Disaster Recovery Call Tree Non-Essential Staff Notification

### 3.6.3 Damage Assessment

When emergencies or disasters occur even the best protective measures may not prevent damage to a system. Damage assessment activities will be performed by the Incident/Disaster Recovery Team. Cleaning, salvaging, and disposal of equipment and media will be performed per standard operating procedures (SOPs) to ensure protection of sensitive information.

#### *3.6.4 Access to Damaged Facility*

Access to a damaged facility can be a risky operation and should be carefully planned and executed. That is beyond the scope of this Contingency Planning Policy and Contingency Plan, but should be planned out and governed by the facility disaster recovery plan. It is understood that any access to a damaged facility to ascertain the specific damage to the SCGSC system will be at the discretion and support of the building owner and management company, SCG President, and Vice President of Administration. The facilities that house the SCGSC system are leased by SCG and located in Gaithersburg, Maryland. The SCG President or Vice President of Administration will notify the Incident/Disaster Recovery Team when the damaged building is safe to enter.

If the physical facilities in Gaithersburg are intact and safe to enter, the Incident/Disaster Response Team should begin the restoration of systems and data to work toward full operational capability. If the Gaithersburg facility is unsafe, destroyed, or will be unavailable for an extended period of time, actions must be taken to restore the functionality of the SCGSC at the alternate site in Frederick, Maryland.

The contact information for the specific recovery team leaders is provided in Appendix B.

#### *3.6.5 Salvage and Offsite Storage*

The salvage activity is managed by the Incident/Disaster Recovery Team. Retrieval and transport of items from the disaster site will be performed per SOPs noted in the vital record referenced in Appendix E.

The Incident/Disaster Recovery Team should begin documentation as assessment and recovery operations begin. This will facilitate preparation of the disaster recovery report detailing what happened, how it happened, what response was taken, the results of the response, and the casualty report of damage to records. A camera, notebook, and pen should be available. Notes should be made and photographs should be taken to show the conditions of the building and damaged equipment and records, and the procedures followed in recovery. All resources used to cope with the disaster, including personnel, materials, time, and expenses, should be documented.

The Incident/Disaster Recovery Team should assess the situation to determine the most appropriate initial course of action for salvage operations. Each situation will present unique specifics that must be considered in selecting the order. Any equipment that can be cleaned and salvaged will be the top priority. For equipment that is only slightly damaged or damp, fan-drying or air-drying on site may be suitable. Any equipment too damaged to be salvaged will be destroyed in accordance with SCG's SOPs to ensure protection of sensitive information.

Backup hardware and software are stored at SCG's Frederick facility, along with tape backups of the SCGSC system. The Frederick facility is located at 7315A Grove Road, Frederick, Maryland, 21703. This would be the alternate site for restoring the SCGSC system should the Gaithersburg facility be damaged and closed to SCG staff.

### **3.7 Recovery Operations**

#### **3.7.1 Recovery Time Objective (RTO)**

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

RTO defines the maximum amount of time that a system resource can remain unavailable before there is an unacceptable impact on other system resources, supported mission/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. When it is not feasible to immediately meet the RTO and the MTD is inflexible, a Plan of Actions & Milestones (POA&M) should be initiated to document the situation and plan for its mitigation. The amount of time elapsed from the time of a disaster until the system is once again in operation is defined as the RTO. These times are determined by the NIDDK. For the purpose of this plan, the system's, RTO is 14 calendar days.

#### **3.7.2 Recovery Point Objective (RPO)**

The Recovery Point Objective (RPO) represents the point in time, prior to a disruption or system outage, to which mission/business process data can be recovered (given the most recent backup copy of the data) after an outage. Unlike RTO, RPO is not considered as part of MTD. Rather, it is a factor of how much data loss the mission/business process can tolerate during the recovery process. For this system, the RPO is 1 calendar day. The system can be restored from the daily backup tape should a disaster require restoration of the system in Gaithersburg or at the alternate site in Frederick.

#### **3.7.3 Recovery Procedures**

The checklist should assume the people are already at the alternate processing site. At a minimum, the Incident/Disaster Recovery Team members should check off each step in the recovery as it is completed and the Team leader should update the SCG President and Vice President of Administration on a previously agreed timeframe (hourly, every 2 hours, etc.). It may be advantageous to have the recovery procedures created as a checklist, where the person(s) executing the recovery can check off each step and sign the checklist after the recovery is completed.

### **3.8 Return to Normal Operations**

Return to normal operations (reconstitution phase) means recovery activities are terminated and normal operations are transferred back to the primary facility, original or new. Once the original or new site is restored to the level that it can support the SCGSC system and its normal processes, the system may be transitioned back to the original or to the new site. This determination is made by the IT Director in consultation with the

Vice President of Administration, who will coordinate the transition with the Program Manager and project staff. The reconstitution procedures in Appendix G provide sufficient detail to transition the SCGSC system from the Frederick facility to the original or new SCG facility in Gaithersburg. These coordinated procedures detail how the transition will take place, and they are attached to this plan (Appendix G).

*The goal is to provide a seamless transition of operations from the alternate site to SCG's original or new facility in Gaithersburg, Maryland.*

### *3.8.1 Original or New Site Restoration*

The Incident/Disaster Recovery Team will follow procedures to restore or replace the original site so normal operations may be transferred. IT equipment and telecommunications connections must be tested.

### *3.8.2 Concurrent Processing*

SCG will operate the SCGSC system at the Frederick facility in coordination with the system at the original or new site in Gaithersburg to allow for adequate testing. These procedures should include testing the original or new system until it is functioning properly and the contingency system is shut down smoothly and efficiently.

### *3.8.3 Plan Deactivation*

The Reconstitution Checklist identifies the procedures and tasks the Team needs to complete to clean the alternate site of any equipment or other materials belonging to the SCGSC system, with a focus on handling sensitive information. Because SCG maintains the Frederick facility for the NIDDK call center and publications warehouse, the equipment will remain at the Frederick site but all sensitive information will be removed to prevent unauthorized access. Any items that need to be transferred to the Gaithersburg facility should be properly packaged, labeled, and transported to the original or new location in Gaithersburg. Team members should be instructed to return to work at the original or a new site.

## **4. Testing, Training, and Exercise (TT&E)**

The Business Owner and IT Director shall establish criteria for validation/testing of a Contingency Plan and an annual test schedule, and ensure implementation of the testing. This process also will serve as training for personnel involved in the plan's execution. At a minimum the Contingency Plan shall be tested annually (within 365 days). The types of validation/testing exercises include tabletop and technical testing. Contingency Plans for all application systems must be tested at a minimum using the tabletop testing process. However, if the application system Contingency Plan is included in the technical testing of its respective support systems that technical test will satisfy the annual requirement.

### **4.1 Tabletop Testing**

Tabletop testing should be conducted in accordance with the Center for Medicaid & Medicare Services (CMS) Contingency Planning Tabletop Test Procedures. The primary

objective of the tabletop test is to ensure designated personnel are knowledgeable and capable of performing the notification/activation requirements and procedures as outlined in the Contingency Plan, in a timely manner. The exercises include, but are not limited to:

- Testing to validate the ability to respond to a crisis in a coordinated, timely, and effective manner, by simulating the occurrence of a specific crisis; and
- Crisis communications and call tree verification.

## **4.2 Technical Testing**

The primary objective of the technical test is to ensure the communication processes and data storage and recovery processes can function at an alternate site to perform the functions and capabilities of the system within the designated requirements. Technical testing shall include, but is not limited to:

- Process from backup system at the alternate site;
- Restore system using backups (backups will be tested monthly); and
- Data telecommunications to alternate processing site.

## **4.3 Contingency Plan Testing Communication Procedures**

The IT Director notifies the SCG President or the Vice President of Administration that there is an event and the IT Contingency Plan call tree needs to be activated. The SO will initiate the call tree; the call tree exercise will be concluded when the SO or Vice President of Administration has been contacted by the last person in the call tree. If the next person in the tree cannot be contacted, the last person contacted will contact the SO and explain what happened. This will conclude the exercise. The SCG Contingency Plan communication call tree is depicted in Figure 2.

# **5. Contingency Plan Maintenance**

## **5.1 Review and Update**

The Contingency Planning Team will review the Contingency Plan at least once a year and revise the plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing.

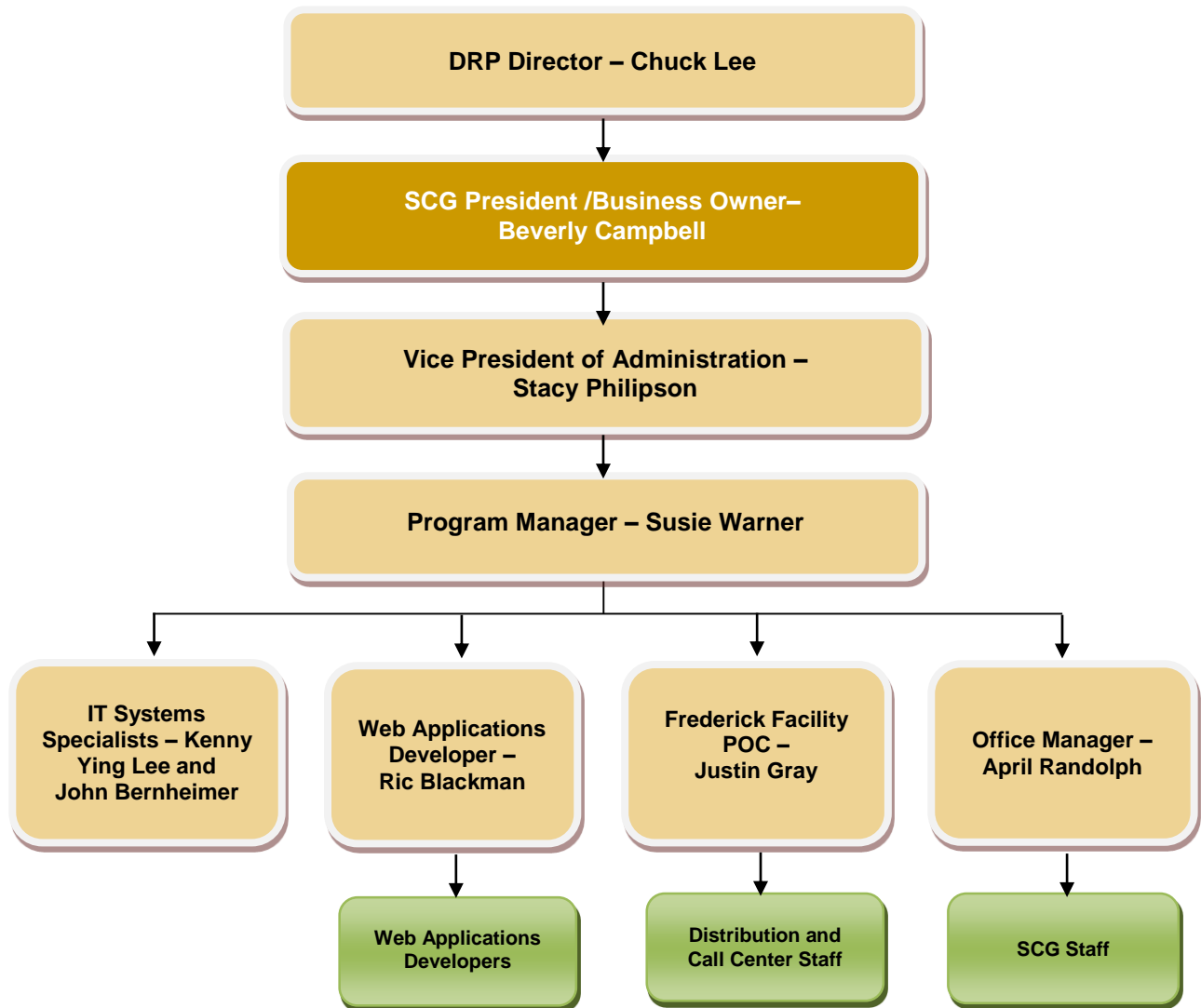
## **5.2 Distribution/Access List**

The SCGSC system Contingency Planning Policy and Contingency Plan is accessible in a read-only version to all SCG staff on the SCG Intranet. The electronic file of the Contingency Planning Policy and Contingency Plan and backup are maintained by the IT Director. The Contingency Planning Policy and Contingency Plan is distributed to each member of the Incident/Disaster Recovery Team, SCG managers, and other key personnel responsible for contingency planning, incident response, and disaster recovery. The Contingency Planning Policy and Contingency Plan also will be distributed to the NIDDK as requested.



The IT Director maintains a current copy of production contingency documents on a shared drive, as well as updates that are in progress.

**Figure 2. SCG Contingency Plan Communication Call Tree**



## **Appendix A: Subordinate Contingency Plan List and NIDDK Contacts**

### **A.1 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](mailto:sheetsdm@mail.nih.gov)

NIDDK Information Systems Security Officer (ISSO) Contact: Warren Herder, Information System Security Officer, Computer Technology Branch, NIDDK/NIH, 301-443-9292, [herderjw@nid.dk.nih.gov](mailto:herderjw@nid.dk.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](mailto: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](mailto:kelly.yager@nih.gov).

### **A.2 Facility DRP Director Contact**

SCG Facility DRP Director Contact: Chuck Lee, IT Director, 301-670-4990 (W), 301-366-3273 (C), [cleec@scgcorp.com](mailto:cleec@scgcorp.com)

### **A.3 Facility Disaster Recovery Plans**

The following disaster recovery plan is related to this Contingency Plan:

*Disaster Recovery Plan for the SCG Secure Cloud System*

## Appendix B: Key Personnel Contact List

This appendix contains a list of key personnel at SCG responsible for the SCGSC, and their contact information, who should be contacted in the event of an incident or disaster. If the emergency occurs outside of regular business hours, contact the mobile (C) phone number before trying the home number.

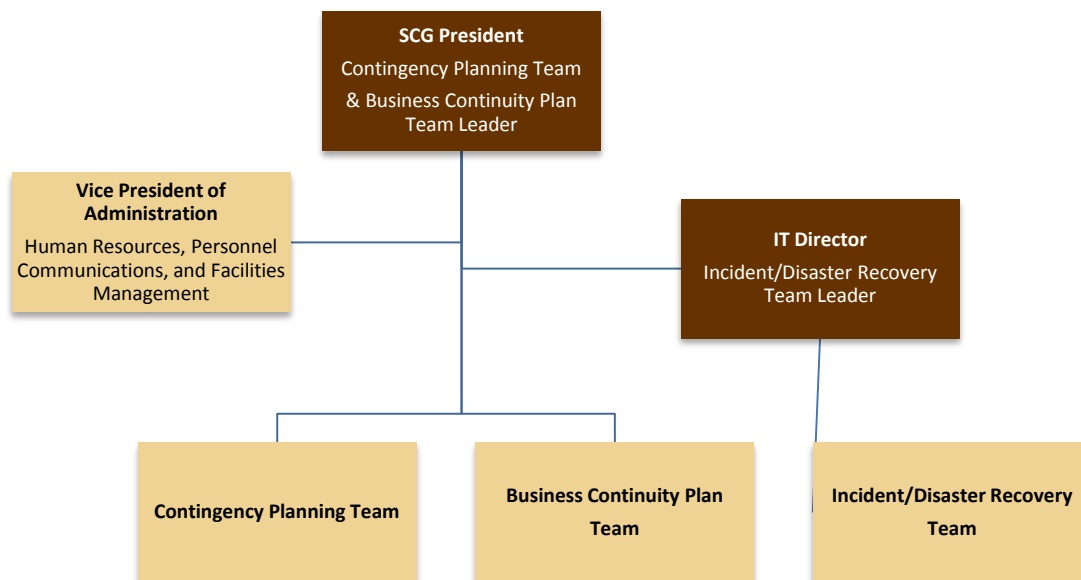
Title	Name	Contact Information	Emergency Role
IT Director	Chuck Lee	301-670-4990 (W) 301-366-3273 (C) 301-637-4355 (H) clee@scgcorp.com	Damage Assessment, Incident Response/Disaster Recovery Team Leader DRP Director
SCG President	Beverly Campbell	301-670-4990 (W) 301-461-1109 (C) 540-887-9829 (H) bcampbell@scgcorp.com	Damage Assessment, CP Activation Decision, and Contingency Planning Team Leader
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, Incident Response/Disaster Recovery Team Member
Program Manager	Susie Warner	301-670-4990 (W) 301-366-3217 (C) 301-355-4388 (H) swarner@scgcorp.com	SCG Secure Cloud Contract Management, Incident Response/Disaster Recovery Team Member
IT Systems Specialist	Kenny Ying Lee	301-670-4990 (W) 315-956-7796 (C) ylee@scgcorp.com	Incident Response/Disaster Recovery Team Member
IT Systems Specialist	John Bernheimer	301-670-4990 (W) 410-428-1330 (C)	Incident Response/Disaster Recovery Team Member
Web Development Director	Ric Blackman	301-670-4990 (W) 301-529-0760 (C) rblackman@scgcorp.com	Applications and Web Development, Incident Response/Disaster Recovery Team Member
Information Center Manager	Justin Gray	301-670-4990 (W) 301-524-2986 (C) jgray@scgcorp.com	Incident Response/Disaster Recovery Team Member Frederick Facility POC
Office Manager	April Randolph	301-670-4990 (W) 240-848-6803 (C) arandolph@scgcorp.com	Incident Response/Disaster Recovery Call Tree Non-Essential Staff Notification
<b>Note: If the incident/disaster occurs when staff members are not in the facility, call mobile phone numbers before trying home numbers.</b>			

## Appendix C: Vendor Contact List

This appendix contains vendor contact information for the SCG Secure Cloud system. The equipment/services provided by each vendor is identified, along with contact numbers. A copy of this information is maintained in the CP located at the Frederick facility.

Vendor	Contact Information	Equipment/Component
APC	800-555-2725	APC 42U Rack, APC Smart UPS SC 620 VA
Startech	800-265-1844	StarTech.com 1U 17" Rack Mount LCD Console
Hewlett Packard	800-334-5144	HP ProliantDL360 Gen9 – Xeon E5-2620V3 2.4 GHz – 80 GB RAM, 900 GB HD
Cisco	800-553 2447	Tandberg StorageLoader LTO-6 and LTO-4 running BackupExec 2015 Enterprise, Cisco 5512-X Firewall, Cisco 2960 Switch, and Cisco SG110D-08 Switch
Netgear	855-776-7233	Netgear FS524S Switch, Netgear GS108 Switch
Microsoft	800-936-4900	Windows 2008 R2 Enterprise (x64), SQL Server 2012 Standard (x64), SharePoint Foundation 2010, Active Directory
VMWare	877-486-9273	VMware VSphere ESXi 6.0 update 2
Adobe	888-649-2990	Coldfusion 9
Symantec	800-342-0652	Symantec Protection Suite Enterprise 2015
SolarWinds	855-498-4157	Kiwi Syslog

## Appendix D: Hierarchical Recovery Team Diagram



## Appendix E: Vital Records and Instructions for Restoring Operations

Name of Vital Record	Electronic / Paper	Accessible Offsite Location	Point of Contact
SCG Secure Cloud Incidence Response Plan	Electronic and Paper	Frederick Facility	Chuck Lee 301-670-4990 (W) 301-366-3273 (C) 301-637-4355 (H) clee@scgcorp.com
SCG Secure Cloud Disaster Recovery Plan	Electronic and Paper	Frederick Facility	Chuck Lee 301-670-4990 (W) 301-366-3273 (C) 301-637-4355 (H) clee@scgcorp.com
SCG Secure Cloud System Configuration and Management Plan	Electronic and Paper	Frederick Facility	Chuck Lee 301-670-4990 (W) 301-366-3273 (C) 301-637-4355 (H) clee@scgcorp.com

## Appendix F: Recovery Checklist

This Recovery Checklist should be used during the recovery of the SCG Secure Cloud system.

SCGSC Recovery Checklist		
Task	Completed	Completed By
<b>SYSTEM DISRUPTION—INITIAL NOTIFICATION</b>	(✓)	
The IT Director contacts the appropriate recovery team(s) to monitor the status of overall outage assessment activities.		
a. Designate a work area for the recovery team members to collaborate and convene.		
b. Ensure the appropriate contact information is readily available for the IT Director and Director's Alternate.		
c. Copy and distribute the outage assessment report form to the appropriate recovery team members.		
d. If applicable, coordinate with facilities contact to request that the computer room's power not be restored until an outage assessment has been completed and the computer is deemed safe.		
e. Building access permitting, conduct a visual inspection of the server area. Visually inspect all SCG Secure Cloud equipment for external and internal damage. DO NOT POWER UP ANY EQUIPMENT PRIOR TO PASSING THIS INSPECTION.		
f. Determine whether or not the vendor should be contacted to service any affected equipment.		
g. Note the position of the equipment power switch during inspection. If visual inspection determines that the switch is in the "on" position, switch it to the "off" position.		
h. Ensure that any hardware that is determined to be unsafe to operate is appropriately labeled. If determined to be safe, unplug equipment from the power source.		
i. When equipment is ready for power up testing, advise the facilities contact. Stand-by until advised that power has been restored.		
j. Working in concert with the appropriate recovery team members, power up one-piece-at-a-time each of the SCG Secure Cloud components.		
k. Annotate the condition of each component on the outage assessment report form (see outage assessment procedures below).		
l. Determine the status of the data stored within SCG Secure Cloud and whether data backups need to be retrieved from onsite or offsite storage.		
m. Work with the appropriate recovery team members to determine the estimated time to repair/replace or reconstruct major elements of the system.		
n. Based on outage assessment findings, be prepared to recommend either partial or full activation of the ITCP.		
o. Provide a completed outage assessment report to IT Director on the overall outage assessment findings.		

SCGSC Recovery Checklist		
Task	Completed	Completed By
<b>OUTAGE ASSESSMENT PROCEDURES</b>	(✓)	
Complete an outage assessment report.		
a. Check the cause of the disruption, including type, scope, location, and time of disruption.		
b. Check whether the outage is localized (this only) or widespread.		
c. Check the location of failing components and those users without service.		
d. Check the impact of the disruption or components damaged.		
e. Check the functional status of all components (e.g., fully functional, partially functional, nonfunctional).		
f. Check the potential for additional disruption or damage.		
g. Check the Identification of a single point of failure (if possible).		
h. Check items to be replaced (e.g., hardware, software, firmware, supporting materials).		
i. Check anticipated downtime of the system (e.g., longer than two days).		
j. Classify disruption as 'minor system failure' or 'major system failure.'		
<b>MINOR SYSTEM FAILURE</b>	Completed	Completed By
<b>Recovery and Resumption Procedures</b>	(✓)	
The assigned recovery team(s) provide an estimated recovery time to the SCG President and Program Manager and begin repair of the components (i.e., the databases, servers, infrastructure or the software).		
The IT Director notifies all users that the 'minor system failure' is being recovered and will be functioning under normal conditions within the estimated recovery period. An Info Alert will be sent through the SCG Intranet and email system on the status of the SCG Secure Cloud and recovery time.		
The minor system failure is recovered and situation is closed.		
<b>MAJOR SYSTEM FAILURE</b>	Completed	Completed By
<b>Activation/Notification Procedures</b>	(✓)	
The IT Director reviews the outage assessment report and contacts the SCG President to formally activate the Contingency Plan.		
Are secondary processing procedures required? If yes, document these procedures in a new appendix in the ITCP.		
The IT Director notifies all affected SCG Secure Cloud user groups, application owners, and POCs that the 'major system failure' is being recovered and will be functioning under normal conditions within the estimated recovery period. An Info Alert will be sent through normal channels, if available, on the status of the SCG Secure Cloud and recovery time.		
The IT Director leads the efforts of the Recovery Team and monitors the status of overall recovery and resumption activities.		
<b>Recovery Procedures – Building and Facility Services</b>	(✓)	
The Recovery Team coordinates with the facilities manager to obtain an estimated time that the building will be cleared for reentry.		



SCGSC Recovery Checklist		
Task	Completed	Completed By
The facilities manager provides updates to the IT Director on the status of the building's reopening.		
The IT Director provides periodic updates to the Incident/Disaster Recovery Team regarding the restoration of facilities services.		
<b>Recovery Procedures – Supporting System Infrastructure</b>	(✓)	
The IT Director monitors the progress of Recovery Team personnel and recovery status, as appropriate.		
The IT Director coordinates with the facilities manager to support recovery of the IT infrastructure.		
<b>Recovery Procedures – SCG Secure Cloud System</b>	(✓)	
The Incident/Disaster Recovery Team obtains and restores data from SCG backup facilities to assist in the restoration of all components; the Incident/Disaster Recovery Team works in conjunction with other recovery teams to ensure seamless recovery of the SCG Secure Cloud system.		
The Incident/Disaster Recovery Team conducts all necessary activities to restore the SCG Secure Cloud software and data, as appropriate; the Incident/Disaster Recovery Team also may work in conjunction with the other recovery teams to ensure seamless recovery.		
Once the affected SCG Secure Cloud components have been recovered, the Incident/Disaster Recovery Team and other assigned personnel test all recovered components and associated applications using a logical sequence to ensure complete functionality has been restored.		
The IT Director contacts the SCG President and Program Manager upon the recovery of the SCG Secure Cloud, and recovery operations move into the resumption phase when the system is operating under normal conditions.		
<b>Resumption Procedures</b>	(✓)	
The Incident/Disaster Recovery Team returns all materials, plans, and equipment used during recovery and testing back to storage.		
The Incident/Disaster Recovery Team ensures that all sensitive material is destroyed or properly returned to safe storage.		
Recovery Team personnel assisting with the recovery, conclude their activities and report back to their primary sites.		
The IT Director notifies the user groups regarding the resumption of normal business operations.		
The IT Director develops an AAR and distributes it to the SCG President, Vice President of Administration, and Program Manager. The official record is maintained by the IT Director.		
The IT Director officially deactivates the plan.		

## Appendix G: Reconstitution Checklist

The following issues need to be considered when the detailed plan for reconstitution is developed. This is not intended to be a complete list nor contain detail information.

SCGSC Reconstitution Checklist	
Check	Migration Considerations
	1. Concurrent processing on any systems? If yes, define logistics.
	2. Data/system synchronization between systems and between locations during migration.
	3. Physical move logistics.
	4. Production risk and mitigation.
Check	Activities at Reconstitution Site
	1. Ensure adequate infrastructure support for:
	a. Electric Power (generator, UPS, other)
	b. Heating and Cooling
	c. Physical Security (badging system, fob access, other)
	d. Environmental Controls (fire suppression, smoke detector, moisture detector, other)
	e. Office Equipment (fax machines, copiers, printers, workstations, other)
	f. Telecommunications (circuits, patch panels, multiple providers, other)
	g. Voice Communication (PBX, telephones, voicemail system, other)
	2. Install system:
	a. Network & system hardware, firmware, patches, and configuration (servers, routers, switches, firewalls, other)
	b. Network & system software, patches, and configuration (OS, database tools, Web enablement, other)
	c. Application software, configuration, and patches that are not included when backup tapes are restored
	3. Establish connectivity
	a. Network components and user locations
	b. External systems / Interconnect agreements
	4. Test system operations to:
	a. Ensure full application functionality
	b. Ensure all 'normal' operational support functions resume (e.g., backup schedule, mirroring tasks, off-site tape rotation, other)
	c. Ensure all security controls are functional
	5. Restore contingency system operational data to reconstituted site (for testing, migration, etc.)

SCGSC Reconstitution Checklist	
Check	Activities at Contingency Site
	1. Backup operational data on the contingency system (for production backup, testing, migration, etc.)
	2. Shut down the contingency system
	3. Terminate contingency operations
	4. Ensure all sensitive materials at the contingency site are:
	a. Secured
	b. Removed
	c. Relocated
	5. Arrange for recovery personnel to return to the original facility

## Appendix H: System Hardware and Software Inventory

Configuration Item Name	Item Description	Type	Function	Software/Version
VHOST1	HP ProLiant DL360 Gen9 – Xeon E5-2620V3 2.4 GHz, 80 GB RAM, 900 GB HD, RAID 5 Serial #: MXQ44002RJ	Hardware	Server	VMware VSphere ESXi 6.0 update 2
VHOST2	HP ProLiant DL360 Gen9 – Xeon E5-2620V3 2.4 GHz, 80 GB RAM, 900 GB HD, RAID 5 Serial #: MXQ4400250	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
SCGSCSW01	Cisco 2960 Manageable Switch Mode3I: WS-C2960-48TC-L Serial #: F0C1148U3EG	Hardware	Routes traffic to non-privileged user network (internet to apps)	15.0(2)SE7

Configuration Item Name	Item Description	Type	Function	Software/Version
SCGSCSW02 (Unmanaged Switch)	Netgear FS524S 24-Port Switch Serial #: FS5A1C003773	Hardware	Routes traffic to management network	NA
SCGSCSW03 (Unmanaged Switch)	Netgear GS108 8-Port Gigabyte Switch Serial #: 1DR16B3Y0024E	Hardware	Routes traffic to the DMZ network	NA
SCGSCSW04 (Unmanaged Switch)	Cisco SG110D-08 8-Port Gigabyte Switch Serial #: DNI20120CF0	Hardware	iSCSI connection from hosts to NAS device	NA
SCGSCFW02	Cisco ASA 5512-X Model: ASA 5512v3 Serial #: FTX185110VX	Hardware	Filters traffic and maps internal network to external	Cisco Firewall ASA 9.1.2
SCGSCIPS	Added module for Cisco ASA 5512-X Model: ASA 5512v3 Serial #: NA	Hardware/ Software	Continuously prevents intrusion, Trojans, and hackers	IME ver. 7.3
SCGSCUPS	APC Smart-UPS 3000VA Serial #: AS1350133484	Hardware	Uninterruptable Power Supply	NA
SCGSCRACKCONV	Startech LCD Serial #: E071X4A40184	Hardware	Display, keyboard, mouse	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.

## Appendix I: Acronyms

AAR	After Action Report
AO	Authorizing Official
BIA	Business Impact Analysis
C	Mobile (or Cell) Phone
CMS	Center for Medicaid & Medicare Services
CP	Contingency Plan
DAA	Designated Approving Authority
DNS	Domain Name System
DRP	Disaster Recovery Plan
FCD	Federal Continuity Directive
FIPS	Federal Information Processing Standard
FISMA	Federal Information Security Management Act
H	Home Phone
HHS	Department of Health and Human Services
HSPD	Homeland Security Presidential Directive
ISSO	Information System Security Officer
IT	Information Technology
ITCP	Information Technology Contingency Plan
LCD	Liquid Crystal Display
MTD	Maximum Tolerable Downtime
NDEP	National Diabetes Education Program
NIDDK	National Institute of Diabetes and Digestive and Kidney Diseases
NIST	National Institute of Standards and Technology
NKDEP	National Kidney Diseases Education Program
OCPL	Office of Communications and Public Liaison
OMB	Office of Management and Budget
OS	Operating System
POA&M	Plan of Actions and Milestones
PUB	Publication
RPO	Recovery Point Objective
RTO	Recovery Time Objective
SCGSC	Scientific Consulting Group Secure Cloud
SOP	Standard Operating Procedures
SP	Special Publication
SSP	System Security Plan
TT&E	Testing, Training and Exercise

UPS	Uninterruptible Power Supply
VM	Virtual Machine
W	Work Phone