The Scientific Consulting Group, Inc.

Operations and Maintenance Plan

for the

SCG Secure Cloud System

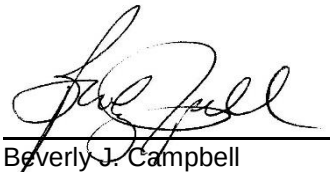
Version 1.5

May 20, 2016

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

Operations and Maintenance Plan Approval

The Operations and Maintenance Plan for the SCG Secure Cloud (SCGSC) must be approved by the SCG President, Vice President of Administration, and Information Technology (IT) Director. The undersigned acknowledge that they have reviewed the Operations and Maintenance Plan for the SCGSC system and agree with the information presented within this document. The IT Director and SCG President will review this document at least once every three (3) years and revise the plan as necessary to address system/organizational changes to the SCGSC system. Changes to this Operations and Maintenance Plan will be coordinated with, and approved by, the undersigned, or their designated representatives.



5/20/16

Beverly J. Campbell
President

DATE

5/20/16

Stacy E. Philipson
Vice President of Administration

DATE

5/20/16

Chuck C. Lee
Director of Information Technology

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 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
SCG Vice President of Administration	
Name	Stacy Philipson
Contact Number	301-670-4990 (W); 301-742-5954 (C)
E-mail Address	bcampbell@scgcorp.com

Document Revision and History			
Revision	**Date**	**Author**	**Comments**
1.0	2/6/15	R. Blackman	Draft plan
1.1	2/20/15	B. Campbell	Minor editing and revisions throughout plan
1.2	2/25/15	B. Campbell	Minor edits to plan
1.3	2/26/15	B. Campbell	Minor edits to plan
1.4	2/27/15	C. Lee/B. Campbell	Minor edits to plan
1.5	5/20/16	B. Campbell	Edits throughout plan

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

List of Tables

List of Figures

1. Introduction

1.1 Document Scope

The scope of this document is limited to the SCG Secure Cloud (SCGSC) system and its hosted applications. This plan is reviewed at least once every three (3) years and updated as needed. It also is updated whenever changes are made to the SCGSC architecture and components.

1.2 Document Purpose and Dissemination

The information contained in this document is for use by administrators, developers, or other technical employees who are tasked with the operations, maintenance, and upkeep of the SCGSC system. The document is disseminated to the SCG President, Vice President of Administration, and SCG IT staff assigned the operation and maintenance roles and responsibilities for the SCGSC system. It also is posted on the SCG Intranet in a read-only format to facilitate easy access by employees.

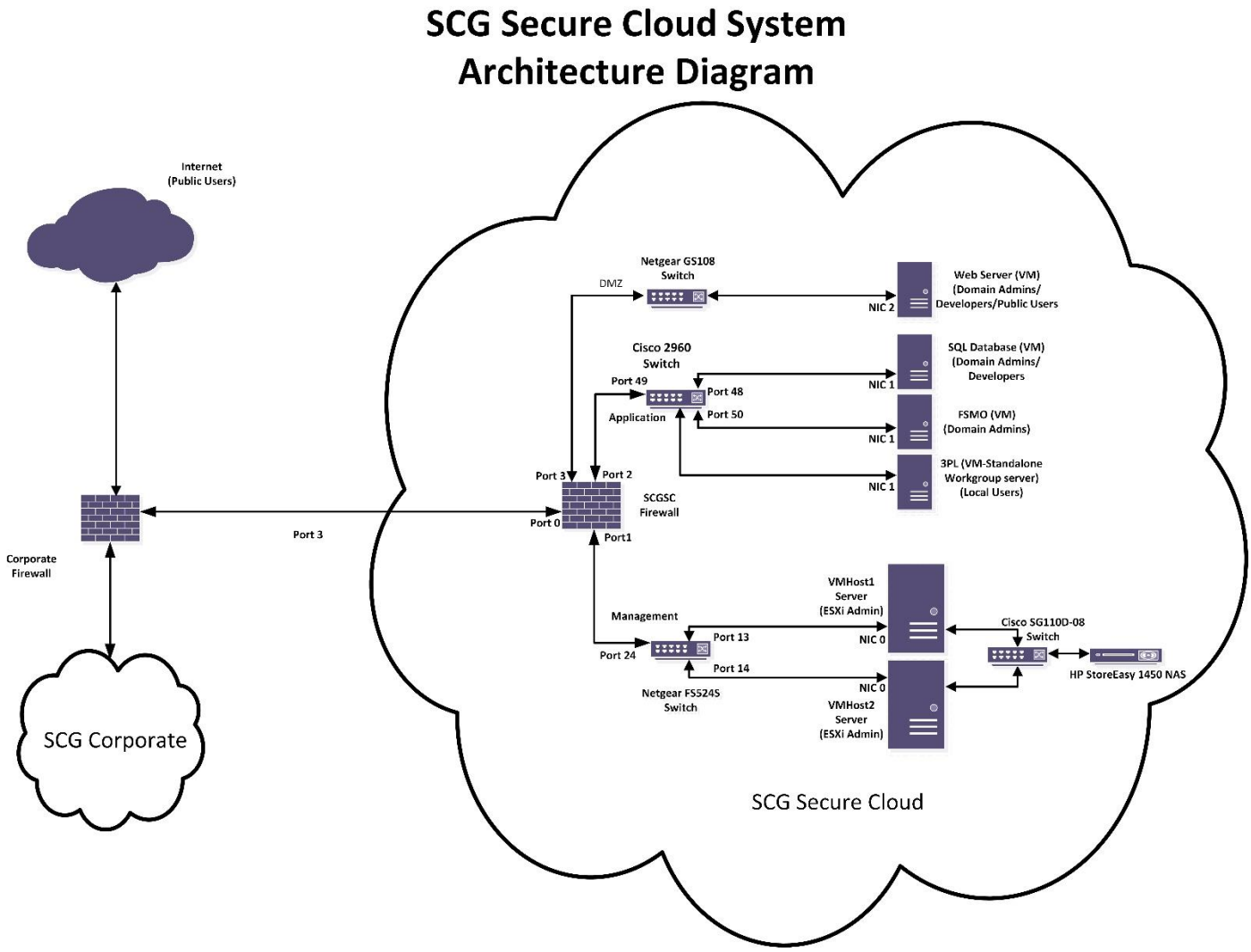
1.3 Project Overview

The SCGSC system is created to support the 3-year contract awarded to SCG to provide Support for National Information Clearinghouses and Campaign-Focused Programs for the National Institute of Diabetes and Digestive and Kidney Diseases' (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. Based on the statement of work for the contract, the SCGSC System will contain the Inventory Tracking System for the NIDDK Clearinghouses, Secure Online Ordering Catalog, Mailing List Database, Websites, Videos, and other items.

The SCGSC system is the primary system that supports the NIDDK Clearinghouses and national education campaigns. It will be used by SCG, NIDDK, and other users on a daily basis. This system is continuously used during business and non-business hours, providing health information that supports NIDDK's mission. The confidentiality, integrity, and availability of the SCGSC system is critical, i.e., ensuring that data are only received by the persons and applications that they are intended for, that data are not subject to unauthorized or accidental alterations, and that the resources are available when needed.

The architecture of the SCG Secure Cloud system is presented in Figure 1.

Figure 1. SCG Secure Cloud System Architecture



1.4 General Information

The SCG Secure Cloud system is up and operational. The primary point of contact (POC) for the system is Chuck Lee, Information Technology (IT) Director at SCG. The Program Manager for the NIDDK contract for which the SCGSC is created is Susie Warner.

1.5 Roles

1.5.1 SCG Coordination Entities

Business Sponsors

The business sponsors for the SCG Secure Cloud system are:

- Beverly Campbell, President of SCG
- Stacy Philipson, Vice President of Administration

- Susie Warner, Program Manager

Executive Steering Committee

The members of the Executive Steering Committee for the SCG Secure Cloud system are:

- Beverly Campbell, SCG President
- Stacy Philipson, Vice President of Administration
- Susie Warner, Program Manager

Integrated Project Team

The Integrated Project Team for SCG Secure Cloud system includes:

- Chuck Lee, IT Director
- Susie Warner, Program Manager
- Ric Blackman, Web Development Director
- Adam Mann, Web Developer
- Kenny Lee, IT Systems Specialist
- John Bernheimer, IT Systems Specialist
- Justin Gray, Call Center Manager

Change Control Board

The members of the Change Control Board for the SCG Secure Cloud are:

- Susie Warner, Program Manager
- Chuck Lee, IT Director
- Beverly Campbell, SCG President

1.5.2 System Operations Roles

Business Sponsors

The Business Sponsors are accountable to the NIDDK for the overall performance of the SCGSC system. The Business Sponsors delegate day-to-day monitoring and management of the SCGSC system to the IT Director who also serves on the Integrated Project Team. The IT Director provides reports on SCGSC activities and status to the Business Sponsors. The Business Sponsors have responsibility to negotiate funding and develop revenues to support the SCGSC program, and to report system progress and issues to the NIDDK.

Executive Steering Committee

The Executive Committee is responsible for setting the direction of the SCGSC system and the Committee responsibilities include:

- Review and approve the updates of the SCG Secure Cloud System Operations and Maintenance Plan.
- Review and approve the annual budget for the SCG Secure Cloud system.

- Review and approve standards for policy and technical direction as recommended by the Integrated Project Team.
- Review system performance and perform risk assessment activities.
- Address issues regarding enforcement and use of standards and best practices escalated from the Integrated Project Team.
- Resolve other issues escalated from the Integrated Project Team.

Integrated Project Team

The SCG Secure Cloud system Integrated Project Team is accountable to the Executive Steering Committee. Responsibilities of the Integrated Project Team include:

- Develop/update the SCGSC Operations and Maintenance Plan for review and approval by the Executive Steering Committee.
- Develop an organized document repository for critical system information, so team members can easily access, store, and reference system documents from all life cycle phases.
- Recommend policy updates for the SCG Secure Cloud system to the Executive Steering Committee.
- Support system operations, perform software and data administration, and perform system maintenance.
- Update system documentation.
- Enhance system configuration as needed.
- Monitor system security.
- Ensure production environment is fully functional and performs as specified.
- Acquire system supplies (e.g., backup tapes) before supply is exhausted.
- Perform routine backup and recovery procedures.
- Perform physical security functions by ensuring all system staff and end users have the proper clearances and access privileges.
- Ensure currency and testing of contingency planning for disaster recovery.
- Ensure periodic training on current and new processes for administrators and end users.
- Monitor performance measurements, statistics, and system logs.
- Perform production control and quality control functions.
- Interface with other functional areas to maintain system integrity.
- Install, configure, upgrade, and maintain databases and update any related system documentation.
- Develop and perform data and database backup and recovery routines for data integrity and recoverability.

- Develop and maintain a performance and tuning plan for online processes and databases.
- Perform configuration and design audits to correct software, system, parameter, and configuration deviations.
- Monitor the performance of the system in regard to hardware, software, and data.
- Monitor the use of approved standards and best practices and escalate enforcement issues to the Executive Steering Committee.
- Inventory SCG Secure Cloud applications and services and coordinate data and application development efforts.
- Provide a forum for discussion of technical issues and address programmatic issues.
- Develop and recommend standards and best practices for the SCG Secure Cloud system to the Executive Steering Committee.
- Prepare quarterly reports on the status of the SCG Secure Cloud system.

Change Control Board

The Change Control Board reviews and approves or disapproves Requests for Change (RFC) that are submitted by the Integrated Project Team. Daily operations of the SCG Secure Cloud system require identifying and implementing minor modifications for it to function optimally and correctly. These modifications must be documented using a Request for Change form in the configuration management repository, and follow the change management process to receive approval for the modifications. The Integrated Team may implement changes to the SCG Secure Cloud system to upgrade hardware and add new or remove old functionality. These enhancements might originate with user requests for specific capabilities or from the Integrated Project Team's identifying solutions to substantive routine system problems. Any enhancements must be documented using a RFC form and reviewed and approved by the Change Control Board.

The responsibilities of the Change Control Board are to:

- Evaluate change requests to determine completeness and clarity.
- Determine the validity, scope, and priority of proposed changes.
- Adjudicate change requests.
- Identify proposed priorities, staff hours, and impacts of RFCs.
- Recommend proposed release schedules for changes to configuration items.
- Present RFC recommendations to the Executive Steering Committee.

2. Hardware and Software Environment

2.1 System Overview

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.

2.2 Naming Conventions

A proper configuration identification schema identifies each component of the network and provides traceability between the component and its configuration status information. Each CI added to the SCG Secure Cloud system managed infrastructure becomes part of a complex variety of technical systems co-existing within the organization. The location, purpose, and relationship of the new CI is identified and recorded according to the SCG Secure Cloud system Naming and Labeling Policy.

The CI Naming Convention Policy includes:

- Every CI registered in the Configuration Management Database (CMDB) requires a unique name.
- The name given to a CI remains with it throughout its lifecycle.
- The name should provide some meaning as to the type of CI it represents.
- To ensure uniqueness of each name, the CI Names should be constructed from CI attributes that will not change.
- Common names for components such as “HOSTNAME”, are not replaced by the CI Name, but are registered as an attribute of the CI.
- CIs will have their CI Names affixed to a visible label on the device or embedded in the firmware or software.

2.3 System Hardware and Software

The system hardware and software for the SCG Secure Cloud system are identified in Table 1 and the equipment is depicted in Figure 2.

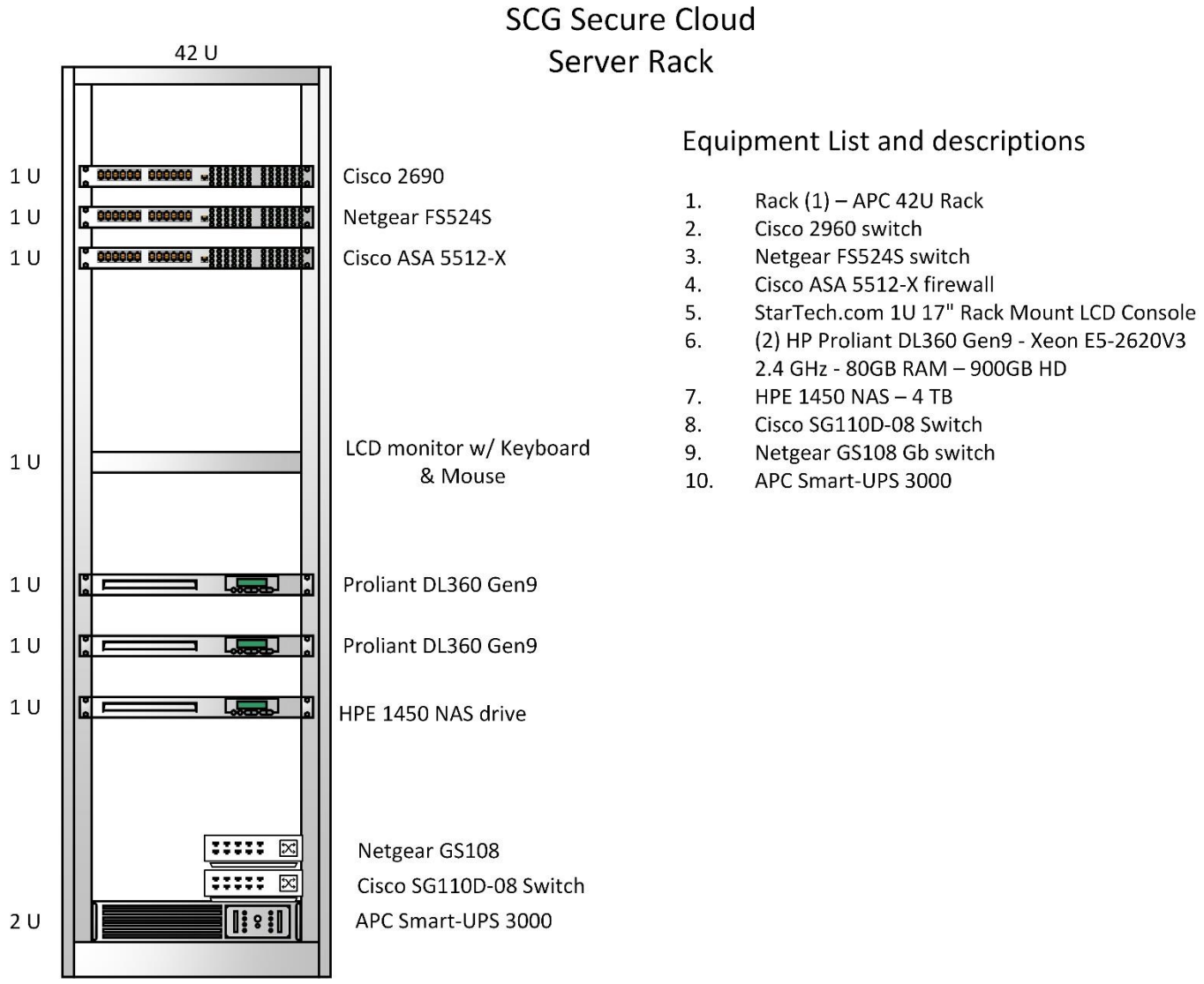
Table 1. SCG Secure Cloud System Hardware and Software

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 Mode3l: 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
SCNAS01	HPE 1450 NAS	Hardware	Host Virtual Machines (VMs)	Windows Storage Server 2012 R2
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.

Figure 2. SCG Secure Cloud System Equipment



3. Server Information

3.1 Virtual Machine 1 (VM 1)

3.1.1 Server Name

The server name for VM1 is SCSQL-PROD.

3.1.2 Application/Services Loaded

The applications/services loaded on VM1 are listed in Table 2.

Table 2. VM 1 Applications/Services

Applications/Services for VM 1
Windows 2008 R2 Enterprise (x64) SP1
SQL Server 2012 Standard (x64) SP2
Kiwi Syslog
DNS (secondary)
Symantec Protection Suite Enterprise 2015

3.1.3 Administrative Accounts

The administrative accounts for VM 1 are listed in Table 3.

Table 3. Administrative Accounts for VM 1

VM 1 Administrative Accounts	
System Administrator	Administrator
Administrative Accounts	CLee YLee JBerheimer

3.1.4 System Dependencies

The applications/services on this VM 1 were listed in Table 2.

3.2 Virtual Machine 2 (VM 2)

3.2.1 Server Name

The server name for VM 2 is SCCOLDSHARE-PROD.

3.2.2 Applications/Services Loaded

The applications/services loaded on VM 2 are listed in Table 4.

Table 4. VM 2 Applications/Services

Applications/Services for VM 2
Windows 2008 R2 Enterprise (x64)
IIS 7.0
ColdFusion 9
SharePoint Foundation 2010
Symantec Protection Suite Enterprise 2015

3.2.3 Administrative Accounts

The administrative accounts for VM 2 are listed in Table 5.

Table 5. Administrative Accounts for VM 2

VM 2 Administrative Accounts	
System Administrator	Administrator
Administrative Accounts	CLee YLee JBernheimer

3.2.4 System Dependencies

The services/applications on VM 2 were identified in Table 4.

3.3 Virtual Machine 3 (VM 3)

3.3.1 Server Name

The server name for VM 3 is SCFSMO.

3.3.2 Applications/Services Loaded

The applications/services loaded on VM 3 are listed in Table 6.

Table 6. VM 3 Applications/Services

Applications/Services for VM 3
Windows 2008 R2 Enterprise (x64)
Active Directory
DNS (primary)
Symantec Protection Suite Enterprise 2015

3.3.3 Administrative Accounts

The administrative accounts for VM 3 are listed in Table 7.

Table 7. Administrative Accounts for VM 3

VM 3 Administrative Accounts	
System Administrator	Administrator
Administrative Accounts	CLee YLee JBernheimer

3.3.4 System Dependencies

The services/applications on VM 3 were identified in Table 6.

3.4 Virtual Machine 4 (VM 4)

3.4.1 Server Name

The server name for VM 4 is 3PL.

3.4.2 Applications/Services Loaded

The applications/services loaded on VM 4 are listed in Table 8.

Table 8. VM 4 Applications/Services

Applications/Services for VM 4
Windows 2008 R2 Enterprise (x64)
MS Dynamics NAV
Symantec Protection Suite Enterprise 2015

3.4.3 Administrative Accounts

The administrative accounts for VM 4 are listed in Table 9.

Table 9. Administrative Accounts for VM 4

VM 4 Administrative Accounts	
System Administrator	Administrator
Administrative Accounts	CLee YLee JBernheimer

3.4.4 System Dependencies

The services/applications on VM 4 were identified in Table 8.

4. System Maintenance Procedures

4.1 System Equipment Maintenance Procedures

The maintenance activities for the SCGSC system equipment include, but are not limited to:

- Running VMWare Operations Manager to diagnose virtualization system
  - High Availability (Fault tolerance) status
  - Replication
- Running hard drive diagnostics on the server using VMWare Operations Manager
- Removing dust and debris
- Updating firmware

4.1.1 Running VMWare Operations Manager to diagnose virtualization system

SCG will perform the following preventive maintenance services on the SCGSC VMWare hosts every 3 months using VMWare Operations Manager:

- Use VMWare Operations Manager to diagnose High Availability (Fault Tolerance):
  - Log into VRealize Operations Manager
  - Select vSphere Clusters tab
  - Select SCGSCCluster.
  - View Summary tab for Health, Risk, and Efficiency optimization opportunities.
  - Select Alerts, Analysis, and Troubleshooting tabs to diagnose any potential issue.

- Use VMWare vSphere Web Client to diagnose Replication:
  - Log into vSphere Web Client.
  - Select vSphere Replication from the list on the left side.
  - Highlight scgvcenter, and then select Monitor.
  - View the Status of each VM's replication and the replication details.
  - Select Reports from the list to view replication statistics, such as transferred bytes, site connectivity, etc.

4.1.2 Maintaining the SCGSC HP Proliant DL360 Gen9 Server

HP recommends the following preventive maintenance procedures be performed every 6 months on the HP Proliant DL360 Gen9 server; therefore, SCG will perform the following tasks every 6 months:

- Perform hard drive diagnostics on the HP Proliant DL360 Gen9 server as follows:
  - Restart the server.
  - Press F10 to enter the Intelligent Provisioning options.
  - Select "Perform Maintenance."
  - Select Array Configuration Utility.
  - Select the Smart Array Controller.
  - Select the Diagnostics/SmartSSD tab.
  - Select Run Diagnostic Report.
  - Address any warnings found.
- Perform firmware updates on the HP Proliant DL360 Gen9 server as follows:
  - Restart the server.
  - Press F10 to enter the Intelligent Provisioning options.
  - Select "Perform Maintenance."
  - Select "Firmware Update."
  - Click Next to update all firmware.
- Verify security and server functionality as follows:
  - Power on the server.
  - Login as Domain Admin.
  - Run Server Manager.
  - Expand "Diagnostics" and click on Device Manager.
  - Ensure no errors are listed on the devices.

4.1.3 Maintaining the SCGSC Cisco ASA 5512-X Firewall

SCG has a Smartnet agreement with SCGSC's ASA 5512-X firewall. This agreement protects the device with all hardware warrantees. In addition, all software/firmware updates are free through this agreement.

SCG will perform the following preventive maintenance procedures for the Cisco ASA 5512-X firewall every 3 months:

- Run the ASDM utility.
- Click Tools, Check for ASA ASDM updates…
- Enter Smartnet credentials.
- When the Upgrade Wizard comes up, click on Next.
- Select the highest version available and click Next.
- When the Review page comes up, review it and then click Next.
- When the upgrade is completed, click Next.
- Ensure Save and reload configuration are checked.
- Click Finish.

After preventive maintenance activities are completed, the IT Director will verify security and system functionality as follows:

- Log onto the firewall as the administrator using the ASDM interface.
- Restart firewall.
- Log back onto the firewall using the ASDM interface.
- View message at the bottom to see if traffic is being blocked/allowed.

4.1.4 Maintaining the APC UPS

APC recommends the preventive maintenance services be performed every 3 months. Therefore, SCG will perform the following procedures every 3 months:

- Shutdown all devices attached to the APC uninterruptible power supply (UPS).
- Disconnect all power plugs connected to the back of the UPS.
- Press the "Test" button in the front of the UPS and ensure no errors are detected
- If an error occurs, log onto the web interface and correct the error using logs.

4.1.5 Cleaning Dust and Debris

Every 3 months, SCG will clean dust and debris from all SCGSC equipment, rack, and server room as follows:

- Use a handheld dust wipe and clean the outside of all devices.
- Use a HEPA filter vacuum cleaner to vacuum the server room.

4.1.6 Controlled Maintenance

- Maintenance activities are scheduled every 3 months unless specified otherwise above for an SCGSC device per the manufacturer's recommendations. When maintenance is performed, a description of the maintenance activity, the individual performing the maintenance, the date the maintenance was performed, and the IT Director review and approval of the maintenance activity are documented in the SCGSC Maintenance Log (see Table 12 at the end of the document).
- The SCG IT staff is authorized to perform all maintenance procedures. Any other individual who will perform maintenance on the SCGSC system must be selected and authorized by the IT Director after review of the individual's credentials and qualifications to perform the maintenance activity. All maintenance activities for SCGSC must be monitored by a knowledgeable member of the SCG IT staff.
- All system maintenance or repairs for the SCGSC system are performed at SCG's facility. No off-site maintenance or repairs will be allowed.
- Sanitization of equipment for off-site maintenance prior to removal is not applicable because no off-site maintenance or repairs are permitted for the SCGSC system.
- Following maintenance or repair, the IT Director will check to ensure that no security controls have been changed, that they are operating normally, and that the system functionality is normal. The steps are identified in Table 6.

Table 6. Maintenance and Repair Follow-up Steps

Device	Steps Following Maintenance Activities
Firmware	1. Connect device and turn on the power 2. Verify device powers up 3. Verify device shuts down 4. Verify functionality
Tape Drive – Verify Read	1. Connect device and turn on the power 2. Log into server with Administrator privilege 3. Run Backup Exec 2010 4. Click Devices 5. Expand server name SCSQL-PROD on the left pane 6. Right click on HP 001 on the right pane and choose Catalog 7. When Catalog is done, click on Restore 8. Click the View by Media tab 9. Current tape should be listed there 10. Expand current tape and ensure that the data were properly read
Tape Drive – Verify Write	1. Click Backup 2. Click Custom Selections 3. Browse and select a file on the C drive (a small file) and click Next

Device	Steps Following Maintenance Activities
	4. Click Next to choose Full Backup 5. Ensure only Backup Now is selected and click Next 6. Select Tape Device and click Next 7. Select Keep Data Indefinitely and click Next 8. Give the job a name and click Next
Server	1. Verify that the device powers up and shuts down correctly. 2. Turn power on 3. Log into the server with Administrator privilege 4. Right click on Computer and choose Manage 5. Click continue when User Access Control displays 6. Expand diagnostic and click on Device Manager 7. Ensure there is no “X” or “!” on any device 8. Address any errors found
Firewall	1. Connect to firewall using Cisco ASDM 2. Double click on ASDM 3. Log onto firewall using the Administrator’s credentials 4. View the messages at the bottom

4.1.7 Maintenance Tools

SCG approves, controls, and monitors information system maintenance tools used for the SCGSC system. The tools approved for use on the SCGSC system include, but are not limited to, the following:

- Compressed air canisters
- Handheld dust cleaners
- Cleaning tape media
- Cisco firmware utility (software)
- HP Proliant DL380 Intelligent Provisioning Utility (software)
- HEPA filter vacuum cleaner

Any tools brought into the SCG facility for use on the SCGSC system for repairs and/or maintenance will be inspected by the IT Director. All work performed of the SCGSC system will be monitored by the IT Director.

All media that will be used for maintenance on the SCGSC (e.g., Cisco firmware utility) will be inspected and scanned for malicious code or other malware before it is permitted to be used in the SCGSC environment using Symantec Endpoint Protection Enterprise software.

4.1.8 Non-Local Maintenance and Diagnostic Connections

There will be no non-local maintenance or diagnostic connections for the SCGSC system. All maintenance and diagnostics for the system will be performed on the premises.

4.1.9 Maintenance Personnel

The SCG IT staff members, Chuck Lee, Ying (Kenny) Lee, and John Bernheimer are the SCG personnel approved for maintaining and repairing the SCGSC system. Any other SCG employee (i.e., non-escorted personnel) who would be tasked with repairing or performing maintenance on the system must be vetted (credentials, knowledge, experience) and authorized by the IT Director. All maintenance and repair activities would be monitored by an approved SCG IT maintenance staff member.

4.1.10 Timely Maintenance

SCG has a plan for restoring the entire SCGSC system as part of our 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 are documented in the formal Contingency Plan for the SCGSC, and are reviewed at least every three (3) years and updated as necessary.

To ensure timely maintenance and repair of the SCGSC system, SCG stores some spare parts on site. For example the SCGSC server is equipped with a spare hard drive that can be used to quickly replace the existing drive in the event of its failure. In addition, the server is equipped with redundant power supplies that will ensure that SCG can keep it operational in the event of a power supply failure.

SCG has good relationships with trusted vendors that supply hardware/software and parts to SCG, which can be shipped overnight when necessary to repair the SCGSC system.

4.2 System Software Maintenance Procedures

4.2.1 System Startup Procedures

The startup procedures for the SCGSC system are identified in Table 7.

Table 7. SCGSC System Startup Procedures

Startup Procedures for SCG Secure Cloud	
Network Devices (switches, firewall, and VMWare ESXi Host)	1. Plug devices to network 2. Plug power cords into devices 3. Manually power devices up but pressing “ON” button
VMWare ESXi Hosts	1. Assure all power connections s are connected to host servers

Startup Procedures for SCG Secure Cloud	
	2. Press the Power On button in front of the computer one at a time
Virtual Machines (VMs)	1. Connect to VMWare Host using VSphere Client software 2. Open VM's Console 3. Click <Power On Virtual Machine>

4.2.2 System Shutdown Procedures

The shutdown procedures for the SCGSC system are presented in Table 8.

Table 8. SCGSC System Shutdown Procedures

System Shutdown Procedures for SCG Secure Cloud System	
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 Hosts	1. Connect to VMWare host using VSphere Client software 2. Click <Shutdown> 3. Perform step 1 and 2 on the other host
Network Devices (switches and firewall)	1. Manually power devices down by pressing the "OFF" button 2. Unplug power plug

4.2.3 Recovery from System Outages

Procedures for recovering the system from an outage are defined in the SCG Secure Cloud Contingency Plan, Incident Response Plan, and Disaster Recovery Plan. The SCG Secure Cloud Recovery Checklist in Appendix F of the Contingency Plan should be used to guide the system recovery efforts. 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 President and Vice President of Administration on the progress of the recovery on a previously agreed timeframe (hourly, every 2 hours, etc.).

4.2.4 Maintenance Procedures

Service Startup and Shutdown

The SCG Secure Cloud services are:

- IIS 7.0

- ColdFusion 9
- SharePoint Foundation 2010
- SQL Server 2012 Standard
- Kiwi Syslog
- Active Directory
- DNS
- Symantec Protection Suite Enterprise 2015

All of these services are configured to run as a service, which means that when the server starts up, they also will start up. When the server is shut down, they also are shut down. These services also can be manually shutdown.

Symantec Protection Suite Enterprise 2015

- Virus Definition Updates—Virus definitions are automatically updated through port 8014 to the Symantec server.
- Virus Software Updates—Virus software updates are maintained manually by the IT Director on a quarterly basis.
- Virus Scanning—Virus scanning occurs continuously via Symantec Protection Suite Enterprise 2015. A full scan of the SCG Secure Cloud system is performed weekly.

Windows Updates

Windows updates are configured to download automatically but not install automatically. The Domain Administrator is notified that an update is available and has been downloaded by a pop-up box that asks if the update should be installed. All updates are applied to the development environment first to ensure stability. The Domain Administrator will install new Windows updates on a weekly basis as follows:

- Log onto the server with Domain Admin privilege.
- Click Start, All Programs and choose Windows Updates.
- Click “Check for Updates.”
- Click Install.

Microsoft SQL and SharePoint Updates

The Domain Administrator will do the following to download SQL updates:

- Go to the Microsoft Download Center.
- Search for (Microsoft SQL Standard 2012 and Microsoft SharePoint Foundation 2010) service packs and updates.
- Download and install any new updates found.

Cisco ASA 5512-X Software/Firmware Updates

Firewall software/firmware updates are performed every 3 months with the preventive maintenance activities as described above.

Intrusion detection occurs continuously using Cisco Intrusion Prevention System (IPS). Cisco's IPS automatically checks for intrusions and performs updates as needed. Cisco's IPS technology, backed by Cisco Security Intelligence Operations (SIO), identifies and mitigates attackers and attacks up to Layer 7 with market-leading, context-aware threat prevention that augments the SCG Secure Cloud firewall.

Symantec Protection Suite Enterprise 2015 also performs intrusion detection on a continuous basis. Symantec's Intrusion Detection System (IDS) detects and notifies the system administrator of unauthorized or anomalous access to the SCG Secure Cloud system. Symantec's IDS helps identify attacks and probes by monitoring traffic for attack signatures that represent hostile activity. Symantec's software includes intrusion protection as well as intrusion detection.

Operating System Patch Management

Patch management is a subset of the overall configuration management process. The Configuration Management Plan contains a strategy for establishing, documenting, maintaining, and changing the configuration of any component of the SCG Secure Cloud system. SCG evaluates the criticality and applicability of the software patch before applying it to the SCG Secure Cloud system. This is where configuration management, risk management, and patch management converge. The risk assessment as to whether to apply the patch should include the risks of not patching the reported vulnerability, extended downtime, impaired functionality, and lost data. SCG's patch management process includes risk analysis and mitigation strategies, and implementation of automated tools to maintain the patch level of the computing platform. The phases of SCG's patch management process are:

- **Baseline and harden**—Gather and consolidate inventory data on every server, switch, and other components in the system. Scan the system for vulnerabilities using appropriate tools. Identify the criticality of each component to the system's mission.
- **Develop a test environment**—Test patches in a test environment that mirrors the production environment. Evaluate and verify system stability and patch installation. VMWare is a cost effective means of establishing a test environment.
- **Develop a backout plan**—Prepare full backup of data and server configuration information before patch is installed and periodically test the restore process to ensure integrity of the backup data.
- **Patch evaluation and collection**—Establish procedures for checking for the existence of available patches, assessing the applicability of the patches, and testing the patches. Evaluate patches to determine which ones are critical, useful, or unnecessary.

- **Configuration management**—Document proposed changes to the system and the results of the patch testing, submit the RFC, and obtain the approval of the Change Control Board and Executive Steering Committee.
- **Patch rollout**—Deploy that patch after it has passed internal testing and configuration management review. Patching should be done manually during off hours whenever possible and allow time for recovery if necessary. Document any adverse events that occur during deployment and incorporate that information into future testing. Test the system after patch deployment.

4.3 Disaster Recovery Services

SCG's disaster recovery and reconstitution services are defined in the SCG Secure Cloud System Contingency Plan and Disaster Recovery Plan.

4.4 Notification Services

The Cisco IPS and the Symantec Protection Suite Enterprise 2015 notify the IT Director of any security or virus detected in the System.

The Cisco IPS Manager Express (IME) is configured to send an e-mail notification message (alerts) to the IT Director when Event Rules are triggered by Cisco IPS sensors. The IME can be configured to identify in the alert message the Signature ID, the source and destination of the alert, and many other variables.

The Symantec Endpoint Protection Manager (SEPM) is configured to generate custom notifications based on a variety of criteria (such as the "Single Risk Event" notification). Various notifications can be configured within the SEPM Monitors tab. These notifications can be sent by e-mail to one or more e-mail addresses in addition to triggering other events and being written into the database.

Audit review, analysis, and reporting are done in accordance with the schedule specified in the SSP for the SCGSC system using Symantec Protection Suite Enterprise 2015 and Kiwi Syslog.

4.5 Backup Services

Automated backups of the SCG Secure Cloud system are done daily during off peak hours (night time) using Symantec BackupExec 2015 from both the primary site (Gaithersburg, MD) and the alternate site (Frederick, MD). Full backups are done every Friday and differential backups (files that have been modified) are done Monday through Thursday. The full backup tape that is run the following Friday becomes the weekly backup tape for the following week. The weekly tapes (5) are reused through the month. The weekly tapes are securely stored until the end of the month, when they are replaced by the monthly backup tape run the Friday following the end of the month. Monthly backup tapes are stored indefinitely. All backup tapes are stored in a fire safe cabinets in the IT Director's office at the primary and in the conference room at the alternate sites. The IT Director conducts monthly testing of backup tapes to ensure that they are complete and the system can be restored. Backup testing is conducted whenever there is a major hardware or software change to the backup system.

If a catastrophic event occurs that results in activation of the Contingency Plan, the processes and procedures identified in the Contingency Plan and Disaster Recovery Plan will be implemented to recover the SCG Secure Cloud system from the most recent backup tape or the SAN at the Frederick facility.

4.6 Monitoring Services

Windows logs and Symantec logs are reviewed and analyzed weekly by the IT Director or a member of the IT Security Team. This review addresses security threats, viruses, hard drive capacity. Kiwi Syslog software monitors all windows logs and centralizes them so reports can be generated. The Symantec Protection Suite Enterprise 2015 monitors viruses and intrusions. This log also will be extracted and reviewed.

Any events or issues that are identified in the environment are immediately communicated to the IT Director and SCG President for assessment and action. The system has an Incident Response Plan and a Contingency Plan that provide the procedures and practices related to strong audit, security response, and issue remediation. The system's Operations and Maintenance Plan is used to govern the review functions for the system.

The IT Director determines appropriate log volumes needed to allow for the system to perform and capture all log data. The volume of storage is reviewed periodically by the IT Director in accordance with the Operation and Maintenance Plan. Storage concerns are addressed in accordance with the procedures identified in the Operation and Maintenance Plan.

The websites hosted on the public facing portion of the SCG Secure Cloud system are monitored by a third-party vendor, Monitis. Each of the websites is checked for specific keyword and heartbeat every 30 seconds from 3 different locations worldwide. These locations are the East Coast (United States), West Coast (United States), and the United Kingdom (UK). When this service fails to contact the website three times from at least two locations, alerts will be sent to the IT Director and the Program Manager through emails and texts.

The SCG Secure Cloud system is managed in accordance with the defined Operation and Maintenance Plan, which does require periodic review of audit logs and any actions are managed in accordance with the Incident Response Plan or Contingency Plan. In addition, vulnerability scans of the SCGSC are performed on a monthly basis.

4.7 Calendar of Events

The maintenance calendar for the SCG Secure Cloud system is outlined in Table 9.

Table 9. Maintenance Calendar for the SCG Secure Cloud System

Period	Details
Daily	• Backup (diffential backup [files that have been modified] Monday through Thursday) • Report Level 1 and Level 2 incidents
Weekly	• Full backup (every Friday) • Full virus scan • Windows updates • Report Level 3 incidents
Monthly	• Vulnerability scan • Full backup • Report Level 4 incidents
Quarterly (Jun, Sep, Dec, Mar)	• Symantec Protection Suite Enterprise 2015 software update • Audit, review, and analyze Kiwi Syslog logs and Symantec Protection Suite Enterprise 2015 logs • Tandberg StorageLoader tape backup preventive maintenance service • Cisco ASA 5512-X preventive maintenance service • APC UPS preventive maintenance service • Dust and debris cleaning
Biannually (Sep, Mar)	• HP Proliant DL360 Gen9 server preventive maintenance
Annually	• TT&E events addressing CP, DRP, and IRP • Security Awareness and Privacy Training • Rules of Behavior Review/Update • Signed acknowledgment of Rules of Behavior • Review/approve System Security Plan • Review system architecture • Review/update access agreements • Review/update facility access list • Review/update Incident Response Plan • Review/Update Risk Assessment • Update/modify list of auditable events
At the End of Each Operation Year Anniversary (Mar)	• Full backup • Symantec Protection Suite Enterprise 2015 software update • Audit, review, and analyze Kiwi Syslog logs and Symantec Protection Suite Enterprise 2015 logs

Period	Details
Every Three (3) Years	• Review/update Contingency Plan • Review/update System Services Acquisition Policy and Procedures • Review/update Personnel Security Screening Policy and Procedures • Review/update Position Risk Designations • Review/update Facility and System Access Policy and Procedures • Review/update Security Authorization • Review/update Configuration Management Plan • Review/update System Design Document • Review/update System and Information Integrity Policy and Procedures • Review/update Operations and Maintenance Plan • Review/update Media Protection Policy and Procedures • Review/update Security Awareness and Training Policy and Procedures • Review/update Audit and Accountability Policy and Procedures • Role-based training • Re-certification of FISMA compliancy

5. Physical Environment

The IT staff will ensure that the SCGSC server room remains locked at all times to prohibit unauthorized physical access. The policies for securing and accessing the server room are defined in the SCGSC Facility and Systems Access Policies and Procedures document. SCG prohibits the use of any transmission medium (such as cellular phones) or output devices in the server room.

The electrical panel for the server room is located in a locked mechanical room on the same floor in the building and the cabling into the server room is not accessible without authorized access. An emergency power shutoff is located in the mechanical room with the electrical panel. A UPS to provide a short-term uninterruptible power supply to allow time for an orderly shutdown of the SCGSC system is available in the event of a primary power source loss. The building has emergency lighting that activates in the event of a power outage, and a flashlight and extra batteries are located in the server room to provide emergency lighting in the event of a power outage. The server room is equipped with a fire extinguisher, sprinkler system, and a plastic tarp to protect the equipment in the event the sprinkler activates. The water shutoff is located in the locked mechanical room, which can be accessed by the IT Director or Vice President of Administration to shut off the water in the event of a leak.

The server room is equipped with a device that monitors the temperature and humidity in the room. When the temperature rises above acceptable operating conditions (95ºF), an e-mail alert is sent to the IT Director and Vice President of Administration. An e-mail alert also is sent to the IT Director when the humidity rises above or falls below the acceptable operating level (30-40%). SCG uses a dedicated AC unit in the server room where the SCGSC resides to maintain the room temperature at optimum operating conditions. A portable humidifier and a dehumidifier are available to maintain the humidity in the server room at the ideal operating range.

The server room at the alternate site is similarly equipped to ensure adequate protection of the physical environment of the SCGSC system.

6. System Contact Information

The contacts for the SCG Secure Cloud system are identified in Table 10.

Table 10. SCG Secure Cloud System Points of Contact

Role	Name, Title, and Contact Information
SCG President	Beverly Campbell, SCG President 301-670-4990 (W) 301-461-1109 (C) bcampbell@scgcorp.com
Program Manager/Liaison with NIDDK (client)	Susie Warner, Program Manager 301-670-4990 (W) 301-366-3217 (C) 301-355-4388 (H) swarner@scgcorp.com
System Administrator	Chuck Lee, IT Director 301-670-4990 (W) 301-366-3273 (C) 301-637-4355 (H) clee@scgcorp.com
Web and Applications Development	Ric Blackman, Web Development Director 301-670-4990 (W) 301-529-0760 (C) rblackman@scgcorp.com

6.1 After Hours/Emergency Points of Contact

The after-hours/emergency points of contact are listed in Table 11.

Table 11. After Hours/Emergency Points of Contact for SCG Secure Cloud System

Role	Name, Title, and Contact Information
System Administrator, Incident/Disaster Response	Chuck Lee, IT Director 301-670-4990 (W) 301-366-3273 (C) 301-637-4355 (H) clee@scgcorp.com
SCG President	Beverly Campbell, SCG President 301-670-4990 (W) 301-461-1109 (C) 540-887-9829 (H) bcampbell@scgcorp.com
Facilities Management, Contingency Planning/ Disaster Response	Stacy Philipson, Vice President of Administration 301-670-4990 (W) 301-742-5954 (C) 301-363-5707 (H) sphilipson@scgcorp.com
NIDDK (Client) Liaison, Incident/Disaster Response	Susie Warner, Program Manager 301-670-4990 (W) 301-366-3217 (C) 301-355-4388 (H) swarner@scgcorp.com
Incident/Disaster Response	Kenny Lee, Computer Systems Specialist 301-670-4990 (W) 315-956-7796 (C) ylee@scgcorp.com
Incident/Disaster Response	John Bernheimer, IT Systems Specialist 301-670-4990 (W) 410-428-1330 (C) jbernheimer@scgcorp.com
Web and Applications Development	Ric Blackman, Web Development Director 301-670-4990 (W) 301-529-0760 (C) rblackman@scgcorp.com
Incident/Disaster Response, Alternate Facility Contact	Justin Gray, Information Center Manager 240-629-3238 (W) 301-524-2986 (C) 301-524-2986 (H) jgray@scgcorp.com
SCG Gaithersburg Office Manager	April Randolph, Office Manager 301-670-4990 (W) 240-848-6803 (C) arandolph@scgcorp.com

SCG uses a call tree notification method when information must be communicated to a SCG personnel quickly and efficiently. The call tree is an effective means of conveying the communication sequence in which leadership, recovery personnel, and facility points of contact should be alerted.

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

- Chuck Lee, IT Director
- Beverly Campbell, SCG President
- Stacy Philipson, Vice President of Administration
- Susie Warner, Program Manager
- Kenny Lee, Computer Systems Specialist
- John Bernheimer, IT Systems Specialist
- Ric Blackman, Web Development Director
- Justin Gray, Frederick Facility POC/Information Center Manager
- April Randolph, Gaithersburg 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 SCG Secure Cloud leadership, recovery personnel, and any facility points of contact who are to be alerted of the DRP activation is presented in Figure 3.

Figure 3. Call Tree for SCG Secure Cloud System Incidents/Disasters

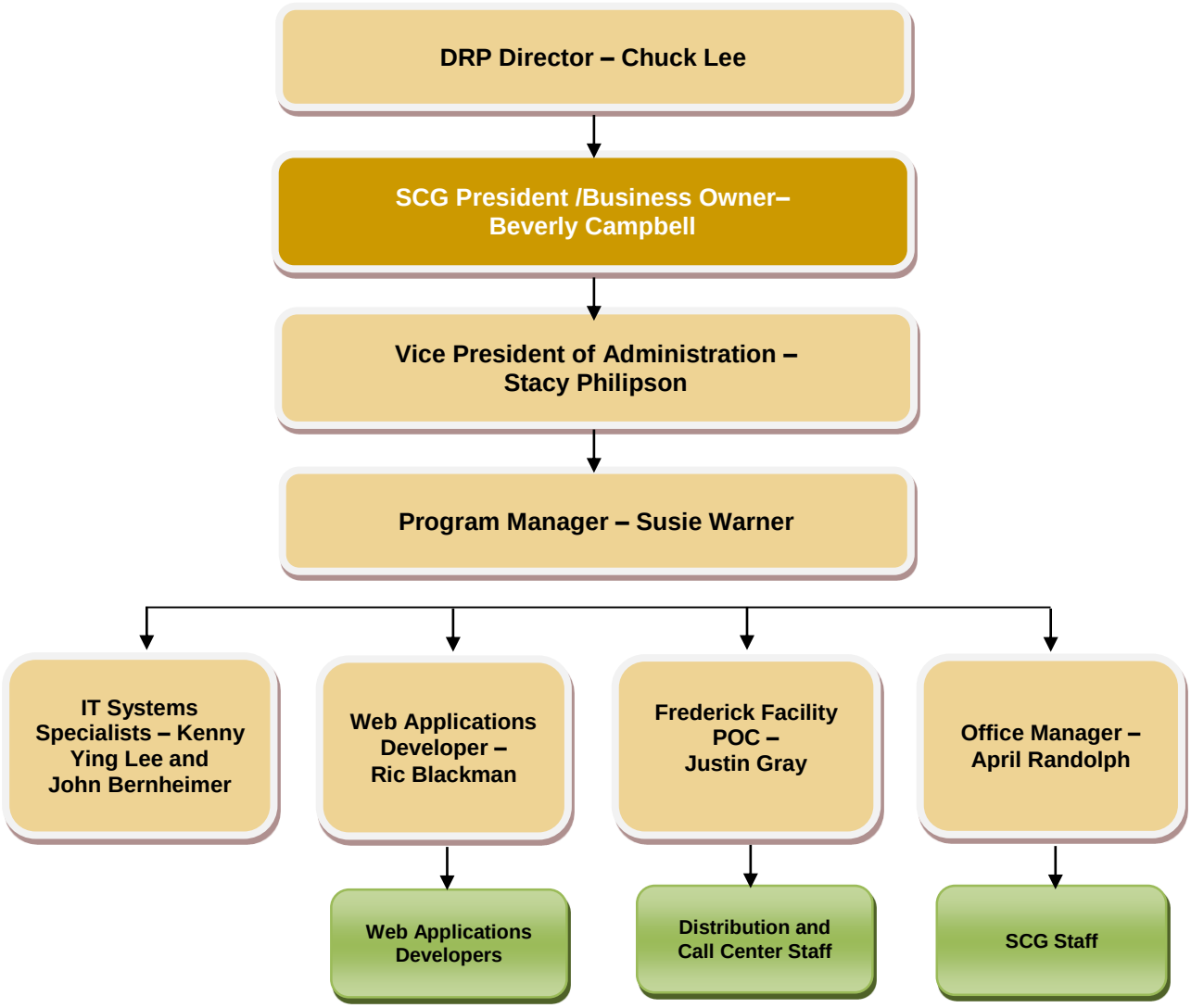


Table 12. SCGSC Maintenance and Repair Log

SCGSC Device	Description of Maintenance/Repair (M/R) Performed	Person Performing M/R	Date M/R Performed	Date M/R Reviewed by IT Director	IT Director Approval

Appendix A: Acronyms

C	Cell (Mobile) Phone
CMDB	Configuration Management Database
H	Home Phone
HEPA	High-Efficiency Particulate Air
HP	Hewlett Packard
IDS	Intrusion Detection System
IME	IPS Manager Express
IPS	Intrusion Prevention System
IT	Information Technology
M/R	Maintenance/Repair
NIDDK	National Institute of Diabetes and Digestive and Kidney Diseases
POC	Point of Contact
RFC	Request for Change
SAN	Storage Area Network
SEPM	Symatec Endpoint Protection Manager
SCG	The Scientific Consulting Group, Inc.
SCGSC	SCG Secure Cloud
UPS	Uninterruptible Power Supply
VM	Virtual Machine
W	Work Phone