The Scientific Consulting Group, Inc.

Configuration Management Plan

for the

SCG Secure Cloud System

Version 1.6

April 18, 2016

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

Configuration Management Plan Approval

The undersigned acknowledge that they have reviewed the SCG Secure Cloud Configuration Management Plan and agree with the information presented within this document. This plan will be reviewed annually and any changes to this Configuration Management Plan will be coordinated with, and approved by, the undersigned or their designated representatives.

4/18/16

Beverly J. Campbell DATE
SCG President

Chuck C. Lee
4/18/16

Chuck C. Lee DATE
Information Technology Director

Stacy E. Philipson
4/18/16

Stacy E. Philipson DATE
Vice President of Administration

Susie Warner
4/18/16

Susie Warner DATE
Vice President/Program Manager

Document Information and Revision History

Document Owners	
SCG President	
Name	Beverly J. Campbell
Contact Number	301-670-4990 (W); 301-461-1109 (C)
E-mail Address	bcampbell@scgcorp.com
SCG Vice President of Administration	
Name	Stacy Philipson
Contact Number	301-670-4990 (W); 301-742-5954 (C)
E-mail Address	bcampbell@scgcorp.com
SCG Information Technology Director	
Name	Chuck Lee, Information Technology Director
Contact Number	301-670-4990 (W); 301-366-3273 (C)
E-mail Address	clee@scgcorp.com
SCG Program Manager	
Name	Susie Warner, Program Manager
Contact Number	301-670-4990 (W); 301-366-3217 (C); 301-355-4388 (H)
E-mail Address	swarner@scgcorp.com

Document Revision and History			
Revision	**Date**	**Author**	**Comments**
1.0	1/30/15	K. Martinez/C. Berry	Create SCG Secure Cloud elements
1.1	2/5/15	B. Campbell/C. Lee	Draft Configuration Management Plan
1.2	2/17/15	K. Martinez/C. Berry	Minor modifications and formatting
1.3	2/25/15	B. Campbell	Minor change on p. 4
1.4	3/11/15	B. Campbell	Replaced Tables 1 and 2 and other minor revisions
1.5	11/20/15	B. Campbell	Edits throughout document
1.6	4/18/16	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

List of Tables

1. Introduction

1.1 Purpose of the Configuration Management Plan

This SCG Secure Cloud System Configuration Management Plan (CMP) document describes the SCG Secure Cloud (SCGSC) system configuration management (CM) and the change management process. The purpose of this plan is to establish a configuration management program for the SCGSC and specify responsibilities, compliance requirements, and overall principles for configuration and change management processes to support information technology management of the SCGSC.

The overall objective of a CMP is to document and inform project stakeholders about CM of the SCGSC system, what CM tools will be used, and how they will be applied by SCG to promote success. The SCG Secure Cloud System CMP defines the project's structure and methods for:

- Identifying, defining, and baselining configuration items (CI).
- Controlling modifications and releases of CIs.
- Reporting and recording status of CIs and any requested modifications.
- Ensuring completeness, consistency, and correctness of CIs.
- Controlling storage, handling, and delivery of the CIs.

Configuration management is the process used during system development and maintenance to identify, control, and report functional and physical configurations of system and software engineering products (e.g., hardware, system architectural design(s), interfacing equipment/systems, drawings, source code, executable code, databases, test scenarios and data, and documentation).

Information systems are typically dynamic, causing the system state to change frequently as a result of upgrades to hardware, software, firmware or modifications to the surrounding environment in which a system resides. Industry standards, including those issued by the Government Accounting Office (GAO) and the Office of Management and Budget (OMB), and several National Institute of Standards and Technology (NIST) Federal Information Processing Standards (FIPS) and Special Publications (SP), stress that information systems must document and assess the potential impact that proposed system changes may have on the operational processes and security posture of the system. Information technology (IT) industry best practices recognize this as an essential aspect of effective system management, as well as being part of the continuous monitoring and maintenance of security accreditation of federal systems required by the Federal Information Security Management Act (FISMA).

Configuration management is a critical control for ensuring the integrity, security, and reliability of the SCGSC. Absent a disciplined process for controlling configuration changes, management cannot be assured that the system will operate as intended, or that the system's maintenance will be performed in a cost-effective or timely manner.

This plan will be reviewed and updated as needed at least once every year or revised as necessary when there is a change in the SCGSC system configuration.

1.2 Audience and Distribution

The intended audience of the CM Plan is the SCGSC Program Manager, project team, and any senior leaders who have roles that are directly responsible for the configuration, management, oversight, and successful day-to-day operations of the SCGSC hardware, software, and applicable documentation. The plan is distributed to the SCG staff and managers responsible for the SCGSC system. It also is posted in read-only format on the SCG Intranet to facilitate access by SCG staff.

2. Policy

This policy is applicable to the SCGSC hardware, software, and documentation changes that might impact the SCGSC system performance, operations, and security.

SCG staff must abide by all federal regulatory policies and procedures that affect configuration and change management processes to be implemented on the SCGSC system. Staff must document, implement, and maintain configuration and change management processes, in collaboration with the policies and procedures defined in the documents specific to the SCGSC system. These processes must include the following:

(1) documenting and maintaining the configuration baseline(s) applicable to the deployed system; (2) effectively managing and tracking all system configuration and associated document changes, as well as the integrity, availability and maintainability of the system; (3) effectively planning to ensure the ability to reverse a deployment or implementation; and (4) effectively tracking all system changes made, including installation of patches, to hardware, software, firmware, and documentation, through development, approval, testing, and controlled implementation of changes delivered into production environments.

Configuration and change management processes must incorporate applicable industry best practices, which support optimum production system availability and effective system management. These practices include: (1) using standardized documented methods, processes, and procedures; (2) effectively tracking and communicating all system changes made to hardware, software, firmware, and documentation, through planning, approving, notifying, developing, testing, scheduling, and managing the implementation of changes; and (3) making effective risk-based decisions to maintain the SCGSC system’s mission capability, authorized security posture, and minimized risk.

SCG must establish a Change Control Board (CCB) to ensure that changes to the SCGSC infrastructure are reviewed and processed in accordance with the established SCGSC configuration and change management processes and procedures. SCG must track relevant information about configuration items, their attributes, baselines, documentation, changes, and relationships. Changes to portions of the SCGSC environment that might impact security, performance, or operations must be tracked and documented.

3. Roles and Responsibilities

The roles and responsibilities for configuration management for the SCGSC are described in this section.

3.1 SCG President (Business Owner)

The SCG President, the owner of SCG, is responsible for:

- Approving and issuing policies, procedures, and guidance for implementing and coordinating the SCGSC configuration management program.
- Overseeing implementation of the SCGSC configuration and change management program, as appropriate.
- Serving as a member of the Change Control Board.
- Reviewing and approving configuration change requests before they are promoted from the testing into the production environment.
- Directing, monitoring, and enforcing implementation and maintenance of, and compliance with, the SCGSC configuration and change management program.
- Periodically reviewing and evaluating the SCGSC system to determine effectiveness and compliance with the SCGSC configuration and change management program.

3.2 Change Control Board (CCB)

The CCB reviews and approves or disapproves Requests for Change (RFC) that are submitted by the SCGSC project team. Any configuration changes and enhancements to the SCGSC system must be documented using an RFC form and reviewed and approved by the CCB.

The CCB is responsible for:

- Reviewing and approving changes to the SCGSC system and ensuring that the changes are reviewed and processed in accordance with established change management processes and procedures.
- Determining the validity, scope, and priority of proposed changes.
- Adjudicating change requests.
- Identifying proposed priorities, staff hours, and impacts of RFCs.
- Recommending proposed release schedules for changes to configuration items.
- Presenting RFC recommendations to the Executive Steering Committee (i.e., SCG President, Vice President of Administration, and Program Manager).
- Incorporating risk management, communication management, and process compliance management to the change process environment for the SCGSC system.

- Establishing a secure and sound configuration management framework ensuring definition and maintenance of configuration baselines and the identification, management, and tracking of associated hardware, software, and documentation configuration items for the SCGSC system.
- Ensuring all changes to configuration items adhere to SCG policy and are documented, tested, and approved. This includes ensuring changes are evaluated to determine the impact to system security before implementation.
- Ensuring that SCGSC configuration and change management process documents are maintained as a CI component and placed under configuration management control.
- Reporting on the effectiveness of the configuration and change management activities to the SCG President.

3.3 SCG Information Technology (IT) Director

The IT Director is responsible for:

- Providing procedures, standards, and guidance to managers and staff in support of the SCGSC configuration management policy.
- Instituting and supervising change management processes and performing day-to-day configuration management activities, including initiating and tracking the status of configuration requests and participating in configuration management audits.
- Tracking and documenting relevant information about SCGSC configuration items, their attributes, baselines, documentation, changes, and relationships, particularly changes that might impact security, performance, or operations.
- Addressing questions and concerns regarding interpretation of the SCGSC configuration and change management policy and accompanying procedures.
- Collaborating with the SCG President and Change Control Board members in the development and revision of configuration and change management processes and procedures.
- Ensuring that SCG is in compliance with the SCGSC configuration management policy and procedures.
- Periodically testing and evaluating the SCGSC system to determine effectiveness and compliance with the SCGSC configuration and change management program.

3.4 SCG IT Staff

The SCG IT staff is responsible for:

- Complying with the SCGSC configuration and change management policy and procedures.
- Working with the IT Director to implement and test configuration changes and enhancements.

4. Configuration Management

4.1 Approach

CM approach refers to the repeatable method of performing an action or creating a product. CM creates standards relating to CM functions. These CM standards include:

- Naming Conventions – Establishing a naming standard that standardizes numbering schemes for all CIs, this includes application software, system software, hardware, and documents.
- Application Identifier – Establishing a naming standard to standardize and identify application software.
- Release Numbering Conventions – Standardizing the identification of each new application version release. A new release number indicates that an upgrade, modification, or enhancement has occurred to the software.
- Version Labels – Assigning version labels to products at different points in the System Development Life Cycle (SDLC). These labels identify the product and the version of the product.

4.2 Organization

SCG's Information Technology (IT) Department manages CM activities for the SCGSC platform including operating system, the network, software, and hardware. The content is managed by the Program Manager. The CM Team group is responsible for content development, updates, and revisions.

4.3 Training

All users having access to the SCGSC are required to:

- Review and acknowledge the NIH General Rules of Behavior for computer and information system access, which hold users accountable for their actions for information security, prior to receiving SCGSC access and annually thereafter.
- Take and pass NIH's Information Security and Privacy Awareness courses on an annual basis.

In addition, personnel responsible for contingency roles and responsibilities with respect to the SCGSC are trained for fulfilling these roles on an annual basis, in conjunction with incident response and disaster recovery training to users consistent with their assigned roles and responsibilities. In addition, personnel assigned security roles and responsibilities must complete the appropriate HHS' role-based training course.

5. Configuration Management Procedures

Configuration management identifies, controls, and provides the status of defined items (hardware, software, firmware) that comprise the SCGSC system. Key components are managed and placed under CM control, including: source code, related documentation, hardware, software, and identified data. This document also should be placed under CM control. These items result in a system baseline produced by the engineering design and implementation processes that start with the formal functional requirements. The following paragraphs describe the procedures required to identify the system baseline configuration and manage changes to that baseline.

5.1 Configuration Identification

Configuration management begins with configuration identification. Configuration identification results in a product structure that includes the selection and identification of the configuration structure for all the Configuration Items (CIs) in the SCGSC infrastructure. This process also allocates identifiers and version numbers for CIs, labeling each CI, and entering it into the SCGSC system inventory. This section identifies the types of items that will be placed under configuration control. A description of the CI will be included in the SCGSC System Inventory. The following criteria are used to identify configuration items:

- The item is a manageable entity.
- The item is critical to the SCGSC’s mission, cost, or scheduled objective.
- The item has specific requirements for performance control.
- The item is expected to undergo a high degree of change after it becomes operational.
- The item will require maintenance, training, and logistics support.
- The item has been designated by the SCG President, Program Manager, and IT Director to be placed under CM control.

The identification process initiates because of the following two main triggers:

- A response to a project scope (it is assumed that this deliverable will be designed, developed, tested, etc.; this deliverable is placed under CM).
- An approved Request for Change (RFC) that alters the existing baseline already governed under the CM process.

Configuration items are an aggregation of hardware, software, and documents that satisfy an end use function. There are three types of CIs: (1) computer software CIs, (2) hardware CIs, and (3) documentation CIs (i.e., the SCGSC System Inventory and the SCGSC Configuration Management Plan).

Once the CIs are identified, documented, and controlled, pertinent information is recorded in the SCGSC System Inventory. CIs are organized and documented to describe their functionality, system relationships, and physical characteristics. A unique identifier is established for each CI supporting tracking and status accounting purposes. The SCGSC system inventory is contained in the SCGSC System Design Document and referred to in numerous documents associated with the SCGSC system.

5.2 Establish Identification Schema (Naming Convention)

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 SCGSC 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 SCGSC system Naming and Labeling Policy.

The CI Naming convention policy includes:

- Every CI listed in the SCGSC System Inventory 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.

Table 1 provides an example of the CI naming convention for the SCGSC system.

Table 1. SCGSC System CI Naming Example

Hardware Equipment and Network Devices		
Class Name (Capability)	**CI Types**	**CI Naming Convention**
SCG Secure Cloud System	[CI function][number] ***Examples:*** ***SW = switch*** ***FW = firewall***	[SCG-optional]SC+[CI type]+[number of device]+[status type-optional] ***Examples:*** ***SCGSCSW01*** ***SCGSSCSQL-PROD***

The CIs for the SCGSC system are identified in Table 2.

Table 2. SCGSC Configuration Items

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

Configuration Item Name	Item Description	Type	Function	Software/Version
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 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) SP1 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) SP1 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
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

Configuration Item Name	Item Description	Type	Function	Software/Version
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
SCNAS01	HPE 1450 NAS	Hardware	Host Virtual Machines	Windows Storage Server 2012 R2
SCGSCRACKCONV	Startech LCD Serial #: E071X4A40184	Hardware	Display, keyboard, mouse	NA
Important Items Outside the SCG Secure Cloud				
SCGSC Tandberg (Tape Backup at Gaithersburg)	Tandberg StorageLoader LTO-6 Tape Autoloader, LTO Ultrium – SAS-2 Serial #: AAS1SA020983	Hardware	Automated Backup of VM 1, VM 2, VM 3, and VM 4	BackupExec 2015 Enterprise
SCGSC Tandberg (Tape Backup at Frederick)	Tandberg StorageLoader LTO-4 Tape Autoloader, LTO Ultrium – SAS-2 Serial #: PW0850BBA00669	Hardware	Automated Backup of VM 1, VM 2, VM 3, and VM 4	BackupExec 2015 Enterprise
SCGSC Configuration Management Plan	Describes SCGSC configuration management and change management policy and process Serial #: NA	Document	Establish CM program for the SCGSC	Version 1.6

Configuration Item Name	Item Description	Type	Function	Software/Version
SCGSC System Inventory	Lists SCGSC system components	Document	Identify specific SCGSC hardware and software	Table 5 of SCGSC System Design Document, v. 1.3

* 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.

5.3 Configuration Management Baseline

The configuration of a system at a specific point in time is designated a baseline. The physical parts and associated documentation define the configuration of that baseline. For the SCGSC system, the baseline includes the System Design Document, system hardware and specifications, software, and documentation.

A configuration baseline includes the approved configuration documentation for a System or CI at a milestone event. Configuration baselines represent:

- Snapshots, which capture the configuration or partial configuration of a CI at specific points in time.
- Commitment points representing approval of a CI at a particular milestone in its development.
- Control points that serve to focus management attention.

Depending on the SDLC phase (see Table 3, Mapping SDLC Phase to CM Baseline), establishing different baselines aids in controlling specific deliverables throughout the SDLC phases.

Table 3. Mapping SDLC Phase to CM Baseline

SDLC Phase	Established Baseline
Planning	None
Requirement Analysis	Functional
Design	Allocated
Development	Development
Integration/Acceptance	Test/pre-production (Benchmark Testing)
Deployment	Production

A baseline is a group of CIs (products, deliverables) formally accepted and developed during a specific phase of the development process. Change to an established baseline occurs only through a formal change process. A brief description of each baseline, mapped to the associated SDLC phase, follows:

- Functional Baseline – The main technical products of the Requirements Analysis Phase. Customer concurrence is required to establish this baseline and is critical as development or change is implemented in later SDLC phases.
- Allocated Baseline – Established during the Design Phase, it defines the configuration items making up a system. The allocated baseline defines how a system functions and performance requirements are allocated across lower level configuration items.
- Development Baseline – Established during the Development Phase by the approval of the technical documentation that defines the functional and detailed design (including documentation of interfaces and databases for the computer software). Normally, this configuration corresponds to the timeframe spanning the preliminary design review and the critical design review.
- Benchmark Testing – Tests that use representative sets of programs and data designed to evaluate the performance of computer hardware and software in a given configuration.
- Product Baseline – Established by approval during the End of Phase Review. The product baseline is the approved product configuration documentation, sometimes referred to as the "as-built" configuration. The Product Baseline is established after all documentation is verified.

5.3.1 Hardware and COTS Software Items for Product Baselines

In addition to code and custom developed software, other products may be incorporated into the SCGSC system software baseline including: commercial off-the-shelf (COTS), patches, service packs, and builds to the packages. All COTS system software, including patches and service packs, will be approved by the IT Director and SCG President through the RFC process.

The hardware baseline includes only the SCGSC system approved hardware configurations. Hardware is defined as devices or equipment including: servers, routers, hubs, and switches. The standard configurations of the hardware will be baselined. CM maintains the hardware baseline, which provides information on approved and procured equipment for the SCGSC system.

The System Design Document contains a current baseline configuration and settings for the SCGSC system. The information in that document would be used to bring the system back to a known state and the most recent tape backup would be used to restore the system settings.

5.3.2 Document Configuration Items, Identification Schema, Baselines

CM Controlled Library

The CM controlled library is where software, documents, and deliverables are logged and stored to ensure all CI masters are protected and remain accessible.

The CM controlled library consists of both a physical and an electronic CM library. Once an identification name or number is assigned to a controlled CI, it cannot be changed. This restriction preserves the item's unique identifier, and its change history[1].

CM Library Inventory contains a record for each inventoried item and assigns it a CI number. The CI number provides a means of easily tracking the item. The CI number enables the creation of an inventory list, which verifies that inventoried items are still intact.

Currently, CM maintains an Electronic Document Library in a secure folder on the domain controller in Excel or Word format. When documented deliverables are accepted (via the Program Manager), the IT Director will update the version and upload the document(s) to maintain any changes required.

CM Library Inventory

The CM Library is an inventory of everything submitted to the CM baseline. Automatically, each item receives a CI number cross-referenced in the CM repository archive (within the change description). Each inventory record contains the following information:

- Description of the product.
- The product that is associated with the RFC.
- Status of the product.
- What was used to create the product (Active Server Pages, .NET, etc.).
- When/if the item was promoted. If it was promoted, the CI number of the promoted item is cross-referenced to its parent CI.

The IT Director for each application is responsible for submitting CI records and keeping all inventory information up-to-date. Configuration status accounting (CSA) information is obtained from the CM Inventory database, including the Documentation Baseline that is compiled by the CM Program Website from the CM Inventory database.

CM Physical Library

The CM Physical Library contains the CD/DVD software “Masters,” and documentation “Masters.” The CM Physical Library also contains all CM generated documentation, logs, and memos. Items checked into the CM Physical Library contain a CI number and are listed in the SCGSC System Inventory. The CM Physical Library can be sorted by application, version, and item type.

CM Electronic Library

The CM Electronic Library is managed by the IT Director who controls the check-in and check-out of controlled electronic files from protected archives. Archived electronic files are all controlled software and dependencies, all generated documentation, and any other types of electronic files that require change control.

[1] The restriction applies even when the CI is removed from the active list.

6. Configuration Control

Daily operations of the SCGSC system require identifying and implementing minor modifications for it to function optimally and correctly. To manage changes to the SCGSC configuration, its CIs, and related documentation and procedures, configuration management ensures that only authorized and identifiable CIs are accepted, recorded, and approved. Configuration control becomes active once a baseline is established.

Configuration control encompasses the submission of an RFC form (see Appendix A), the evaluation process, and ultimate approval or disapproval of the RFC. The evaluation process will consider the merit of a change to the baseline, including effects on system costs, schedules, performance, and maintenance and logistics. The authority for the review and decision of changes to the SCGSC resides with the Change Control Board. The roles and responsibilities of the CCB are described in Section 3 of this document.

Configuration control includes the evaluation of all RFCs and their subsequent approval and disapproval. Configuration change control includes the following:

- Tracking RFC submissions.
- Ensuring that changes are reversible (there is a rollback plan in place to back-out the change).
- Implementing version control.

The method for submitting proposed changes to the approved baseline is the RFC. The CM program will use an Excel spreadsheet to track and record the progress of RFCs (see Appendix B). Each RFC is classified as one of the following types of changes:

- New Software Release Version
- Software/Firmware Patch Release
- Hardware Purchase
- Hardware Upgrade/License
- Existing Software Maintenance/Enhancement
- Other (specify)
- New Application
- Hardware/Software Support Services
- Documentation Update
- Software Purchase
- Firewall Upgrade/Change

6.1 Procedures for Submitting RFCs

System modifications begin with submission of an RFC form. Changes to systems, such as corrections of deficiencies and improvements to functionality, must be approved by the CCB. The project team may need to implement changes to the SCGSC system to upgrade hardware and add new or remove old functionality. These enhancements might originate with user requests for specific capabilities or from the project team's identifying solutions to substantive routine system problems.

Formal change control consists of a series of steps that include a systematic proposal, justification, evaluation, decision, scheduling, implementation, and follow-up audit of approved change. This entire process is initiated with a RFC form (see Appendix A).

A typical change request is processed in the following steps:

1. A RFC form is completed electronically and submitted to the CCB.
2. The IT Director previews the form for completion, and if incomplete, requests additional information from the submitter.
3. The CCB members review the request and meet to discuss its disposition.
4. The CCB makes the decision to approve or disapprove the change, or request additional information.
5. If the change is approved, the IT Director develops an implementation plan and then executes the change.
6. Implementation of the change is verified by audit.
7. The change is marked as completed on the RFC by the IT Director, and the SCGSC system baseline is updated.

Change control does allow for an emergency implementation process for changes that need immediate action due to greatly extenuating circumstances, such as those that include the threat of loss of life, severe injury, or great property damage or where the SCGSC mission is jeopardized. When emergency changes are necessary, the intermediate actions taken and the original threat shall be documented in a follow-up formal RFC that will undergo full review and final solution decision in accordance with this policy and the established authority structure.

6.2 Change Control Board

A major focus of any change control process is a timely change decision. SCGSC change control authority ultimately resides with SCG's President, who delegates authority to the Change Control Board as defined in this document.

7. Configuration Auditing/Reporting

Configuration status accounting involves creating and organizing a knowledge base of information necessary to manage configuration effectively. It provides a reliable source of configuration information that is required for configuration management and to support other program activities, such as program management, systems engineering, software development and maintenance, logistics support, modification, and maintenance. Some of the results configuration status accounting (CSA) tries to accomplish within configuration management are:

- Provide traceability of configuration baselines and changes.

- Collect and document data concerning configuration identification, such as proposed changes and approved changes.

7.1 Status Accounting and Reporting

Status accounting is the recording activity of CM and reports all current and historical data concerned with each CI throughout its lifecycle. This enables changes to CIs and their records to be fully traceable. Baselines form the foundation for status accounting and reporting. Changes to the baseline are fully documented through the RFC process. CSA documentation will include identification of:

- Technical documentation comprising the CI.
- Essential CI data elements, the current version/revision/release of each entity under CM control.
- Proposed changes to the configuration and the status of such changes.
- Approved changes to the configuration, including specific number and kind of CIs to which these changes apply, the implementation of such changes, and the individual responsible for implementation.
- The required records for CSA will use these data elements and their related data items, code, identifiers, and data changes.
- Problem reports, proposed changes, deviations, and implementation status.

7.2 Types of Reports

Data from the Excel spreadsheet supports the compilation of the CSA status reports and/or lists to satisfy status reporting requirements and managerial needs. The types of reports include CM Reports, Problem Reports (PRs), and CM Measurements.

7.2.1 CM Reports

Reports give a direct view into the processes and procedures of CM. Some typical reports that CM will provide include the following:

- Hardware Baseline – The hardware baseline consists of all approved systems, components, and parts utilized by the SCGSC system activities at the production site. The hardware baseline is maintained in the SCGSC System Inventory to identify, record, and report all approved system hardware.
- System Software Baseline – The system software baseline consists of all approved COTS packages, patches, builds, service packs, and step-ups, utilized by the SCGSC system. The software baseline is maintained in the SCGSC System Inventory to identify, record, and report all approved system software.
- Software Status Report – The Software Status Report provides information on the latest operational release and any releases currently in the development lifecycle. This includes the status of the release (Dev and Production), the changes implemented in the release (RFCs), and any other significant information.

- Software/Documentation Audit Findings – Reports for CM and QA management on internal audits. All audit reports are archived by the IT Director.
- Custom Reports – The PM as well as the SCGSC system personnel may periodically require the generation of special reports. CM will acquire and prepare requested information in the specified report format.

7.2.2 Problem Reports

Problem Reports (PRs) will be used to document problems found during review and/or testing of products. PRs are used as an interface between Independent Testing and the developers. A generated PR may spawn an RFC. Any unique identifiers, such as RFC and PR numbers, are cross-referenced to each other. Any PRs that result from a defect from a previous release should immediately spawn an RFC. Any PRs that introduce a new defect and cannot be corrected prior to release are approved by the PM to create RFCs for fixing later. These defects are noted as known defects. PRs and defect reports that do not initiate RFCs are items noted during testing but do not require documentation or source code update. These include defects introduced in a new version corrected prior to the completion of testing.

7.2.3 Metrics

Metrics generated for the CSA report can be presented in graphs and charts. Metrics are calculated and reported on an ad hoc basis.

7.2.4 CM Measures

The IT Director takes CM measures to monitor the CM process throughout the SDLC. These measures will allow management to analyze the effectiveness and performance of the CM activities taking place. Management also will use the metric data to identify trends and problems allowing them to confirm or disprove any perceptions of product/system problems.

Appendix A: SCGSC Request for Change Form

SCGSC REQUEST FOR CHANGE FORM

RFC ID No.:	**RFC Initiator:**
Date Submitted:	**Change Priority:** □ Very High □ Moderate □ High □ Low
Basis of RFC: □ Corrective □ Problem Prevention □ Improvement	**Type of Change Requested:** □ Hardware □ Documentation Only □ Software
Statement of Requirement, Problem, or Deficiency:	
Known or Proposed Solution/Justification (include purpose, benefits, consequences for not implementing change):	
Risks (include reversion procedures and back-out strategy):	
Time Schedule:	
Resource Estimate (personnel, hours, cost):	
Date of Change Control Board Review:	**Decision of the Change Control Board:** □ Change Approved □ Change Disapproved □ Deferred to Later Review □ Other (explain): ____________________

Authorizing Signatures:

____________________	____________________
Beverly J. Campbell **SCG President**	**Date**
____________________	____________________
Susie Warner **Program Manager**	**Date**

THE SECTION BELOW TO BE COMPLETED BY THE IT DIRECTOR FOR APPROVED CHANGES ONLY

Date Change Initiated:	**Date Change Tested:**	**Date Change Finalized:**

Appendix B: Configuration Change Record Report Template

Configuration Change RFC No.	Purpose of Change	Current Status	Status Date	Notes/Comments

Appendix C: Acronyms

CCB	Change Control Board
CD	Compact Disc
CI	Configuration Item
CM	Configuration Management
CMDB	Configuration Management Data Base
CMP	Configuration Management Plan
COTS	Commercial Off-The-Shelf
CSA	Configuration Status Accounting
CSCI	Computer Software Configuration Item
DCI	Document Configuration Items
DEV	Development
DVD	Digital Versatile Disc
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
GAO	Government Accounting Office
HHS	Department of Health and Human Services
HWCI	Hardware Configuration Item
ISCI	Information Security Configuration Item
IT	Information Technology
NIH	National Institutes of Health
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
PM	Program Manager
PR	Problem Report

RFC	Request For Change
SCGSC	Scientific Consulting Group Secure Cloud
SDLC	Systems Development Life Cycle