The Scientific Consulting Group, Inc.

System Security Plan

for the

SCG Secure Cloud System

Version 1.8

July 1, 2016

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

System Security Plan Approval/Signatory Authority

We, the undersigned, approve the content of this System Security Plan for the SCG Secure Cloud system maintained by The Scientific Consulting Group, Inc. (SCG) located at 656 Quince Orchard Road, Suite 210, Gaithersburg, Maryland, including the system boundary, the FIPS 199 Impact Level of Moderate, and the FIPS 200 security controls as tailored specifically for this system.

Dana Sheets System Owner	Date
Chandan Sastry Approving Authority	Date
Warren Herder Information System Security Officer	Date

Document Revision History

Document Revision and History				
Version	**Date**	**Pages Affected**	**Author**	**Comments**
1.0	1/29/15	All pages	C. Berry	Initial Draft. Based on "Information System Security Plan" Template from NIST Special Publication 800-18, February 2006.
1.1	2/5/15	All pages	B. Campbell C. Lee	Revised Draft. Tailored generic draft to be specific to SCG Secure Cloud system
1.2	2/25/15	pp. 19, 25, 28	B. Campbell	Made minor revisions on 3 pages
1.3	3/12/15	All pages	C. Berry B. Campbell C. Lee	Updated security control families, updated Figure 2, updated Table 4, updates throughout to make SSP consistent with NIST SP 800-53, Rev 4 and HHS Information Security and Privacy Policy – 2014 Edition
1.4	3/18/15	All pages	C. Berry B. Campbell	Added risk assessment results; made minor modifications throughout. Add signature page and minor revisions
1.5	4/3/15	pp. 18, 25, 26, 31, 104, 107, 108, 116, 121, 126, 127, 129	B. Campbell	Made revisions based on comments received from NIDDK review
1.6	2/10/16	Numerous pages	B. Campbell	Updated document to reflect changes to policy, procedures, and equipment.
1.7	5/20/16	All pages	B. Campbell C. Lee	Updated document to reflect changes to the system configuration requested by the ISSO.
1.8	7/1/16	All Pages	B. Campbell C. Lee	Updated document to reflect recommended changes by independent consultants.

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.

Change Management

The SCG Secure Cloud System Security Plan (SSP) is a formal living document that provides an overview of the security requirements and describes the security controls in place to meet those requirements. The SSP is required for Security Assessment and Authorization of an information system per the Federal Information Security Management Act (FISMA) and federal regulations. Additionally, the SCG Secure Cloud Security Team was given guidance by the National Institute of Diabetes and Digestive and Kidney Diseases (NIDDK) to follow the National Institute of Standards and Technology, NIST 800-37, Rev. 1, "Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach" methodology for the Security Assessment and Authorization (CA) of the SCG Secure Cloud (SCGSC). Per NIST requirements the SCG Secure Cloud Security Team will use NIST 800-18 "Guide for Developing Security Plans for Information Technology Systems," to develop the SSP format that will provide the NIDDK a standardized approach across the National Institutes of Health (NIH) enterprise.

Per NIST 800-37 the CA process consists of four distinct phases, with requirements for updating the SSP at the end of each phase. The SSP contains both technical information and policy requirements derived from system vulnerability scans, system design documentation, security policies, and the security assessment that will be conducted by the SCG Secure Cloud Security Team. The SSP will be used by individuals responsible for IT security at the system level and at the organization level to ensure that the SCGSC system security requirements are met according to Department of Health and Human Services (HHS), NIH, and federal policies and guidelines.

Changes to the SSP will be performed only by the SCG Secure Cloud Security Team or Information System Security Officer (ISSO). This is necessary to preserve the impartial and unbiased nature of the information contained within the SSP. This ensures that the Authorizing Official receives the most objective information possible to make accreditation decisions regarding the SCGSC system. Therefore, version control must be maintained on the document to ensure the integrity of the information contained herein.

In addition, the SCGSC SSP contains "Sensitive but Unclassified" information and security information and all government employees and government contractor employees are obligated to protect this information from unauthorized disclosure, and it cannot be distributed outside of NIDDK/NIH unless such disclosure is approved in writing by both SCG and NIDDK/NIH.

Table of Contents

1. Introduction 1
2. System Identification 1
   2.1 System Name/Identifier 1
   2.2 System Categorization 2
   2.3 General Description of Information Sensitivity 2
   2.4 Protection/Certification Requirements 2
   2.5 System Owner 3
   2.6 Authorizing Official/Designated Approving Authority/Certification Agent 4
   2.7 Information System Security Officer 4
   2.8 Assignment of Security Responsibility/Other Designated Contacts 5
   2.9 Information System Operational Status 5
   2.10 Information System Type 9
   2.11 General Description and Purpose 10
   2.12 System Environment 10
   2.13 System Interconnection/Information Sharing 14
   2.14 Related Laws, Regulations, and Policies 14
3. Security Controls Summary for SCGSC 15
4. Access Control (AC) 17
5. Awareness and Training (AT) 8
6. Audit and Accountability (AU) 11
7. Security Assessment and Authorization (CA) 9
8. Configuration Management (CM) 16
9. Contingency Planning (CP) 29
10. Identification and Authentication (IA) 1
11. Incident Response (IR) 8
12. Maintenance (MA) 13
13. Media Protection (MP) 18
14. Physical and Environmental Protection (PE) 22
15. Planning (PL) 30
16. Personnel Security (PS) 33
17. Risk Assessment (RA) 39
18. System and Services Acquisition (SA) 41
19. System and Communications Protection (SC) 50
20. System and Information Integrity (SI) 60
21. Program Management (PM) 69
22. Authority and Purpose (AP) 77

23. Accountability, Audit, and Risk Management (AR) 78
24. Data Quality and Integrity (DI) 82
25. Data Minimization and Retention (DM) 83
26. Individual Participation and Redress (IP) 85
27. Security (SE) 87
28. Transparency (TR) 88
29. Use Limitation (UL) 90
Appendix A: References 92
Appendix B: Acronyms 94
Appendix C: Glossary 95
Appendix D: SCG Secure Cloud System Rules of Behavior 110
Appendix E: Information System Media 116
Appendix F: Risk Assessment 117
Appendix G: Configuration Management Plan 117
Appendix H: Contingency Plan 117
Appendix I: Incident Response Plan 117
Appendix J: Privacy Impact Assessment 117
Appendix K: Security Controls to Related References/ Publications/Directives 118

List of Tables

Table 1. SCG Secure Cloud System Categorization 3
Table 2. Security Responsibility/Other Designated Contacts 5
Table 3. SCGSC System Status 6
Table 4. SCGSC System Deployments and Schedule 6
Table 5. SCGSC Information System Type 9
Table 6. SCGSC System Equipment List 13
Table 7. Controls Status Summary Table 15

List of Figures

Figure 1. SCG Secure Cloud System Technical Architecture Diagram 7
Figure 2. Logical Boundaries 8
Figure 3. SCG Secure Cloud Network System 9
Figure 4. SCG Secure Cloud System Enterprise Topology 12

1. Introduction

The objective of system security planning is to improve protection of information technology (IT) resources. All federal systems have some level of sensitivity and require protection as part of good management practice. The protection of a system must be documented in a system security plan. The completion of system security plans is a requirement of the Office of Management and Budget (OMB) Circular A-130, “Management of Federal Information Resources,” Appendix III, “Security of Federal Automated Information Resources,” and Public Law 100-235, “Computer Security Act of 1987.”

The purpose of the security plan is to provide an overview of the security requirements of the system and describe the controls in place or planned for meeting those requirements. The system security plan also delineates responsibilities and expected behavior of all individuals who access the system. The security plan should be viewed as documentation of the structured process of planning adequate, cost-effective security protection for a system. It should reflect input from various managers with responsibilities concerning the system, including system owner, the system administrators, and the system security manager. Additional information may be included in the basic plan and the structure and format organized according to agency needs, so long as the major sections described in this document are adequately covered and readily identifiable.

For the plans to adequately reflect the protection of the resources, a management official must authorize a system to process information or operate. The authorization of a system to process information, granted by a management official, provides an important quality control. By authorizing processing in a system, the manager accepts its associated risk.

Management authorization should be based on an assessment of management, operational, and technical controls. Because the security plan establishes and documents the security controls, it should form the basis for the authorization, supplemented by more specific studies as needed. In addition, a periodic review of controls should contribute to future authorizations. Re-authorization should occur prior to a significant change in processing, but at least once every year. It should be done more often where there is a high risk and potential magnitude of harm.

2. System Identification

2.1 System Name/Identifier

System Name: SCG Secure Cloud
System Acronym: SCGSC
Unique Identifier: B33818CD-9106-4972-B50F-036484936D53
System Type: General Support System

2.2 System Categorization

In accordance with the provisions of Federal Information Processing Standard (FIPS) 199, Standards for Security Categorization of Federal Information and Information Systems, the security category for the SCG Secure Cloud system is MODERATE.

The SCG Secure Cloud 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 SCG Secure Cloud system will contain the Inventory Tracking System for the NIDDK Clearinghouses, Secure Online Ordering Catalog, Mailing List Database, Websites, Videos, and other items.

The SCG Secure Cloud 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 SCG Secure Cloud system is critical, i.e., ensuring that data only are 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. Due to the importance of this information system, all personnel with system administration rights and roles will be required to have a Public Trust Clearance from NIH and sign confidentiality agreements with SCG.

2.3 General Description of Information Sensitivity

In accordance with FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems*, information categorization is calculated based on the three basic security objectives: confidentiality, integrity, and availability. NIST Publication 800-60 *Guide for Mapping Types of Information and Information System to Security Categories* provides implementation guidance in completing this activity.

Table 1 describes the Information Category from NIST SP 800-60. A general description of the information handled by the SCG Secure Cloud system and the need for protective measures is provided in Section 1.4 of this SSP.

2.4 Protection/Certification Requirements

Table 1 identifies the information system categorization of impact levels for SCGSC. For an information system, the potential impact values assigned to the respective security objectives (confidentiality, integrity, availability) shall be the highest values (i.e., high water mark) from among those security categories that have been determined for each type of information that resides on the information system. The information in the

SCGSC includes titles of publications and the names, addresses, and telephone numbers of individuals who order the publications. The moderate ranking for SCGSC results from the inclusion of names, addresses, and telephone numbers in the system.

Table 1. SCG Secure Cloud System Categorization

Security Objective	**Impact Levels** *(Low-Mod-High)*
Confidentiality	Mod
Integrity	Mod
Availability	Mod
Security Category (SC)	**Moderate**

The following are the fields the SCGSC system collects from public requests:

- First Name (required)
- Last Name (required)
- Organization Name (optional)
- Daytime Phone (required)
- Fax (optional)
- Email address (required)
- Address (required)
- Address 2 (optional)
- City (required)
- State (required)
- Zip Code (required)
- Profession (required)
- Setting (required)

All of the information above is deleted from the SCGSC every 30 days.

2.5 System Owner

For all phases the responsible System Owner and organizations are identified below.

The System Owner is:

Dana Sheets
Digital Engagement Lead
Office of Communications and Public Liaison
National Institute of Diabetes and Digestive and Kidney Diseases (NIDDK)
National Institutes of Health (NIH)
Tel: 301-496-7059
Email: sheetsdm@mail.nih.gov

The data contained in the SCGSC system and the controls that use the data are owned by:

NIH/NIDDK
Bethesda, Maryland

The SCGSC system is maintained by:

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

2.6 Authorizing Official/Designated Approving Authority/Certification Agent

The Authorizing Official/Designated Approving Authority (AO/DAA) is the senior management official or executive with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals. The Authorizing Official/Designated Approving Authority has the following responsibilities related to the system security plan:

- Approves the system security plan,
- Authorizes operation of the information system,
- Issues an interim authorization to operate the information system under specific terms and conditions, or
- Denies authorization to operate the information system (or if the system is already operational, halts operations) if unacceptable security risks exist.

The AO/DAA formally assumes responsibility for the operations of the SCG Secure Cloud system at an acceptable level of risk to agency operations, agency assets, or individuals. The AO/DAA and Certification Agency for the SCG Secure Cloud is:

Chandan Sastry
IT Director and CIO
Computer Technology Branch
NIDDK/NIH
Tel: 301-496-9555
Email: sastrych@mail.nih.gov

2.7 Information System Security Officer

The Information System Security Office responsible for the SCG Secure Cloud system is:

Warren Herder
Information System Security Officer
Computer Technology Branch

NIDDK/NIH
Tel: 301-443-9292
Email: herderjw@niddk.nih.gov

2.8 Assignment of Security Responsibility/Other Designated Contacts

The designated person(s) in Table 2 has sufficient knowledge of the SCG Secure Cloud system to be able to provide additional information or points of contact regarding the security plan and the system, as needed. This table includes the designated person(s) responsible for the security of the system who has been assigned responsibility in writing to ensure that the SCG Secure Cloud system has adequate security and is knowledgeable of the management, operational, and technical controls used to protect the system.

Table 2. Security Responsibility/Other Designated Contacts

System Role	Name	Title/Organization	Address/Phone/Email
Authorizing Official/Designated Approving Authority (AO/DAA)/Certification Agent (CA)	Chandan Sastry		NIDDK Bethesda, MD 301-496-9555 sastrych@mail.nih.gov
System Owner	Dana Sheets	Digital Engagement Lead, Office of Communications and Public Liaison	NIDDK 31 Center Dr. Bldg 31 Rm 9A06 Bethesda, MD 20814 301-496-7059 sastrych@mail.nih.gov
Information System Security Officer	Warren Herder	Information System Security Officer	NIDDK Bethesda, MD 301-827-1752 john.herder@nih.gov
Privacy Officer	Kelly Yager	Privacy Officer (PO)	NIDDK Bethesda, MD 301-496-9555 kelly.yager@nih.gov
SCG IT Director and SCGSC Administrator	Chuck Lee	SCG IT Director/SCGSC Administrator	SCG 656 Quince Orchard Road, Suite 210 Gaithersburg, MD 301-670-49909 clee@scgcorp.com

2.9 Information System Operational Status

The status of the SCG Secure Cloud system is specified in Table 3.

Table 3. SCGSC System Status

System	Status	Date
SCG Secure Cloud	This system currently is in operation.	3/12/15

The system deployments and schedule are shown in Table 4.

Table 4. SCGSC System Deployments and Schedule

System	Completion Dates	Description
SCG Secure Cloud System Design and Configuration	5/6/2016	2 host servers (VHOST1 and VHOST2) consisting of an HP ProLiant DL360 Gen9 – Xeon E5-2620V3 2.4 GHz, 80 GB RAM, 900 GB HD, and RAID 5 running VMware VSphere ESXi 6.0 update 2 and Symantec Endpoint Protection Suite Enterprise 2015. Within this host environment, the system is running four (4) virtual machines: VM 1 (SCSQL-PROD), VM 2 (SCCOLDSHARE-PROD), VM 3 (SCFSMO), and VM 4 (3PL). SCG Secure Cloud includes two switches (Cisco 2960 and Netgear FS524S), 2 8-port gigabit switches (Netgear GS108 and Cisco SG110D-08), a firewall (Cisco 5512-X), and an APC Smart-UPS 3000VA.
SCG Secure Cloud Deployment	4/10/2015	Dynamic web application that allows public users to browse through and order free health-related materials on various topics and diseases affecting public health. The Catalog site is developed (by Developers) in ColdFusion 9 and hosted on a web application server with a Windows Server 2008 R2 Enterprise operating system that utilizes a data source connection to interact with a SQL Server 2012 database server for all data retrieval and processing requests. The Domain Admins maintain the Operating Systems and ensure that all the applications are fully functional. All virtual servers are managed by the host administrators (root). Local users on 3PL are kept isolated from the SCGSC forest.

The Enterprise Technical Architecture presented in Figure 1 shows the systems that are connected. The logical boundaries of the SCGSC system are depicted in Figure 2, and the network system is illustrated in Figure 3.

Figure 1. SCG Secure Cloud System Technical Architecture Diagram

Figure 2. Logical Boundaries

This figure depicts the physical and logical/certification boundaries of the SCG Secure Cloud.

The Secure Cloud is hosted in a VMware virtualized environment consisting of two logical network segments. Each network segment is protected by a stateful firewall with Intrusion Detection.

Management Network – The Management Network is a protected physical segment with no in-bound access from external sources. This boundary isolates all management network traffic from potential exposure. This traffic includes management of the virtual environment and data backup.

Application Network – The Application Network segment is used to provide access to the Secure Cloud via the Internet. In-bound access is restricted to secure communications protocols.

User Types –
Public Users: General users from the internet who can only access the front end of the web server
Host Administrators: The root user is used to access the management network
Developers: Web developers who access the back end of the database and webserver for development
Local Users: Users that only exist on the server (3PL)
Domain Admins: Administrator privileged users who have full access to the whole Active Directory forest

Figure 3. SCG Secure Cloud Network System

2.10 Information System Type

The SCGSC system is a General Support System (see Table 5).

Table 5. SCGSC Information System Type

Major Application		**General Support System**	**X**

2.11 General Description and Purpose

The SCG Secure Cloud system supports the development and communications of health information that improves public health and quality of life.

The SCG Secure Cloud system is created to support the 3-year contract awarded to SCG to provide support for the National Information Clearinghouses and Campaign-Focused Programs for the NIDDK Office of Communications and Public Liaison, in Bethesda, Maryland. This contract enables NIDDK to ensure that the science-based knowledge gained from NIDDK-funded research is imparted to NIDDK target audiences, including health care providers and the public for the direct benefit of patients and their families. The main Statement of Work areas for this contract are:

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

NIDDK supports a wide range of medical research through grants to universities and other medical research institutions across the country. The Institute also supports government scientists who conduct basic, translational and clinical research across a broad spectrum of topics and serious, chronic diseases and conditions related to the Institute's mission. In addition, the NIDDK supports research training for students and scientists at various stages of their careers and a range of education and outreach programs to bring science-based information to patients and their families, health care professionals and the public.

The SCG Secure Cloud system architecture diagram was presented in Figure 1.

2.12 System Environment

The SCG Secure Cloud system is housed in a secure office building in Gaithersburg, Maryland. SCG has the entire second floor of the building where the system is located. There is controlled access to SCG's offices and the server is located in a locked room with electronic security that logs the name of the individuals entering the room and the

date and time of access. The SCG Secure Cloud system has two host servers consisting of a HP ProLiant DL360 Gen9 – Xeon E5-2620V3, 2.4 GHz - 80GB RAM – 900GB HD, and RAID5 running VMWare VSphere ESXi 6.0 update 2 and Symantec Endpoint Protection Suite Enterprise 2015. Within this host environment, the system is running four virtual machines: VM 1 (SCSQL-PROD), VM 2 (SCCOLDSHARE-PROD), VM 3 (SCFSMO), and VM 4 (3PL). The operating system for all virtual servers is Windows 2008 R2 Enterprise (x64). VM 1 has SQL Server 2012 Standard (x64) and is a secondary DNS Server. It also is the Kiwi Syslog server that gathers all system logs. VM 2 is the webserver and has ColdFusion 9 and SharePoint Foundation 2010. VM 3 is the domain controller and maintains all domain roles and active directory; it also is the primary DNS Server. VM 4 is a standalone server that keeps track of publication inventory and shipping status for the warehouse. SCG Secure Cloud has two main switches—Cisco 2960 Manageable Switch and Netgear FS524S Unmanaged Switch—for connecting the management network and the back end application network segments. There also are two non-rack mountable 8-port gigabyte switches (Netgear GS108 and Cisco SG110D-08) used for routing traffic to the DMZ and access to the NAS device where all the virtual servers reside. There is one firewall—Cisco 5512-X. The external IP address for VM 2 is 206.130.148.40. The system also includes an APC Smart-UPS 3000VA.

To ensure less downtime/outages, VMWare High Availability failover or fault tolerance is configured between the two hosts to keep the virtual servers online. If one fails, the other will take over. Also, all virtual servers are replicated to an offsite facility in Frederick, Maryland.

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

A diagram of the SCGSC system network segment was presented in Figure 3 and the SCGSC system enterprise topology is depicted in Figure 4. The SCGSC equipment (hardware and software) is listed in Table 6.

Figure 4. SCG Secure Cloud System Enterprise Topology

Table 6. SCGSC System Equipment List

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) Kiwi Syslog
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 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
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.

2.13 System Interconnection/Information Sharing

The SCG Secure Cloud is a standalone system connected to the Internet. It is not connected to any other systems.

2.14 Related Laws, Regulations, and Policies

In accordance with SCG's contract with NIDDK to support the national clearinghouses and education campaigns, the following laws, regulations, and policies establish specific requirements for confidentiality, integrity, or availability of data/information in SCG Secure Cloud:

- Federal Information Security Management Act (FISMA) of 2002
- OMB Circular No. A 130, Appendix III
- NIST SP 800-18 Rev. 1 - Guide for Developing Security Plans for Federal Information Systems, February 2006
- NIST SP 800-30, Rev. 1 - Guide for Conducting Risk Assessment, Sep 2012
- NIST SP 800-37 Rev. 1 – Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach, Feb 2010
- NIST SP 800-53 Rev. 4– Security and Privacy Controls for Federal Information Systems and Organizations, Apr 2013
- 5 U.S.C. 552, "Freedom of Information Act," c. 1967
- 5 U.S.C. 552a, "Privacy Act," c. 1974
- OMB Circular A-130, Appendix III, “Security of Federal Automated Information Systems”
- FIPS 199, “Standards for Security Categorization of Federal Information and Information Systems”
- FIPS 200, “Minimum Security Requirements for Federal Information and Information Systems”
- FIPS 201-1, “Personal Identity Verification of Federal Employees and Contractors”
- FIPS 140-2, “Security Requirements for Cryptographic Modules”
- 18 U.S.C. 641, “Criminal Code: Public Money, Property or Records”
- 18 U.S.C. 1905, “Criminal Code: Disclosure of Confidential Information” Privacy Act, HHSAR 352.224-70, January 2006 (requires adherence to NIST SP 800-18, SP 900-26 (which has been superseded by NIST SP 800-53A) and FIPS 200).

Note: Appendix K provides a list of security controls and related References, Publications, and Directives.

3. Security Controls Summary for SCGSC

This section summarizes the management, operational and technical control requirements for the SCGSC system and shows their status (in place, planned, or not applicable and the type of control). The controls status summary in Table 7 provides management with a high level summary of the SCGSC control status.

Table 7. Controls Status Summary Table

Control Abbrev.	Control Category	In Place	Planned	Not Applicable	Common	Hybrid	System Specific
AC	Access Controls	27		8			35

Control Abbrev.	Control Category	In Place	Planned	Not Applicable	Common	Hybrid	System Specific
AT	Awareness and Training	5			5		
AU	Audit and Accountability	19					19
CA	Security Assessment and Authorization	8		2			10
CM	Configuration Management	20		1			21
CP	Contingency Planning	22					22
IA	Identification and Authentication	11		11			22
IR	Incident Response	12					12
MA	Maintenance	7		3			10
MP	Media Protection	9					9
PE	Physical and Environmental Protection	18					18
PL	Planning	6					6
PS	Personnel Security	7		1			8
RA	Risk Assessment	7					7
SA	Systems and Services Acquisition	13		1	1		13
SC	System and Communications Protection	23		1			24
SI	System and Information Integrity	19		3			22
PM	Program Management	16			16		
AP	Authority and Purpose	2			2		
AR	Accountability, Audit, and Risk Management	8			5		3
DI	Data Quality and Integrity	2			2		
DM	Data Minimization and Retention	3			1		2

Control Abbrev.	Control Category	In Place	Planned	Not Applicable	Common	Hybrid	System Specific
IP	Individual Participation and Redress	5			2		3
SE	Security	2			2		
TR	Transparency	5			4		1
UL	Use Limitation	2			2		

4. Access Control (AC)

This section describes the access controls applicable to the SCGSC system. The status of the access controls for the system is as indicated in the following table:

<table>
<tr><th>Control Number</th><th>Description of Control</th><th>Control Status/Type</th></tr>
<tr><td>AC-1</td><td>Access Control Policy and Procedures:
The organization:
a. Develops, documents, and disseminates to SCG staff who support the SCGSC:
1. An access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
2. Procedures to facilitate the implementation of the access control policy and associated access controls; and
b. Reviews and updates the current:
1. Access control policy at least once annually; and
2. Access control procedures at least once annually.</td><td><table>
<tr><td>Status</td><td></td><td>Type</td><td></td></tr>
<tr><td>In Place</td><td>X</td><td>Common</td><td></td></tr>
<tr><td>Planned</td><td></td><td>Hybrid</td><td></td></tr>
<tr><td>In Place and Planned</td><td></td><td>System Specific</td><td>X</td></tr>
<tr><td>Not Applicable</td><td></td><td></td><td></td></tr>
</table></td></tr>
<tr><td colspan="3">The SCG Facility and Systems Access Control Policy and Procedures addresses the requirements and mechanisms to be implemented across the SCGSC operating environment. At a high level, this policy addresses the purpose, scope, roles and responsibilities, management commitment, coordination among organizational entities, and requirements to comply with access control. This policy applies to all applications, databases, operating systems, and network devices that store or process SCGSC information other than publicly accessible Internet facing SCG systems. Additionally, this policy outlines requirements to manage and protect all company and NIH information. The policy is consistent with SCG’s mission, and functions with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.</td></tr>
</table>

It is the responsibility of the SCG President, Vice President of Administration, and the Information Technology (IT) Director to develop, disseminate, and annually review/update the SCG **Facility and Systems Access Control Policy and Procedures**. The IT Director disseminates the document to all Privileged Users by emailing a link to the document's location on the SCG Intranet prior to authorizing privileged user status. The IT Director requests a response email from the Privileged User, confirming that Privileged User has read and understands the document.

The policy and procedures are located on the SCG Intranet that is available to all SCG personnel at http://web-dev/intranet-sql. The intranet server is located in the Gaithersburg facility at 656 Quince Orchard Road, Gaithersburg, MD 20878.

AC-2	**Account Management:** The organization: a. Identifies and selects the following types of information system accounts to support SCGSC missions/business functions: Domain Administrator and Developer; b. Assigns account managers for information system accounts; c. Establishes conditions for group and role membership; d. Specifies authorized users of the information system, group and role membership, and access authorizations (i.e., privileges) and other attributes (as required) for each account; e. Requires approvals by the SCG President, Program Manager, and IT Director for requests to create information system accounts; f. Creates, enables, modifies, disables, and removes information system accounts in accordance with defined and documented procedures or conditions; g. Monitors the use of information system accounts; h. Notifies account managers: 1. When accounts are no longer required; 2. When users are terminated or transferred; and 3. When individual information system usage or need-to-know changes; i. Authorizes access to the information system based on: 1. A valid access authorization;	Status		Type	
		In Place	X	Common	
		Planned		Hybrid	
		In Place and Planned		System Specific	X
		Not Applicable			

	2. Intended system usage; and 3. Other attributes as required by the organization or associated missions/business functions; j. Reviews accounts for compliance with account management requirements at least annually; and k. Establishes a process for reissuing shared/group account credentials (if deployed) when individuals are removed from the group.	

The Account Manager for the SCG Secure Cloud is the SCG IT Director. The roles and groups in the system are preconfigured and are not altered as a condition of system specific policy. Users access the system only after a form requesting access is completed and approved by the SCG President and executed by the IT Director. The IT Director personally sets up the users for accessing the system. Any modifications to accounts is managed by the IT Director. All terminations of accounts are executed as part of the corporate off boarding procedures by the IT Director. All accounts are reviewed at three (3) month intervals by the IT Director to validate that access is appropriate for the system and any deviations are immediately resolved upon discovery. Shared accounts are not permitted per policy. External parties to SCG are not permitted access to logical components of the system.

AC-2 (1)	**Account System Account Management:** The organization employs automated mechanisms to support the management of information system accounts.	

Status		Type	
In Place	X	Common	
Planned		Hybrid	
In Place and Planned		System Specific	X
Not Applicable			

The Account Manager for the SCG Secure Cloud is the SCG IT Director. SCG uses Active Directory to support the management of SCGSC accounts. Automated mechanisms to manage accounts are implemented as described below for each type of device and operating system.

The following account types are used for all devices and operating systems:

- Active Directory (AD) – Accounts are managed by Windows AD and policies are enforced by GPO.
- Local – Local accounts may be used in cases where AD is not available.

Devices and Operating Systems:

- **Windows** – Managed using AD. See SCG Facility and Systems Access Policies and Procedures, Version 1.6, May 19, 2016 for details on managing accounts.
- **VMware** –VMware vCenter Server, vSM and vCD are currently managed locally.

- **Databases** – Databases are primarily managed using the existing database management system (DBMS)
- **Domain Services (ADDS)**, and only locally using the vendor's local administrative account when Microsoft Windows Active Directory Domain Services (ADDS) is not available, or when emergency or atypical management needs arise, where applicable. Windows Integrated authentication is the default configuration for Microsoft Windows-based databases, unless vendor or applications require Mixed mode authentication, when applicable.

Active Directory is being used within the SCGSC system to automate the management of information system accounts. Accounts contained in Active Directory are joined to groups in accordance with the principle of least privilege.

AC-2 (2)	**Removal of Temporary Emergency Accounts:** The information system does not automatically remove/disable temporary and emergency accounts after any defined time period. The IT Director disables temporary accounts after 180 days or less, while emergency accounts are disabled after 60 days or less.	Status		Type	
		In Place	X	Common	
		Planned		Hybrid	
		In Place and Planned		System Specific	X
		Not Applicable			

Active Directory does not automatically remove or disable temporary and emergency accounts for the SCGSC system. These accounts are manually disabled by the IT Director when the account is inactive or no longer needed. All accounts are retained indefinitely once disabled. Guest, anonymous, or temporary accounts are not allowed inside of the SCGSC, except were explicitly approved by the IT Director when emergency or atypical management needs arise, where applicable, and terminated upon the expiration date specified in the approval.

- **Windows** – Temporary or guest accounts are configured within AD to terminate thirty (30) days from creation so they expire automatically.
- **VMware** – Temporary or guest accounts are not used.
- **Network devices** – Temporary or guest accounts are not used.
- **Databases** – Temporary or guest accounts are not used.

AC-2 (3)	**Disable Inactive Accounts:** The information system does not automatically disable inactive accounts after any time period. The IT Director disables inactive accounts after 30 days.	Status		Type	
		In Place	X	Common	
		Planned		Hybrid	
		In Place and Planned		System Specific	X
		Not Applicable			

Active Directory does not automatically remove or disable temporary and emergency accounts for the SCGSC system. These accounts are manually disabled by the IT Director when the account is no longer needed or active. SCG uses Dumpsec.exe utility to identify SCGSC accounts that have had no activity within the past thirty (30) days so that they can be disabled by the IT Director.

AC-2 (4)	**Automated Audit Actions:** The information system automatically audits account creation, modification, enabling, disabling, and removal actions, and notifies specific personnel or roles.	Status		Type	
		In Place	X	Common	
		Planned		Hybrid	
		In Place and Planned		System Specific	X
		Not Applicable			

All account activities are logged including account creation, modification, disabling, and termination. Logs are monitored and notifications are sent for abnormal activity. The SCGSC information system is configured to automatically audit account creation, modification, enabling, disabling, and removal actions.

The SCGSC system captures an event log that creates entries for all of the identified events in this control. The Windows Event log can be used to demonstrate this control as being satisfied. All logs are retained on the server for two (2) months and then transferred to tape backup in accordance with the AU-2. The IT Director and System Administrator are responsible for ensuring backups are transferred and retained.

AC-3	**Access Enforcement:** The information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies.	Status		Type	
		In Place	X	Common	
		Planned		Hybrid	
		In Place and Planned		System Specific	X
		Not Applicable			

All users must have an account to log into the SCG Secure Cloud environment. Lack of an account being available will result in a denial of access to the information system. Access control is enforced through Windows Active Directory (AD), Group Policy Objects (GPO), and Local Machine Policies. Authorizations for logical access, GPOs and AD are configured and maintained by the IT Director and System Administrators.

AC-4	**Information Flow Enforcement:** The information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems based on organization-defined information flow control policies.	Status		Type	
		In Place	X	Common	
		Planned		Hybrid	
		In Place and Planned		System Specific	X
		Not Applicable			

System Administrators work with the IT Director to determine information flow implementation. Information flow is controlled by: filtering and routing policies on external firewalls and routers and through the use of security permissions; and read, write, execute, etc., permissions assigned to individuals, folders, and/or files and databases through access control lists.

The IT Director defines applicable policy for controlling the flow of information within the system, and where SCG System Administrators work together to apply the necessary information flow implementations. Information flow is logically controlled by:

- Device Configurations
- Filtering
- Routing Policies
- Access Control Lists (ACLs)

The nature of the application is a secure hosting environment, and there are no information flow activities conducted by the technical system. There are no system interconnections in place or required for SCGSC. Networking equipment within the SCGSC environment has configurations that control the flow of data across the network and prevent unauthorized access to data internally from external and internal requests. Allowed and prohibited ports, protocols, services, and functions are identified and approved by the IT Director.

AC-5	**Separation of Duties:** The organization: a. Separates organization-defined duties of individuals; b. Documents separation of duties of individuals; and c. Defines information system access authorizations to support separation of duties.	Status		Type	
		In Place	X	Common	
		Planned		Hybrid	
		In Place and Planned		System Specific	X
		Not Applicable			

Separation of duties is enforced by ensuring that various roles are assigned to different personnel and personnel are not assigned responsibilities intended for other job functions. For example, roles such as administrator, tester, system maintenance personnel, and software developer are carried out by separate individuals, based on "least privilege" principle, who only have access to the systems and tools needed to perform their job.

Within the system, there are roles and groups that govern what users are able to see and do through global security group memberships, specific database permissions and ACLs.

Features and functions of the system only are available to select users based on job function. The assignment of responsibilities in support of network, applications, and systems are split into multiple administrative position categories. Individuals do not have access permissions to devices, systems, and applications outside of their support responsibilities.

To ensure that separation of duties is maintained, the IT Director must approve all personnel who need to fulfill multiple roles, prior to authorization to assume those roles.

Separation of duties is defined as follows:

- IT Director – Read access to system configurations. No write access to system configurations.
- VMware Administrators – Read and write access to VMware including user management and VM administration. No access to other systems.
- Server Administrators – Read and write access to the appropriate information systems only.
- Network Administrators – Read and write access to network devices. No write access to other types of systems.
- Database Administrators – Read and write access to database servers and databases, but not other types of systems.

AC-6	**Least Privilege:** The organization employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users), which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.	Status		Type	
		In Place	X	Common	
		Planned		Hybrid	
		In Place and Planned		System Specific	X
		Not Applicable			

The Windows OS provides a least privilege security model that implements this control. Users are in a group and local machine policies allow for access only to the assets and data that are permissible by these group permissions. SCG System Administrators manage the SCGSC accounts for users and processes acting on behalf of users, including establishment, activation, modification, review, disablement, and removal. User's privileges, permissions, and access are provided, on least privilege principle based on individual's roles and responsibilities or the process's function, by authorized designated System Administrators upon receiving request from the Program Manager or IT Director. User access is restricted through security groups, ACLs, and firewall restrictions.

AC-6 (1)	**Authorize Access to Security Functions:** The organization explicitly authorizes access to security functions (deployed in hardware, software, and firmware) and security-relevant information to include, at a minimum: • Setting/modifying audit logs and auditing behavior; • Setting/modifying boundary protection system rules; • Configuring/modifying access authorizations (i.e., permissions, privileges); • Setting/modifying authentication parameters; and • Setting/modifying system configurations and parameters.	Status		Type	
		In Place	X	Common	
		Planned		Hybrid	
		In Place and Planned		System Specific	X
		Not Applicable			
The Windows OS provides a least privilege security model that implements this control. Users are in a group and local machine policies allow for access only to the assets and data that are permissible by these group permissions. The SCG President is responsible for the approval of all system accounts with privileged access.					

AC-6 (2)	**Non-Privileged Access for Non-Privileged Functions:** The organization requires that users of information system accounts, or roles, with access to non-security functions and information, use non-privileged accounts or roles, when accessing non-security functions. At a minimum, these organization-defined controlled security functions should include: • Setting/modifying audit logs and auditing behavior; • Setting/modifying boundary protection system rules; • Configuring/modifying access authorizations (i.e., permissions, privileges); • Setting/modifying authentication parameters; and • Setting/modifying system configurations and parameters.	Status		Type	
		In Place	X	Common	
		Planned		Hybrid	
		In Place and Planned		System Specific	X
		Not Applicable			
Non-privileged accounts are not supported by the SCG Secure Cloud system. The SCG President is responsible for the approval of all system accounts with privileged access.					

AC-6 (5)	**Privileged Accounts:** The organization restricts privileged accounts on the information system to system administrator and developer roles.	Status		Type	
		In Place	X	Common	
		Planned		Hybrid	
		In Place and Planned		System Specific	X
		Not Applicable			

The Windows OS provides a least privilege security model that implements this control. Users are in a group and local machine policies allow for access only to the assets and data that are permissible by these group permissions. Only authorized individuals are permitted to have privileged access to the SCGSC information system. These individuals receive authorization from the SCG President and are only granted the level of access necessary to perform their job functions. SCG strictly restricts the assignment of privileged accounts to SCGSC to recognized and authorized roles.

AC-6 (9)	**Least Privilege:** The information system audits the execution of privileged functions.	Status		Type	
		In Place	X	Common	
		Planned		Hybrid	
		In Place and Planned		System Specific	X
		Not Applicable			

The SCGSC information system audits the execution of all privileged functions. Audit records are collected by the Kiwi Syslog and made available to the IT Director and authorized system personnel. The Kiwi Syslog provides a centralized record of all accesses or attempts for access to the SCGSC system. The log is periodically reviewed to detect any misuse of privileged functions by the IT Director. Suspicious activity is investigated by the IT Director.

AC-6 (10)	**Prohibit Non-Privileged Users From Executing Privileged Functions:** The information system prevents non-privileged users from executing privileged functions to include disabling, circumventing, or altering implemented security safeguards/countermeasures.	Status		Type	
		In Place	X	Common	
		Planned		Hybrid	
		In Place and Planned		System Specific	X
		Not Applicable			

The SCGSC system has been built to use Role Based Access Control (RBAC) standards. Through the use of Active Directory, users are placed into groups that limit their permission level to only the functions that are necessary for them to perform their duties. Only System Administrators who have been granted access to Active Directory will have the ability to alter the security parameters of the group objects. All IT Director approved modifications to user and group permissions are audited and collected by the Kiwi Syslog. Non-privileged user accounts are not supported. The system also is patched, updated, and scanned for

vulnerabilities on a regular basis to ensure that security flaws leading to the exploitation of system resources are addressed quickly and appropriately.

AC-7	**Unsuccessful Logon Attempts:** The information system: a. Enforces a limit of five consecutive invalid logon attempts by a user: five user/account attempts within 20 minutes; and b. Automatically locks the account/node until released by the System Administrator when the maximum number of unsuccessful attempts is exceeded.

Status		Type	
In Place	X	Common	
Planned		Hybrid	
In Place and Planned		System Specific	X
Not Applicable			

The Windows OS Event Log provides a record of all successful or unsuccessful attempts to access the system. Excessive failed attempts result in locked accounts based on local machine policies that are configured within the Windows OS environment. User accounts are locked after three (3) unsuccessful logon attempts in twenty (20) minutes. The account remains locked until the System Administrator releases the lock. Resetting of the account is done by the IT Director or System Administrator.

AC-8	**System Use Notification:** The information system: a. Displays to users a warning banner before granting access to the system that provides privacy and security notices consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance and states that: • You are accessing a U.S. Government information system, which includes (1) this computer, (2) this computer network, (3) all computers connected to this network, and (4) all devices and storage media attached to this network or to a computer on this network. This information system is provided for U.S. Government-authorized use only. • Unauthorized or improper use of this system may result in disciplinary action, as well as civil and criminal penalties. • By using this information system, you understand and consent to the following: • You have no reasonable expectation of privacy regarding any communication or data transiting or stored on this information system. At any time, and for any lawful

Status		Type	
In Place	X	Common	
Planned		Hybrid	
In Place and Planned		System Specific	X
Not Applicable			

	Government purpose, the government may monitor, intercept, and search and seize any communication or data transiting or stored on this information system. • Any communication or data transiting or stored on this information system may be disclosed or used for any lawful Government purpose. b. Retains the notification message or banner on the screen until users acknowledge the usage conditions and take explicit actions to log on to or further access the information system; and c. For publicly accessible systems: 1. Displays system use information under organization-defined conditions, before granting further access; 2. Displays references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities; and 3. Includes a description of the authorized uses of the system.	
The Customer System Use Notification message banner is not displayed on the Windows Server Operating Systems, storage appliances, and databases; however, the SCGSC System Use message banner is displayed on publicly accessible sites, VMware applications, and security devices within the SCGSC. There is no authentication for the publicly accessible sites within the SCGSC. SCG ensures that system banners are in place where applicable within the SCGSC system. The banner logon screens are configured to clearly identify that an official system is being accessed.		

AC-11	**Session Lock:** The information system: a. Prevents further access to the system by initiating a session lock after [Assignment: organization-defined time period] of inactivity or upon receiving a request from a user; and b. Retains the session lock until the user reestablishes access using established identification and authentication procedures.	

Status		Type	
In Place	X	Common	
Planned		Hybrid	
In Place and Planned		System Specific	X
Not Applicable			

Any session in the SCGSC system is controlled by Kerberos services and uses Microsoft security services that are available from the OS platform, which directly addresses this control. Applications loaded onto the SCGSC platform are required to implement a session lock when users are inactive for thirty (30) minutes.

All SCGSC system components are configured by System Administrators to initiate a session lock after thirty (30) minutes of inactivity or upon receiving a request from a user. Where applicable or specifically requested by customers, the SCGSC limits the number of concurrent sessions to one session.

- **Windows** – Enforced by GPO, concurrent sessions are limited to one session.
- **VMware** – N/A; Concurrent session control is not currently available.
- **Network Devices** – Network devices are used for administration. Network administrators at times require more than one session. Therefore, concurrent sessions are not enforced on network devices.
- **Databases** – N/A; Concurrent session control is not currently available.

AC-11 (1)	**Pattern-Hiding Displays:** The information system conceals, via the session lock, information previously visible on the display with a publicly viewable image.	Status		Type	
		In Place	X	Common	
		Planned		Hybrid	
		In Place and Planned		System Specific	X
		Not Applicable			

Any session in the SCG Secure Cloud system is controlled by Kerberos services and uses Microsoft security services that are available from the OS platform, which directly addresses this control. SCGSC components and servers do not, as a general rule, have display screens. The SCG components are configured by System Administrators to lock after thirty (30) minutes of inactivity and will display a random pattern until user hits keyboard or mouse (desktop/server screen) and will display the login screen when reestablished.

AC-12	**Session Termination:** The information system automatically terminates a user session after conditions or trigger events (as defined in system settings) requiring session disconnect.	Status		Type	
		In Place	X	Common	
		Planned		Hybrid	
		In Place and Planned		System Specific	X
		Not Applicable			

The edge router/firewall is configured by the System Administrators to terminate sessions at stipulated time frames, depending upon the nature of the communications traffic. See Control SC-10. Firewall sessions are terminated after thirty (30) minutes of inactivity. The firewall also terminates sessions that have lost connection and are trying unsuccessfully to reconnect after 10 minutes. The session timeout of the application is set to twenty (20) minutes.

AC-14	**Permitted Actions w/o Identification or Authentication:** The organization: a. Identifies user actions that can be performed on the information system without identification or authentication consistent with organizational missions/business functions; and b. Documents and provides supporting rationale in the security plan for the information system, user actions not requiring identification or authentication.	Status		Type	
		In Place	X	Common	
		Planned		Hybrid	
		In Place and Planned		System Specific	X
		Not Applicable			

All systems and network devices are configured by System Administrators to use a form of authentication and permission levels assigned by the User Role. No actions are permitted without identification or authentication. Users that fail to login to the system will receive notification of the failure, and the failure will be recorded in the audit logs as a failed attempt to authenticate. No other systems are available without identification and authentication. SCGSC system policies do not permit access from unauthenticated users other than the public accessing the front end of the website, which is the means by which the public requests NIDDK publications.

AC-17	**Remote Access:** The organization: a. Establishes and documents usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed (including access to internal networks by VPN); b. Authorizes remote access to the information system prior to allowing such connections; and c. Access to HHS Webmail using personally-owned equipment is authorized. Access to other systems/networks using personally-owned equipment is prohibited without written authorization from the appropriate manager, or an approved policy allowing the use of personally-owned equipment. If the organization allows the use of personally-owned equipment on Department systems or networks: 1. Personally-owned equipment must be scanned before being connected to Department systems or networks to ensure compliance with system requirements (such as patch management requirements); and	Status		Type	
		In Place	X	Common	
		Planned		Hybrid	
		In Place and Planned		System Specific	X
		Not Applicable			

	2. Personally-owned equipment must be prohibited from processing, accessing, or storing Department sensitive information unless it is approved in writing by the SOP and employs FIPS 140-2-compliant encryption capabilities.	

Only one method of remote access, through Windows Remote Desktop Protocol (RDP), is permitted for SCGSC. However, remote access for SCGSC is disabled and only is manually enabled by the System Administrator (by physically accessing the system in the server room) when necessary to allow a developer access to manage the system. All remote access is monitored by the logs compiled in Kiwi Syslog and remote access is limited to just a few specific IP addresses.

AC-17 (1)	**Automated Monitoring/Control:** The information system monitors and controls remote access methods.	Status		Type	
		In Place	X	Common	
		Planned		Hybrid	
		In Place and Planned		System Specific	X
		Not Applicable			

Only one method of remote access, through Windows Remote Desktop Protocol (RDP), is permitted for SCGSC. However, remote access for SCGSC is disabled and only is manually enabled by the system administrator (by physically accessing the system in the server room) when necessary to allow a developer access to manage the system. All remote access is monitored by the logs compiled in Kiwi Syslog and remote access is limited to just a few specific IP addresses.

AC-17 (2)	**Protection of Confidentiality/ Integrity Using Encryption:** The information system implements cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions.	Status		Type	
		In Place	X	Common	
		Planned		Hybrid	
		In Place and Planned		System Specific	X
		Not Applicable			

Only one method of remote access, through Windows Remote Desktop Protocol (RDP), is permitted for SCGSC. However, remote access for SCGSC is disabled and is only manually enabled by the system administrator (by physically accessing the system in the server room) when necessary to allow him to manage the system. All remote access is monitored by the logs compiled in Kiwi Syslog and remote access is limited to just a few specific IP addresses. No cryptographic mechanisms are used to protect the confidentiality of remote sessions because remote access is manually enabled and encryption is not required as there are no live connections through VPN or the Internet; the connection is direct.

AC-17 (3)	**Remote Access:** The information system routes all remote accesses through a single port.	Status		Type	
		In Place	X	Common	
		Planned		Hybrid	
		In Place and Planned		System Specific	X
		Not Applicable			

SCGSC has no direct remote connections from outside of the SCG corporate network. SCGSC administrative access is restricted to originate from within the SCG corporate network. There is only one port (i.e., 3389) to connect remotely to SCGSC and that must be manually enabled by the system administrator by physically accessing the secure SCGSC server room and logging on to enable remote connection.

AC-17 (4)	**Privileged Commands/Access:** The organization: a. Authorizes the execution of privileged commands and access to security-relevant information via remote access only for the System Administrator to manage the SCGSC; and b. Documents the rationale for such access in the security plan for the information system.	Status		Type	
		In Place	X	Common	
		Planned		Hybrid	
		In Place and Planned		System Specific	X
		Not Applicable			

The IT Director is responsible for determining the usage of remote access. In order to provide real-time service support, critical SCG System Administrators are granted remote access in order to perform necessary functions when not being able to work onsite. Remote access users are authenticated to establish remote connections and their access is restricted based on their roles and responsibilities. Remote access to SCGSC is permitted only by approved SCG IT staff and must be manually enabled by the IT Director as needed. Remote access is necessary, because there are no workstations or other means that can be used to access the virtual servers in the SCGSC system.

AC-18	**Wireless Access:** The organization: a. Establishes usage restrictions, configuration/connection requirements, and implementation guidance for wireless access; b. Authorizes wireless access to the information system prior to allowing such connections; and c. The organization ensures that: 1. For organizations that adopt wireless communications, an appropriate manager approves and distributes the overall	Status		Type	
		In Place		Common	
		Planned		Hybrid	
		In Place and Planned		System Specific	X
		Not Applicable	X		

	wireless plan for his or her respective organization; 2. The organization adheres to the HHS Standard for IEEE 802.11 WLAN; and 3. Mobile and wireless devices, systems, and networks are not connected to wired Department networks except through appropriate controls (e.g., VPN port) or unless specific authorization from Department network management has been received.	
There are no wireless access points or devices supported by SCG that provide access to the component systems of SCGSC. Wireless access within SCG's data center facilities is monitored and reviewed quarterly.		

AC-18 (1)	**Authentication and Encryption:** The information system protects wireless access to the system using authentication of users and/or devices and encryption.	Status		Type	
		In Place		Common	
		Planned		Hybrid	
		In Place and Planned		System Specific	X
		Not Applicable	X		
Wireless services are not supported by this system. Therefore, this control is Not Applicable.					

AC-19	**Access Control for Mobile Devices:** The organization: a. Establishes usage restrictions (including prohibiting unapproved software downloads), configuration requirements (including password-protection consistent with the Department's password requirements, up-to-date system patches, current anti-virus software, and functionality that prevents automatic code execution), connection requirements, and implementation guidance for organization-controlled mobile devices; and b. Authorizes the connection of mobile devices to organizational information systems.	Status		Type	
		In Place		Common	
		Planned		Hybrid	
		In Place and Planned		System Specific	X
		Not Applicable	X		
No authorized mobile devices exist within the SCGSC authorization boundary and mobile device access is not supported by this system. Therefore, this control is Not Applicable.					

AC-19 (5)	**Access Control for Mobile Devices:** The organization employs full-device encryption; container encryption to protect the confidentiality and integrity of information on mobile devices.	Status		Type	
		In Place		Common	
		Planned		Hybrid	
		In Place and Planned		System Specific	X
		Not Applicable	X		
No authorized mobile devices exist within the SCGSC authorization boundary and mobile device access is not supported by this system. Therefore, this control is Not Applicable.					

AC-20	**Use of External Information Systems:** The organization establishes terms and conditions, consistent with any trust relationships established with other organizations owning, operating, and/or maintaining external information systems, allowing authorized individuals to: a. Access the information system from external information systems; and b. Process, store, or transmit organization-controlled information using external information systems. Absent an agreement that establishes such terms, conditions, and trust relationships, employees and contractors are not to utilize unauthorized external information systems (such as personal e-mail or personal online storage accounts) to conduct any Department business whatsoever. Authorized external information systems are either federally-owned, contracted for use by the Department, or approved for use pursuant to a Department or device policy.	Status		Type	
		In Place		Common	
		Planned		Hybrid	
		In Place and Planned		System Specific	X
		Not Applicable	X		
There are no external system interconnections in place or planned for this system. In the event that an external information system is integrated within the system, additional steps will be taken by the SCG President and IT Director to ensure that appropriate security measures are in place.					

AC-20 (1)	**Limits On Authorized Use:** The organization permits authorized individuals to use an external information system to access the information system or to process, store, or transmit organization-controlled information only when the organization: a. Verifies the implementation of required security controls on the external system as specified in the organization's information security policy and security plan; or b. Retains approved information system connection or processing agreements with the organizational entity hosting the external information system.	Status		Type	
		In Place		Common	
		Planned		Hybrid	
		In Place and Planned		System Specific	X
		Not Applicable	X		

There are no external system interconnections in place or planned for this system. In the event that an external information system is integrated within the system, additional steps will be taken by the SCG President and IT Director to ensure that appropriate security measures are in place.

AC-20 (2)	**Portable Storage Devices:** The organization prohibits the use of organization-controlled portable storage devices by authorized individuals on external information systems.	Status		Type	
		In Place		Common	
		Planned		Hybrid	
		In Place and Planned		System Specific	X
		Not Applicable	X		

There are no external system interconnections in place or planned for this system. In the event that an external information system is integrated within the system, additional steps will be taken by the SCG President and IT Director to ensure that appropriate security measures are in place.

AC-21	**Information Sharing:** The organization: a. Facilitates information sharing by enabling authorized users to determine whether access authorizations assigned to the sharing partner match the access restrictions on the information for information sharing circumstances where user discretion is required; and b. Employs automated mechanisms or manual processes]to assist users in making information sharing/collaboration decisions.	Status		Type	
		In Place		Common	
		Planned		Hybrid	
		In Place and Planned		System Specific	X
		Not Applicable	X		

SCG prohibits the use of organization-controlled portable storage media such as backup tapes or USB drives to travel from SCGSC systems and servers outside of the corporate control. There are no external system interconnections in place or planned for this system. In the event that an external information system is integrated within the system, additional steps will be taken by the SCG President and IT Director to ensure that appropriate security measures are in place including the requirement for FIPS 140-2 encryption capability on the device.

AC-22	**Publicly Accessible Content:** The organization: a. Designates individuals authorized to post information onto a publicly accessible information system; b. Trains authorized individuals to ensure that publicly accessible information does not contain nonpublic information; c. Reviews the proposed content of information prior to posting onto the publicly accessible information system to ensure that nonpublic information is not included; and d. Reviews the content on the publicly accessible information system for nonpublic information biweekly and removes such information, if discovered.	Status		Type	
		In Place	X	Common	
		Planned		Hybrid	
		In Place and Planned		System Specific	X
		Not Applicable			

Publicly accessible content is managed by authorized SCGSC web developers through the application back end network. To ensure no nonpublic content is posted on the sites, the content is reviewed by the developers and NIDDK and must be approved by NIDDK before content is deployed to the site. The NIDDK Catalog Site is a publicly accessible site that allows users to order health-related materials on various topics, including diabetes, digestive diseases, and kidney diseases. The information collected from users who request materials (name, address, phone number, etc.) is temporarily stored in a database, and only some of this information is imported into the Camelot system along with the requested publication ordered via the Catalog site. The database is purged every 30 days removing all information. No information is disseminated from the Catalog site. The Clearinghouse sites are hosted by NIDDK and not the SCGSC. Only the development sites that allow SCG to make changes to the Clearinghouse site content are in the SCGSC. No information is disseminated from the development sites. All changes are reviewed by NIDDK before they are deployed to the staging server hosted by NIDDK. The Materials Development Tracking System (MTDS or MatDev) is a SharePoint application hosted by SCGSC that is publicly accessible to those users who are granted access with proper login credentials. These users are NIDDK staff and SCG staff who receive appropriate training to ensure that nonpublic information is not deployed to the NIDDK hosted Clearinghouse sites.

5. Awareness and Training (AT)

The status of awareness and training controls for the SCG Secure Cloud system is as indicated in the following table:

<table>
<tr><th>Control Number</th><th>Description of Control</th><th>Control Status/Type</th></tr>
<tr><td>AT-1</td><td>Security Awareness and Training Policy and Procedures: The organization:
a. Develops, documents, and disseminates to the IT staff members who have access to the SCGSC system:
1. A security awareness and training policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
2. Procedures to facilitate the implementation of the security awareness and training policy and associated security awareness and training controls; and
b. Reviews and updates the current:
1. Security awareness and training policy at least once annually; and
2. Security awareness and training procedures at least once annually.</td><td><table>
<tr><th>Status</th><th></th><th>Type</th><th></th></tr>
<tr><td>In Place</td><td>X</td><td>Common</td><td>X</td></tr>
<tr><td>Planned</td><td></td><td>Hybrid</td><td></td></tr>
<tr><td>In Place and Planned</td><td></td><td>System Specific</td><td></td></tr>
<tr><td>Not Applicable</td><td></td><td colspan="2"></td></tr>
</table></td></tr>
<tr><td colspan="3">The SCGSC Security Awareness and Training Policy and Procedures addresses the requirements and mechanisms to be implemented across SCGSC’s operating environment. At a high level, this policy addresses the purpose, scope, roles and responsibilities, management commitment, coordination among organizational entities, and requirements to comply with security awareness and training. Additionally, this policy outlines requirements to manage and protect all company and NIH information, including low and moderately sensitive information. The policy is consistent with SCG’s mission and functions with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.

It is the responsibility of SCG President, Vice President of Administration, and the Information Technology (IT) Director to develop, disseminate, and annually review/update the SCG Security Awareness Training Policy and Procedures. The IT Director or designee disseminates the policy to all Privileged Users by emailing a link to the SCG Intranet location prior to authorizing privileged user status. The IT Director requests a response email from the Privileged User, confirming that Privileged User has read and understands the document.</td></tr>
</table>

The policy and procedures are located on the SCG Intranet that is available to all SCG personnel at http://web-dev/intranet-sql. The intranet server is located in the Gaithersburg facility at 656 Quince Orchard Road, Gaithersburg, MD 20878.

SCGSC **Awareness and Training Policy and Procedures** facilitates the implementation of the Awareness and Training policy and associated security controls and is updated as necessary to reflect any modifications.

Artifacts of Compliance:

- SCGSC Security Awareness and Training Policy and Procedures

AT-2	**Security Awareness Training:** The organization provides basic security awareness training to information system users (including managers, senior executives, and contractors): a. As part of initial training for new users; b. When required by information system changes; and c. Annually thereafter.

Status		Type	
In Place	X	Common	X
Planned		Hybrid	
In Place and Planned		System Specific	
Not Applicable			

All SCG staff working on the SCG Secure Cloud system are required to complete the NIH Security Awareness and the NIH Privacy Awareness courses as well as the Information Security and Privacy Awareness annual refresher course annually. Staff members obtain certificates upon completion of the training, which are kept on file by the SCG Program Manager. Additional training may be deemed necessary for specific SCG IT staff members. For example, the System Administrators are required to complete the HHS Information Security for IT Administrators course. SCG IT staff who have roles and responsibilities associated with incident response and disaster recover for the SCGSC must participate in TT&E events annually and as scheduled by the IT Director.

SCG provides basic security awareness training to all its employees (including managers, senior executives) as part of initial training for new users, when required by system changes, and annually thereafter. This training is delivered by the NIH Security Awareness and the NIH Privacy Awareness program. It is the responsibility of the SCG Program Manager to ensure that all individuals complete security awareness training and to consider the completion of the training during the annual performance review process.

Security Awareness Courses:

- NIH Privacy Awareness
- NIH Information Security for Administrators
- NIH FDCC System Administrator Training
- NIH Securing for Remote Computers
- NIH Information Security and Privacy Awareness Refresher
- SCG Secure Cloud Technical Training

AT-2 (2)	**Insider Threat:** The organization includes either in its annual security awareness training or in other annual supplemental training (such as a counterintelligence awareness course), information on recognizing and reporting potential indicators of insider threat, such as: inordinate, long-term job dissatisfaction, attempts to gain access to information not required for job performance, unexplained access to financial resources, bullying or sexual harassment of fellow employees, workplace violence, and other serious violations of organizational policies, procedures, directives, rules, or practices. Security awareness training includes how to communicate employee and management concerns regarding potential indicators of insider threat through appropriate organizational channels in accordance with established organizational policies and procedures.	Status		Type	
		In Place	X	Common	X
		Planned		Hybrid	
		In Place and Planned		System Specific	
		Not Applicable			

The NIH Information Security Awareness training course taken by the SCG personnel who have access to the SCGSC addresses internal as well as external threats, and includes training on recognizing and reporting potential indicators of insider threat.

AT-3	**Role-Based Security Training:** The organization provides role-based security training to personnel with assigned security roles and responsibilities: a. Before authorizing access to the information system or performing assigned duties; b. When required by system changes; and c. Within three (3) months of entering a position that requires role-specific training, and at least once annually thereafter.	Status		Type	
		In Place	X	Common	X
		Planned		Hybrid	
		In Place and Planned		System Specific	
		Not Applicable			

SCG requires personnel assigned security roles and responsibilities for the SCGSC system to complete the appropriate HHS' role-based training course. HHS offers Information Security for Executives, Information Security for IT Administrators, and Information Security for Managers (http://www.hhs.gov/ocio/securityprivacy/awarenesstraining/awarenesstraining.html#).

Per the SCGSC **Security Awareness and Training Policy and Procedures**, additional training is appropriate for employees with specific obligations towards information security that are not satisfied by basic security awareness, for example information security management, security administration, site security, and IT personnel. The particular training

requirements will reflect workers' relevant prior experience, training and/or professional qualifications, as well as job needs.

AT-4	**Security Training Records:** The organization: a. Documents and monitors individual information system security training activities including basic security awareness training and specific information system security training; and b. Retains individual training records for 3 years or the life of the contract, whichever is longer.	Status: In Place X; Planned; In Place and Planned; Not Applicable Type: Common X; Hybrid; System Specific
Certificates of completion for all security and privacy awareness courses completed by SCG personnel who have access to the SCGSC, as well as signed Confidentiality Agreements, are kept on file by the Program Manager. Documentation for other training, such as TT&E events for incident response and disaster recovery will be created and maintained by the IT Director. The documentation for specialized training will include the training completed, the date of completion, and the names of each individual who completed the specialized training.		

6. Audit and Accountability (AU)

The status of audit and accountability controls for the SCGSC system is as indicated in the following table:

Control Number	Description of Control	Control Status/Type
AU-1	**Audit and Accountability Policy and Procedures:** The organization: a. Develops, documents, and disseminates to SCG employees with user accounts for the SCGSC system: 1. An audit and accountability policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the audit and accountability policy and associated audit and accountability controls; and	Status: In Place X; Planned; In Place and Planned; Not Applicable Type: Common; Hybrid; System Specific X

	b. Reviews and, if necessary, updates the current: 1. Audit and accountability policy at least once annually; and 2. Audit and accountability procedures at least once annually.	

The SCGSC **Audit and Accountability Procedures** addresses the requirements and mechanisms to be implemented across SCGSC's operating environment. At a high level, this policy addresses the purpose, scope, roles and responsibilities, management commitment, coordination among organizational entities, and requirements to comply with auditing and accountability. The policy describes the mandates for log retention, review, and analysis. Areas covered include minimum log requirements, responsibilities, alert review, problem management, retention, security and protection of logs, and compliance review. The policy is consistent with SCG's mission, and functions with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.

It is the responsibility of the SCG President, Vice President of Administration, and the Information Technology (IT) Director to develop, disseminate, and annually review/update the SCGSC **Audit and Accountability Procedures**. The IT Director disseminates the document to all Privileged Users by emailing a link to the document's SCG Intranet location prior to authorizing privileged user status. The IT Director or Program Manager requests a response email from the Privileged User, confirming that Privileged User has read and understands the document.

The policy and procedures are located on the SCG Intranet that is available to all SCG personnel at http://web-dev/intranet-sql. The intranet server is located in the Gaithersburg facility at 656 Quince Orchard Road, Gaithersburg, MD 20878.

AU-2	**Audit Events:** The organization: a. Determines that the information system is capable of auditing the following events: • Server alerts and error messages • User log-on and log-off (successful or unsuccessful) • System administration activities; • Modification of privileges and access • Start up and shut down • Modifications to the application • Application alerts and error messages • Configuration changes • Account creation, modification, or deletion • (Moderate and High only) Read access to sensitive information	

Status		Type	
In Place	X	Common	
Planned		Hybrid	
In Place and Planned		System Specific	X
Not Applicable			

	• (Moderate and High only) Modification to sensitive information • (Moderate and High only) Printing sensitive information b. Coordinates the security audit function with other organizational entities requiring audit-related information to enhance mutual support and to help guide the selection of auditable events; c. Provides a rationale for why the auditable events are deemed to be adequate to support after-the-fact investigations of security incidents; and d. Determines that the following events are to be audited within the information system at least weekly: • Unsuccessful log-on attempts that result in a locked account/node; • Configuration changes; • Application alerts and error messages; • System administration activities; • Modification of privileges and access; and • Account creation, modification, or deletion.	

SCG has identified auditable events to be logged for the SCGSC system. These events are identified in the **Audit and Accountability Policy and Procedures** document. Audit logs will be reviewed on a weekly basis by the IT Director. SCG has selected the auditable events based on best practices and expert knowledge and experience managing the risks associated with systems similar to the SCGSC. Any events or issues that are identified in the environment are immediately communicated to the System Owner and the Program Manager 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 following events must be identified within server audit logs:

- Server startup and shutdown
- Loading and unloading of services
- Installation and removal of software
- System alerts and error messages
- User logon and logoff
- Windows Local Policy logon, access, or modification
- System administration activities
- Attempted and successful accesses to sensitive information, files, and systems
- Account creation, modification, or deletion

- Modifications of privileges and access controls

The following events must be identified within application and database audit logs:

- Modifications to the application
- Application alerts and error messages
- User logon and logoff
- System administration activities
- Accesses to information and files
- Account creation, modification, or deletion
- Modifications of privileges and access controls

AU-2 (3)	**Auditable Events:** The organization reviews and, if necessary, updates the list of audited events annually and whenever there is a significant system modification.	Status		Type	
		In Place	X	Common	
		Planned		Hybrid	
		In Place and Planned		System Specific	X
		Not Applicable			

The IT Director reviews and updates the list of audited events annually and whenever there is a significant system modification. Any events or issues that are identified in reviewing event logs are immediately communicated to the System Owner and the Program Manager 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 also has an **Operations and Maintenance Plan** that is used to govern the review functions for the system.

AU-3	**Content of Audit Records:** The information system generates audit records containing information that establishes what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any individuals or subjects associated with the event.	Status		Type	
		In Place	X	Common	
		Planned		Hybrid	
		In Place and Planned		System Specific	X
		Not Applicable			

At a minimum, the following elements are identified in each audit record:

- Date and time when the event occurred
- Software or hardware component of the SCGSC system where the event occurred
- Source of the event (e.g., Windows security auditing, servicing, security Kerberos)
- Type of event that occurred
- Subject identity (e.g., user, device)
- The outcome (i.e., success or failure) of the event

AU-3 (1)	**Content of Audit Records:** The information system generates audit records containing the following additional information: name of the accessed file, program or command used to initiate the event, and source and destination address.	Status		Type	
		In Place	X	Common	
		Planned		Hybrid	
		In Place and Planned		System Specific	X
		Not Applicable			

There are no identified audit demands for the SCGSC at the file level. However, the following elements are identified within the server audit record: (1) Application—access and failure of an application; (2) Security—successful logons and failed logon attempts; (3) Setup—installation and removal of programs; and (4) System—configuration changes in Windows.

AU-4	**Audit Storage Capacity:** The organization allocates audit record storage capacity in accordance with parameters defined by the IT Director.	Status		Type	
		In Place	X	Common	
		Planned		Hybrid	
		In Place and Planned		System Specific	X
		Not Applicable			

The SCG IT Staff 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 SCGSC system allocates audit record storage capacity to prevent such capacity being exceeded. The audit storage capacity for the SCGSC server is set at 100 times the default for the application (default = 2 Mb), security (default = 89 Mb), setup (default = 1 Mb), and system (default = 3 Mb) logs (a total of 9.5 Gb storage capacity for the server audit records). The audit storage capacity allocated for the Kiwi Syslog centralized audit records is a minimum of 30 Gb.

AU-5	**Response to Audit Processing Failures:** The information system: a. Alerts the IT Director in the event of an audit processing failure; and b. Takes additional actions (e.g., halting the system in the event of a security log processing failure).	Status		Type	
		In Place	X	Common	
		Planned		Hybrid	
		In Place and Planned		System Specific	X
		Not Applicable			

All incidents, including audit failures, are managed in accordance with the system's **Incident Response Plan**. It should not be necessary to shut down the system because there should always be a minimum of 30Gb for storage, which should last at least 60 days.

The SCGSC system automatically alerts the IT Director in the event of an audit failure or when audit capacity is 12% remaining. This alert is distributed by email. The system also signals this by an audible alarm. The IT Director then ensures the audit logs are backed up and clears the audit logs to free up capacity.

In the event that a local log file capacity is reached, older log entries are removed automatically to allow new entries to be posted, as logs are backed up to tape. When alerted of an audit processing issue or failure, the notified System Administrator remediates the issue, which includes:

- Placing the device in a separate isolated subnet
- Disconnecting the device from the network
- Shutting down the corresponding application
- Shutting down the device

Active Directory GPOs used by SCG invoke a system shutdown in the event of an audit failure (where possible), unless an alternative audit capability exists. Additionally, the SCG practice for this control focuses on component system availability over log preservation, and all applicable SCGSC system components are configured to overwrite the oldest audit records instead of shutting down on moderate impact systems.

AU-5 (2)	**Response to Audit Processing Failures:** The information system provides an alert in [Assignment: organization-defined real-time period] to [Assignment: organization-defined personnel; roles; and/or locations] when the following audit failure events occur: [Assignment: organization-defined audit failure events requiring real-time alerts].	Status		Type	
		In Place	X	Common	
		Planned		Hybrid	
		In Place and Planned		System Specific	X
		Not Applicable			

SCGSC System Administrators configure the Kiwi Syslog server alarm thresholds to notify by email if a minimum or maximum threshold is exceeded. The email message is sent to all the recipients in the "Alarm notification" list (set from the email options).

The email message states the alarm message, the threshold exceeded, the current threshold value, etc.

AU-6	**Audit Review, Analysis, and Reporting:** The organization: a. Reviews and analyzes information system audit records weekly for indications of inappropriate or unusual activity; and b. Reports findings to the System Owner and Program Manager.	

Status		Type	
In Place	X	Common	
Planned		Hybrid	
In Place and Planned		System Specific	X
Not Applicable			

The SCG Secure Cloud system is managed in accordance with the **Operation and Maintenance Plan**, which does require weekly review of audit logs and any actions are managed in accordance with the on file **Incident Response Plan** or **Contingency Plan**.

Audit logs for SCGSC are reviewed and analyzed weekly for the following:
(1) indications of inappropriate or unusual activity
(2) assurance that logging is functioning properly
(3) adherence to logging standards identified in this procedure.

The following review and analysis requirements must be adhered to:

- All logs will be correlated using Kiwi Syslog and examined weekly to determine if any incidents have occurred.
- The level of audit review, analysis, and reporting must be adjusted if there is an increase in risk to SCGSC.

All staff involved with log management responsibilities must be trained on how to review and analyze audit logs, and how to report incidents when applicable. Findings should be reported to the SCG President, Vice President of Administration, and Program Manager.

AU-6 (1)	**Process Integration:** The organization employs automated mechanisms to integrate audit review, analysis, and reporting processes to support organizational processes for investigation and response to suspicious activities.	

Status		Type	
In Place	X	Common	
Planned		Hybrid	
In Place and Planned		System Specific	X
Not Applicable			

The SCGSC system's logs are collected by the Kiwi Syslog. Reports are generated and reviewed monthly. SCG uses Kiwi Syslog to collate log files for audit review and analysis, System Administrators are given access to their system and database log files for review. These reviews are in the interest of identifying any suspicious activity found in log files. In the event that suspicious activity is found, the information is reported and an incident logged with the IT Director. Incidents are further elevated and managed according to the incident reporting policies for the system.

AU-6 (3)	**Correlate Audit Repositories:** The organization analyzes and correlates audit records across different repositories to gain organization-wide situational awareness	Status		Type	
		In Place	X	Common	
		Planned		Hybrid	
		In Place and Planned		System Specific	X
		Not Applicable			

Data correlation is done manually by the IT Director through log reviews that allow for a situation report to be accomplished.

AU-7	**Audit Reduction and Report Generation:** The information system provides an audit reduction and report generation capability that: a. Supports on-demand audit review, analysis, and reporting requirements and after-the-fact investigations of security incidents; and b. Does not alter the original content or time ordering of audit records.	Status		Type	
		In Place	X	Common	
		Planned		Hybrid	
		In Place and Planned		System Specific	X
		Not Applicable			

Kiwi Syslog is used by SCG for audit reduction and report generation capability. It is capable of providing an audit reduction and report generation capability to support near real-time audit review, analysis, and reporting requirements described in AU-6 and after-the-fact investigations of security incidents. Kiwi Syslog does not alter the original audit record and is capable of extracting useful and readable data for the review process. Kiwi Syslog has tools to filter audit logs and generate reports to help reduce the amount of information contained in audit records and distill useful information. It has query applications that have the ability to query an audit log by username, location, application name, date, and time, or other applicable parameters; and the ability to execute reports with the results of the query. It has the capability to automatically process audit records for events of interest based on selectable event criteria.

The SCGSC system's logs are collected by the Kiwi Syslog. Reports are generated and reviewed monthly by the IT Director.

AU-7 (1)	**Audit Reduction and Report Generation:** The information system provides the capability to process audit records for events of interest based on specific audit fields (e.g., identities of individuals, event types, event locations, event times, event dates etc.) within audit records.	Status		Type	
		In Place	X	Common	
		Planned		Hybrid	
		In Place and Planned		System Specific	X
		Not Applicable			

Audit records are centralized using Kiwi Syslog, which provides the capability to process audit records for events of interest based on specific audit fields within audit records. Kiwi Syslog allows customized reporting features based on specific fields of interest.

The following reports can be generated:

- Authentication and Authorization Reports
- Network Activity Reports
- Resource Access Reports
- Failure and Critical Error Reports

The Kiwi Syslog Manual defines what attributes can be selected and what granularity criteria can be specified during Auditor Reporting.

AU-8	**Time Stamps:** The information system: a. Uses internal system clocks to generate time stamps for audit records; and b. Records time stamps for audit records that can be mapped to Coordinated Universal Time (UTC) or Greenwich Mean Time (GMT) and meets the granularity of time measurement required.	Status / Type

Status		Type	
In Place	X	Common	
Planned		Hybrid	
In Place and Planned		System Specific	X
Not Applicable			

The SCGSC system uses an internal system clock to generate time stamps for audit records. Time stamps generated by the system include both the date and time. The time is expressed in Coordinated Universal Time (UTC) to the nearest second. System Administrators are responsible for ensuring the internal time clocks are configured.

The Windows Time service, also known as W32Time, synchronizes the date and time for all computers running in the SCGSC system. The Windows Time service uses the Network Time Protocol (NTP) to synchronize computer clocks on the network so that an accurate clock value, or time stamp, can be assigned to network validation and resource access requests. The service integrates NTP and time providers, making it a reliable and scalable time service for the System Administrator.

AU-8 (1)	**Synchronization with Authoritative Time Source:** The information system: a. Compares the internal information system clocks at least quarterly with one or more of the federally-maintained Network Time Protocol (NTP) stratum 1 servers from either NIST (http://tycho.usno.navy.mil/ntp.html); and b. Synchronizes the internal system clocks to the authoritative time source when the time difference is greater than a time period threshold specified by the IT Director.	Status / Type

Status		Type	
In Place	X	Common	
Planned		Hybrid	
In Place and Planned		System Specific	X
Not Applicable			

NTP is configured such that the SCFSMO server synchronizes with NIST's time server (time-a.nist.gov, time-b.nist.gov, and time-c.nist.gov) every 1024 seconds. The other servers synchronize to the authoritative time source, SCFSMO. The threshold for time

difference is set to 5 minutes (default). System Administrators are responsible for comparing the internal information system clocks at least quarterly.

The SCGSC SCSQL-PROD server compares the internal information system clock every 7 days and it synchronizes the SCGSC system time to the nearest second to time.windows.com, an external authoritative time source. The internal system clock synchronizes to the authoritative time source when the time difference is greater than 1 second.

AU-9	**Protection of Audit Information:** The information system protects audit information and audit tools from unauthorized access, modification, and deletion.	Status		Type	
		In Place	X	Common	
		Planned		Hybrid	
		In Place and Planned		System Specific	X
		Not Applicable			

The SCGSC system protects audit information and audit tools from unauthorized access, modification, and deletion. The audit data for the SCGSC system is accessible only by privileged users, and the windows local machine policies enforce this protection. Audit logs cannot be modified, which ensures audit information integrity. Only the Domain Administrator can clear logs, and accidental or deliberate deleting of logs can be investigated and confirmed through review of system tape backups.

AU-9 (4)	**Access by Subset of Privileged Users:** The organization authorizes access to management of audit functionality to only the Domain Administrators.	Status		Type	
		In Place	X	Common	
		Planned		Hybrid	
		In Place and Planned		System Specific	X
		Not Applicable			

The Domain Administrators are the only privileged users who can access and modify audit configuration settings for the SCGSC system. This is enforced through Windows Local Policy settings, and access level in the firewall enforces this protection. Audit logs track changes in audit configuration settings to protect against accidental and deliberate tampering with audit configuration settings and audit data and records.

AU-11	**Audit Record Retention:** The organization employs measures to ensure that long-term audit records generated by the information system can be retrieved.	Status		Type	
		In Place	X	Common	
		Planned		Hybrid	
		In Place and Planned		System Specific	X
		Not Applicable			

Audit logs are retained to provide support for after-the-fact investigations of IT security incidents for SCGSC and to meet SCG and government information retention requirements. These logs include system, application, and database-level audit logs and logs for network devices.

All audit logs for the SCGSC system are retained for a period of three (3) years in accordance with SCG retention requirements. The most recent sixty (60) days of log files are stored online and the remaining time they are stored as tape backups. Audit logs are archived on monthly backup tapes and stored in a fire safe in the IT Director's office.

AU-12	**Audit Generation:** The information system: a. Provides audit record generation capability for the auditable events defined in AU-2 (d) for the information system components identified by the IT Director; b. Allows the Domain Administrators to select which auditable events are to be audited by specific components of the information system; and c. Generates audit records for the events defined in AU-2 (d) with the content defined in AU-3.	Status		Type	
		In Place	X	Common	
		Planned		Hybrid	
		In Place and Planned		System Specific	X
		Not Applicable			

Audit logs are retained for a minimum of three (3) years. The information system provides audit record generation capability for the list of auditable events defined in AU-2 on the servers and system components. SCG uses Kiwi Syslog to compile audit records in a centralized location. The time stamp on all audit records for components is consistent within the system as all components are synchronized simultaneously to the same external time source. All audit records are stored in Coordinated Universal Time (UTC) format.

7. Security Assessment and Authorization (CA)

The status of security assessment and authorization controls for the SCGSC system is as indicated in the following table:

Control Number	Description of Control	Control Status/Type
CA-1	**Security Assessment and Authorization Policies and Procedures:** The organization: a. Develops, documents, and disseminates to personnel/roles as designated by the IT Director: 1. A security assessment and authorization policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the security assessment and authorization policy and associated security assessment and authorization controls; and b. Reviews and, if necessary, updates the current: 1. Security assessment and authorization policy at least annually; and 2. Security assessment and authorization procedures at least annually.	

Status		Type	
In Place	X	Common	
Planned		Hybrid	
In Place and Planned		System Specific	X
Not Applicable			

The SCGSC **System Design Document v1.4**, May 19, 2016, establishes the policy for implementing security assessment and authorization of the SCGSC environment. At a high level, this policy addresses the purpose, scope, roles and responsibilities, management commitment, coordination among organizational entities, and requirements to comply with security awareness and training. The policy delineates the requirements of SCG personnel to apply the security controls in line with those specified in the Facility and Systems Access Policy and Procedures v1.6 and NIST SP 800-53 Rev.4, pursue Assessment & Authorization (A&A) when required to, and to obtain an Authorization to Operate (ATO) and re-accreditation as required.

The SCGSC System Design Document establishes roles and responsibilities in the A&A process and necessitates all documentation required for a successful accreditations application. The policy is consistent with SCG's mission, and functions with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.

It is the responsibility of SCG President, Vice President of Administration, and Information Technology (IT) Director to develop, disseminate, and annually review/update the SCG System Design Document. The IT Director disseminates the policy to all Privileged Users by emailing a link to the document's SCG Intranet location prior to authorizing privileged user status. The IT Director or Program Manager requests a response email from the Privileged User, confirming that Privileged User has read and understands the document.

The System Design Document is located on the SCG Intranet that is available to all SCG personnel at: http://web-dev/intranet-sql. The intranet server is located in the Gaithersburg facility at 656 Quince Orchard Road, Gaithersburg, MD 20878.

CA-2	**Security Assessments:** The organization: a. Develops a security assessment plan that describes the scope of the assessment including: 1. Security controls and control enhancements under assessment; 2. Assessment procedures to be used to determine security control effectiveness; and 3. Assessment environment, assessment team, and assessment roles and responsibilities; b. Assesses the security controls in the information system and its environment of operation within the scope of the assessment plan, as defined by the AO or their representative, to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting established security requirements; c. Produces a security assessment report that documents the results of the assessment; and d. Provides the results of the security control assessment to the SCG President, Vice President of Administration, IT Director, Program Manager, and ISSO.	Status		Type	
		In Place	X	Common	
		Planned		Hybrid	
		In Place and Planned		System Specific	X
		Not Applicable			

SCGSC is built to comply with the Federal Information Security Management Act (FISMA) and adheres to the FISMA Assessment and Authorization program for its Security and Privacy compliance activities. SCG has contracted a Third Party Assessment Organization (3PAO) to develop a compliant SAP that includes a list of the controls and control enhancements relevant to the assessment. This list is taken from the NIST Special Publication 800-53 Rev.4, Recommended Security Controls for Federal Information Systems and Organizations, and it is maintained, updated, and published by the NIH Program Management Office (PMO) as the FISMA Security Controls.

CA-2 (1)	**Independent Assessors:** The organization employs SCG-defined parameters (e.g., impartial, credible, IT security and audit certification experience, specialized IT certification experience and capability) of independence for assessors or assessment teams to conduct security control assessments.	Status		Type	
		In Place	X	Common	
		Planned		Hybrid	
		In Place and Planned		System Specific	X
		Not Applicable			

SCG has contracted with a Third Party Assessment Organization (3PAO) to conduct an annual assessment of the security controls that apply to the SCGSC system and environment in accordance with FISMA requirements. If controls are found not implemented or not operating as intended during the assessment, control deficiencies are documented as Plan of Action and Milestones (POA&M) items. The POA&M items document the schedules and resources allocated to address the deficiencies until issue closure.

CA-3

System Interconnections: The organization:

a. Authorizes connections from the information system to other information systems through the use of Interconnection Security Agreements (ISAs) or data sharing agreements;
b. Documents, for each interconnection, the interface characteristics, security requirements, and the nature of the information communicated; and
c. Reviews and, if necessary, updates ISAs at least every year and whenever significant changes (that can affect the security state of the information system) are implemented that could impact the validity of the agreement.

The organization also considers the following actions:

- Obtain written authorization from management (e.g., AO or designated representative) before connecting to other information systems.
- Consider that the terms and conditions of an ISA or data sharing agreement do not conflict with or otherwise contradict Department IT security and privacy policies, procedures, controls, and standards; applicable legislation, regulation, or guidance; or other contractual obligations.
- Ensure that system interconnection channels are securely configured commensurate with the confidentiality and integrity of the data being exchanged.
- Obtain authorization from the external System Owner if the Department intends to use, modify, or disclose the external system's information in a manner not authorized by the agreement.

Status		Type	
In Place		Common	
Planned		Hybrid	
In Place and Planned		System Specific	X
Not Applicable	X		

Not applicable: Currently, no connections from the SCGSC System to other information systems exist.

CA-3 (5)	**System Interconnections:** The organization employs a deny-all, permit-by-exception (i.e., whitelisting) policy for allowing SCGSC to connect to external information systems.	Status		Type	
		In Place		Common	
		Planned		Hybrid	
		In Place and Planned		System Specific	X
		Not Applicable	X		

Not applicable: Currently, no connections from SCGSC System to other information systems exist.

CA-5	**Plan of Action and Milestones:** The organization: a. Develops a plan of action and milestones (POA&M) in accordance with the HHS Standard for Plans of Action and Milestones (POA&M) Management and Reporting for the information system to document the organization's planned remedial actions to correct weaknesses or deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities in the system; and b. Updates existing POA&Ms at least quarterly based on the findings from security controls assessments, security impact analyses, and continuous monitoring activities.	Status		Type	
		In Place	X	Common	
		Planned		Hybrid	
		In Place and Planned		System Specific	X
		Not Applicable			

The IT Director has created a Plan of Action and Milestones (POA&M) for SCGSC that documents SCG planned actions to correct any weaknesses, deficiencies, or vulnerabilities discovered during the assessment of the security controls and to reduce or eliminate known vulnerabilities in the system.

The SCG IT Director maintains the POA&M, updating it as a result of system configuration changes or as flaws or vulnerabilities are detected, and delivers it to the NIH for a monthly review.

Controls SI-2, SI-2(3), and RA-5d establish timeframes for remediation of flaws when found in Other Equipment Manufacturer (OEM) applications or firmware: thirty (30) days for Critical and High rated findings and ninety (90) days for Moderate. The IT Director must perform risk mitigation efforts that may include, but are not limited to patching, disabling, or replacing component/software; updating firmware (for devices); changing settings or configurations per vendor instructions, etc.; and documenting actions within the POA&M until full remediation can be implemented.

The IT Director and System Administrators develop a mitigation/risk acceptance strategy to identify the system weakness, pursue remediation efforts (provide a rationale for mitigation in lieu of remediation if needed), and document the risk mitigating factors employed. The IT Director also reports vulnerability information to SCG management and to the NIH ISSO.

The IT Director communicates the results of these activities to the NIH ISSO and ensures all parties fully understand the issues and risks, with the goal that the NIH will approve the mitigation strategy and accept the residual risk.

The IT Director updates the SCGSC POA&M monthly based on the findings from security control assessments (including annual assessments), security impact analyses, corrective actions, and continuous monitoring activities (such as auditing controls, vulnerability and baseline scans).

CA-6	**Security Authorization:** The organization: a. Assigns a senior-level executive or manager as the authorizing official for the information system; b. Ensures that the authorizing official authorizes the information system for processing before commencing operations; and c. Updates the security authorization every three (3) years or when there is a significant change to the system (defined as significant change that is likely to affect the security state of that information system)[1].	Status		Type	
		In Place	X	Common	
		Planned		Hybrid	
		In Place and Planned		System Specific	X
		Not Applicable			

The NIH Authorizing Official (AO) (i.e., organizational officials or senior executive management) will sign and authorize/accredit the system for processing.
Through the security and authorization process, authorizing officials are accountable for the security risk associated with information system operations. Once achieved, the authorization must be updated and re-approved every 3 years at a minimum, or when a significant change occurs to the environment and/or applications. Chandan Sastry is the AO/DAA for the SCG Secure Cloud system. The security authorization will be updated annually.

CA-7	**Continuous Monitoring:** The organization develops a continuous monitoring strategy and implements a continuous monitoring program that includes: a. Establishment of specific metrics to be monitored based on SCGSC security goals and objectives and in accordance with the basic requirements set forth in NIST SP 800-137; b. Establishment of defined frequencies for monitoring and defined frequencies for assessments based on SCGSC security goals and objectives supporting such monitoring;	Status		Type	
		In Place	X	Common	
		Planned		Hybrid	
		In Place and Planned		System Specific	X
		Not Applicable			

[1] Examples of such changes are provided in NIST SP 800-37, Section F.4 “Ongoing Authorization.”

	c. Ongoing security control assessments in accordance with the SCGSC-specific continuous monitoring strategy; d. Ongoing security status monitoring of organization-defined metrics in accordance with the SCGSC-specific continuous monitoring strategy; e. Correlation and analysis of security-related information generated by assessments and monitoring; f. Response actions to address results of the analysis of security-related information; and g. Reporting the security status of the organization and the information system to appropriate personnel or roles as designated by the President, IT Director, and Program Manager.	
SCG employs Symantec Endpoint Protection Suite Enterprise 2015 to continuously monitor the SCG Secure Cloud system. In addition, monthly vulnerability assessments of the system will be performed by the IT Director.		

CA-7 (1)	**Independent Assessment:** The organization employs assessors or assessment teams with appropriate parameters of independence to monitor the security controls in the information system on an ongoing basis.	Status		Type	
		In Place	X	Common	
		Planned		Hybrid	
		In Place and Planned		System Specific	X
		Not Applicable			
SCG has contracted with an accredited independent assessor to perform independent scans on the SCG Secure Cloud. An accredited independent assessor will perform monitoring of the security controls for the system annually.					

CA-9	**Internal System Connections:** The organization: a. Authorizes internal connections of information system components (or classes of components) to the information system; and b. Documents, for each internal connection, the interface characteristics, security requirements, and the nature of the information communicated.	Status		Type	
		In Place	X	Common	
		Planned		Hybrid	
		In Place and Planned		System Specific	X
		Not Applicable			

The SCG Secure Cloud does not authorize internal connections between the information system and mobile devices, notebooks/desktop computers, printers, copiers, facsimile machines, scanners, sensors, and servers that are outside of the boundary. All interactions with the information system must take place through the firewalled boundaries. Access control is strictly enforced.

8. Configuration Management (CM)

The status of configuration management controls for the SCGSC Cloud system is as indicated in the following table:

<table>
<tr><th>Control Number</th><th>Description of Control</th><th>Control Status/Type</th></tr>
<tr><td>CM-1</td><td>Configuration Management Policy and Procedures: The organization:
a. Develops, documents, and disseminates to SCG IT staff responsible for the SCGSC:
1. A configuration management policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
2. Procedures to facilitate the implementation of the configuration management policy and associated configuration management controls; and
b. Reviews and updates the current:
1. Configuration management policy at least annually; and
2. Configuration management procedures at least annually.</td><td><table>
<tr><th>Status</th><th></th><th>Type</th><th></th></tr>
<tr><td>In Place</td><td>X</td><td>Common</td><td></td></tr>
<tr><td>Planned</td><td></td><td>Hybrid</td><td></td></tr>
<tr><td>In Place and Planned</td><td></td><td>System Specific</td><td>X</td></tr>
<tr><td>Not Applicable</td><td></td><td></td><td></td></tr>
</table></td></tr>
<tr><td colspan="3">The SCG Configuration Management Plan addresses the requirements and mechanisms to be implemented across SCGSC’s operating environment. At a high level, this policy addresses the purpose, scope, roles and responsibilities, management commitment, coordination among organizational entities, and requirements to comply with auditing and accountability. The policy describes the mandates for log retention, review and analysis. Areas covered include, minimum log requirements, responsibilities, alert review, problem management, retention, security and protection of logs, and compliance review. The policy is consistent with SCG’s mission, and functions with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.

It is the responsibility of SCG President, Vice President of Administration, and the Information Technology (IT) Director to develop, disseminate, and annually review/update the SCG Configuration Management Plan. The IT Director or designee disseminates the plan to all Privileged Users by emailing a link to the SCG Intranet location prior to authorizing privileged</td></tr>
</table>

user status. The IT Director requests a response email from the Privileged User, confirming that Privileged User has read and understands the document.

The plan is located on the SCG Intranet that is available to all SCG personnel at http://web-dev/intranet-sql. The intranet server is located in the Gaithersburg facility at 656 Quince Orchard Road, Gaithersburg, MD 20878.

CM-2	**Baseline Configuration:** The organization develops, documents, and maintains under configuration control, a current baseline configuration of the information system.	Status		Type	
		In Place	X	Common	
		Planned		Hybrid	
		In Place and Planned		System Specific	X
		Not Applicable			

The SCGSC **System Design Document** contains a current baseline configuration and settings for the SCGSC system. It 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. SCG develops, documents, reviews, and maintains the baseline configuration of the Secure Cloud, annually or more frequently as needed. The SCGSC System Design Document is in accordance with NIST Special Publication 800-128, Guide for Security-Focused Configuration Management of Information Systems, based upon the defined concept of Major Change, or other parameters specified in NIST Special Publication 800-12, An Introduction to Computer Security – The NIST Handbook, and Section 8.4.4.3; Configuration baselines are a formal agreement at specific points in time and are departure points for the control of a configuration. The combination of configuration baselines and approved changes to those baselines constitutes the currently approved configuration.

CM-2 (1)	**Reviews and Updates:** The organization reviews and updates the baseline configuration of the information system: a. Annually or b. When required due to interconnection modifications, critical security patches, upgrades, hardware replacements, emergency changes (such as those resulting from security incidents), organizational guideline changes, and other circumstances as appropriate, defined by the IT Director; and c. As an integral part of information system component installations and upgrades.	Status		Type	
		In Place	X	Common	
		Planned		Hybrid	
		In Place and Planned		System Specific	X
		Not Applicable			

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 Change Control Board and authorized by the SCG President and IT Director through the Request for Change (RFC) process.

The **System Operations and Maintenance Plan** incorporates rigorous test and validation procedures that support and demonstrate satisfaction of this control for any adjustment to the system's baseline configuration.

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. The types of items that will be placed under configuration control are identified. 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.

CM-2 (3)	**Retention of Previous Configurations:** The organization retains tape copies of the previous versions of the baseline configuration (one stored at SCG Gaithersburg, one at SCG Frederick, and one in Staunton, VA) to support rollback.	Status		Type	
		In Place	X	Common	
		Planned		Hybrid	
		In Place and Planned		System Specific	X
		Not Applicable			

The SCGSC system baseline configuration is backed up on tape from the time the system was fully developed and configured. The SCG Secure Cloud System files and data files are backed-up daily using a Tandberg Storage Loader tape back-up system. Baseline files are kept onsite at Gaithersburg with a backup of the baseline stored offsite (at the Frederick facility). A full backup of the SCGSC system is run weekly, and monthly full backup tapes for every month of the contract are stored for a minimum of 3 years and possibly up to 7 years at SCG Gaithersburg and SCG Frederick. The **System Operations and Maintenance Plan** incorporates rigorous test and validation procedures that support and demonstrate satisfaction of this control for any rollback procedures that are deemed necessary.

CM-2 (7)	**Baseline Configuration:** The organization: (a) Issues **no** information systems, system components, or devices with any configurations to individuals traveling to locations that the organization deems to be of significant risk; and (b) Applies [Assignment: organization-defined security safeguards] to the devices when the individuals return.	Status		Type	
		In Place		Common	
		Planned		Hybrid	
		In Place and Planned		System Specific	X
		Not Applicable	X		

No outside device will be allowed in the SCG Secure Cloud system. All devices must connect through the approved firewall. All components of the information system are physically placed in SCG facilities in Gaithersburg, MD and Frederick, MD. The information system does not contain devices that are associated with this control (e.g., notebook computers, mobile devices, etc.). However, in the event that mobile devices are introduced to the information system or devices are issued by individuals traveling to locations that the organization deems to be of significant risk they will be protected through the use of FIPS 140-2 compliant encryption mechanisms. This will ensure that the confidentiality and integrity of the data are preserved regardless of the physical surroundings.

SCG does not predict using the devices that are associated with this control. However, in the event that mobile devices are introduced to the information system, they will be protected through the use of FIPS 140-2 compliant encryption mechanisms. This will ensure that the confidentiality and integrity of the data are preserved regardless of physical surroundings.

CM-3	**Configuration Change Control:** The organization: a. Determines the types of changes to the information system that are configuration-controlled; b. Reviews proposed configuration-controlled changes to the information system and approves or disapproves such changes with explicit consideration for security impact analyses; c. Documents configuration change decisions associated with the information system; d. Implements approved configuration-controlled changes to the information system; e. Retains records of configuration-controlled changes to the information system for a minimum of 3 years and possibly for up to 7 years; f. Audits and reviews activities associated with configuration-controlled changes to the information system; and g. Coordinates and provides oversight for configuration change control activities through	Status		Type	
		In Place	X	Common	
		Planned		Hybrid	
		In Place and Planned		System Specific	X
		Not Applicable			

	the Change Control Board, which convenes on an as needed basis to consider RFCs.	

The types of changes to the SCGSC that are configuration controlled are identified in the **Configuration Management Plan**. SCG's configuration management services vary according to lifecycle, type, and source of change being requested. The change management process can be initiated for updates performed as part of the proactive mandatory patch process, or when the customer requests a change. Configuration change decisions are documented using the Request for Change (RFC) forms. Records of configuration-controlled changes are retained for a minimum of three (3) years (the life of the contract) and possibly up to 7 years. The IT Director audits and reviews configuration changes after they are implemented in the SCGSC system, as documented on the RFC form (see form in Appendix A of the **Configuration Management Plan**).

The types of changes include:

- Software
- Hardware
- Network routing and firewall
- Vendor maintenance

SCG has determined that all components and aspects of the SCGSC information system are configuration controlled. In order for a change to take place within the information system, it must first follow the established change management process and receive approval. The SCGSC Change Control Board coordinates and provides oversight for configuration change decisions. The members of the board are identified in the **Configuration Management Plan**.

CM-3 (2)	**Test/ Validate/ Document Changes:** The organization tests, validates, and documents changes to the information system before implementing the changes on the operational system.	Status		Type	
		In Place	X	Common	
		Planned		Hybrid	
		In Place and Planned		System Specific	X
		Not Applicable			

As specified in the SCGSC **System Operations and Maintenance Plan**, all changes to the SCGSC system are tested and validated before they are implemented. All changes must be audited/reviewed and approved by the IT Director after they are implemented.

CM-4	**Security Impact Analysis:** The organization analyzes changes to the information system to determine potential security impacts prior to change implementation.	Status		Type	
		In Place	X	Common	
		Planned		Hybrid	
		In Place and Planned		System Specific	X
		Not Applicable			

SCG IT Director, System Administrators, and Change Control Board (CCB) members participate in scheduled change control meetings to control timing and method of changes to hardware, software, and baselines to assesses the potential security impacts to the SCGSC system prior to implementing any configuration change. This is considered in the change approval process. The SCGSC **System Operations and Maintenance Plan** incorporates rigorous test and validation procedures that support and demonstrate satisfaction of this control. The testing procedures defined therein directly address the required security testing needs.

Configuration change control for the information system involves systematic proposal, justification, implementation, test/evaluation, review, and disposition of changes to the system, including upgrades and modifications. Configuration change control includes changes to components of the information system, changes to the configuration settings for information technology products (e.g., operating systems applications, firewalls, and routers), emergency changes, and changes to remediate incidents.

All changes within the SCGSC environment are tested prior to their implementation in the SCGSC environment in accordance with policy. All certified configurations are tested for security and compatibility among the different applications.

CM-5	**Access Restrictions for Change:** The organization defines, documents, approves, and enforces physical and logical access restrictions associated with changes to the information system.				
		Status		Type	
		In Place	X	Common	
		Planned		Hybrid	
		In Place and Planned		System Specific	X
		Not Applicable			

Any changes to the hardware and software of the SCG Secure Cloud can potentially have significant effects on the overall security of the system. The IT Director and System Administrators define and document physical and logical access restrictions associated with changes to the information system. The IT Director and Change Control Board (CCB) approve changes to physical and logical access restrictions related to changes to the information system. The SCGSC server is physically secure in a locked rack in a locked room that is accessed using programmed fobs. Of the IT staff, only the System Administrators' fobs are programmed to open the server room. The Vice President of Administration and SCG President also have fobs programmed to open the server room.

SCG limits access to network equipment to those individuals who are authorized to request and make changes through the change management process. Authorized administrators with access to network devices are assigned access based on roles and responsibilities. All access to the network devices is logged for non-repudiation purposes.

SCG leverages Active Directory groups to provide logical access restriction mechanisms in regards to changes to the information system. Only administrators who have been authorized will be members of groups that are able to make configuration modifications to the SCGSC.

Physical access restrictions also are in place and have been specifically defined in the Physical and Environmental Protection (PE) portions of this security plan.

In accordance with the **Configuration Management Plan** all changes are controlled through the Request for Change (RFC). All RFCs are evaluated and must be approved by the Change Control Board and authorized by the SCG President and Program Manager before the change is implemented. Configuration change control includes tracking RFC submissions, ensuring changes are reversible, and implementing version control. SCG limits IT staff privileges to change hardware, software, and firmware components and system information of SCGSC directly within a production environment.

Once the approval has been granted, the ticket is updated and authorized system personnel implement the change to the information system. The approval process includes a detailed consideration of the change being requested, the impact it will have on system functionality, and the given security implications. Personnel involved in implementing the change will vary based on the nature of the change and the component it affects. SCG reviews and reevaluates these privileges annually.

CM-6	**Configuration Settings:** Per HHS Minimum Security Configuration Standards for Departmental Operating Systems and Applications, other configuration-related Department memoranda and standards, and any applicable NIH policy, the organization: a. Establishes and documents configuration settings for information technology products employed within the information system that reflect the most restrictive mode consistent with operational requirements; b. Implements the configuration settings; c. Identifies, documents, and approves any deviations from established configuration settings for SCGSC system components based on system operational requirements; and d. Monitors and controls changes to the configuration settings.	Status		Type	
		In Place	X	Common	
		Planned		Hybrid	
		In Place and Planned		System Specific	X
		Not Applicable			

SCG configures the security settings of the SCG Secure Cloud system to the most restrictive mode consistent with information system operational requirements. The settings are derived from the NIST recommended configurations and checklists found at http://checklists.nist.gov. Configuration settings must be implemented and exceptions from the mandatory configuration settings must be identified, documented, and approved for individual components within the system based on explicit operational requirements. Changes to the configuration settings must be monitored and controlled in accordance with SCG policies and procedures. Changes must be approved by the SCG President and IT Director or approved through the RFC process (i.e., Change Control Board). Detection of unauthorized, security-relevant configuration changes

must be incorporated into the incident response capability to ensure that such detected events are tracked, monitored, corrected, and available for historical purposes.

CM-7	**Least Functionality:** The organization: a. Configures the information system to provide only essential capabilities; and b. Prohibits or restricts the use of high-risk functions, ports, protocols, and/or services (e.g., Telnet, FTP).	Status		Type	
		In Place	X	Common	
		Planned		Hybrid	
		In Place and Planned		System Specific	X
		Not Applicable			

SCG configures the information system to provide only essential capabilities. Only essential services/ports are open for business needs and they are properly secured to minimize risk. The allowable/open ports, services, and functions for SCGSC are identified in the **System Design Document** (Table 1) with appropriate justification in the document. All other ports/services are closed, prohibited, or restricted.

CM-7 (1)	**Periodic Review:** The organization: a. Reviews the information system upon encountering a significant risk, or at least every 30 days, to identify unnecessary and/or nonsecure functions, ports, protocols, and services; and b. Disables functions, ports, protocols, and services within the information system deemed to be unnecessary and/or nonsecure.	Status		Type	
		In Place	X	Common	
		Planned		Hybrid	
		In Place and Planned		System Specific	X
		Not Applicable			

On a monthly basis, the SCGSC System Administrator or IT Director will validate that the functions, ports, protocols and services are limited to those that are defined in the list of permitted functions, ports, protocols and services. Additionally, the inventory will be validated against the list of prohibited functions, ports, protocols and services. If any are identified in the scan, the System Administrator would disable them. Some ports are kept disabled and must be manually enabled by the System Administrator as needed.

All functions, ports, protocols and services not designated as permitted will be:

1. Deleted, along with the component that utilizes these items.
2. Be added to the list of permitted functions, ports, protocols and services through the change control process, and all documentation updated.

Validation will take place by leveraging the Nessus scanner to ensure that ports, protocols, and services are locked down in accordance with the principle of least functionality. The SCGSC information system disables all unnecessary functions, ports, protocols, and services when they are detected. All functions, ports, protocols and services not designated as permitted will be disabled.

CM-7 (2)	**Prevent Program Execution:** The information system prevents program execution in accordance with SCG-defined policies regarding software program usage and restrictions and, when necessary, rules authorizing the terms and conditions of software program usage.	Status		Type	
		In Place	X	Common	
		Planned		Hybrid	
		In Place and Planned		System Specific	X
		Not Applicable			

The SCGSC system has been configured to provide only essential capabilities and SCG prevents program execution in accordance with restrictions and rules authorizing the terms and conditions of software program usage. Only the approved software identified in the **System Design Document** are permitted on the SCGSC. Only approved programs will be permitted to execute within the information system authorization boundary. SCG uses white listing to identify software programs that are authorized to execute on the SCGSC system, which are the ones identified in the SCG Secure Cloud **Configuration Management Plan** and **System Design Document.** Any other software would have to be approved through the RFC process.

Only the Domain Administrators are permitted through privileged access to load software on the SCGSC. In accordance with the SCGSC **Configuration Management Plan**, SCG system documentation will be immediately updated to reflect any additions or removals from the white list. All software installation/execution must be approved by the Change Control Board (CCB) and the IT Director. Only authorized personnel have the ability to install software within the SCG authorization boundary.

CM-7 (4)	**Unauthorized Software/Blacklisting:** The organization: a. Identifies software programs authorized to execute on the information system; b. Employs a deny-all, allow-by-exception policy to prohibit the execution of unauthorized software programs on the information system; and c. Reviews and updates the list of authorized software programs at least every 365 days, or upon acquiring or discovering new software within the categories identified in (a).	Status		Type	
		In Place	X	Common	
		Planned		Hybrid	
		In Place and Planned		System Specific	X
		Not Applicable			

SCG uses white listing to identify software programs that are authorized to execute on the SCGSC system. Only the software identified in the SCG Secure Cloud **Configuration Management Plan** and **System Design Document** (Tables 1 and 5) are authorized for execution on the SCGSC. SCG employees a deny-all, allow-by-exception policy to prohibit the execution of unauthorized software programs on SCGSC. This policy is enforced by limiting access and authority for software changes on the SCGSC to the Domain Administrator. The IT Director reviews the list of approved software programs periodically. If additional software needs to be added, the IT Director will prepare and submit an RFC.

CM-8	**Information System Component Inventory:** The organization: a. Develops and documents an inventory of information system components that: 1. Accurately reflects the current information system; 2. Includes all components within the authorization boundary of the information system; 3. Is at the level of granularity deemed necessary for tracking and reporting; and 4. Includes information identified in Appendix H to achieve effective information system component accountability; and b. Reviews and updates the information system component inventory annually or when one or more system components change.	Status		Type	
		In Place	X	Common	
		Planned		Hybrid	
		In Place and Planned		System Specific	X
		Not Applicable			

The current SCGSC system component inventory is documented in the **System Design Document,** Version 1.4 (Table 5) and referenced in the **Configuration Management Plan**, **Contingency Plan**, and **Disaster Recovery Plan**. This inventory includes all components (hardware and software) within the boundary of the SCGSC system. Each component is tagged with a unique name (ID) to facilitate component tracking. The inventory is reviewed and updated annually or when one or more system components change.

CM-8 (1)	Updates During Installations/ Removals: The organization updates the inventory of information system components as an integral part of component installations removals, and information system updates.	Status		Type	
		In Place	X	Common	
		Planned		Hybrid	
		In Place and Planned		System Specific	X
		Not Applicable			

The SCGSC system component inventory is documented in the **System Design Document** (Table 5). Each component is tagged with a unique name for tracking. The inventory is updated annually or when one or more system components change. Configuration control includes maintaining a record of CI:

- Changes
- Versions
- Location
- Custodianship/ownership
- Machine name
- Network interface configuration
- Manufacturer
- Type
- Model

- Serial Number
- Physical Location
- Component Owner
- Database Servers
- Web Application Servers
- Server Operating System

CM-8 (3)	**Automated Unauthorized Component Detection:** The organization: a. Employs automated mechanisms at least weekly to detect the presence of unauthorized hardware, software, and firmware components within the information system; and b. Takes the following actions when unauthorized components are detected: • disables network access by such components • isolates the components • notifies the IT Director.	Status		Type	
		In Place	X	Common	
		Planned		Hybrid	
		In Place and Planned		System Specific	X
		Not Applicable			

SCG has designed the SCGSC system with adequate controls to prevent the introduction of unauthorized hardware, software, and firmware. Only approved programs will be permitted to execute within the information system authorization boundary. The IT Director will review the system logs compiled by Kiwi Syslog weekly to detect the presence of and attempts to add unauthorized software and firmware components within the SCGSC system. In addition, once SCG begins running monthly vulnerability scans of the SCGSC, the IT Director will review the results of the vulnerability scans to detect the presence of unauthorized components. Unauthorized hardware is prevented by limiting physical access to the SCGSC server room. If unauthorized software or firmware are detected, the IT Director will take appropriate actions to disable (unplug and disconnect hardware/firmware) or isolate (uninstall software) the unauthorized component, and remove it from SCGSC. The IT Director will notify the SCG President and Program Manager when unauthorized components are detected and disabled/removed.

CM-8 (5)	**No Duplicate Accounting of Components:** The organization verifies that all components within the authorization boundary of the information system are not duplicated in other information system inventories.	Status		Type	
		In Place	X	Common	
		Planned		Hybrid	
		In Place and Planned		System Specific	X
		Not Applicable			

SCG verifies that all components within the authorization boundary of the SCG Secure Cloud system are not duplicated in other information system inventories. Windows prohibits the duplication of component names or IP addresses.

Corporate Responsibility: All systems and devices within SCGSC boundaries are inventoried and documented in the **System Design Document**.

System Responsibility: System Administrators and the IT Director verify annually:

1. The state of SCGSC's CI.
2. Conduct a random and periodic, but not more than monthly, spot check of the CI.

Specific change control processes around the handling of the CI during patching, upgrades, and deployments.

Inventory lists are reviewed annually or as needed due to system changes to validate that SCGSC assets are only contained in the appropriate inventory listing.

CM-9	**Configuration Management Plan:** The organization develops, documents, and implements a configuration management plan for the information system that: a. Addresses roles, responsibilities, and configuration management processes and procedures; b. Establishes a process for identifying configuration items throughout the system development life cycle and for managing the configuration of the configuration items; c. Defines the configuration items for the information system and places the configuration items under configuration management; and d. Protects the configuration management plan from unauthorized disclosure and modification.	Status		Type	
		In Place	X	Common	
		Planned		Hybrid	
		In Place and Planned		System Specific	X
		Not Applicable			

The SCGSC **Configuration Management Plan** (CMP) is written to provide all the roles, responsibilities, organizational structure, and process definitions that were used to create the documentation for the controls defined in the System Security Plan (SSP). The SCGSC CMP is approved by the Configuration Control Board (CCB) and maintained by the Configuration Manager, and kept under change control.

CM-10	**Software Usage Restrictions:** The organization: a. Uses software and associated documentation in accordance with contract agreements and copyright laws; b. Tracks the use of software and associated documentation protected by quantity licenses to control copying and distribution; and c. Controls and documents the use of peer-to-peer file sharing technology to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work.	Status / Type In Place: X Planned: In Place and Planned: Not Applicable: Common: Hybrid: System Specific: X

In accordance with the NIH IT General Rules of Behavior, which are distributed and signed by all staff granted access to the SCGSC, SCG prohibits the copying or distributing of intellectual property including music, software, documentation, videos, and other copyrighted materials without permission or license from the copyright owner. The IT Director tracks the use and associated documentation protected by quantity licenses to control copying and distribution. SCG also prohibits the use of peer-to-peer file sharing software; any exceptions must be reviewed and approved by the IT Director and SCG President. Only software identified in the SCGSC inventory in the **System Design Document** is permitted for use in the SCGSC environment.

CM-11	**User Installed Software:** The organization: a. Prohibits the installation of software by users on all government-furnished equipment (GFE); b. Enforces software installation policies through system access privileges; and c. Monitors policy compliance by reviewing system logs at least monthly.	Status / Type In Place: X Planned: In Place and Planned: Not Applicable: Common: Hybrid: System Specific: X

End users are not permitted to install any form of software onto the information system. This is restricted in the SCG Acceptable Use Policy signed by every user, and also is restricted through the use of configuration management controls. For more information, see CM-8(3) of this System Security Plan (SSP). The SCGSC **Facility and Systems Access Policy and Procedures** document establishes policies governing the installation of software. Only the Domain Administrator has access privileges to install software on the SCGSC system and only approved software can be installed. This policy also is enforced by physically securing the SCGSC server room and server (software installation would require accessing the fob-controlled server room and the locked rack). The approved software is identified in the SCGSC inventory in the **System Design Document**. Any additional software must be approved by the SCG President and IT Director through an RFC per Section 3.2 of the **Configuration Management Plan** document. The IT Director's review of the weekly system logs and the monthly system scans would detect any violation of the SCGSC software installation policy. Software installation policies are enforced through the use of Active Directory groups and access control. End users of the applications are not capable of gaining access necessary to install software within the SCGSC system.

9. Contingency Planning (CP)

The status of contingency planning controls for the SCGSC system is as indicated in the following table:

<table>
<tr><th>Control Number</th><th>Description of Control</th><th>Control Status/Type</th></tr>
<tr><td>CP-1</td><td>Contingency Planning Policy and Procedures:
The organization:
a. Develops, documents, and disseminates to SCG personnel responsible for contingency planning, management, and response:
1. A contingency planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
2. Procedures to facilitate the implementation of the contingency planning policy and associated contingency planning controls; and
b. Reviews and, if necessary, updates the current:
1. Contingency planning policy at least annually; and
2. Contingency planning procedures at least annually.</td><td>
<table>
<tr><th>Status</th><th></th><th>Type</th><th></th></tr>
<tr><td>In Place</td><td>X</td><td>Common</td><td></td></tr>
<tr><td>Planned</td><td></td><td>Hybrid</td><td></td></tr>
<tr><td>In Place and Planned</td><td></td><td>System Specific</td><td>X</td></tr>
<tr><td>Not Applicable</td><td></td><td></td><td></td></tr>
</table>
</td></tr>
</table>

The SCG Secure Cloud **Contingency Planning Policy and Contingency Plan** addresses the requirements and mechanisms to be implemented across SCGSC's operating environment. At a high level, this policy addresses the purpose, scope, roles and responsibilities, management commitment, coordination among organizational entities, and requirements to comply with security awareness and training. This policy applies to all applications, databases, operating systems, and network devices that store or process SCG information other than publicly accessible Internet facing SCG systems. The policy does not apply to SCG customer end users. Additionally, this policy outlines requirements to manage and protect all company and client information, including low and moderately sensitive information. The policy is consistent with SCG's mission, and functions with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.

It is the responsibility of SCG President, Information Technology (IT) Director, and Vice President of Administration to develop, disseminate, and annually review/update the SCGSC Contingency Plan. The IT Director disseminates the plan to all Privileged Users by emailing a link to the document's SCG Intranet location prior to authorizing privileged user status. The IT Director requests a response email from the Privileged User, confirming that Privileged User has read and understands the document.

The SCGSC Contingency Planning Policy and Contingency Plan is located on the SCG Intranet that is available to all SCG personnel at http://web-dev/intranet-sql. The intranet server is located in the Gaithersburg facility at 656 Quince Orchard Road, Gaithersburg, MD 20878.

CP-2	**Contingency Plan:** The organization: a. Develops an information technology contingency plan (ITCP) in accordance with NIST SP 800-34 for all information systems that: 1. Identifies essential missions and business functions and associated contingency requirements; 2. Provides recovery objectives, restoration priorities, and metrics; 3. Addresses contingency roles and responsibilities and assigned individuals with contact information; Note: The ITCP specifically identifies personnel/roles with significant contingency responsibilities and documents procedures for notifying them. 4. Addresses maintaining essential missions and business functions despite an information system disruption, compromise, or failure; 5. Addresses eventual, full information system restoration without deterioration of the security safeguards originally planned and implemented; and 6. Is reviewed, approved, and signed by, at a minimum, the SCG President and IT Director. Note: The ITCP also is reviewed by other personnel/roles as appropriate (e.g., System Administrator, Program Manager, ISSO, database administrator). However, these individuals are typically not required to sign the ITCP as documentation of formal approval. Note: The ITCP includes procedures for activation of the plan; recovery of the system (to the original or alternative location if needed); reconstitution of the system; and test procedures to ensure that the system is fully functional and accessible once it has been restored. b. Distributes copies of the ITCP to the ISSO, President, CPC, IT Director, System Administrator, Incident/Disaster Recovery Team members, SCG managers, and other personnel as appropriate;	Status		Type	
		In Place	X	Common	
		Planned		Hybrid	
		In Place and Planned		System Specific	X
		Not Applicable			

	c. Coordinates contingency planning activities with incident handling activities; d. Reviews the ITCP for the information system annually; e. Updates the ITCP to address changes to the organization, information system, or environment of operation and problems encountered during ITCP implementation, execution, or testing; f. Communicates ITCP changes to the ISSO, SCG President, CPC, System Administrator, Incident/Disaster Recovery Team members, SCG managers, and other personnel as appropriate; and g. Protects the ITCP from unauthorized disclosure and modification.	

The Contingency Planning Team is responsible for reviewing and updating as needed the **SCGSC Contingency Planning Policy and Contingency Plan** at least annually. The Plan also will be updated as needed following exercises and incidents.

- The IT Director must distribute copies of the contingency plan to key personnel and organizational elements, including FISMA personnel.
- A process to coordinate contingency planning activities with incident handling activities must be established.
- The SCG President and IT Director must review the contingency plan for the SCGSC at least annually and revise the contingency plan to address any changes to the SCGSC, its information system, or environment of operation and problems encountered during contingency plan implementation, execution, or testing.
- Changes to the contingency plan must be communicated to key personnel and organizational elements, including FISMA personnel.
- As part of the contingency planning process, the Contingency Planning Team must coordinate the information system's contingency plan development with organizational elements responsible for related plans.
- The contingency plan must conduct capacity planning in order for information processing, telecommunications, and environmental support exists during contingency operations.

CP-2 (1)	**Coordinate with Related Plans:** The organization coordinates contingency plan development with organizational elements responsible for related plans (e.g., Business Continuity Plan, Disaster Recovery Plan, Continuity of Operations Plan, Business Recovery Plan, and Incident Response Plan).	Status: In Place X; Planned; In Place and Planned; Not Applicable Type: Common; Hybrid; System Specific X

Contingency Plan development and maintenance is coordinated with the development and maintenance of the other plans associated with the SCGSC. The SCG President, IT Director, and Vice President of Administration are involved in the development, update, review and approval of all the plans. The Business Continuity Plan Team ensures that critical business functions can continue if a disaster occurs. This team works with the Incident/Disaster Recovery Team and Contingency Planning Team to ensure the establishment of operations at an alternate site until SCG is able to either resume operations at its primary site or select a new primary location. The SCG President directs the Business Continuity Plan Team.

CP-2 (3)	**Resume Essential Mission/ Business Functions:** The organization plans for the resumption of essential missions and business functions within 7 days of ITCP activation.	Status: In Place X; Planned; In Place and Planned; Not Applicable Type: Common; Hybrid; System Specific X

Once the SCGSC **Contingency Plan** is activated, the SCGSC system will be temporarily restored from backup at the alternate site in Frederick, Maryland, following the procedures defined in the **Disaster Recovery Plan** (DRP). The DR Team will be responsible for implementing these procedures to recover the system.

CP-2 (8)	**Contingency Plan:** The organization identifies critical information system assets supporting essential missions and business functions.	Status: In Place X; Planned; In Place and Planned; Not Applicable Type: Common; Hybrid; System Specific X

The information system assets critical for the functioning of the SCGSC system are identified in the **Contingency Plan** and **Disaster Recovery Plan**.

Combined Responsibility: SCG capacity planning for the system has been conducted by both the IT Director and Program Manager to ensure that personnel, hardware, and software components necessary to ensure continued operations for the customer's production system has been procured.

CP-3	**Contingency Training:** The organization provides contingency training to information system users consistent with assigned roles and responsibilities: a. Within three (3) months of assuming a contingency role or responsibility; b. When required by information system changes; and c. Annually thereafter.	Status: In Place X; Planned; In Place and Planned; Not Applicable Type: Common; Hybrid; System Specific X
SCG trains personnel in their contingency roles and responsibilities with respect to the SCGSC system and provides refresher training annually. The DRP Director will be responsible for the contingency training. Each component of the SCGSC will be reconstructed individually in a beta test environment.		

CP-4	**Contingency Plan Testing:** The organization: a. Tests the ITCP for the information system at least every 365 days using NIST SP 800-34, NIST SP 800-84, and other tests and exercises (as defined by the IT Director and SCG President) to determine the effectiveness of the plan and the organizational readiness to execute the plan; b. Reviews the ITCP test results; and c. Initiates corrective actions, if needed.	Status: In Place X; Planned; In Place and Planned; Not Applicable Type: Common; Hybrid; System Specific X
Contingency Plan testing and exercises are conducted in conjunction with disaster recovery testing, training, and exercises in accordance with the schedule identified in the **Disaster Recovery Plan**, which specifies annual training and testing, including a structured walk-through and an integrated business operations/information systems exercise per year.		

CP-4 (1)	**Contingency Plan Testing and Exercises:** The organization coordinates contingency plan testing with organizational elements responsible for related plans.	Status: In Place X; Planned; In Place and Planned; Not Applicable Type: Common; Hybrid; System Specific X
The SCG President and IT Director shall establish criteria for validation/testing of a Contingency Plan and coordinate testing with the three contingency planning and operations teams to test/exercise their Contingency Plan in coordination with management personnel and organizational elements responsible for related plans. The functional testing of the SCGSC Contingency Plan takes place with contributions from the Incident Response Team and organizational Disaster Recovery Team. This process ensures effective communication and response mechanisms in the event of an outage.		

CP-6	**Alternate Storage Site:** The organization: a. Establishes an alternate storage site including necessary agreements to permit the storage and retrieval of information system backup information; and b. Ensures that the alternate storage site provides information security safeguards equivalent to that of the primary site.	Status: In Place X; Planned; In Place and Planned; Not Applicable Type: Common; Hybrid; System Specific X

Per the SCGSC **Contingency Planning Policy and Contingency Plan**, an alternate site must be established, including necessary agreements to permit the storage and recovery information and system backup information. The current alternate site location is at SCG's facility in Frederick, Maryland. The current alternate site must be separated from the primary site to prevent susceptibility of the same hazards.

The alternate storage site at SCG Frederick has fob security access at the main door to the building, which allows only authorized employees to enter the building. The server room is secured with a key lock door. The members of the Disaster Recovery Team have fobs to access the building and keys to access the server room. Other key personnel involved in contingency plan operations also have fobs and keys to access the Frederick facility. The server room is equipped with a fire extinguisher, and a tarp to cover equipment in the event of a water leak. There is a sign posted stating "No cellular phone usage", and a log book is present for visitors to document their access to the room.

CP-6 (1)	**Separation from Primary Site:** The organization identifies an alternate storage site that is separated from the primary storage site to reduce susceptibility to the same threats.	Status: In Place X; Planned; In Place and Planned; Not Applicable Type: Common; Hybrid; System Specific X

Backups of all software necessary to restore the SCG Secure Cloud system as well as tape backups of the data are stored at both the SCG Gaithersburg and the SCG Frederick facilities. Daily, weekly, and monthly data backup occurs at both facilities. This ensures that there are two copies of the system available at all times. The virtual servers also are being replicated from SCG Gaithersburg to a host at SCG Frederick as a third mean of backup. Copies of monthly backup tapes also are stored at a location in Staunton, Virginia, about 185 miles from the Gaithersburg facility.

CP-6 (3)	**Accessibility:** The organization identifies potential accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster and outlines explicit mitigation actions.	Status		Type	
		In Place	X	Common	
		Planned		Hybrid	
		In Place and Planned		System Specific	X
		Not Applicable			

In the event of a widespread disaster that affects both the Gaithersburg and Frederick facilities, SCG stores backups required to recover the SCG Secure Cloud system at a secure location in Staunton, Virginia (approximately 185 miles from Gaithersburg). Per the SCGSC **Contingency Planning Policy and Contingency Plan**, a process to identify potential accessibility problems to the alternate site must be established in the event of an area-wide disruption or disaster. Explicit mitigation actions must be defined to those potential accessibility problems.

CP-7	**Alternate Processing Site:** The organization: a. Establishes an alternate processing site including necessary agreements to permit the transfer and resumption of SCGSC system operations for essential missions/business functions within 7 days (a time period specified in the ITCP and consistent with recovery time and recovery point objectives) when the primary processing capabilities are unavailable; b. Ensures that equipment and supplies required to transfer and resume operations are available at the alternate processing site or contracts are in place to support delivery to the site within the organization-defined time period for transfer/resumption; and c. Ensures that the alternate processing site provides information security safeguards equivalent to that of the primary site.	Status		Type	
		In Place	X	Common	
		Planned		Hybrid	
		In Place and Planned		System Specific	X
		Not Applicable			

The **Disaster Recovery Plan** specifies the arrangements and agreements SCG has in place to permit the recovery of the SCG Secure Cloud system operations within 7 days at the alternate site in Frederick, Maryland. The information security safeguards at Frederick are equivalent to those at the Gaithersburg facility. Per the SCGSC **Contingency Planning Policy and Contingency Plan**, an alternate processing site must be established, including necessary agreements to permit the resumption of information system operations for essential mission and business functions within defined time periods when primary processing capabilities become unavailable. The current alternate processing site location is SCG's facility in Frederick, Maryland. It is the responsibility of the IT Director to develop a Contingency Plan that is consistent with the recovery time objectives and business impact analysis for submission to the Contingency Planning Team for review and approval.

CP-7 (1)	**Separation from Primary Site:** The organization identifies an alternate processing site that is separated from the primary processing site to reduce susceptibility to the same threats.	Status		Type	
		In Place	X	Common	
		Planned		Hybrid	
		In Place and Planned		System Specific	X
		Not Applicable			

As stated in the SCGSC **Contingency Planning Policy and Contingency Plan**, the current alternate processing site must be separated from the primary processing site to prevent susceptibility of the same hazards. The alternate processing site in Frederick, Maryland, is located approximately 30 miles from the Gaithersburg facility. SCG leases the Frederick site and has full access to the facility 24/7 in the event of an emergency.

CP-7 (2)	**Accessibility:** The organization identifies potential accessibility problems to the alternate processing site in the event of an area-wide disruption or disaster and outlines explicit mitigation actions.	Status		Type	
		In Place	X	Common	
		Planned		Hybrid	
		In Place and Planned		System Specific	X
		Not Applicable			

The **Disaster Recovery Plan** outlines SCG's approach to recovering the SCGSC system in the event of a widespread disaster that impacts both the Frederick and Gaithersburg facilities. A process to identify potential accessibility problems to the alternate processing site must be established in the event of an area-wide disruption or disaster. Explicit mitigation actions must be defined for those potential accessibility problems

CP-7 (3)	**Priority of Service:** The organization develops alternate processing site agreements that contain priority-of-service provisions in accordance with organizational availability requirements (including recovery time objectives).	Status		Type	
		In Place	X	Common	
		Planned		Hybrid	
		In Place and Planned		System Specific	X
		Not Applicable			

The alternate processing site in Frederick is located approximately 30 miles from the Gaithersburg facility. SCG leases the Frederick site and has full access to the facility 24/7 in the event of an emergency. All agreements are in place to permit the recovery of the SCG Secure Cloud system at SCG Frederick.

CP-8	**Telecommunications Services:** The organization establishes alternate telecommunications services including necessary agreements to permit the resumption of SCGSC system operations for essential missions and business functions within 7 days when the primary telecommunications capabilities are unavailable at either the primary or alternate processing or storage sites.	Status		Type	
		In Place	X	Common	
		Planned		Hybrid	
		In Place and Planned		System Specific	X
		Not Applicable			

SCG has telecommunications contracts for telephone and mobile phone service. Analog phones are available at the Frederick facility should the phone system be down. E-mail and text messaging are additional forms of communications that will be employed in the event of a disaster. The ISP for Gaithersburg is Level3 and for Frederick is Comcast Enterprise and XO Communications.

CP-8 (1)	**Telecommunications Services:** The organization: a. Develops primary and alternate telecommunications service agreements that contain priority-of-service provisions in accordance with organizational availability requirements (including recovery time objectives); and b. Requests Telecommunications Service Priority for all telecommunications services used for national security emergency preparedness in the event that the primary and/or alternate telecommunications services are provided by a common carrier.	Status		Type	
		In Place	X	Common	
		Planned		Hybrid	
		In Place and Planned		System Specific	X
		Not Applicable			

The Internet connection is critical for full functionality of the SCG Secure Cloud system. The primary site functions on a 200 MB fiber optic circuit through Level3, with an SLA of 99.9% uptime. It has a redundancy 10 MB fiber optic circuit through Comcast Enterprise with an SLA of 99.9%. The alternate site functions on a 100 MB fiber optic circuit through Comcast Enterprise, which guarantees an SLA of 99.9% uptime. The alternate site also has an XO Communications (guaranteed SLA of 99.9% uptime) circuit for voice. This circuit will be used for implementing the **Contingency Plan** and **Disaster Recovery Plan**. Additional ISPs are available in Gaithersburg and Frederick and contracts will be executed should existing ISPs fail to provide service.

CP-8 (2)	**Single Point of Failure:** The organization obtains alternate telecommunications services to reduce the likelihood of sharing a single point of failure with primary telecommunications services.	Status		Type	
		In Place	X	Common	
		Planned		Hybrid	
		In Place and Planned		System Specific	X
		Not Applicable			

The Internet connection is critical for full functionality of the SCG Secure Cloud system. The primary site functions on a 200 MB fiber optic circuit through Level3 with an SLA of 99.9% uptime. It has a redundancy 10 MB fiber optic circuit through Comcast Enterprise with an SLA of 99.9%. The alternate site functions on a 100 MB dedicated EPL fiber optic circuit through Comcast Enterprise, which guarantees an SLA of 99.9%. This circuit is private and it connects the primary site directly to the alternate site. Additional ISPs are available in Gaithersburg and Frederick and contracts will be executed should existing ISPs fail to provide service.

CP-9	**Information System Backup:** The organization: a. Conducts backups of user-level information contained in the information system daily; b. Conducts backups of system-level information contained in the information system daily; c. Conducts backups of information system documentation including security-related documentation daily; and d. Protects the confidentiality, integrity, and availability of backup information at storage locations.	Status		Type	
		In Place	X	Common	
		Planned		Hybrid	
		In Place and Planned		System Specific	X
		Not Applicable			

The IT Director is responsible for all aspects of information system backup. SCG Secure Cloud is automatically backed up on a daily basis using the Tandberg Storage Loader LTO-6 Tape Autoloader, LTO Ultrium - SAS-2 running BackupExec 2015 Enterprise at both the primary and alternate sites. Data and system backups occur daily. Backup tapes are archived weekly and monthly. Monthly backup tapes are retained indefinitely. Tape backups at the primary site are stored in a locked fire safe in the IT Director's office (SCG Gaithersburg). Tape backups at the alternate site are stored in a locked fire safe in the conference room (SCG Frederick). A duplicate of each monthly backup tape also is stored at a distant offsite location (Staunton, VA). Duplicate backups are archived weekly. Monthly duplicate backup tapes are retained indefinitely. Information system documentation, including all policy and procedures documents, are backed up daily on the SCG corporate server.

CP-9 (1)	**Testing for Reliability/Integrity:** The organization tests backup information at least semi-annually to verify media reliability and information integrity, and documents test results.	Status		Type	
		In Place	X	Common	
		Planned		Hybrid	
		In Place and Planned		System Specific	X
		Not Applicable			

The IT Director is responsible for all aspects of system backup and testing. Verification procedures are scheduled to run automatically right after each daily backup is completed to maintain information integrity. The IT Director will manually test backup information at least once every 6 months to verify media reliability and information integrity. The results of the manual testing will be documented by the IT Director.

CP-10	**Information System Recovery and Reconstitution:** The organization provides for the recovery and reconstitution of the information system to a known state after a disruption, compromise, or failure.	Status		Type	
		In Place	X	Common	
		Planned		Hybrid	
		In Place and Planned		System Specific	X
		Not Applicable			

Recovery and reconstitution of the SCG Secure Cloud system is the responsibility of the Disaster Recovery Team, which is led by the DRP Director. Procedures for recovering and reconstituting the system are outlined in the **Disaster Recovery Plan**.

CP-10 (2)	**Transaction Recovery:** The information system implements transaction recovery for systems that are transaction-based.	Status		Type	
		In Place	X	Common	
		Planned		Hybrid	
		In Place and Planned		System Specific	X
		Not Applicable			

When a system crashes, several transactions may be in the process of being executed and various files may be opened to modify data items. Transactions as a whole must be maintained, that is, either all operations are executed or none. First, logs should be checked to determine the states of all transactions that were being executed. If a transaction is determined to be mid-operation, it should be checked to see if it can be completed now or needs to be rolled back. No transaction should be left incomplete.

10. Identification and Authentication (IA)

The status of identification and authentication controls for the SCGSC system is as indicated in the following table:

Control Number	Description of Control	Control Status/Type			
IA-1	**Identification and Authentication Policy and Procedures:** The organization: a. Develops, documents, and disseminates to the staff who have access to the SCGSC: 1. An identification and authentication policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and	Status		Type	
		In Place	X	Common	
		Planned		Hybrid	
		In Place and Planned		System Specific	X
		Not Applicable			

	2. Procedures to facilitate the implementation of the identification and authentication policy and associated identification and authentication controls; and b. Reviews and updates the current: 1. Identification and authentication policy at least once annually; and 2. Identification and authentication procedures at least once annually.	
SCG supports a system access request process for the SCGSC system. Any user granted access to a system must have this approved form on file. These forms are approved by the SCG President and IT Director and they are reviewed quarterly for all individuals who are granted access to the SCGSC system.		

IA-2	**Identification and Authentication (Organizational Users):** The information system uniquely identifies and authenticates organizational users (or processes acting on behalf of organizational users).	Status		Type	
		In Place	X	Common	
		Planned		Hybrid	
		In Place and Planned		System Specific	X
		Not Applicable			
SCG assigns individual accounts within the SCGSC system that are accessible only by that individual. Shared accounts are not permitted per SCG policy. Authentication to information systems requires the user to logon and provide his/her UserID and password to obtain access to the system. SCG uses Active Directory for identification and authentication of users accessing the SCG Secure Cloud system.					

IA-2 (1)	**Network Access to Privileged Accounts:** The information system implements multifactor authentication for network access to privileged accounts.	Status		Type	
		In Place		Common	
		Planned		Hybrid	
		In Place and Planned		System Specific	X
		Not Applicable	X		
Utilization of token-based access (soft or hard token) is not supported in the current operating system of the SCG Secure Cloud. Therefore, this control is Not Applicable.					

IA-2 (2)	**Network Access to Non-Privileged Accounts:** The information system implements multifactor authentication for network access to non-privileged accounts.	Status		Type	
		In Place		Common	
		Planned		Hybrid	
		In Place and Planned		System Specific	X
		Not Applicable	X		
Non-privileged accounts are not permissible in the SCG Secure Cloud system per organizational policy.					

IA-2 (3)	**Local Access to Privileged Accounts:** The information system implements multifactor authentication for local access to privileged accounts.	Status		Type	
		In Place		Common	
		Planned		Hybrid	
		In Place and Planned		System Specific	X
		Not Applicable	X		
Utilization of token-based access (soft or hard token) is not supported in the current operating system of the SCG Secure Cloud. Future configurations may be implemented to support this when NIDDK clearly identifies that these controls are warranted and necessary to protect the system.					

IA-2 (8)	**Network Access to Privileged Accounts – Replay Resistant:** The information system implements replay-resistant authentication mechanisms for network access to privileged accounts.	Status		Type	
		In Place	X	Common	
		Planned		Hybrid	
		In Place and Planned		System Specific	X
		Not Applicable			
Authentication to the SCG Secure Cloud system does not support persistent session, which removes any capability to support replay attacks to the environment. The SCGSC system utilizes Microsoft Authentication capabilities that leverage Kerberos services. Utilization of this authentication framework allows for ticket granting services that resist replay attacks to the environment. Additional security can be configured when the NIDDK determines it is necessary for this system. SCG has set the FIPS local/group security policy flag in Windows Group Policy to ensure consistency with FIPS 140 Security Policy.					

IA-2 (11)	**Remote Access – Separate Device:** The information system implements multifactor authentication for remote access to privileged and non-privileged accounts such that one of the factors is provided by a device separate from the system gaining access and the device meets organization-defined strength of mechanism requirements.	Status / Type

Status		Type	
In Place		Common	
Planned		Hybrid	
In Place and Planned		System Specific	X
Not Applicable	X		

SCG does not implement multifactor authentication for remote access to privileged accounts for the SCGSC. Content that is provided by the applications that are hosted in the SCG Secure Cloud system is offered through a web connection to the Public Internet, and is subject to the individual security models of the applications. These authentication capabilities are out of scope for this assessment, as they are supported in the manner that the applications demand and are restricted in nature to the applications that allow for public domain access. Non-privileged accounts are not supported in the SCG Secure Cloud system by organizational policy.

IA-2 (12)	**Acceptance of PIV Credentials:** The information system accepts and electronically verifies Personal Identity Verification (PIV) credentials.	Status / Type

Status		Type	
In Place		Common	
Planned		Hybrid	
In Place and Planned		System Specific	X
Not Applicable	X		

The system is not required by the government to support PIV logon services.

IA-3	**Device Identification and Authentication:** The information system uniquely identifies and authenticates the virtual machines (e.g., SCSQL-PROD, SCCOLDSHARE-PROD) before establishing a local connection. If remote authentication is provided by the system itself, the system must be in compliance with OMB Memorandum 04-04, E-Authentication Guidance for Federal Agencies.	Status / Type

Status		Type	
In Place	X	Common	
Planned		Hybrid	
In Place and Planned		System Specific	X
Not Applicable			

SCG uses Active Directory to support machine level authentication to the SCG Secure Cloud system environment. Machines are loaded with certificates from an AD central management capability using auto-enrollment. Each user and device account is assigned a unique Microsoft identification number (SID).

IA-4	**Identifier Management:** The organization manages information system identifiers by: a. Receiving authorization from the IT Director to assign an individual, group, role, or device identifier; b. Selecting an identifier that identifies an individual, group, role, or device; c. Assigning the identifier to the intended individual, group, role, or device; d. Preventing reuse of identifiers indefinitely by disabling rather than removing the identifier; and e. Disabling the identifier after 30 days of inactivity.	

Status		Type	
In Place	X	Common	
Planned		Hybrid	
In Place and Planned		System Specific	X
Not Applicable			

a. All privileged users are required to request access to the SCGSC system through a request form that is approved by the SCG President and IT Director.
b. All privileged users are provided unique accounts that permit access to the SCG Secure Cloud system.
c. Accounts must be unique as part of the Windows Operating System enforcement models.
d. Accounts are disabled as part of SCG's off boarding processes at a corporate level. Accounts are disabled rather than removed to prevent account reuse.
e. The four virtual machines in SCGSC are assigned unique device names and a unique SID. Devices are disabled rather than removed when they are no longer part of the system.

IA-5	**Authenticator Management:** The organization manages information system authenticators by: a. Verifying, as part of the initial authenticator distribution, the identity of the individual, group, role, or device receiving the authenticator; b. Establishing initial authenticator content for authenticators defined by the organization; c. Ensuring that authenticators have sufficient strength of mechanism for their intended use; d. Establishing and implementing administrative procedures for initial authenticator distribution, for lost/compromised or damaged authenticators, and for revoking authenticators; e. Changing default content of authenticators prior to information system installation;	

Status		Type	
In Place	X	Common	
Planned		Hybrid	
In Place and Planned		System Specific	X
Not Applicable			

	f. Establishing minimum and maximum lifetime restrictions and reuse conditions for authenticators; g. Changing/refreshing authenticators at the following intervals: • Passwords – every 60 days, immediately in the event of known or suspected compromise, and immediately upon system installation (e.g., default or vendor-supplied passwords) • PIV Compliant Access Cards – no longer than every five (5) years • PKI certificates issued in accordance with Federal PKI Common Policy – no longer than every three (3) years • All other authenticators – managed by the IT Director h. Protecting authenticator content from unauthorized disclosure and modification; i. Requiring individuals to take, and having devices implement, specific security safeguards to protect authenticators; j. Changing authenticators for group/role accounts when membership to those accounts changes. k. Any PKI authentication request must be validated by Online Certificate Status Protocol (OCSP) or certificate revocation list (CRL) to ensure that the certificate being used for authentication has not been revoked.	
a. Users are provided an account by the IT Director after the request for access is approved by the SCG President and IT Director. The initial account authenticator is provided by the IT Director to the individual in person. The individual must change the authenticator at first logon. The subsequent authenticator is known only by the individual user. b. Authenticators adhere to policies that are implemented for the SCG Secure Cloud system. c. The authenticator (password) rules are established in the Windows Local Policy settings and are enforced by this COTS system. d. The SCG IT Director personally manages these processes with in person validation of identity and ensures that authenticators adhere to organizational policy. The IT Director also implements administrative procedures for lost/compromised or damaged authenticators, and for revoking authenticators.		

e. The default passwords for the SCG Secure Cloud system were all changed during installation.
f. The Windows Local Policy settings establish the rules for a maximum of 60 days for password longevity.
g. The SCG Secure Cloud system utilizes a Windows based mechanism for password change that is secure and enforceable through Windows Local Policy settings.
h. Passwords are known only to the account holder and are encrypted by Microsoft to keep them from being discovered. The passwords are masked on the monitor and presented as a secure hash to the Operating System utilizing a symmetric key exchange style of approach, which adequately protects from password discovery.
i. Individuals are required to protect the confidentiality of their authenticators (passwords) as specified in the rules of behavior agreement. When a user logs on, the authenticator (password) remains encrypted and only a secure hash is exchanged with the MS Kerberos service protecting the password from discovery.
j. Passwords are not assigned by group or role. They are unique to each user. Therefore, group and membership changes are not applicable to the SCGSC system.

IA-5 (1)	**Authenticator Management:** The information system, for password-based authentication: a. Enforces minimum password complexity of at least one (1) character from each of the four character categories (A-Z, a-z, 0-9, and special characters), minimum length of eight (8) characters for regular user passwords and minimum length of fifteen (15) characters for administrators or privileged users; b. Enforces at least the following number of changed characters when new passwords are created: at least 75% of characters; c. Stores and transmits only encrypted representations of passwords; (d) Enforces password minimum password age of one (1) day and maximum password age of 60 days; (e) Prohibits password reuse for at least six (6) generations; and (f) Allows the use of an initial password for system logons with an immediate change to a permanent password.	Status		Type	
		In Place	X	Common	
		Planned		Hybrid	
		In Place and Planned		System Specific	X
		Not Applicable			

a. A minimum password length of 8 characters for all users has been established for the Windows OS environment.
b. At least 75% of the characters must be changed when new passwords are created.
c. Only encrypted representations of passwords are stored in the SCGSC system. Passwords are masked when entered to maintain password protection.
d. SCG enforces password minimum and maximum lifetime restrictions of 1 and 60 days, respectively.
e. Passwords cannot be reused for at least 24 generations per the settings in the Windows OS environment.
f. The use of an initial/temporary password for system logons is permitted with an immediate change to a permanent password at first logon.

IA-5 (2)	**PKI-Based Authentication:** The information system, for PKI-based authentication: a. Validates certifications by constructing and verifying a certification path to an accepted trust anchor including checking certificate status information; b. Enforces authorized access to the corresponding private key; c. Maps the authenticated identity to the account of the individual or group; and d. Implements a local cache of revocation data to support path discovery and validation in case of inability to access revocation information via the network.	Status		Type	
		In Place	X	Common	
		Planned		Hybrid	
		In Place and Planned		System Specific	X
		Not Applicable			
The SCGSC system uses Entrust and DigiCert SSL certificates to support PKI-based authentication.					

IA-5 (3)	**In-Person or Trusted Third-Party Registration:** The organization requires that the registration process to receive passwords be conducted in person by the IT Director with authorization by the SCG President.	Status		Type	
		In Place	X	Common	
		Planned		Hybrid	
		In Place and Planned		System Specific	X
		Not Applicable			
The SCG IT Director conducts an in-person exchange of information to register and establish a user for accessing the SCG Secure Cloud system.					

IA-5 (11)	**Hardware Token-Based Authentication:** The information system, for hardware token-based authentication, employs mechanisms that satisfy token quality requirements.	Status		Type	
		In Place		Common	
		Planned		Hybrid	
		In Place and Planned		System Specific	X
		Not Applicable	X		

The system does not have a requirement to support hardware tokens. Therefore, this control is Not Applicable.

IA-6	**Authenticator Feedback:** The information system obscures feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.	Status		Type	
		In Place	X	Common	
		Planned		Hybrid	
		In Place and Planned		System Specific	X
		Not Applicable			

The SCG Secure Cloud system uses Microsoft Kerberos authentication solution that effectively masks and encrypts password information, which meets this control.

IA-7	**Cryptographic Module Authentication:** The information system implements mechanisms for authentication to a cryptographic module that meet the requirements of applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance for such authentication.	Status		Type	
		In Place	X	Common	
		Planned		Hybrid	
		In Place and Planned		System Specific	X
		Not Applicable			

The SCGSC system uses Entrust and DigiCert SSL certificates to support Cryptographic Module Authentication.

IA-8	**Identification and Authentication (Non-Organizational Users):** The information system uniquely identifies and authenticates non-organizational users (or processes acting on behalf of non-organizational users) prior to gaining access to all Department systems and networks (unless a risk-based decision is made for a particular system that does not require non-organization user authentication).	Status		Type	
		In Place		Common	
		Planned		Hybrid	
		In Place and Planned		System Specific	X
		Not Applicable	X		

Non-organizational users are not permitted access to the SCG Secure Cloud system per organizational policy. Therefore, this control is Not Applicable.

IA-8 (1)	**Acceptance of PIV Credentials from Other Agencies:** The information system accepts and electronically verifies Personal Identity Verification (PIV) credentials from other federal agencies.	Status		Type	
		In Place		Common	
		Planned		Hybrid	
		In Place and Planned		System Specific	X
		Not Applicable	X		

The SCG Secure Cloud system does not support PIV authentication services as there is no requirement for this in the technical solution from the government. Therefore, this control is Not Applicable.

IA-8 (2)	**Acceptance of Third-Party Credentials:** The information system accepts only FICAM-approved third-party credentials.	Status		Type	
		In Place		Common	
		Planned		Hybrid	
		In Place and Planned		System Specific	X
		Not Applicable	X		

The SCG Secure Cloud system does not support FICAM authentication services as there is no requirement in the technical solution from the government. Therefore, this control is Not Applicable.

IA-8 (3)	**Use of FICAM-Approved Products:** The organization employs only FICAM-approved information system components in information systems to accept third-party credentials.	Status		Type	
		In Place		Common	
		Planned		Hybrid	
		In Place and Planned		System Specific	X
		Not Applicable	X		

The SCG Secure Cloud system does not support FICAM authentication services as there is no requirement in the technical solution from the government. Therefore, this control is Not Applicable.

IA-8 (4)	**Use of FICAM-Issued Profiles:** The information system conforms to FICAM-issued profiles.	Status		Type	
		In Place		Common	
		Planned		Hybrid	
		In Place and Planned		System Specific	X
		Not Applicable	X		

The SCG Secure Cloud system does not support FICAM authentication services as there is no requirement in the technical solution from the government. Therefore, this control is Not Applicable.

11. Incident Response (IR)

The status of incident response controls for the SCGSC system is as indicated in the following table:

<table>
<tr><th>Control Number</th><th>Description of Control</th><th>Control Status/Type</th></tr>
<tr><td>IR-1</td><td>Incident Response Policy and Procedures:
The organization:
a. Develops, documents, and disseminates to the SCG IT staff and managers:
1. An incident response policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance, in accordance with the HHS Policy for Information Technology Security and Privacy Incident Reporting and Response, and HHS Policy for Responding to Breaches of Personally Identifiable Information; and
2. Procedures to facilitate the implementation of the incident response policy and associated incident response controls; and
b. Reviews and, if necessary, updates the current:
1. Incident response policy at least annually; and
2. Incident response procedures at least annually.</td><td><table>
<tr><th>Status</th><th></th><th>Type</th><th></th></tr>
<tr><td>In Place</td><td>X</td><td>Common</td><td></td></tr>
<tr><td>Planned</td><td></td><td>Hybrid</td><td></td></tr>
<tr><td>In Place and Planned</td><td></td><td>System Specific</td><td>X</td></tr>
<tr><td>Not Applicable</td><td></td><td></td><td></td></tr>
</table></td></tr>
<tr><td colspan="3">Incident response policies and procedures for the SCG Secure Cloud system can be found in the Incident Response Plan (IRP). The IRP addresses the requirements and mechanisms to be implemented across the SCGSC’s operating environment. At a high level, this policy addresses the purpose, scope, roles and responsibilities, management commitment, coordination among organizational entities, and requirements to comply with incident response.

The objective of this plan is to insure information security incidents are responded to in a timely and appropriate manner and recovery from incidents is efficient and effective. The</td></tr>
</table>

policy is consistent with SCG's mission, and functions with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. The SCGSC IRP contains procedural information about Incident communication, roles and responsibilities, incident response, report generation, and post-incident activities.
It is the responsibility of SCG President, Vice President of Administration, and the Information Technology (IT) Director to develop, disseminate, and annually review/update the SCG Incident Response Policy. The IT Director disseminates the policy to all Privileged Users by emailing a link to the document's SCG intranet location prior to authorizing privileged user status. The IT Director requests a response email from the Privileged User, confirming that Privileged User has read and understands the document. The plan is distributed to the SCG IT staff and managers and is available in read-only format on the SCG Intranet. The policy and procedures will be reviewed at least annually or following a major incident response and updated as needed.

The Incident Response Plan is located on the SCG Intranet that is available to all SCG personnel at http://web-dev/intranet-sql. The intranet server is located in the Gaithersburg facility at 656 Quince Orchard Road, Gaithersburg, MD 20878.

IR-2	**Incident Response Training:** The organization provides incident response training to information system users consistent with assigned roles and responsibilities: a. Within one (1) month of assuming an incident response role or responsibility; b. When required by information system changes; and c. Annually thereafter.	Status		Type	
		In Place	X	Common	
		Planned		Hybrid	
		In Place and Planned		System Specific	X
		Not Applicable			

Information on incident response testing, training, and exercise can be found in Section 13 of the **Incident Response Plan**.

IR-3	**Incident Response Testing:** The organization tests the incident response capability for the information system annually using appropriate tests and exercises (e.g., the use of checklists, walk-through or tabletop exercises, simulations [parallel/full interrupt], comprehensive exercises) to determine the incident response effectiveness and documents the results.	Status		Type	
		In Place	X	Common	
		Planned		Hybrid	
		In Place and Planned		System Specific	X
		Not Applicable			

Information on incident response testing, training, and exercise can be found in Section 13 of the **Incident Response Plan**. Annual TT&E events will be conducted that address contingency planning, incident response, and disaster recovery policies and procedures. The results of TT&E events are documented in the after-action report (AAR).

IR-3 (2)	**Coordination with Related Plans:** The organization coordinates incident response testing with organizational elements (e.g., physical security, emergency preparedness, response, and notification) responsible for related plans (e.g., Contingency Plans, Disaster Recovery Plans).	Status		Type	
		In Place	X	Common	
		Planned		Hybrid	
		In Place and Planned		System Specific	X
		Not Applicable			

Information on incident response training can be found in Section 13 of the **Incident Response Plan**, Version 1.4. To ensure coordination with related plans, the annual TT&E events will be designed to address contingency planning, incident response, and disaster recovery policies and procedures. In addition, the **Operations and Maintenance Plan** incorporates rigorous test and validation procedures that are used as a regular part of exercises and tests that strengthen the system's overall security posture.

IR-4	**Incident Handling:** The organization: a. Implements an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery; b. Coordinates incident handling activities with contingency planning activities; and c. Incorporates lessons learned from ongoing incident handling activities into incident response procedures, training, and testing/exercises, and implements the resulting changes accordingly.	Status		Type	
		In Place	X	Common	
		Planned		Hybrid	
		In Place and Planned		System Specific	X
		Not Applicable			

Guidance and procedures for incident response can be found in Section 9 of the **Incident Response Plan**, Version 1.4. The section addresses preparation, prevention, detection and analysis, documentation, reporting, containment, eradication, recovery, and post-incident activities.

IR-4 (1)	**Automated Incident Handling Processes:** The organization employs automated mechanisms to support the incident handling process.	Status		Type	
		In Place	X	Common	
		Planned		Hybrid	
		In Place and Planned		System Specific	X
		Not Applicable			

SCG employs automated detection capabilities including the Cisco IPS and Symantec anti-virus software to support incident handling for the SCGSC system. The system logs also assist SCG in handling and responding to incidents.

IR-5	**Incident Monitoring:** The organization tracks and documents information system security incidents.	Status		Type	
		In Place	X	Common	
		Planned		Hybrid	
		In Place and Planned		System Specific	X
		Not Applicable			

Information about documentation of information system security incidents can be found in Section 9.2.4 of the **Incident Response Plan**, Version 1.4.

IR-6	**Incident Reporting:** The organization: a. Requires personnel to report suspected security incidents to the IRT Manager as soon as possible and no more than 1 hour following the discovery for Level 1 and Level 2 incidents; and b. Reports security incidents to the NIDDK ISSO and HHS CSIRC.	Status		Type	
		In Place	X	Common	
		Planned		Hybrid	
		In Place and Planned		System Specific	X
		Not Applicable			

Information about incident reporting can be found in Section 9.2.6 of the **Incident Response Plan**, Version 1.4.

IR-6 (1)	**Automated Reporting:** The organization employs automated mechanisms to assist in the reporting of security incidents.	Status		Type	
		In Place	X	Common	
		Planned		Hybrid	
		In Place and Planned		System Specific	X
		Not Applicable			

SCG Secure Cloud's firewall is the first line of defense against hackers/intrusions. It is equipped with an IPS (Intrusion Prevention System) added feature that automatically updates its database with Cisco's database. All known signatures of hackers/intrusions are detected and blocked continuously. All logs are sent to a centralized log server using Kiwi Syslog. The second line of defense is Symantec Endpoint Protection Suite Enterprise. It runs continuous on all SCGSC servers and prevents spams, viruses, and intrusions. All databases are scanned weekly and all (security and virus) alerts are emailed directly to the IT Director.

IR-7	**Incident Response Assistance:** The organization provides an incident response support resource, integral to the organizational incident response capability that offers advice and assistance to users of the information system for the handling and reporting of security incidents.	Status: In Place X; Planned; In Place and Planned; Not Applicable Type: Common; Hybrid; System Specific X

The IT Director will review Security Incidences, Security Alerts, Product Security Bulletins, and Virus Bulletins to keep abreast of the security measures, types of attacks, potential vulnerabilities, and other developments in cybersecurity. The IT Director will review and take actions where needed to ensure the SCGSC system is protected against serious vulnerabilities. Details on Vulnerability Management are outlined in Section 10 of the **Incident Response Plan** (IRP).

IR-7 (1)	**Automation Support for Availability of Information/ Support:** The organization employs automated mechanisms to increase the availability of incident response-related information and support.	Status: In Place X; Planned; In Place and Planned; Not Applicable Type: Common; Hybrid; System Specific X

An added feature of the SCG Secure Cloud's firewall IPS (Intrusion Prevention System) provides reports that are queried and saved. The Symantec Endpoint Protection Suite Enterprise sends security and virus alerts directly to the IT Director via e-mail.

IR-8	**Incident Response Plan:** The organization: a. Develops an incident response plan that: 1. Provides the organization with a roadmap for implementing its incident response capability; 2. Describes the structure and organization of the incident response capability; 3. Provides a high-level approach for how the incident response capability fits into the overall organization; 4. Meets the unique requirements of the organization, which relate to mission, size, structure, and functions; 5. Defines reportable incidents; 6. Provides metrics for measuring the incident response capability within the organization;	Status: In Place X; Planned; In Place and Planned; Not Applicable Type: Common; Hybrid; System Specific X

	7. Defines the resources and management support needed to effectively maintain and mature an incident response capability; and 8. Is reviewed and approved by the SCG President, Vice President of Administration, and IT Director; b. Distributes copies of the incident response plan to the SCG IT staff and managers responsible for the SCGSC system; c. Reviews the incident response plan at least annually; d. Updates the incident response plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing; e. Communicates incident response plan changes to the SCG IT staff and managers responsible for the SCGSC system; and f. Protects the incident response plan from unauthorized disclosure and modification.	
The **Incident Response Plan** for the SCG Secure Cloud system provides the policy and procedures for responding to incidents. The plan is tailored to the specific design and requirements of the SCGSC system. The plan is distributed to the SCG IT personnel and managers responsible for the SCGSC system. The policy and procedures for incident response will be reviewed and updated annually or when system changes dictate, and the plan will be updated accordingly. The plan will be posted on the SCG Intranet in a read-only format to facilitate access by SCG staff.		

12. Maintenance (MA)

The status of maintenance controls for the SCGSC system is as indicated in the following table:

Control Number	Description of Control	Control Status/Type
MA-1	**System Maintenance Policy and Procedures:** The organization: a. Develops, documents, and disseminates to the IT personnel: 1. A system maintenance policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and	Status: In Place X; Planned; In Place and Planned; Not Applicable Type: Common; Hybrid; System Specific X

	2. Procedures to facilitate the implementation of the system maintenance policy and associated system maintenance controls; and b. Reviews and updates the current: 1. System maintenance policy at least annually; and 2. System maintenance procedures at least annually.	

System Operations and Maintenance Plan document addresses the requirements and mechanisms to be implemented across SCGSC's operating environment. At a high level, this policy addresses the purpose, scope, roles and responsibilities, management commitment, coordination among organizational entities, and requirements to comply with auditing and accountability. Maintenance is performed through security patch updates, hardened and current configurations, continuous monitoring of systems, and active management for all system components. The policy is consistent with SCG's mission, and functions with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.

It is the responsibility of the SCG President, Vice President of Administration, and Information Technology (IT) Director to develop, disseminate, and annually review/update the SCGSC Maintenance policy and plan. The document is posted on the SCG Intranet for access by all SCG personnel. The IT Director disseminates the policy to all Privileged Users by emailing a link to the document's SCG intranet location prior to authorizing privileged user status. The plan is reviewed and updated at least annually and whenever there is a change in the SCGSC system components (e.g., new switch or tape backup equipment). The IT Director or Program Manager requests a response email from the Privileged User, confirming that Privileged User has read and understands the document.

The **System Operations and Maintenance Plan** is located on the SCG Intranet that is available to all SCG personnel at http://web-dev/intranet-sql. The intranet server is located in the Gaithersburg facility at 656 Quince Orchard Road, Gaithersburg, MD 20878.

MA-2	**Controlled Maintenance:** The organization: a. Schedules, performs, documents, and reviews records of maintenance and repairs on information system components in accordance with manufacturer or vendor specifications and/or organizational requirements; b. Approves and monitors all maintenance activities, whether performed on site or remotely and whether the equipment is serviced on site or removed to another location; c. Requires that the IT Director explicitly approve the removal of the information system or	

Status		Type	
In Place	X	Common	
Planned		Hybrid	
In Place and Planned		System Specific	X
Not Applicable			

	system components from organizational facilities for off-site maintenance or repairs; d. Sanitizes equipment to remove all information from associated media prior to removal from organizational facilities for off-site maintenance or repairs; e. Checks all potentially impacted security controls to verify that the controls are still functioning properly following maintenance or repair actions; and f. Includes the type of maintenance performed, who performed it, when it was performed, and any comments regarding the maintenance in organizational maintenance records. The records also note review of maintenance activities by IT Director.	

Controlled maintenance information for the SCGSC system can be found in the **Operations and Maintenance Plan for the SCG Secure Cloud System** document. All maintenance and servicing of the SCGSC occurs onsite at the Gaithersburg facility. There is no remote maintenance for the SCGSC and SCG prohibits the removal of SCGSC components from the SCG facility for maintenance or servicing. All maintenance is performed by qualified, experienced SCG IT staff or if an outside technician is called in to service an SCGSC component, the work is supervised by SCG IT personnel. All maintenance activities are documented in a log that notes the service performed, the individual who performed it, the date it was performed, the date it was reviewed by the IT Director, and the IT Director's approval of the work. It is SCG's policy that security controls are checked and verified as functioning properly after each maintenance activity is performed. This check is performed by the IT Director when he inspects and approves the maintenance work.

MA-3	**Maintenance Tools:** The organization approves, controls, and monitors information system maintenance tools.	Status		Type	
		In Place	X	Common	
		Planned		Hybrid	
		In Place and Planned		System Specific	X
		Not Applicable			

There is a list of maintenance tools approved for use in the SCGSC environment in Section 4.1.7 of the **System Operations and Maintenance Plan**, Version 1.5. These tools are stored in the locked office of a member of the IT staff.

MA-3 (1)	**Inspect Tools:** The organization inspects all maintenance tools (e.g., diagnostic and test equipment) carried into a facility by maintenance personnel for obvious improper modifications.	Status		Type	
		In Place	X	Common	
		Planned		Hybrid	
		In Place and Planned		System Specific	X
		Not Applicable			

Any tools brought into the SCG Secure Cloud facility for use in repairing or maintaining SCGSC components will be inspected by the IT Director to ensure they are appropriate for use on the equipment. All work performed on SCGSC equipment will be monitored by the IT Director or another qualified, experienced member of the SCG IT staff. System and security functionality will be checked following each maintenance activity regardless of who performs the work.

MA-3 (2)	**Maintenance Tools:** The organization checks all media containing diagnostic and test programs (e.g., software or firmware used for system maintenance or diagnostics) for malicious code before the media are used in the information system.	Status		Type	
		In Place	X	Common	
		Planned		Hybrid	
		In Place and Planned		System Specific	X
		Not Applicable			

Per the **System Operation and Maintenance Plan**, all media will be scanned for malicious code or other malware before it is allowed to be used for diagnostics or maintenance in the SCG Secure Cloud environment.

MA-4	**Nonlocal Maintenance:** The organization: a. Approves and monitors nonlocal maintenance and diagnostic activities; b. Allows the use of nonlocal maintenance and diagnostic tools only as consistent with organizational policy and documented in the security plan for the information system; c. Employs strong authenticators in the establishment of nonlocal maintenance and diagnostic sessions; d. Maintains records for nonlocal maintenance and diagnostic activities; and e. Terminates session and network connections when nonlocal maintenance is completed.	Status		Type	
		In Place		Common	
		Planned		Hybrid	
		In Place and Planned		System Specific	X
		Not Applicable	X		

All maintenance for the SCG Secure Cloud system will be performed on premise. Therefore, this control is Not Applicable.

MA-4 (1)	**Auditing and Review:** The organization: a. Audits nonlocal maintenance and diagnostic sessions and other audit events, if necessary; and b. Reviews the records of the maintenance and diagnostic sessions.	Status		Type	
		In Place		Common	
		Planned		Hybrid	
		In Place and Planned		System Specific	X
		Not Applicable	X		

All maintenance for the SCG Secure Cloud system will be performed on premise. Therefore, this control is Not Applicable.

MA-4 (2)	**Document Nonlocal Maintenance:** The organization documents in the security plan for the information system, the policies and procedures for the establishment and use of nonlocal maintenance and diagnostic connections.	Status		Type	
		In Place		Common	
		Planned		Hybrid	
		In Place and Planned		System Specific	X
		Not Applicable	X		

All maintenance for the SCG Secure Cloud system will be performed on premise. Therefore, this control is not applicable.

MA-5	**Maintenance Personnel:** The organization: a. Establishes a process for maintenance personnel authorization and maintains a list of authorized maintenance organizations or personnel; b. Ensures that non-escorted personnel performing maintenance on the information system have required access authorizations; and c. Designates organizational personnel with required access authorizations and technical competence to supervise the maintenance activities of personnel who do not possess the required access authorizations.	Status		Type	
		In Place	X	Common	
		Planned		Hybrid	
		In Place and Planned		System Specific	X
		Not Applicable			

SCGSC maintenance personnel, their roles, and authorizations are defined in the **System Operations and Maintenance Plan**, Version 1.5. Maintenance will be performed under the supervision of the IT Director by SCG IT staff. In the event a technician is brought in to service an SCGSC component, the work will be supervised by the IT Director or a qualified, experienced member of the SCG IT staff. The IT Director designates the personnel with the technical competence to perform and supervise maintenance activities. The SCG IT staff members are the only individuals who possess the required access authorization to perform the maintenance.

MA-6	**Timely Maintenance:** The organization obtains maintenance support and/or spare parts for SCGSC components as identified in the SSP within 7 days of failure (which is within the RTO).	Status: In Place X; Planned; In Place and Planned; Not Applicable Type: Common; Hybrid; System Specific X
SCG has a plan for restoring the entire SCG Secure Cloud 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 a formal **Contingency Plan**, and are reviewed at least annually 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 also maintains good relationships with trusted vendors that supply hardware/software and parts to SCG, which can be shipped overnight when necessary and used by SCG IT staff to repair the SCGSC system as quickly as possible, usually less than 7 days from the time of failure.		

13. Media Protection (MP)

The status of media protection controls for the SCGSC system is as indicated in the following table:

Control Number	Description of Control	Control Status/Type
MP-1	**Media Protection Policy and Procedures:** The organization: a. Develops, documents, and disseminates to the SCG IT staff: 1. A media protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the media protection policy and associated media protection controls; and b. Reviews and updates the current: 1. Media protection policy at least annually; and 2. Media protection procedures at least annually.	Status: In Place X; Planned; In Place and Planned; Not Applicable Type: Common; Hybrid; System Specific X

The SCGSC **Media Protection Policy and Procedures** addresses the requirements and mechanisms to be implemented across SPCG's operating environment. At a high level, this policy addresses the purpose, scope, roles and responsibilities, management commitment, coordination among organizational entities, and requirements to comply with media protection. It applies to all SCG electronic media, CDs, DVDs, and USB drives that are used internally or in a capacity to provide client services. Additionally, the policy focuses the handling of other security risks associated with media protection such as loss, theft, or physical damage to disks and other removable media devices. The policy is consistent with SCG's mission, and functions with applicable Federal Laws, Executive Orders, directives, policies, regulations, standards, and guidance.

It is the responsibility of SCG President, Vice President of Administration, and the Information Technology (IT) Director to develop, disseminate, and annually review/update the SCGSC Media Protection Training Policy. The IT Director or Program Manager disseminates the policy to all Privileged Users by emailing a link to the document's SCG intranet location prior to authorizing privileged user status. The IT Director requests a response email from the Privileged User, confirming that Privileged User has read and understands the document.

The policy and procedures are located on the SCG Intranet that is available to all SCG personnel at http://web-dev/intranet-sql. The intranet server is located in the Gaithersburg facility at 656 Quince Orchard Road, Gaithersburg, MD 20878.

MP-2	**Media Access:** The organization restricts access to SCGSC digital media (i.e., backup tapes) to SCG IT personnel.	Status		Type	
		In Place	X	Common	
		Planned		Hybrid	
		In Place and Planned		System Specific	X
		Not Applicable			

In accordance with the **Media Protection Policy and Procedures for SCG Secure Cloud System,** SCG restricts access to digital media to authorized individuals. The individuals authorized to access digital media for the SCGSC system are the SCG IT personnel. There are no non-digital media for the SCGSC system.

MP-3	**Media Marking:** The organization: a. Marks information system media indicating the distribution limitations, handling caveats, and applicable security markings (if any) of the information commensurate with the FIPS 199 security categorizations for confidentiality and integrity of the data; and b. Exempts no digital media from marking even if the media remains within secure SCG facilities.	Status		Type	
		In Place	X	Common	
		Planned		Hybrid	
		In Place and Planned		System Specific	X
		Not Applicable			

SCG's policies and procedures for media marking are defined in the **Media Protection Policy and Procedures for SCG Secure Cloud System** document. The digital media for the SCGSC system (i.e., backup tapes) must be marked to indicate that they contain "Sensitive but Unclassified" information. They also must be marked appropriately to facilitate retrieval by IT staff. Specific marking instructions are specified in the policy and procedures document.

MP-4	**Media Storage:** The organization: a. Physically controls and securely stores digital media (i.e., backup tapes) within access controlled storage cabinets; and b. Protects information system media until the media are destroyed or sanitized using approved equipment, techniques, and procedures.	Status		Type	
		In Place	X	Common	
		Planned		Hybrid	
		In Place and Planned		System Specific	X
		Not Applicable			

SCG's policies and procedures for media storage are defined in the **Media Protection Policy and Procedures for SCG Secure Cloud System** document. Digital media (i.e., backup tapes) for the SCGSC are stored in the IT Director's locked office inside a locked fire safe. Access to the backup tapes is limited to the IT staff. The backup tapes stored at the alternate site (Frederick, MD facility) are stored in an access controlled building inside a locked fire safe cabinet. The IT Director authorizes access to the stored digital media. Digital media are stored for a minimum of 3 years but may be retained for up to 7 years. The IT staff test a sample of archived digital media annually to ensure the media are in good condition and are readable.

MP-5	**Media Transport:** The organization: a. Protects and controls digital media (i.e., tape backups) during transport outside of controlled areas using cryptography (in the case of sensitive information), or security safeguards commensurate with the FIPS 199 security categorizations for confidentiality and integrity of the data; b. Maintains accountability for information system media during transport outside of controlled areas; c. Documents activities associated with the transport of information system media; and d. Restricts the activities associated with the transport of information system media to authorized personnel.	Status		Type	
		In Place	X	Common	
		Planned		Hybrid	
		In Place and Planned		System Specific	X
		Not Applicable			

SCG's policies and procedures for protecting and controlling media during transport are defined in the **Media Protection Policy and Procedures for SCG Secure Cloud System** document. Only the SCG President is permitted to transport SCGSC tape backups from the Gaithersburg to offsite storage in Staunton, VA. Backups are performed at both primary and alternate site so no transport of tapes is necessary between these two locations. All backup tapes are encrypted using 128-bit AES encryption with an 8-character pass phrase key to protect the "Sensitive but Unclassified" information on the tapes.

MP-5 (4)	**Cryptographic Protection:** The information system implements cryptographic mechanisms to protect the confidentiality and integrity of information stored on digital media during transport outside of controlled areas.	Status		Type	
		In Place	X	Common	
		Planned		Hybrid	
		In Place and Planned		System Specific	X
		Not Applicable			

In accordance with the **Media Protection Policy and Procedures for SCG Secure Cloud System** document, SCG uses cryptographic mechanisms to protect the confidentiality and integrity of information stored on digital media (i.e., backup tapes) during transport from SCG Gaithersburg to Staunton, VA. The tapes transported are encrypted using 128-bit AES encryption with an 8-character pass phrase key to protect the "Sensitive but Unclassified" information on the tapes.

MP-6	**Media Sanitization:** The organization: a. Sanitizes digital media (i.e., tapes and hard drives) pursuant to Appendix A prior to disposal, release out of organizational control, or release for reuse using Symantec BackupExec's Long Erase in accordance with applicable federal and organizational standards and policies; and b. Employs sanitization mechanisms with the strength and integrity commensurate with the security category or classification of the information.	Status		Type	
		In Place	X	Common	
		Planned		Hybrid	
		In Place and Planned		System Specific	X
		Not Applicable			

In accordance with the **Media Protection Policy and Procedures for SCG Secure Cloud System** document, SCG employs appropriate sanitization techniques and procedures to sanitize information system media prior to disposal, release, or reuse. For sanitizing SCGSC backup tapes for reuse, SCG performs Long Erase on the digital media using Symantec BackupExec, which ensures that the information on the media cannot be recovered. This sanitization method has been approved by the SO and the IT Director, who deem them appropriate for the sensitivity of the information contained on the digital media for the SCGSC system. SCG sanitizes hard drives using the manufacturer-specific utility for low-level formatting. This writes 0s to all sectors on the hard drive making rendering recovery of the data infeasible.

MP-7	**Media Use:** The organization prohibits the use of portable storage devices in the SCGSC environment using physical security safeguards.	Status		Type	
		In Place	X	Common	
		Planned		Hybrid	
		In Place and Planned		System Specific	X
		Not Applicable			

SCG's policies and procedures for media use are defined in the **Media Protection Policy and Procedures for SCG Secure Cloud System** document. SCG prohibits the use of portable storage devices in the SCGSC environment. This policy is enforced by the IT Director by limiting access to the SCGSC system. The USB port on the host server is not enabled, which is a configuration safeguard to prevent the use of a portable storage device.

MP-7 (1)	**Prohibit Use Without Owner:** The organization prohibits the use of portable storage devices in organizational information systems when such devices have no identifiable owner.	Status		Type	
		In Place	X	Common	
		Planned		Hybrid	
		In Place and Planned		System Specific	X
		Not Applicable			

In accordance with the **Media Protection Policy and Procedures for SCG Secure Cloud System** document, SCG prohibits the use of any portable storage device in the SCGSC environment regardless of ownership. Currently, the only storage device approved by SCG for storing SCGSC data is the tape backup. SCG prohibits the use of portable storage devices in the SCGSC environment. This policy is enforced by the IT Director by limiting access to the SCGSC system. The USB port on the host server is not enabled, which is a configuration safeguard to prevent the use of a portable storage device.

14. Physical and Environmental Protection (PE)

The status of physical and environmental protection controls for the SCGSC system is as indicated in the following table:

Control Number	Description of Control	Control Status/Type			
PE-1	**Physical and Environmental Protection Policy and Procedures:** The organization: a. Develops, documents, and disseminates to SCG personnel: 1. A physical and environmental protection policy that addresses purpose, scope, roles, responsibilities, management commitment,	Status		Type	
		In Place	X	Common	
		Planned		Hybrid	
		In Place and Planned		System Specific	X
		Not Applicable			

	coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the physical and environmental protection policy and associated physical and environmental protection controls; and b. Reviews and, if necessary, updates the current: 1. Physical and environmental protection policy at least annually; and 2. Physical and environmental protection procedures at least annually.	

The SCGSC **Facility and Systems Access Policies and Procedures** addresses the requirements and mechanisms to be implemented across SCGSC's operating environment. At a high level, this policy addresses the purpose, scope, roles and responsibilities, management commitment, coordination among organizational entities, and requirements to comply with security awareness and training. Additionally, this policy outlines requirements to manage and protect all company and client information, including low and moderately sensitive information. The policy is consistent with SCG's mission, and functions with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.

It is the responsibility of SCG President, IT Director, and Vice President of Administration to develop, disseminate, and annually review/update the SCG Facility and Systems Access Policy. The Vice President of Administration and IT Director will monitor sources and notices and notify staff when there is a need to implement increased vigilance and heighten security operations. This policies and procedures document must be disseminated to the SCG employees who have user accounts for the SCG Secure Cloud system. It also is available to all SCG employees on the SCG Intranet.

The policy and procedures are located on the SCG Intranet that is available to all SCG personnel at: http://web-dev/intranet-sql. The intranet server is located in the Gaithersburg facility at 656 Quince Orchard Road, Gaithersburg, MD 20878.

PE-2	**Physical Access Authorizations:** The organization: a. Develops, approves, and maintains a list of individuals with authorized access to the facility where the information system resides; b. Issues authorization credentials for facility access; c. Reviews the access list detailing authorized facility access by individuals at least annually; and d. Removes individuals from the facility access list when access is no longer required.	

Status		Type	
In Place	X	Common	
Planned		Hybrid	
In Place and Planned		System Specific	X
Not Applicable			

Only authorized individuals are granted access to the SCG facilities in both Gaithersburg and Frederick Maryland. Access to both SCGSC environments is further restricted to only those personnel requiring access to SCGSC equipment.

Entrances to SCG's offices on the second and seventh floors are locked at all times and programmed fobs are required to access the office space on both the second and seventh floors. When an employee swipes a fob for access to SCG offices, an electronic record is created that reports the employee's name, date, and time of entry. SCG staff also must sign in and out to ensure that the receptionist knows who is in the office and to create a hardcopy record of arrivals and departures.

The two additional entrances to SCG's second floor offices are locked at all times and accessible only by SCG staff using the fob access, which creates an electronic log of the individual accessing the space and time of access. In addition, SCG's entrances and priority rooms are monitored by surveillance cameras that record events on a DVR when triggered by detected motion. All entrances into SCG space are equipped with alarms that will activate in the event of unauthorized access and when a door is propped open for more than 1 minute.

PE-3	**Physical Access Control:** The organization: a. Enforces physical access authorizations at entry/exit points to the facility where the information system resides by; 1. Verifying individual access authorizations before granting access to the facility; and 2. Controlling ingress/egress to the facility using fob access to the office space and the server room; b. Maintains physical access audit logs for the office and server room at the points of entry/exit; c. Provides security safeguards to control access to areas within the facility officially designated as publicly accessible; d. Escorts all visitors and monitors visitor activity within SCG's secure office space; e. Secures keys, combinations, and other physical access devices; f. Inventories fobs and keys on an annual basis; and g. Changes combinations and keys when keys are lost, combinations are compromised, or individuals are transferred or terminated.	Status		Type	
		In Place	X	Common	
		Planned		Hybrid	
		In Place and Planned		System Specific	X
		Not Applicable			

The SCGSC **Facility and Systems Access Policies and Procedures** document describes how SCG controls physical access to the facility and room where the SCG Secure Cloud system resides. These policies and procedures ensure that only authorized individuals have access to the room where the SCGSC system resides. SCG's office space on the second and seventh floors of 656 Quince Orchard Boulevard in Gaithersburg are locked at all times. Employee's access facilities using individually programmed fobs; visitors must be granted access through the main entry and sign into the visitor's log. All visitors must be escorted and their activities monitored by SCG staff when they are within SCG's secure office space.

PE-4	**Access Control for Transmission Medium:** The organization controls physical access to the SCGSC server room and prohibits cell phone usage within that room using posted signage and enforcement of disciplinary action for failure to comply.	Status		Type	
		In Place	X	Common	
		Planned		Hybrid	
		In Place and Planned		System Specific	X
		Not Applicable			

Access to information system distribution and transmission lines within the SCGSC Gaithersburg facility is controlled within the facility by facility physical security controls. Cabling is labeled appropriately for easy identification and run in cable trays or conduit in an orderly manner under a raised floor to protect against damage.

To prevent unauthorized individuals from obtaining access to confidential output, physical access to the information system output devices is limited to crash carts for the use of administrators. Video surveillance and programmed fob or key access provide security monitoring with physical access to the power equipment and power cabling for SCG and SCGSC.

Access to all transmission medium within the building is controlled either by key or individually programmed fob reader.

PE-5	**Access Control for Output Devices:** The organization controls physical access to information system output devices to prevent unauthorized individuals from obtaining the output.	Status		Type	
		In Place	X	Common	
		Planned		Hybrid	
		In Place and Planned		System Specific	X
		Not Applicable			

To prevent unauthorized individuals from obtaining access to confidential output access controls are set in place separate for SCG and authorized SCGSC personnel. Only authorized SCGSC personnel have access to unlock the server room door on the 7th floor of the Gaithersburg, MD facility. Furthermore, appliances that interact with SCGSC information are stored in locked server cages. Video cameras are installed outside of the server room and directed towards the server door for added surveillance. No cell phones and printers are permitted inside of the server room.

PE-6	**Monitoring Physical Access:** The organization: a. Monitors physical access to the facility where the information system resides to detect and respond to physical security incidents; b. Reviews physical access logs weekly and upon occurrence of a security breach or indications of potential events; and c. Coordinates results of reviews and investigations with the organizational incident response capability.	Status: In Place X; Planned; In Place and Planned; Not Applicable Type: Common; Hybrid; System Specific X

The SCGSC **Facility and Systems Access Policies and Procedures** document describes how SCG monitors physical access to SCG facilities and the server room where the SCG Secure Cloud System resides. When a security breach is suspected, access logs and video surveillance footage are reviewed by the Vice President of Administration and IT Director to investigate the event.

PE-6 (1)	**Intrusion Alarms/Surveillance Equipment:** The organization monitors physical intrusion alarms and surveillance equipment.	Status: In Place X; Planned; In Place and Planned; Not Applicable Type: Common; Hybrid; System Specific X

The SCGSC **Facility and Systems Access Policies and Procedures** document describes how SCG monitors physical access to SCG facilities and the server room where the SCG Secure Cloud system resides. When a security breach is suspected, access logs and video surveillance footage are reviewed by the Vice President of Administration and IT Director to investigate the event.

PE-8	**Visitor Access Records:** The organization: a. Maintains visitor access records to the facility where the information system resides (except for those areas officially designated as publicly accessible) for a minimum of 3 years; and b. Reviews visitor access records at least monthly or when a potential security breach is suspected.	Status: In Place X; Planned; In Place and Planned; Not Applicable Type: Common; Hybrid; System Specific X
In accordance with the SCGSC **Facility and Systems Access Policies and Procedures**, visitor access records are maintained. These records are reviewed when a potential security breach is suspected and on an annual basis when logs are scanned and electronically archived.		

PE-9	**Power Equipment and Power Cabling:** The organization protects power equipment and power cabling for the information system from damage and destruction.	Status: In Place X; Planned; In Place and Planned; Not Applicable Type: Common; Hybrid; System Specific X
The electric panels and cabling are located in a locked mechanical room on each floor of the building. In accordance with the SCGSC **System Operation and Maintenance Plan v1.5**, the key to the mechanical room is kept in a secure location by the IT Director who controls access to this room. Only authorized personnel are allowed access to the mechanical room.		

PE-10	**Emergency Shutoff:** The organization: a. Provides the capability of shutting off power to the information system or individual system components in emergency situations; b. Places emergency shutoff switches or devices in the locked mechanical room to facilitate safe and easy access for personnel; and c. Protects emergency power shutoff capability from unauthorized activation.	Status: In Place X; Planned; In Place and Planned; Not Applicable Type: Common; Hybrid; System Specific X
Emergency power shutoff is located in the locked mechanical room of each floor of the building. The IT Director is responsible for controlling access to this room to prevent unauthorized activation of emergency power shutoff. Installing a shutoff in the server room where the SCG Secure Cloud system is located would be cost prohibitive and unnecessary.		

PE-11	**Emergency Power:** The organization provides a short-term uninterruptible power supply to facilitate an orderly shutdown of the SCGSC system and/or transition of the SCGSC system to a long-term alternate power source in the event of a primary power source loss.	Status		Type	
		In Place	X	Common	
		Planned		Hybrid	
		In Place and Planned		System Specific	X
		Not Applicable			

The organization provides a short-term uninterruptible power supply to facilitate an orderly shutdown of the SCGSC system and/or transition of the SCGSC system to a long-term alternate power source in the event of a primary power source loss. SCG provides a short-term uninterruptible power supply (UPS) to allow time for the IT staff to conduct the orderly shutdown of the SCG Secure Cloud system in the event of a primary power source loss.

PE-12	**Emergency Lighting:** The organization employs and maintains automatic emergency lighting systems that activate in the event of a power outage or disruption and that cover emergency exits and evacuation routes within the facility.	Status		Type	
		In Place	X	Common	
		Planned		Hybrid	
		In Place and Planned		System Specific	X
		Not Applicable			

SCG provides a flashlight and extra batteries in the server room where the SCG Secure Cloud system is located to provide emergency lighting in the event of a power outage. Emergency lighting located throughout the SCG office space activates in the event of a power outage. In compliance with fire codes, the emergency lighting covers emergency exits and evacuation routes in the facility.

PE-13	**Fire Protection:** The organization employs and maintains fire suppression and detection devices/systems for the information system that are supported by an independent energy source.	Status		Type	
		In Place	X	Common	
		Planned		Hybrid	
		In Place and Planned		System Specific	X
		Not Applicable			

A fire extinguisher is located in the server room where the SCG Secure Cloud system resides. The server room also contains a battery powered smoke detector (batteries are changed annually). In addition, the UPS senses room temperature and sends an e-mail alert to the IT Director and Vice President of Administration if the room temperature rises above normal conditions.

PE-13 (3)	**Automatic Fire Suppression:** The organization employs an automatic fire suppression capability for the information system when the facility is not staffed on a continuous basis.	Status		Type	
		In Place	X	Common	
		Planned		Hybrid	
		In Place and Planned		System Specific	X
		Not Applicable			

The building (including the server room where the SCG Secure Cloud system is located) is equipped with a sprinkler system that activates in the event of a fire. A plastic tarp is available to cover and protect equipment in the event the sprinkler system activates.

PE-14	**Temperature and Humidity Controls:** The organization: a. Maintains temperature and humidity levels within the facility where the information system resides at acceptable levels (between 60 and 95ºF and 30-40% humidity); and b. Monitors temperature and humidity levels continuously. An e-mail notification is automatically sent to the IT Director when the temperature and humidity levels are outside this range.	Status		Type	
		In Place	X	Common	
		Planned		Hybrid	
		In Place and Planned		System Specific	X
		Not Applicable			

The server room where the SCG Secure Cloud system resides 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.

PE-15	**Water Damage Protection:** The organization protects the information system from damage resulting from water leakage by providing master shutoff or isolation valves that are accessible, working properly, and known to key personnel.	Status		Type	
		In Place	X	Common	
		Planned		Hybrid	
		In Place and Planned		System Specific	X
		Not Applicable			

A plastic tarp is available in the server room where the SCG Secure Cloud system is located to cover and protect the system from damage in the event of a water leak or sprinkler activation. The water shutoff is located in the stairwells, which can be shut off in the event of a leak.

PE-16	**Delivery and Removal:** The organization authorizes, monitors, and controls access to the SCGSC server room and the equipment, software, and tools entering and exiting the SCGSC server room and maintains records of those items.	Status: In Place X; Planned; In Place and Planned; Not Applicable Type: Common; Hybrid; System Specific X
In accordance with the SCGSC **Facility and Systems Access Policies and Procedures,** SCG controls and monitors access to the server room where the SCG Secure Cloud system resides. The IT Director monitors and controls all deliveries of equipment, system components, and other items to the server room and maintains records of those items and the dates they were placed in the room.		

PE-17	**Alternate Work Site:** The organization: a. Employs facility, server room, and system access controls at alternate work sites; b. Assesses as feasible, the effectiveness of security controls at alternate work sites; and c. Provides a means for employees to communicate with information security personnel in case of security incidents or problems.	Status: In Place X; Planned; In Place and Planned; Not Applicable Type: Common; Hybrid; System Specific X
In accordance with the **SCG Contingency Plan**, SCG has designated its Frederick facility as the Alternate Work Site. Security controls at the Frederick facility emulate the controls employed at SCG's Gaithersburg facility.		

15. Planning (PL)

The status of security planning controls for the SCGSC system is as indicated in the following table:

Control Number	Description of Control	Control Status/Type
PL-1	**Security Planning Policy and Procedures:** The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, security planning policy that addresses purpose, scope, roles, responsibilities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the security planning policy and associated security planning controls.	Status: In Place X; Planned; In Place and Planned; Not Applicable Type: Common; Hybrid; System Specific X

The SCG Secure Cloud (SCGSC) **Security Planning Procedure v1.0** for the SCGSC system are documented in this **System Security Plan** (SSP) and address the requirements and mechanisms to be implemented across SCGSC's operating environment. At a high level, this policy addresses the purpose, scope, roles and responsibilities, management commitment, coordination among organizational entities, and requirements to comply with SCG security planning activities. The policy is consistent with SCG's mission, and functions with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.

It is the responsibility of the SCG President, the Vice President of Administration, the Information Technology (IT) Director, and the Program Manager to develop, disseminate, and annually review/update the SCG Security Planning Procedure v1.0. The IT Director disseminates the policy to all Privileged Users by emailing a link to the document's SCG intranet location prior to authorizing privileged user status. The IT Director or Program Manager requests a response email from the Privileged User, confirming that Privileged User has read and understands the document.

The policy and procedures are located on the SCG Intranet that is available to all SCG personnel at: http://web-dev/intranet-sql. The intranet server is located in the Gaithersburg facility at 656 Quince Orchard Road, Gaithersburg, MD 20878.

PL-2	**System Security Plan:** The organization develops and implements a security plan for the information system that provides an overview of the security requirements for the system and a description of the security controls in place or planned for meeting those requirements. Designated officials within the organization review and approve the plan.	Status		Type	
		In Place	X	Common	
		Planned		Hybrid	
		In Place and Planned		System Specific	X
		Not Applicable			

The **SCG Secure Cloud System Security Plan** (SSP) provides an overview of the security requirements for the system and a description of the security controls in place and planned to meet those requirements. The SSP is reviewed and approved annually by the SCG President, Vice President of Administration, IT Director, and Program Manager as well as the NIDDK System Owner, ISSO, and AO/DAA.

PL-2 (3)	**System Security Plan:** The organization plans and coordinates security-related activities affecting the information system with System Owner, IT Director/System Administrator, and ISSO before conducting such activities in order to reduce the impact on other organizational entities.	Status		Type	
		In Place	X	Common	
		Planned		Hybrid	
		In Place and Planned		System Specific	X
		Not Applicable			

All security related activities (i.e., security assessments, audits, contingency plan testing, patch management, etc.) affecting this system are coordinated with the System Owner, IT Director/System Administrator, and ISSO.

PL-4	**Rules of Behavior:** The organization establishes and makes readily available to all information system users a set of rules that describes their responsibilities and expected behavior with regard to information system usage. The organization receives signed acknowledgement from users indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to the information system.

Status		Type	
In Place	X	Common	
Planned		Hybrid	
In Place and Planned		System Specific	X
Not Applicable			

SCG makes available to all SCG Secure Cloud users the NIH IT General Rules of Behavior, which hold users accountable for their actions and responsible for information security. Users acknowledge that they have received, read, understand, and agree to abide by these Rules of Behavior by their signature of the acknowledgement statement before access to SCGSC is authorized. The signed acknowledgement statements are maintained by the SCG Human Resources Manager in the personnel files.

PL-4 (1)	**Social Media and Networking Restrictions:** The organization includes in the rules of behavior, explicit restrictions on the use of social media/networking sites and posting organizational information on public websites.

Status		Type	
In Place	X	Common	
Planned		Hybrid	
In Place and Planned		System Specific	X
Not Applicable			

SCG adheres to the NIH Social and New Media Policy (2809) with respect to social media and networking restrictions. This Policy provides guidance on the use of social and new media, including but not limited to, NIH hosted and/or funded social media sites, Web applications, and mobile Web sites. The NIH Social and New Media Policy is part of the NIH Policy Manual and is available at http://oma1.od.nih.gov/manualchapters/ management/2809/. All SCGSC users acknowledge that they have read, understand, and agree to abide by these Rules of Behavior by their signature of the acknowledgement statement before access to SCG Secure Cloud is authorized. The signed acknowledgement statements are maintained by the Vice President of Administration in the personnel files.

PL-8	**Information Security Architecture:** The organization describes the overall philosophy, requirements, and approach to be taken with regard to protecting the confidentiality, integrity, and availability of organizational information and describes how the information security architecture is integrated into and supports the enterprise

Status		Type	
In Place	X	Common	
Planned		Hybrid	
In Place and Planned		System Specific	X

	architecture and describes any information security assumptions about, and dependencies on, external services. The organization reviews and updates the information security architecture annually or after architecture updates to reflect updates in the enterprise architecture; and ensures that planned information security architecture changes are reflected in the security plan, the security Concept of Operations (CONOPS), and organizational procurements/acquisitions.	Not Applicable:
SCG updates information on the SCG Secure Cloud system architecture at least annually or after updates in the architecture. The architecture and dependencies are described in the SCGSC **System Design Document** as well as the **Contingency Plan** and **Disaster Recovery Plan** for the system.		

16. Personnel Security (PS)

The status of personnel security controls for the SCGSC system is as indicated in the following table:

Control Number	Description of Control	Control Status/Type
PS-1	**Personnel Security Policy and Procedures:** The organization: a. Develops, documents, disseminates to the SCG President, Vice President of Administration, and SCG senior managers: 1. A personnel security policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; 2. Procedures to facilitate the implementation of the personnel security policy and associated personnel security controls; and b. Reviews and, if necessary, updates the current: 1. Personnel security policy at least annually; and 2. The personnel security procedures at least annually.	Status: In Place X; Planned; In Place and Planned; Not Applicable Type: Common; Hybrid; System Specific X
SCG has adopted the Personnel Security principles established in NIST SP 800-53 “Personnel Security,” Control Family guidelines, as the official policy for the SCG Secure Cloud system. The **SCG Personnel Security Screening Policy** document outlines the personnel security standards that constitute SCG policy.		

PS-2	**Position Risk Designation:** The organization: a. Assigns a risk designation to all organizational positions; b. Establishes screening criteria for individuals filling those positions; c. Ensures that all individuals with significant security responsibilities possess, at a minimum, a Level 5 Public Trust; d. Ensures that individuals are designated to position-sensitivity levels that are commensurate with the responsibilities and risks associated with the position; and e. Reviews and, if necessary, updates position risk designations at least annually or whenever a position's duties are changed/revised/realigned, and ensures that these risk designations are consistent with U.S. Office of Personnel Management (OPM) policy and guidance.	Status / Type In Place: X Planned: In Place and Planned: Not Applicable: Common: Hybrid: System Specific: X

In accordance with the **SCG Personnel Security Screening Policy and Procedures**, SCG has assigned a risk designation to the organizational positions associated with the NIDDK contract for which the SCG Secure Cloud system is created. The screening criteria for the individuals filling the positions are specified in the **SCG Personnel Security Screening Policy and Procedures**. Risk designation positions are reviewed and updated when new positions are added to the contract and when changes in position responsibilities necessitate a change in risk designation.

PS-3	**Personnel Screening:** The organization: a. Screens individuals prior to authorizing access to the information system; b. Rescreens individuals anytime they move to a new position with a higher risk designation; c. Conducts background investigations in a manner commensurate with OPM and HHS Human Resources policy and guidance; d. Performs reinvestigations in accordance with guidance provided by current personnel security policy; and e. Refuses employees and contractors access to information systems until they have: 1. Been granted an interim clearance, and 2. Signed the appropriate access agreements.	Status / Type In Place: X Planned: In Place and Planned: Not Applicable: Common: Hybrid: System Specific: X

SCG's personnel screening policy is defined in the **SCG Personnel Security Screening Policy** document. Individuals in high risk positions are rescreened every five (5) years for the duration of the contract. The SCG IT staff who have access to the SCGSC system have undergone background investigations and fingerprinting by the NIH to receive an NIH ID and access to NIH information systems, which is more stringent than the screening implemented by SCG for new employees.

PS-4	**Personnel Termination:** The organization, upon termination of individual employment: a. Disables information system access as soon as possible but no longer than one (1) calendar day following involuntary termination or, if necessary, prior to the formal termination action and within seven (7) days for employees who voluntarily resign; b. Terminates/revokes any authenticators/credentials associated with the individual; c. Conducts exit interviews that include a discussion of the return of all security-related property (e.g., IDs, tokens, fobs, keys, and garage openers) as well as data confidentiality obligations beyond SCG employment; d. Retrieves all security-related organizational information system-related property; e. Retains access to organizational information and information systems formerly controlled by terminated individual; and f. Notifies the IT Director and Vice President of Administration as soon as possible, but not more than one (1) calendar day after the involuntary termination or voluntary resignation/termination of an employee.	Status		Type	
		In Place	X	Common	
		Planned		Hybrid	
		In Place and Planned		System Specific	X
		Not Applicable			

SCG's policy concerning securing information systems upon termination of an employee is defined in the **SCG Personnel Security Screening Policy** document. SCG disables system access immediately upon involuntary termination and within 7 days for employees who voluntarily resign. The employee's supervisor notifies the IT Director and Vice President of Administration immediately upon receipt of a resignation letter from an employee he/she supervises. The Vice President of Administration must approve all involuntary terminations so only the IT Director requires notification of the termination, which is done just before termination or during the termination.

PS-5	**Personnel Transfer:** The organization: a. Reviews and confirms ongoing operational need for current logical and physical access authorizations to information systems/facilities when individuals are reassigned or transferred to a new position within the organization; b. Initiates the re-evaluation of that individual's logical and physical access controls as soon as possible, no later than 30 days of the formal transfer action; c. Modifies access authorization as needed to correspond with any changes in operational need due to reassignment or transfer; and d. Notifies the IT Director and PM of the pending transfer/reassignment within 1 day of approval and notifies the SCG President that reassignment/transfer tasks are complete within 2 business days of completion.	Status / Type In Place: X Planned: In Place and Planned: Not Applicable: Common: Hybrid: System Specific: X

Although personnel transfers within SCG are infrequent, the **SCG Personnel Security Screening Policy** addresses personnel security and transfers within the company. Transfers/reassignments must be approved by the Vice President of Administration. The Vice President would notify the IT Director and PM of the transfer/reassignment approval within 1 day of approval. There is usually a 2-week transition period to facilitate the transfer or reassignment of employees. Prior to the end of the transition period, the Vice President of Administration would collect IDs, fobs, keys, and similar property no longer required by the employee and issue any new IDs, fobs, keys, etc., required for the new assignment. In addition, the IT Director would disable any system credentials/authenticators for accounts no longer required by the employee and create new accounts required for the new assignment. The Vice President of Administration and IT Director would notify the SCG President when transfer/reassignment tasks are completed within 2 business days of completion.

PS-6	**Access Agreements:** The organization: a. Develops and documents access agreements for organizational information systems; b. Reviews and updates the access agreements annually; and c. Ensures that individuals requiring access to organizational information and information systems: 1. Sign appropriate access agreements prior to being granted access; and 2. Re-sign access agreements to maintain access to organizational information systems when access agreements have been updated or annually.	Status / Type In Place: X Planned: In Place and Planned: Not Applicable: Common: Hybrid: System Specific: X

SCG's policies and procedures for accessing information systems, including access agreements, are defined in the SCGSC **Facility and Systems Access Policies and Procedures** document. Access agreements are reviewed by the IT Director quarterly. Rules of Behavior are updated annually and acknowledgements are re-signed annually.

PS-7	**Third-Party Personnel Security:** The organization: a. Establishes personnel security requirements including security roles and responsibilities for third-party providers; b. Requires third-party providers to comply with personnel security policies and procedures established by the organization; c. Documents personnel security requirements; d. Requires third-party providers to notify [Assignment: organization-defined personnel or roles] of any personnel transfers or terminations of third-party personnel who possess organizational credentials and/or badges, or who have information system privileges as soon as possible within a maximum of seven (7) days from the formal transfer or termination action; and e. Monitors provider compliance.	Status		Type	
		In Place		Common	
		Planned		Hybrid	
		In Place and Planned		System Specific	X
		Not Applicable	X		
SCG does not allow third-party access to the SCGSC system. Therefore, this control is Not Applicable.					

PS-8	**Personnel Sanctions:** The organization: a. Employs a formal sanctions process (that may include termination of employment, removal or disbarment from work on federal contracts or projects, suspension of access privileges, revocation of access to federal information systems and/or facilities; criminal penalties) for individuals failing to comply with established information security policies and procedures; and b. Notifies the employee's supervisor, PM, and IT Director as soon as possible but not more than 7 days when a formal employee sanctions process is initiated, identifying the individual sanctioned and the reason for the sanction.	Status		Type	
		In Place	X	Common	
		Planned		Hybrid	
		In Place and Planned		System Specific	X
		Not Applicable			
The SCGSC **Facility and Systems Access Policies and Procedures** document states that disciplinary action will be taken when employees fail to comply with SCG's established security policies and procedures. The specific disciplinary action taken will be commensurate with the severity and maliciousness of the employee's actions. Sanctions and the reasons for the sanctions will be documented in the employee's personnel file. The employee's supervisor, IT Director, and PM will be notified of the sanctions and the reasons for them as soon as possible but not more than 7 days of the decision for sanctions.					

17. Risk Assessment (RA)

The status of risk assessment controls for the SCGSC system is as indicated in the following table:

Control Number	Description of Control	Control Status/Type
RA-1	**Risk Assessment Policy and Procedures:** The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented risk assessment policy that addresses purpose, scope, roles, responsibilities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the risk assessment policy and associated risk assessment controls.	

Status		Type	
In Place	X	Common	
Planned		Hybrid	
In Place and Planned		System Specific	X
Not Applicable			

The risk assessment policy and procedures for the SCG Secure Cloud (SCGSC) are documented in the **Risk Assessment Report for the SCG Secure Cloud System**, Version 1.1 and address the risk assessment methodology to be implemented across the SCGSC's operating environment. At a high level, this policy addresses the purpose, scope, roles and responsibilities, management commitment, coordination among organizational entities, and compliance as it relates to risk assessment. The policy is consistent with SCG's mission, and functions with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.

It is the responsibility of SCG President, IT Director, and Vice President of Administration to develop, disseminate, and annually review/update the SCG Risk Assessment Report. The IT Director disseminates the policy to all Privileged Users by emailing a link to the document's SCG intranet location prior to authorizing privileged user status. The IT Director or Program Manager requests a response email from the Privileged User, confirming that Privileged User has read and understands the document.

The Risk Assessment Report is located on the SCG Intranet that is available to all SCG personnel at http://web-dev/intranet-sql. The intranet server is located in the Gaithersburg facility at 656 Quince Orchard Road, Gaithersburg, MD 20878.

RA-2	**Security Categorization:** The organization categorizes the information system and the information processed, stored, or transmitted by the system in accordance with FIPS 199 and documents the results (including supporting rationale) in the system security plan. The federal System Owner and ISSO review and approve the security categorizations.	

Status		Type	
In Place	X	Common	
Planned		Hybrid	
In Place and Planned		System Specific	X
Not Applicable			

The SCG Secure Cloud system is categorized as MODERATE in accordance with FIPS 199 because the Secure Online Ordering Catalog and Mailing List Database for the NIDDK Clearinghouses may contain names, home addresses, and telephone numbers. The security categorization is reviewed and approved by the federal System Owner and ISSO as indicated in this SSP.

RA-3	**Risk Assessment:** The organization conducts assessments of the risk and magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets of the agency (including information and information systems managed/operated by external parties).	Status		Type	
		In Place	X	Common	
		Planned		Hybrid	
		In Place and Planned		System Specific	X
		Not Applicable			

A risk assessment of the SCG Secure Cloud System was conducted by a third-party in accordance with the policies, processes, and procedures described in the **Risk Assessment Report for the SCG Secure Cloud System,** Version 1.1. Subsequent risk assessments will be conducted in accordance with the schedule specified in that document.

RA-5	**Vulnerability Scanning:** Using appropriate vulnerability scanning tools and techniques, the organization scans for vulnerabilities in the information system or when significant new vulnerabilities affecting the system are identified and reported. *Moderate and High systems require scanning for vulnerabilities at least monthly.*	Status		Type	
		In Place	X	Common	
		Planned		Hybrid	
		In Place and Planned		System Specific	X
		Not Applicable			

The SCG Secure Cloud system is scanned monthly for vulnerabilities using appropriate tools and techniques in accordance with the policies, processes, and procedures described in the **Risk Assessment Report for the SCG Secure Cloud System,** Version 1.1 and other documentation for the SCGSC system.

RA-5 (1)	**Vulnerability Scanning:** Vulnerability scanning tools include the capability to readily update the list of vulnerabilities scanned.	Status		Type	
		In Place	X	Common	
		Planned		Hybrid	
		In Place and Planned		System Specific	X
		Not Applicable			

A list of vulnerabilities identified in the monthly scans will be reviewed and addressed by the IT Director after conducting the vulnerability scan. Scans are submitted to the System Owner as well for review.

RA-5 (2)	**Vulnerability Scanning:** The organization updates the list of information system vulnerabilities or when significant new vulnerabilities are identified and reported.	Status		Type	
		In Place	X	Common	
		Planned		Hybrid	
		In Place and Planned		System Specific	X
		Not Applicable			
A record of system vulnerabilities is maintained in an Excel spreadsheet that is updated by the IT Director as results of monthly vulnerability scans are obtained.					

RA-5 (5)	**Vulnerability Scanning:** The information system implements privileged access authorization to SCG-identified information system components for selected vulnerability scanning activities.	Status		Type	
		In Place	X	Common	
		Planned		Hybrid	
		In Place and Planned		System Specific	X
		Not Applicable			
SCG does not grant privileged access to third-party organizations to conduct vulnerability scanning of the SCGSC system. NIDDK conducts vulnerability scans of the SCGSC public facing website on a quarterly basis.					

18. System and Services Acquisition (SA)

The status of system and services acquisition controls for the SCGSC system is as indicated in the following table:

Control Number	Description of Control	Control Status/Type			
SA-1	**System and Services Acquisition Policy and Procedures:** The organization develops: a. Develops, documents, and disseminates to SCG personnel designated by the Vice President of Administration: 1. A system and services acquisition policy that addresses purpose, scope, roles, responsibilities, and management commitment, coordination among entities, and compliance; and 2. Procedures to facilitate the implementation of the system and services acquisition policy and associated system and services acquisition controls; and b. Reviews and, if necessary, updates the current:	Status		Type	
		In Place	X	Common	
		Planned		Hybrid	
		In Place and Planned		System Specific	X
		Not Applicable			

	1. System and services acquisition policy at least annually; and 2. System and services acquisition procedures at least annually.	

System and Services Acquisition Procedure addresses the requirements and mechanisms to be implemented across SCG's Secure Cloud operating environment. At a high level, this policy addresses the purpose, scope, roles and responsibilities, management commitment, coordination among organizational entities, and requirements to comply with auditing and accountability.

It is the responsibility of SCG President, the Vice President of Administration, the Information Technology Director, and the Program Manager to develop, disseminate, and annually review/update the SCG System and Services Acquisition Procedure. The IT Director disseminates the procedure to all Privileged Users by emailing a link to the document's SCG intranet location prior to authorizing privileged user status. The IT Director requests a response email from the Privileged User, confirming that Privileged User has read and understands the document.

The procedure is located on the SCG Intranet that is available to all SCG personnel at: http://web-dev/intranet-sql. The intranet server is located in the Gaithersburg facility at 656 Quince Orchard Road, Gaithersburg, MD 20878.

SA-2	**Allocation of Resources:** The organization determines, documents, and allocates as part of its capital planning and investment control process the resources required to adequately protect the information system and establishes a complete line item for information security in organizational programming and budgeting documentation.	Status		Type	
		In Place	X	Common	
		Planned		Hybrid	
		In Place and Planned		System Specific	X
		Not Applicable			

Information security requirements were developed and documented during the SCG Secure Cloud design planning process. Security planning and evaluation have been built into the process of SCGSC environment development lifecycle. The information security requirements for the SCGSC or information system service are consistent to support a FIPS-199 Moderate categorization. The information security control requirements are documented in this System Security Control Plan (SSP).

SCG's budget planning includes resources to adequately protect and secure the SCG Secure Cloud system. A cost estimate for replacing the hardware, software, and other components of the system is documented as part of SCG's contingency planning. SCG also maintains an inventory of equipment necessary to rebuild the SCGSC with minimal purchases should existing hardware/equipment fail.

SA-3	**System Development Life Cycle:** The organization: a. Manages the information system using a formally defined and documented system development life cycle (SDLC) process that incorporates information security considerations; b. Defines and documents information security roles and responsibilities throughout the SDLC; c. Identifies individuals having information security roles and responsibilities; and d. Integrates the organizational information security risk management process into SDLC activities.	Status		Type	
		In Place	X	Common	
		Planned		Hybrid	
		In Place and Planned		System Specific	X
		Not Applicable			

SCG considers security in all phases of the system development lifecycle (SDLC). Security is an integral part of system development. The SDLC methodology used for the SCGSC system is Agile because the system already was developed by a previous contractor when SCG began supporting it. When developing from scratch, however, SCG typically uses the Waterfall style.

Using an iterative approach along with close communications with the client, SCG developers quickly design and develop applications using this methodology. It also facilitates a strong collaborative atmosphere and a dynamic interaction that brings the client into the process. This allows the client to not only see the development process in action, giving them the opportunity to make changes as they see development happen, as well as a sense of ownership of the application as it is realized.

Entity Relationship Modeling is used by SCG to define the information needs of the client. It provides a firm foundation for delivering high-quality, appropriate systems that meet the needs of the client. Using various computer-aided software engineering (CASE) tools, SCG builds diagrams and documents to outline functional requirements, data entities, and relational diagrams that support the developer during the RAD process. These tools and methods are used to give “clarity” and definition to complex entity relationship models.

SA-4	**Acquisition Process:** The organization includes the following requirements, descriptions, and criteria, explicitly or by reference, in the acquisition contract for the information system, system component, or information system service in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, guidelines, and organizational mission/business needs: a. Security functional requirements; b. Security strength requirements; c. Security assurance requirements; d. Security-related documentation requirements; e. Requirements for protecting security-related documentation;	Status		Type	
		In Place	X	Common	
		Planned		Hybrid	
		In Place and Planned		System Specific	X
		Not Applicable			

	f. Description of the information system development environment and environment in which the system is intended to operate; and g. Acceptance criteria.	

Security-related documentation requirements address all phases of the System Development Life Cycle (SDLC). SCG includes security-related documentation requirements in the acquisition contract for the information system. In the development/acquisition phase of the SDLC, security documentation is produced, including the System Security Plan (SSP) and its supporting documentation. Security documentation should begin as early as possible. SCG security documentation includes a configuration management plan, contingency plan, and an incident response plan.

SA-4 (1)	**Acquisition Process:** The organization requires the developer of the information system, system component, or information system service to provide a description of the functional properties of the security controls to be employed.	Status		Type	
		In Place	X	Common	
		Planned		Hybrid	
		In Place and Planned		System Specific	X
		Not Applicable			

The functional properties of the system are formally documented within a **System Design Document** that has been approved by the System Owner, ISSO, and AO/DAA.

Corporate Responsibility: SCG requires that acquisition documents that developers provide include functional properties of the security controls to be employed within the information system, information system components, or information system services in sufficient detail to permit analysis and testing of the controls. SCG also requires that each information system component associated with the SCGSC be included specific to the SCGSC system and reflected in supporting documentation.

System Responsibility: Security functional requirements include security capabilities, security functions, and security mechanisms, which are expressed in terms of security controls and their enhancements. The SCGSC **System and Services Acquisitions Procedure**, states that all SCG assigned and/or shared technology must be secured in accordance with SCG security policies and procedures. Security functional requirements are outlined in the controls contained in this System Security Plan (SSP).

SA-4 (2)	**Acquisition Process:** The organization requires the developer of the information system, system component, or information system service to provide design and implementation information for the security controls to be employed that includes selection of one or more of the following: • Security-relevant external system interfaces; • Source code or hardware schematics;	Status		Type	
		In Place	X	Common	
		Planned		Hybrid	
		In Place and Planned		System Specific	X
		Not Applicable			

	• Other IT Division-defined design/implementation information at an appropriate level of detail.	

SCG requires the System Architect of the information system to provide design and implementation information for the security controls to be employed that includes security-relevant external system interfaces, with high-level design, and diagrams that provide sufficient detail to demonstrate the implementation of controls. Controls in this System Security Plan (SSP) define security control requirements, how the controls are implemented, who is responsible for the implementation, and how often the control is reviewed.

In the case that external Information Technology service acquisitions are required in SCGSC, security control's functional properties employed are documented in the Interconnection Security Agreement (ISA), Memorandum of Understanding (MOU) or Memorandum of Agreement (MOA), with sufficient detail to permit analysis and testing of the controls.

When contracting with third-party providers, SCG purchasing and procurement ensures the contract contains requirements for adequate security controls, that these controls are documented and provide sufficient information that describes the functional capabilities of the security controls. Vendor/Contractor information and documentation must provide adequate detail to permit analysis and testing of the controls.

The SDLC process requires appropriate design reviews as part of system implementation and addresses all requirements including security requirements, which are incorporated into the **System Design Document for the SCG Secure Cloud System**.

SA-4 (9)	**Functions/ Ports/ Protocols/ Services In Use:** The organization requires the developer of the information system, system component, or information system service to identify early in the system development life cycle, the functions, ports, protocols, and services intended for organizational use.	Status		Type	
		In Place	X	Common	
		Planned		Hybrid	
		In Place and Planned		System Specific	X
		Not Applicable			

The SDLC process requires appropriate design reviews as part of system implementation and addresses all requirements including security requirements, which are incorporated into the **System Design Document**.

SA-4 (10)	**Acquisition Process:** The organization employs only information technology products on the FIPS 201-approved products list for Personal Identity Verification (PIV) capability implemented within organizational information systems.	Status		Type	
		In Place		Common	
		Planned		Hybrid	
		In Place and Planned		System Specific	X
		Not Applicable	X		

This control is Not Applicable as the system does not employ any HSPD-12 requirement or make use of PIV technologies.

SA-5	**Information System Documentation:** The organization: a. Obtains administrator documentation for the information system, system component, or information system service that describes: 1. Secure configuration, installation, and operation of the system, component, or service; 2. Effective use and maintenance of security functions/mechanisms; and 3. Known vulnerabilities regarding configuration and use of administrative (i.e., privileged) functions; b. Obtains user documentation for the information system, system component, or information system service that describes: 1. User-accessible security functions/mechanisms and how to effectively use those security functions/mechanisms; 2. Methods for user interaction, which enables individuals to use the system, component, or service in a more secure manner; and 3. User responsibilities in maintaining the security of the system, component, or service; c. Documents attempts to obtain information system, system component, or information system service documentation when such documentation is either unavailable or nonexistent and any other appropriate actions (as defined by the IT Director) in response; d. Protects documentation as required, in accordance with the risk management strategy; and e. Distributes documentation to personnel/roles as designated by the SCG President and IT Director.	

Status		Type	
In Place	X	Common	
Planned		Hybrid	
In Place and Planned		System Specific	X
Not Applicable			

Information regarding system documentation, secure configuration, operation, maintenance, system components, and user responsibilities can be found in the **System Design Document**, **System Operations and Maintenance Plan**, and the **Configuration Management Plan**. SCGSC Administrators obtain administrator documentation for all components of the Secure Cloud. These documents typically are published by the components vendor and contain information describing the secure configuration, installation, and operation of the referenced component.

The most common form of administrator documentation collected for system components are user guides and manuals. These manuals contain specific guidance on maintenance, security functions, and known vulnerabilities regarding specific configurations.

SCGSC personnel download the related guidance documents and maintain a local copy within the SCG Intranet repository for future reference. This is done to make sure that manufacturer documentation is available to the system personnel even in the event that the manufacturer ceases to supply the guidance.

SA-8	**Security Engineering Principles:** The organization designs and implements the information system using security engineering principles.	Status		Type	
		In Place	X	Common	X
		Planned		Hybrid	
		In Place and Planned		System Specific	
		Not Applicable			

Security is a primary focus and concern for SCG. SCG applies security principles to all aspects of the System Development Life Cycle (SDLC) to ensure that only secure methodologies are used in the design and implementation of the solution. Risk Management Framework (RMF) controls also are considered in the engineering of the SCGSC environment as appropriate.

As guidance, the design of the SCG information system incorporates government-defined security best practices into the SDLC, in accordance with NIST SP 800-27 Revision A, Engineering Principles for Information Technology Security.

The Engineering approach used for SCG is identifying:

- what is the design to do
- what is the "AS IS" environment
- what is the process and how is the “TO BE” environment developed
- what are the metrics and measurements to ensure the solution is completed

A four step process is used:

- System Requirement Review - reviewing the "AS IS", and what the requirements are
- Preliminary Design Review - initial design
- Critical Design Review - polished design

- Operational Design Review - final design and approval to move forward with implementation

Each review is presented to SCG IT Director, System Architects, System Administrators and the Change Control Board (CCB).

SA-9	**External Information System Services:** The organization: a. Requires that providers of external information system services comply with organizational information security requirements and employ security controls as specified by SCG in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance; b. Formally defines and documents government oversight and user roles and responsibilities with regard to external information system services; and c. Employs processes, methods, and techniques to monitor security control compliance by external service providers on an ongoing basis.	Status		Type	
		In Place	X	Common	
		Planned		Hybrid	
		In Place and Planned		System Specific	X
		Not Applicable			
FISMA compliance reviews are conducted annually for the SCG Secure Cloud. SCG does not leverage services from external information systems.					

SA-9 (2)	**External Information System Services:** The organization requires providers of external information system services to identify the functions, ports, protocols, and other services required for the use of such services.	Status		Type	
		In Place	X	Common	
		Planned		Hybrid	
		In Place and Planned		System Specific	X
		Not Applicable			
FISMA compliance reviews are conducted annually for the SCG Secure Cloud. SCG does not leverage services from external information systems.					

SA-10	**Developer Configuration Management**: The organization requires the developer of the information system, system component, or information system service to: a. Perform configuration management during system, component, or service design and operation; b. Document, manage, and control the integrity of changes to configuration items under	Status		Type	
		In Place	X	Common	
		Planned		Hybrid	
		In Place and Planned		System Specific	X
		Not Applicable			

	configuration management (as defined by the Configuration Management Plan); c. Implement only organization-approved changes to the system, component, or service; d. Document approved changes to the system, component, or service and the potential security impacts of such changes; and e. Track security flaws and flaw resolution within the system, component, or service and report findings to the SCG President and Program Manager, and the personnel designated by the IT Director.	
All activity within the SCG Secure Cloud is managed by the configuration management process that has been described in the Configuration Management control family of this System Security Plan (SSP). System developers must adhere to all aspects of the SGCSC Configuration Management Plan, and the controls outlined within the SCG SSP. Configuration management controls can be found in Section 3.3 of the **Configuration Management Plan for the SCG Secure Cloud System**.		

SA-11	**Developer Security Testing and Evaluation:** The organization requires the developer of the information system, system component, or information system service to: a. Create and implement a security assessment plan; b. Perform unit, integration, system, and/or regression testing/evaluation at the level of depth and coverage specified by the IT Director; c. Produce evidence of the execution of the security assessment plan and the results of the security testing/evaluation; d. Implement a verifiable flaw remediation process; and e. Correct flaws identified during security testing/evaluation prior to entering the operations and maintenance phase of the SDLC.	

Status		Type	
In Place	X	Common	
Planned		Hybrid	
In Place and Planned		System Specific	X
Not Applicable			

Security Assessment Plans (SAP) have been integrated into the SCG information system development methodologies. When a new component is scheduled to be deployed to the information system, System Architects develop a SAP that outlines both testing and implementation phases. Vulnerability scanning is included in the test plan. The SAP is updated annually.

Once the system component is procured or created, it is placed in a development environment to be tested for security flaws, integration with existing components, and regression testing, if applicable. Once the component has been thoroughly tested according

to the SAP, it is a candidate for release into the production environment (pending authorization from the Change Control Board). Information describing security testing and evaluation can be found in the **System Operations and Maintenance Plan**.

19. System and Communications Protection (SC)

The status of system and communications protection controls for the SCG Secure Cloud system is as indicated in the following table:

Control Number	Description of Control	Control Status/Type
SC-1	**System & Communications Protection Policy & Procedures:** The organization: a. Develops, documents, and disseminates to the SCG IT staff who have access to the SCGSC system: 1. A system and communications protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the system and communications protection policy and associated system and communications protection controls; and b. Reviews and updates the current: 1. System and communications protection policy at least once annually; and 2. System and communications protection procedures at least once annually.	Status: In Place X; Planned; In Place and Planned; Not Applicable Type: Common; Hybrid; System Specific X

SCG has developed and disseminated the SCGSC **System Design Document**, which addresses the requirements and mechanisms to be implemented across SCGSC's operating environment. At a high level, this policy addresses the purpose, scope, roles and responsibilities, management commitment, coordination among organizational entities, and requirements to comply with secure communications requirements. The policy is consistent with SCG's mission, and functions with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.

It is the responsibility of SCG President, Vice President of Administration, and the Information Technology (IT) Director to develop, disseminate, and annually review/update the SCGSC **System Design Document**. The IT Director disseminates the document to all Privileged Users by emailing a link to the document's SCG Intranet location prior to authorizing privileged user status. The IT Director requests a response email from the Privileged User, confirming that Privileged User has read and understands the document.

The SCGSC **System Design Document** is located on the SCG Intranet that is available to all SCG personnel at http://web-dev/intranet-sql. The intranet server is located in the Gaithersburg facility at 656 Quince Orchard Road, Gaithersburg, MD 20878.

SC-2	**Application Partitioning:** The information system separates user functionality (including user interface services) from information system management functionality.	Status		Type	
		In Place	X	Common	
		Planned		Hybrid	
		In Place and Planned		System Specific	X
		Not Applicable			

The SCGSC system local user accounts only permit access to the hosting platforms for applications and systems (e.g., Windows logon). Access is not transferable to hosted applications. Each individual application that is hosted in the SCGSC system maintains its own respective access control as defined by the application owner. In addition, the current firewall rules are set to isolate communications from Applications, Data, and DMZ tiers established in the secure network enclave. The configurations are documented as part of a System Development Life Cycle (SDLC) artifact, the SCGSC **System Design Document**.

SC-4	**Information in Shared Resources:** The information system prevents unauthorized and unintended information transfer via shared system resources.	Status		Type	
		In Place	X	Common	
		Planned		Hybrid	
		In Place and Planned		System Specific	X
		Not Applicable			

There are no shared resources in the SCGSC system. A user must be logged in to see any data or information. The configurations are documented as part of an SDLC artifact, the **System Design Document**.

SC-5	**Denial of Service Protection:** The information system protects against or limits the effects of the following types of denial of service attacks: buffer overflow, ping of death, smurf attack, TCP SYN attack, and teardrop by employing Stateful Packet Inspection and Intrusion Prevention System at the edge router/firewall. Refer to NIST SP 80-61 and employ appropriate security safeguards.	Status		Type	
		In Place	X	Common	
		Planned		Hybrid	
		In Place and Planned		System Specific	X
		Not Applicable			

Stateful Packet Inspection and Intrusion Prevention System are in use at the edge router/firewall. Internal firewall OS options to prevent denial of service (DoS) attacks are configured such as limited packet fragmentation, Unicast Reverse-Path Forwarding, and DHCP are disabled. The configurations are documented as part of an SDLC artifact, the **System Design Document**.

SC-7	**Boundary Protection:** The information system: a. Monitors and controls communications at the external boundary of the system and at key internal boundaries within the system; b. Implements subnetworks for publicly accessible system components that are physically separated from internal organizational networks; and c. Connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture.	Status		Type	
		In Place	X	Common	
		Planned		Hybrid	
		In Place and Planned		System Specific	X
		Not Applicable			

The SCGSC system utilizes an edge router/firewall to create three different physical subnets. The boundary is established by creating a physically separated network that remains isolated from all other networks. A proper DMZ has been established with access permitted from only specified internal hosts and ports. External networks and systems are not supported. Firewall 2 is monitoring and controlling communications at the external boundary of the system. Symantec is monitoring communications internally in the Apps Network of the SCGSC.

SC-7 (3)	**Access Points:** The organization limits the number of external network connections to the information system.	Status		Type	
		In Place	X	Common	
		Planned		Hybrid	
		In Place and Planned		System Specific	X
		Not Applicable			

There are no external connections permitted other than a single connection point that permits publicly routable content to the Internet of specified ports for http/https (80/443). BackupExec, Symantec, VSphere, and Microsoft Dynamics NAV connect to SCGSC via specific ports (21, 80, 88, 135, 137, 138, 139, 443, 445, 902, 1125, 1434, 3106, 3527, 5989, 6102, 6103, 6106, 7046, 7047, 8014, 10000, 31031, and 44046) for backup, anti-virus communications, and managing virtual servers.

SC-7 (4)	**External Tele-Communications Services:** The organization: a. Implements a managed interface for each external telecommunication service; b. Establishes a traffic flow policy for each managed interface; c. Protects the confidentiality and integrity of the information being transmitted across each interface; d. Documents each exception to the traffic flow policy with a supporting mission/business need and duration of that need; and e. Reviews exceptions to the traffic flow policy periodically (at least annually) and removes exceptions that are no longer supported by an explicit mission/business need.	Status		Type	
		In Place	X	Common	
		Planned		Hybrid	
		In Place and Planned		System Specific	X
		Not Applicable			

There are no telecommunication services in use with the SCGSC system. All data exchanges are configured to be done securely using https (443). The SCGSC is documented with an SDLC artifact, the **System Design Document**. All open ports are identified in this artifact. Policies and technical configurations are reviewed periodically by the IT Director. New policies are established as the demand for them is identified, and they are reviewed and approved by the System Owner. An external and independent assessment team is used to validate that appropriate configurations are in place to meet all FISMA requirements, with annual reviews and re-certifications conducted.

SC-7 (5)	**Deny by Default/Allow by Exception:** The information system at managed interfaces denies network communications traffic by default and allows network communications traffic by exception (i.e., deny all, permit by exception).	Status		Type	
		In Place	X	Common	
		Planned		Hybrid	
		In Place and Planned		System Specific	X
		Not Applicable			
The edge router/firewall is configured with an “Explicit Deny Any Any” for every interface. This satisfies this control directly and completely.					

SC-7 (7)	**Boundary Protection:** The information system, in conjunction with a remote device, prevents the device from simultaneously establishing non-remote connections with the system and communicating via some other connection to resources in external networks.	Status		Type	
		In Place	X	Common	
		Planned		Hybrid	
		In Place and Planned		System Specific	X
		Not Applicable			
Split tunneling (simultaneous connections made outside an established VPN connection), is not used within the SCGSC system. The edge router/firewall is configured to not allow Split Tunneling through any interface.					

SC-8	**Transmission Confidentiality and Integrity:** The information system protects the confidentiality and integrity of transmitted information. Any transmitted data containing sensitive information, including but not limited to e-mail, must be encrypted using a FIPS 140-2 compliant encryption solution.	Status		Type	
		In Place	X	Common	
		Planned		Hybrid	
		In Place and Planned		System Specific	X
		Not Applicable			
The SCGSC does not use proxy services and does not use the Internet directly as a mechanism for communicating with users or administrators. The SCGSC information system protects the confidentiality and integrity of traffic as it flows within the information system and through ingress and egress ports. SSL 3.0/TLS 1.0 cryptographic mechanisms, encryption methodologies, and technologies have been implemented to ensure that data remains secure. There is no transmission of information in the SCGSC environment.					

SC-8 (1)	**Transmission Confidentiality and Integrity:** The information system implements cryptographic mechanisms to prevent unauthorized disclosure of information and detect changes to information during transmission unless otherwise protected by alternative physical safeguards.	Status		Type	
		In Place	X	Common	
		Planned		Hybrid	
		In Place and Planned		System Specific	X
		Not Applicable			

The SCGSC does not use proxy services and does not use the Internet directly as a mechanism for communicating with users or administrators. The SCGSC information system protects the confidentiality and integrity of traffic as it flows within the information system and through ingress and egress ports. SSL 3.0/TLS 1.0 cryptographic mechanisms, encryption methodologies, and technologies have been implemented to ensure that data remains secure. There is no transmission of information in the SCGSC environment.

SC-10	**Network Disconnect:** The information system terminates the network connection to the firewall at the end of the session or after 30 minutes of inactivity.	Status		Type	
		In Place	X	Common	
		Planned		Hybrid	
		In Place and Planned		System Specific	X
		Not Applicable			

The edge router/firewall is configured to drop all connections to the firewall after timeout conn 0:30:00 minutes, half-closed 0:10:00 minutes, UDP 0:02:00 minutes, ICMP 0:00:02 seconds. These configurations are consistent with the Defense Information Systems Agency (DISA) Security Technical Implementation Guide (STIG).

Communication session's network connections are terminated no later than thirty (30) minutes for the following session types:

- At the end of the communication session
- Firewall Idle connections
- Firewall TCP half-closed connections
- Web servers network connections

SC-12	**Cryptographic Key Establishment and Management:** The organization establishes and manages cryptographic keys for required cryptography employed within the information system in accordance with HHS Standard for Encryption of Computing Devices.	Status		Type	
		In Place	X	Common	
		Planned		Hybrid	
		In Place and Planned		System Specific	X
		Not Applicable			

Cryptographic services are not supported or required for this system, with the exception of Windows CAPI based activities that are utilized by the Windows Kerberos service. A Class 3 SSL PKI certificates was generated from a centralized, federally approved Digicert and Entrust Certificate Authorities (CA) to support the L2TP/IPsec and SSL 3.0/TLS 1.0 cryptographic mechanisms employed. These cryptographic mechanisms are used to create secure tunnels between designated endpoints, which comply with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.

SC-13	**Cryptography Protection:** The information system implements cryptographic mechanisms as defined in the HHS Standard for Encryption of Computing Devices in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards.	Status		Type	
		In Place	X	Common	
		Planned		Hybrid	
		In Place and Planned		System Specific	X
		Not Applicable			

Cryptographic services are not supported or required for this system, with the exception of Windows CAPI based activities that are utilized by the Windows Kerberos service. A Class 3 SSL PKI certificates was generated from a centralized, federally approved Digicert and Entrust Certificate Authorities (CA) to support the L2TP/IPsec and SSL 3.0/TLS 1.0 cryptographic mechanisms employed. These cryptographic mechanisms are used to create secure tunnels between designated endpoints, which comply with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.

SC-15	**Collaborative Computing Devices:** The information system: a. Prohibits remote activation of collaborative computing devices with no exceptions; and b. Provides an explicit indication of use to users physically present at the devices.	Status		Type	
		In Place	X	Common	
		Planned		Hybrid	
		In Place and Planned		System Specific	X
		Not Applicable			

All hosting platforms in the SCGSC system are configured to not permit Windows Remote Desktop Protocol (RDP) to Windows servers without a manual change to the firewall. RDP is enabled manually only on an as-needed basis and is restricted to system administrators. BackupExec, Symantec, VSphere, and Dynamics NAV connections are permitted to allow access to ESXi hosts, but only from specific IP addresses. These connections are directly permitted via edge router/firewall rules to allow for appropriate protection mechanisms for accessing the hosting environment. No indication of use to users is physically present at the devices because no collaborative computing devices are permitted at the ESXi host.

SC-17	**Public Key Infrastructure Certificates:** The organization issues public key certificates under the Department certificate policy or obtains public key certificates from an approved service provider.	Status		Type	
		In Place	X	Common	
		Planned		Hybrid	
		In Place and Planned		System Specific	X
		Not Applicable			

A Class 3 SSL PKI certificates was generated from a centralized, federally approved Digicert and Entrust Certificate Authorities (CA) to support the L2TP/IPsec and SSL 3.0/TLS 1.0 cryptographic mechanisms employed. These cryptographic mechanisms are used to create secure tunnels between designated endpoints, which comply with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.

SC-18	**Mobile Code:** The organization: a. Defines acceptable and unacceptable mobile code and mobile code technologies; b. Establishes usage restrictions and implementation guidance for acceptable mobile code and mobile code technologies; and c. Authorizes, monitors, and controls the use of mobile code within the information system.	Status		Type	
		In Place	X	Common	
		Planned		Hybrid	
		In Place and Planned		System Specific	X
		Not Applicable			

Mobile code is not used within the SCGSC environment. None of the SCGSC or NIDDK Clearinghouse sites have mobile code nor are the sites designed for mobile technology. Should that change in the future, SCG will define acceptable and unacceptable mobile code technologies and establish usage restrictions and implementation guidance for acceptable mobile code and mobile code technologies.

SC-19	**Voice Over Internet Protocol:** The organization: a. Establishes usage restrictions and implementation guidance for Voice over Internet Protocol (VoIP) technologies based on the potential to cause damage to the information system if used maliciously; and b. Authorizes, monitors, and controls the use of VoIP within the information system.	Status		Type	
		In Place		Common	
		Planned		Hybrid	
		In Place and Planned		System Specific	X
		Not Applicable	X		

VoIP is not authorized by the SCGSC system. In the event the use of VoIP technologies is required by the SCGSC information system, it must be authorized, monitored, and controlled by the IT Director.

SC-20	**Secure Name/Address Resolution Service (Authoritative Source):** The information system: a. Provides additional data origin and integrity artifacts along with the authoritative name resolution data the system returns in response to external name/address resolution queries; and b. Provides the means to indicate the security status of child zones and (if the child supports secure resolution services) to enable verification of a chain of trust among parent and child domains, when operating as part of a distributed, hierarchical namespace.	Status / Type

Status		Type	
In Place	X	Common	
Planned		Hybrid	
In Place and Planned		System Specific	X
Not Applicable			

The DNS servers are used internally to provide name-to-address resolution services to the SCGSC information system. The Start of Authorization (SOA) source is SCFSMO and has no child domains. It is used for internal name resolution only. An external DNS (Google) is used as a forwarder if the internal DNS cannot resolve the names.

SC-21	**Secure Name/Address Resolution Service (Recursive or Caching Resolver):** The information system requests and performs data origin authentication and data integrity verification on the name/address resolution responses the system receives from authoritative sources.	Status / Type

Status		Type	
In Place	X	Common	
Planned		Hybrid	
In Place and Planned		System Specific	X
Not Applicable			

DNS ensures the authenticity and data integrity of name/resolution responses the system receives from authoritative sources. SCGSC uses recursive resolver for name resolution. The integrity of the data is ensured by Active Directory, which restricts access to DNS Admins, Domain Admins, Enterprise Admins, Administrators, and Enterprise Domain Controllers.

SC-22	**Architecture and Provisioning For Name/Address Resolution Service:** The information systems that collectively provide name/address resolution service for an organization are fault-tolerant and implement internal/external role separation.	Status / Type

Status		Type	
In Place	X	Common	
Planned		Hybrid	
In Place and Planned		System Specific	X
Not Applicable			

SCFSMO provides name and address resolution for the SCGSC system. SCGSC's information system is protected against DoS attacks using a defense-in-depth security approach. Data origin authentication and name/address integrity verification resolution response is received from authoritative sources when requested by SCGSC systems components. For the Active Directory domain, the DNS server is configured for fault tolerance with SCSQL-Prod server.

SC-23	**Session Authenticity:** The information system protects the authenticity of communications sessions.	Status		Type	
		In Place	X	Common	
		Planned		Hybrid	
		In Place and Planned		System Specific	X
		Not Applicable			

The edge router/firewall for the SCGSC system is configured to prohibit reverse lookups and denial of 'spoofed' IP addresses.

SC-28	**Protection of Information at Rest:** The information system protects the confidentiality and integrity of information at rest.	Status		Type	
		In Place	X	Common	
		Planned		Hybrid	
		In Place and Planned		System Specific	X
		Not Applicable			

SCG ensures media and the information on the media of the SCGSC system are protected from unauthorized access. This includes, but is not limited to, backup media such as tapes or disks. Only approved SCG removable digital media must be used to store data. The SCGSC backup tapes are encrypted (128-bit AES encryption with an 8-character pass phrase key) to protect the Personally Identifiable Information (PII) contained on the tapes.

SC-39	**Process Isolation:** The information system maintains a separate execution domain for each executing process.	Status		Type	
		In Place	X	Common	
		Planned		Hybrid	
		In Place and Planned		System Specific	X
		Not Applicable			

SCGSC uses Microsoft Windows Server Operating system, which handles memory allocation. The OS isolates processes using Data Execution Prevention (DEP). DEP marks areas of memory as either "executable" or "non-executable", and allows only data in an "executable" area to be run.

20. System and Information Integrity (SI)

The status of system and information integrity controls for the SCGSC system is as indicated in the following table:

<table>
<tr><th>Control Number</th><th>Description of Control</th><th>Control Status/Type</th></tr>
<tr><td>SI-1</td><td>System and Information Integrity Policy and Procedures: The organization:
a. Develops, documents, and disseminates to SCG IT personnel who have access to the SCGSC, the SCG President, Vice President of Administration, and the Program Manager:
1. A system and information integrity policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
2. Procedures to facilitate the implementation of the system and information integrity policy and associated system and information integrity controls; and
b. Reviews and updates the current:
1. System and information integrity policy at least annually; and
2. System and information integrity procedures at least annually.</td><td>
<table>
<tr><th>Status</th><th></th><th>Type</th><th></th></tr>
<tr><td>In Place</td><td>X</td><td>Common</td><td></td></tr>
<tr><td>Planned</td><td></td><td>Hybrid</td><td></td></tr>
<tr><td>In Place and Planned</td><td></td><td>System Specific</td><td>X</td></tr>
<tr><td>Not Applicable</td><td></td><td colspan="2"></td></tr>
</table>
</td></tr>
<tr><td colspan="3">The SCGSC System and Information Integrity Policy and Procedures addresses the requirements and mechanisms to be implemented across SCGSC’s operating environment. At a high level, this policy addresses the purpose, scope, roles and responsibilities, management commitment, coordination among organizational entities, and requirements to comply with auditing and accountability.

Maintenance is performed through security patch updates, hardened and current configurations, continuous monitoring of systems, and active management for all systems through the Software Development Lifecycle. The policy is consistent with SCG’s mission, and functions with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.

It is the responsibility of the SCG President, Vice President of Administration, and the IT Director to develop, disseminate, and annually review/update the SCGSC System and Information Integrity Policy and Procedures. The IT Director disseminates the policy to all Privileged Users by emailing a link to the document’s SCG intranet location prior to authorizing privileged user status. The IT Director requests a response email from the Privileged User, confirming that Privileged User has read and understands the document.</td></tr>
</table>

The policy is located on the SCG Intranet that is available to all SCG personnel at http://web-dev/intranet-sql. The intranet server is located in the Gaithersburg facility at 656 Quince Orchard Road, Gaithersburg, MD 20878.

SI-2	**Flaw Remediation:** The organization: a. Identifies, reports, and corrects information system flaws; b. Tests software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation; c. Installs security-relevant software and firmware updates within 2 business days for high priority critical vulnerabilities, 7 business days for moderate priority vulnerabilities, or 30 days for low priority vulnerabilities of the release of the updates; and d. Incorporates flaw remediation into the organizational configuration management process.	Status		Type	
		In Place	X	Common	
		Planned		Hybrid	
		In Place and Planned		System Specific	X
		Not Applicable			

The SCGSC **System Operations and Maintenance Plan** incorporates rigorous test and validation procedures that support and demonstrate satisfaction of this control for parts b, c, and d through the use of formal testing approaches that allow for mature flaw remediation to be engaged for the system. SCG maintains an inventory of SCGSC components that specifies the hardware equipment, operating systems, and software applications in operation. SCG incorporates flaw remediation in the Configuration Management Plan for the SCGSC. The IT Director is responsible for monitoring and coordinating with vendors for update and patch release support. Information security patches are installed in accordance with the Configuration Management Plan. SCG installs security-relevant software and firmware updates within 2 business days of update release for high priority vulnerabilities, 7 business days of update release for moderate priority vulnerabilities, or 30 days of update release for low priority vulnerabilities. The IT staff monitors security sources for vulnerability announcements and emerging threats that correspond to the software in the SCGSC inventory. SCG has a SmartNet account with Cisco to obtain notifications about the availability and priority of patches, updates, etc., for the firewall. Similarly, SCG has a Symantec account that notifies the IT Director about the availability and criticality of updates, patches, etc.

SI-2 (2)	**Automated Flaw Remediation:** The organization employs an automated mechanism at least quarterly to determine the state of information system components with regard to flaw remediation.	Status		Type	
		In Place	X	Common	
		Planned		Hybrid	
		In Place and Planned		System Specific	X
		Not Applicable			

SCG employs several automated mechanisms to monitor the state of the system. Descriptions can be found in Section 9 of the **Incident Response Plan**. The SCG IT Director receives automated notifications from Cisco, Windows, and Symantec regarding updates, patches, etc. The IT Director determines which updates, patches, etc., need to be installed and the priority for installation. The IT Director also conducts quarterly searches to identify updates, patches, etc. The administrator runs vulnerability scans quarterly to identify vulnerabilities and available patches, updates, etc.

SI-3

Malicious Code Protection: The organization:

a. Employs malicious code protection mechanisms at information system entry and exit points to detect and eradicate malicious code;
b. Updates malicious code protection mechanisms whenever new releases are available in accordance with organizational configuration management policy and procedures;
c. Configures malicious code protection mechanisms to:
   1. Perform scans of the information system at least monthly and real-time scans of files from external sources at endpoint and network entry points as the files are downloaded, opened, or executed in accordance with organizational security policy; and
   2. Block and quarantine malicious code and send an e-mail alert to the IT Director in response to malicious code detection; and
d. Addresses the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the information system.

Status		Type	
In Place	X	Common	
Planned		Hybrid	
In Place and Planned		System Specific	X
Not Applicable			

The SCGSC **System Operation and Maintenance Plan** incorporates rigorous test and validation procedures that support and demonstrate satisfaction of this control through security testing that is incorporated into the best practice approaches used as part of system operations and maintenance. The IPS and Symantec Endpoint Protection Suite Enterprise 2015 continuously scan for malicious code and send e-mail alerts to the IT Director when malicious code is detected. A full Symantec Endpoint Protection scan of the virtual servers is conducted weekly. The IT Director investigates the alert and determines if it was a false positive or remediates as necessary.

SI-3 (1)	**Central Management:** The organization centrally manages malicious code protection mechanisms.	Status		Type	
		In Place	X	Common	
		Planned		Hybrid	
		In Place and Planned		System Specific	X
		Not Applicable			

SCG uses Symantec Endpoint Protection Suite Enterprise as its mechanism for centrally managed malicious code protection. Malicious code alerts are logged into the SCG Symantec server and are centrally managed.

SI-3 (2)	**Automatic Updates:** The information system automatically updates malicious code protection mechanisms.	Status		Type	
		In Place	X	Common	
		Planned		Hybrid	
		In Place and Planned		System Specific	X
		Not Applicable			

SCG uses Symantec Endpoint Protection Suite Enterprise as its mechanism for centrally managed malicious code protection. Updates are received automatically from Symantec. The firewall IPS also protects against malicious code and it is updated automatically from Cisco.

SI-4	**Information System Monitoring:** The organization: a. Monitors the information system to detect: 1. Attacks and indicators of potential attacks in accordance with SCGSC monitoring objectives; and 2. Unauthorized local, network, and remote connections; b. Identifies unauthorized use of the information system through Active Directory; c. Deploys monitoring devices: (i) strategically within the information system to collect organization-determined essential information; and (ii) at ad hoc locations within the system to track specific types of transactions of interest to the organization; d. Protects information obtained from intrusion-monitoring tools from unauthorized access, modification, and deletion; e. Heightens the level of information system monitoring activity whenever there is an	Status		Type	
		In Place	X	Common	
		Planned		Hybrid	
		In Place and Planned		System Specific	X
		Not Applicable			

	indication of increased risk to organizational operations and assets, individuals, other organizations, or the Nation based on law enforcement information, intelligence information, or other credible sources of information; f. Obtains legal opinion with regard to information system monitoring activities in accordance with applicable federal laws, Executive Orders, directives, policies, or regulations; and g. Provides the results of the log reviews to the SCG President and Program Manager when there is a security concern that needs to be escalated.	

A full outline of the SCGSC monitoring processes and procedures can be found in the **Incident Response Plan.** The Cisco firewall log data and Windows event log data are reviewed weekly by the IT Director to detect unauthorized access (login failures, odd login times, and unfamiliar IP addresses), unauthorized modifications or deletions, and similar items. IPS and Symantec Endpoint Protection Suite Enterprise protect the SCGSC and the alert feature is turned on to notify the IT Director via e-mail in the event of a detection. The IT Director heightens system monitoring when there is an indication of increased risk. The logs contain no sensitive information that would require a legal opinion on applicability of federal laws, etc.

SI-4 (2)	**Automated Tools for Real-Time Analysis:** The organization employs automated tools to support near-real-time analysis of events.	Status		Type	
		In Place	X	Common	
		Planned		Hybrid	
		In Place and Planned		System Specific	X
		Not Applicable			

The tools employed by SCG for monitoring and analyzing events are described in the **System and Information Integrity Policy and Procedures for the SCG Secure Cloud System**. Both IPS and Symantec monitor the SCGSC continuously and send automatic alerts to notify the IT Director of event detection, which allows the IT Director to conduct near-real-time analysis of events and take timely remedial action as needed.

SI-4 (4)	**Inbound and Outbound Communications Traffic:** The information system monitors inbound and outbound communications traffic continuously for unusual or unauthorized activities or conditions.	Status		Type	
		In Place	X	Common	
		Planned		Hybrid	
		In Place and Planned		System Specific	X
		Not Applicable			

The procedures employed by SCG for monitoring communications are described in the **System and Information Integrity Policy and Procedures** for the **SCG Secure Cloud System**. Both IPS and Symantec Endpoint Protection Suite Enterprise monitor inbound and outbound communications for unusual or unauthorized activities or conditions.

SI-4 (5)	**System-Generated Alerts:** The information system alerts the IT Director when the following indications of compromise or potential compromise occur: warnings and critical alerts.	Status		Type	
		In Place	X	Common	
		Planned		Hybrid	
		In Place and Planned		System Specific	X
		Not Applicable			

The SCGSC system employs a Kiwi Syslog server to consolidate the logs used to monitor the overall system. In the event of critical alert, the IT Director would receive an e-mail from the server detailing the event. Both IPS and Symantec Endpoint Protection Suite Enterprise alert the IT Director when a warning or critical alert is generated.

SI-5	**Security Alerts, Advisories, and Directives:** The organization: a. Receives information system security alerts, advisories, and directives from the manufacturers of the firewall (Cisco), anti-virus software (Symantec), and Microsoft (Windows) as well as US-CERT on an ongoing basis; b. Generates internal security alerts, advisories, and directives as deemed necessary; c. Disseminates security alerts, advisories, and directives to SCG IT staff; and d. Implements security directives in accordance with established time frames, or notifies the issuing organization of the degree of noncompliance.	Status		Type	
		In Place	X	Common	
		Planned		Hybrid	
		In Place and Planned		System Specific	X
		Not Applicable			

The SCGSC system employs a Kiwi Syslog server to consolidate logs for the overall system. In the event of critical alert, SCG's IT Director would receive emails from the server detailing the event. The IT Director receives information security alerts, advisories, and directives from Cisco (SmartNet account), Symantec, and Microsoft on an ongoing basis. The IT Director generates security alerts, advisories, and directives as necessary and disseminates them to the SCG IT staff who have access to the SCGSC system. The IT Director implements security directives in accordance with established time frames specified in the **System and Information Integrity Policy and Procedures** document. The IT Director also has subscribed to receive the US-CERT alerts, tips, and updates. There are no external organizations that need to be notified by SCG regarding security alerts, advisories, and directives for the SCGSC. If there is a requirement that NIDDK be notified of these alerts, advisories, and directives, the IT Director will ensure that NIDDK receives them.

SI-6	**Security Function Verification:** The organization: a. Verifies the correct operation of [Assignment: organization-defined security functions]; b. Performs this verification [Selection (one or more): [Assignment: organization-defined system transitional states]; upon command by user with appropriate privilege; [Assignment: organization-defined frequency]]; c. Notifies [Assignment: organization-defined personnel or roles] of failed security verification tests; and d. [Selection (one or more): shuts the information system down; restarts the information system; [Assignment: organization-defined alternative action(s)]] when anomalies are discovered.	Status / Type In Place: X Planned: In Place and Planned: Not Applicable: Common: Hybrid: System Specific: X

SCGSC verifies the correct operation of AV signatures, ability to update, server auditing, and file integrity monitoring during start up or on demand by System Administrators. SCGSC verifies operation with Windows OS self-tests during initial start-up (on power on) to demonstrate the correct operation of the system. Manual validation of operations or restarts will be performed monthly by SCGSC System Administrators. Failed security validation tests will trigger a notification for System Administrators; this is accomplished by email alert. Failed tests or anomalies will restart the affected SCGSC instance.

SI-7	**Software, Firmware, and Information Integrity:** The organization employs integrity verification tools to detect unauthorized changes to the SCGSC software, firmware, and information.	Status / Type In Place: X Planned: In Place and Planned: Not Applicable: Common: Hybrid: System Specific: X

The SCGSC backup system is configured to verify data integrity upon backup. The SCGSC Kiwi Syslog logs would serve as the tool to detect unauthorized changes to the SCGSC software and firmware. The IT Director reviews these logs on a weekly basis. Authority for modifying the SCGSC software and firmware is limited to the System Administrator. SCG uses diagnostic (memory, hard drive, etc.) tests in BIOS (which is built into the server) to verify firmware integrity for SCGSC. SCG uses the Windows Error-Checking tool to verify the integrity of the Windows operating system, and automatically fix performance issues and file and system errors. These integrity checks will be performed monthly and following any security-related events. For firmware, each device performs an integrity check of the firmware at startup and rejects incorrect firmware before it is installed (aborts installation) to avoid damaging the device. Similar rejection occurs if someone attempts to install incorrect software.

SI-7 (1)	**Integrity Checks:** The information system performs an integrity check of software, firmware, and information at least quarterly and following security-relevant events.	Status		Type	
		In Place	X	Common	
		Planned		Hybrid	
		In Place and Planned		System Specific	X
		Not Applicable			

The SCG Secure Cloud system is configured to detect unauthorized changes to software and information. Integrity verification applications are employed on the information system to look for evidence of information tampering, errors, and omissions. Good software engineering practices are employed on the information system with regard to commercial off-the-shelf integrity mechanisms and tools are used to automatically monitor the integrity of the information system. The date and time a resource was last modified or accessed is recorded for sensitive resources. SCG shall reassess the integrity of software and information by performing monthly scans of the system and following security-related events.

SI-7 (7)	**Integration of Detection and Response:** The organization incorporates the detection of unauthorized security-relevant changes (configuration changes [e.g., IP address changes, elevated privileges] and physical changes [e.g., wiring changes, equipment removal]) into the organizational incident response capability.	Status		Type	
		In Place	X	Common	
		Planned		Hybrid	
		In Place and Planned		System Specific	X
		Not Applicable			

SCG tracks unauthorized security-relevant changes (e.g., configuration setting changes, elevation of privileges) to the SCGSC by reviewing the weekly logs. Any detection would be investigated and remediated in accordance with Section 10 of the **Incident Response Plan**, and documented for the historical record per policy in the **System and Information Integrity Policy and Procedures** document. Good software engineering practices are employed on the information system with regard to commercial off-the-shelf integrity mechanisms, and tools are used to automatically monitor the integrity of the information system and the applications it hosts. The date and time a resource was last modified or accessed is recorded for sensitive resources. SCG will reassess the integrity of software and information by performing quarterly integrity scans of the information system.

SI-8	**Spam Control:** The organization: a. Employs spam protection mechanisms at information system entry and exit points to detect and take action on unsolicited messages; and b. Update spam protection mechanisms when new releases are available in accordance with organizational configuration management policy and procedures.	Status		Type	
		In Place		Common	
		Planned		Hybrid	
		In Place and Planned		System Specific	X
		Not Applicable	X		

There are no mail servers within the SCGSC system. Therefore, this control is Not Applicable.

SI-8 (1)	**Central Management:** The organization centrally manages spam protection mechanisms.	Status		Type	
		In Place		Common	
		Planned		Hybrid	
		In Place and Planned		System Specific	X
		Not Applicable	X		

There are no mail servers within the SCGSC system. Therefore, this control is Not Applicable.

SI-8 (2)	**Automatic Updates:** The information system automatically updates spam protection mechanisms.	Status		Type	
		In Place		Common	
		Planned		Hybrid	
		In Place and Planned		System Specific	X
		Not Applicable	X		

There are no mail servers within the SCGSC system. Therefore, this control is Not Applicable.

SI-10	**Information Input Validity:** The information system checks the validity of information inputs.	Status		Type	
		In Place	X	Common	
		Planned		Hybrid	
		In Place and Planned		System Specific	X
		Not Applicable			

The SCGSC system is configured to check the validity of information inputs such as passwords for Active Directory, the Cisco firewall, and Symantec. Rules for checking the valid syntax and semantics of information system inputs (e.g., character set, length, numerical range, acceptable values) are in place to verify that inputs match specified definitions for format and content. The system is configured to perform type checks, format and syntax checks, and parameter and character validity checks.

SI-11	**Error Handling:** The information system: a. Generates error messages that provide information necessary for corrective actions without revealing information that could be exploited by adversaries; and b. Reveals error messages only to the SCG IT staff authorized to access SCGSC.	Status		Type	
		In Place	X	Common	
		Planned		Hybrid	
		In Place and Planned		System Specific	X
		Not Applicable			

The SCGSC system generates error messages that are recorded in logs (Windows and IPS logs) compiled in Kiwi Syslog. These logs are reviewed by the IT Director weekly and are accessible only by the SCG IT personnel who have authorized access to the SCGSC system. Serious errors are addressed by IT staff as soon as possible. There is no sensitive information contained in the error logs.

SI-12	**Information Handling and Retention:** The organization handles and retains information within the information system and information output from the system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements.	Status		Type	
		In Place	X	Common	
		Planned		Hybrid	
		In Place and Planned		System Specific	X
		Not Applicable			

SCG handles and retains all information within the SCGSC system in accordance with federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements. Information is retained in the system for a minimum of 3 years but may be up to 7 years (in accordance with NARA requirements). There are no outputs in the SCGSC environment.

SI-16	**Memory Protection:** The information system implements Symantec Endpoint Protection Suite Enterprise safeguards to protect its memory from unauthorized code execution.	Status		Type	
		In Place	X	Common	
		Planned		Hybrid	
		In Place and Planned		System Specific	X
		Not Applicable			

Symantec Endpoint Protection Suite Enterprise implements safeguards to protect the SCGSC memory from unauthorized code execution. Only authorized access to the SCG Secure Cloud system is permitted using ports 80 and 443. No other access is possible.

21. Program Management (PM)

The FISMA requires organizations to develop and implement an organization-wide information security program to address information security for the information and information systems that support the operations and assets of the organization, including those provided or managed by another organization, contractor, or other source. The information security program management (PM) controls described below are typically implemented at the organization level and not directed at individual organizational information systems. The program management controls have been designed to facilitate compliance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards. The controls are independent of any FIPS Publication 200 impact levels and therefore, are not directly associated with any of the security control baselines. The program management controls do, however,

complement the security controls in and focus on the programmatic, organization-wide information security requirements that are independent of any particular information system and are essential for managing information security programs.

The status of program management controls for the SCG Secure Cloud system is as indicated in the following table:

<table>
<tr><th>Control Number</th><th>Description of Control</th><th colspan="4">Control Status/Type</th></tr>
<tr><td rowspan="6">PM-1</td><td rowspan="6">Information Security Program Plan: The organization:
a. Develops and disseminates an organization-wide information security program plan that:
1. Provides an overview of the requirements for the security program and a description of the security program management controls and common controls in place or planned for meeting those requirements;
2. Includes the identification and assignment of roles, responsibilities, management commitment, coordination among organizational entities, and compliance;
3. Reflects coordination among organizational entities responsible for the different aspects of information security (i.e., technical, physical, personnel, cyber-physical); and
4. Is approved by a senior official with responsibility and accountability for the risk being incurred to organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation;
b. Reviews and, if necessary, updates the organization-wide information security program plan at least every 365 days;
c. Updates the plan to address organizational changes and problems identified during plan implementation or security control assessments; and
d. Protects the information security program plan from unauthorized disclosure and modification.</td><td>Status</td><td></td><td>Type</td><td></td></tr>
<tr><td>In Place</td><td>X</td><td>Common</td><td>X</td></tr>
<tr><td>Planned</td><td></td><td>Hybrid</td><td></td></tr>
<tr><td>In Place and Planned</td><td></td><td>System Specific</td><td></td></tr>
<tr><td>Not Applicable</td><td></td><td colspan="2"></td></tr>
<tr><td colspan="5">The Information Security Program Plan is developed and administered by HHS. See the HHS Information Systems Security and Privacy Policy – 2014 Edition.</td></tr>
</table>

PM-2	**Senior Information Security Officer:** The organization appoints a senior information security officer with the mission and resources to coordinate, develop, implement, and maintain an organization-wide information security program.	Status		Type	
		In Place	X	Common	X
		Planned		Hybrid	
		In Place and Planned		System Specific	
		Not Applicable			
NIH has appointed a senior Information System Security Officer who is located in the Computer Technology Branch, NIDDK/NIH. See the HHS Information Systems Security and Privacy Policy – 2014 Edition.					

PM-3	**Information Security Resources:** The organization: a. Ensures that all capital planning and investment requests include the resources needed to implement the information security program and documents all exceptions to this requirement; b. Employs a business case/Exhibit 300/Exhibit 53 to record the resources required; and c. Ensures that information security resources are available for expenditure as planned.	Status		Type	
		In Place	X	Common	X
		Planned		Hybrid	
		In Place and Planned		System Specific	
		Not Applicable			
The HHS Capital Planning and Investment Process is managed by the HHS CIO. See the HHS Information Systems Security and Privacy Policy – 2014 Edition.					

PM-4	**Plan of Action and Milestones Process:** The organization: a. Implements a process for ensuring that plans of action and milestones for the security program and associated organizational information systems: 1. Are developed and maintained; 2. Document the remedial information security actions to adequately respond to risk to organizational operations and assets, individuals, other organizations, and the Nation; and b. Are reported in accordance with OMB FISMA reporting requirements and other applicable requirements, such as those within the Federal Risk and Authorization Management Program (FedRAMP). c. Reviews plans of action and milestones for consistency with the organizational risk	Status		Type	
		In Place	X	Common	X
		Planned		Hybrid	
		In Place and Planned		System Specific	
		Not Applicable			

	management strategy and organization-wide priorities for risk response actions.	

The Plan of Action and Milestones process is managed by HHS. The roles and responsibility for this process are identified in the HHS Information Systems Security and Privacy Policy – 2014 Edition.

The SCG staff have developed a POAM Remediation Plan_v1.0 that documents the remedial information security actions to adequately respond to risk to the system. The plan is consistent with the HHS risk management strategies. See the HHS Information Systems Security and Privacy Policy – 2014 Edition.

PM-5	**Information System Inventory:** The organization develops and maintains an inventory of all Department information systems, to include those operated on behalf of the Department (e.g., by a contractor, vendor, cloud service provider, or other service provider).	Status		Type	
		In Place	X	Common	X
		Planned		Hybrid	
		In Place and Planned		System Specific	
		Not Applicable			

The Information System Inventory for the Department is managed by HHS. The roles and responsibility for this process are identified in the HHS Information Systems Security and Privacy Policy – 2014 Edition.

An inventory of the SCGSC system is maintained by SCG. It is reported to HHS via NIDDK when requested.

PM-6	**Information Security Performances and Measures:** The organization develops, monitors, and reports on the results of information security measures of performance to evaluate the effectiveness of IT security and privacy policies, procedures, and controls. The measures and metrics must provide information on measures of implementation, efficiency, effectiveness, and impact.	Status		Type	
		In Place	X	Common	X
		Planned		Hybrid	
		In Place and Planned		System Specific	
		Not Applicable			

The Information Security Performances and Measures is managed by HHS. The roles and responsibility for this process are identified in the HHS Information Systems Security and Privacy Policy – 2014 Edition.

PM-7	**Enterprise Architecture:** The organization develops and implements an enterprise architecture with consideration for information security and the resulting risk to organizational operations, organizational assets, individuals, other organizations, and the Nation.	Status		Type	
		In Place	X	Common	X
		Planned		Hybrid	
		In Place and Planned		System Specific	
		Not Applicable			

The Enterprise Architecture is managed by HHS. The roles and responsibility for this process are identified in the HHS Information Systems Security and Privacy Policy – 2014 Edition.

PM-8	**Critical Infrastructure:** The organization addresses information security issues in the development, documentation, and updating of a critical infrastructure and key resources protection plan.	Status		Type	
		In Place	X	Common	X
		Planned		Hybrid	
		In Place and Planned		System Specific	
		Not Applicable			

The Critical Infrastructure is managed by HHS. The roles and responsibility for this process are identified in the HHS Information Systems Security and Privacy Policy – 2014 Edition.

PM-9	**Risk Management Strategy:** The organization: a. Develops a comprehensive strategy to manage risk to organizational operations and assets, individuals, other organizations, and the Nation associated with the operation and use of information systems; b. Implements the risk management strategy consistently across the organization; and c. Reviews and updates the risk management strategy at least every 365 days or as required, to address organizational changes.	Status		Type	
		In Place	X	Common	X
		Planned		Hybrid	
		In Place and Planned		System Specific	
		Not Applicable			

The Risk Management Strategy is managed by HHS. The roles and responsibility for this process are identified in the HHS Information Systems Security and Privacy Policy – 2014 Edition. A risk assessment of the SCGSC system currently is being conducted. The assessment will be reviewed and updated at a minimum of every 365 days.

PM-10	**Security Authorization Process:** The organization: a. Manages (i.e., documents, tracks, and reports) the security state of organizational information systems and the environments in which those systems operate through security authorization processes; b. Designates individuals to fulfill specific roles and responsibilities within the organizational risk management process; and c. Fully integrates the security authorization processes into an organization-wide risk management program.	Status		Type	
		In Place	X	Common	X
		Planned		Hybrid	
		In Place and Planned		System Specific	
		Not Applicable			

The Security Authorization process is managed by HHS. The roles and responsibility for this process are identified in the HHS Information Systems Security and Privacy Policy – 2014 Edition.

PM-11	**Mission/ Business Process Definition:** The organization: a. Defines mission/business processes with consideration for information security and the resulting risk to organizational operations, organizational assets, individuals, other organizations, and the Nation; and b. Determines information protection needs arising from the defined mission/business processes and revises the processes as necessary, until achievable protection needs are obtained.	Status		Type	
		In Place	X	Common	X
		Planned		Hybrid	
		In Place and Planned		System Specific	
		Not Applicable			

The Mission/ Business process is managed by HHS. The roles and responsibility for this process are identified in the HHS Information Systems Security and Privacy Policy – 2014 Edition.

PM-12	**Insider Threat Program:** The organization implements an insider threat program that includes a cross-discipline insider threat incident handling team.	Status		Type	
		In Place	X	Common	X
		Planned		Hybrid	
		In Place and Planned		System Specific	
		Not Applicable			

The Insider Threat Program is managed by HHS. The roles and responsibility for this process are identified in the HHS Information Systems Security and Privacy Policy – 2014 Edition.

PM-13	**Information Security Workforce:** The organization establishes an information security workforce development and improvement program.	Status		Type	
		In Place	X	Common	X
		Planned		Hybrid	
		In Place and Planned		System Specific	
		Not Applicable			

The Information Security Workforce is managed by HHS. The roles and responsibility for this process are identified in the HHS Information Systems Security and Privacy Policy – 2014 Edition.

PM-14	**Testing, Training, and Monitoring:** The organization: a. Implements a process for ensuring that organizational plans for conducting security testing, training, and monitoring activities associated with organizational information systems: 1. Are developed and maintained; and 2. Continue to be executed in a timely manner; b. Reviews testing, training, and monitoring plans for consistency with the organizational risk management strategy and organization-wide priorities for risk response actions.	Status		Type	
		In Place	X	Common	X
		Planned		Hybrid	
		In Place and Planned		System Specific	
		Not Applicable			

The Testing, Training, and Monitoring program is managed by HHS. The roles and responsibility for this process are identified in the HHS Information Systems Security and Privacy Policy – 2014 Edition.

PM-15	**Contact with Security Groups & Associations:** The organization establishes and institutionalizes contact with selected groups and associations within the security community: a. To facilitate ongoing security education and training for organizational personnel; b. To maintain currency with recommended security practices, techniques, and technologies; and c. To share current security-related information including threats, vulnerabilities, and incidents.	Status		Type	
		In Place	X	Common	X
		Planned		Hybrid	
		In Place and Planned		System Specific	
		Not Applicable			

Contact with Security Groups and Associations is managed by HHS. The roles and responsibility for this process is identified in the HHS Information Systems Security and Privacy Policy – 2014 Edition.

PM-16	**Threat Awareness Program:** The organization implements a threat awareness program that includes a cross-organization information-sharing capability.	Status		Type	
		In Place	X	Common	X
		Planned		Hybrid	
		In Place and Planned		System Specific	
		Not Applicable			
The Threat and Awareness Program is managed by HHS. The roles and responsibility for this process is identified in the HHS Information Systems Security and Privacy Policy – 2014 Edition.					

Privacy Control Section

The privacy portion of the HHS Information Systems Security and Privacy Policy (henceforth "the Policy") closely follows Appendix J of NIST SP 800-53, Revision 4. Appendix J provides a structured set of controls for protecting privacy and serves as a roadm
ap for organizations to use in identifying and implementing privacy controls concerning the entire life cycle of PII, regardless of format. This privacy introduction acts as a supplement to the introductory material for the entire Policy.

The rationale for following these controls is derived from SP 800-53, stating that the Appendix J controls are "primarily for use by an organization's Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO) when working with program managers, mission/business owners, information owners/stewards, Chief Information Officers, Chief Information Security Officers, information system developers/integrators, and risk executives to determine how best to incorporate effective privacy protections and practices (i.e., privacy controls) within organizational programs and information systems and the environments in which they operate. The privacy controls facilitate the organization's efforts to comply with privacy requirements affecting those organizational programs and/or systems that collect, use, maintain, share, or dispose of PII or other activities that raise privacy risks.

As stated in the overall scope for the Policy, these privacy controls apply to all HHS organizational components (OpDivs and StaffDivs), and all personnel conducting business for, and on behalf of, the Department, whether directly or through contractual relationships. The term "the organization" is used throughout these controls to make clear that, unless a component is specifically mentioned, these are a baseline regardless of organizational component or system, and may be enhanced as necessary based on that component's mission.

It is noted that Appendix J is meant to be implemented consistent with the Privacy Act of 1974, 5 U.S.C. § 552a. Any terms that appear in the Policy derived from the Act (such as notice, system of records, or disclosure) are meant to have the same definition. In

addition, certain HHS components have additional privacy and security obligations under the Health Insurance Portability and Accountability Act (HIPAA) Rules with respect to PII that is protected health information, and may have obligations under other laws such as the Confidential Information Protection and Statistical Efficiency Act. Nothing in this policy should be construed to remove or modify the Department's obligation to ensure that it and its components comply with the applicable requirements of other laws.

22. Authority and Purpose (AP)

This family of controls ensures that organizations: (i) identify the legal bases that authorize a particular PII collection or activity that impacts privacy; and (ii) specify in their notices the purpose(s) for which PII is collected.

The status of authority and purpose controls for the SCGSC system is as indicated in the following table:

<table>
<tr><th>Control Number</th><th>Description of Control</th><th>Control Status/Type</th></tr>
<tr><td>AP-1</td><td>Authority to Collect: The organization determines and documents the legal authority that permits the collection, use, maintenance, and sharing of personally identifiable information (PII), both generally and in support of a specific program or information system need.</td><td>
<table>
<tr><th>Status</th><th></th><th>Type</th><th></th></tr>
<tr><td>In Place</td><td>X</td><td>Common</td><td>X</td></tr>
<tr><td>Planned</td><td></td><td>Hybrid</td><td></td></tr>
<tr><td>In Place and Planned</td><td></td><td>System Specific</td><td></td></tr>
<tr><td>Not Applicable</td><td></td><td colspan="2"></td></tr>
</table>
</td></tr>
<tr><td colspan="3">The NIDDK Privacy statement located on the NIH/NIDDK website with a link on the Catalog website identifies the types of information collected and the authority for collecting the information. The SCGSC system collects only the name, address, and phone number of users who wish to obtain a document listed in the clearinghouse catalog on the website. This information is protected using 256-bit Secure Socket Layer (SSL) protocol. This information is not shared and it is purged from the system every 30 days.</td></tr>
</table>

<table>
<tr><td>AP-2</td><td>Purpose Specification: The organization, at the system or application level, describes the purpose(s) for which PII is collected, used, maintained, and shared in privacy compliance documentation and in its privacy notices (e.g., Privacy Impact Assessments [PIAs], System of Records Notices [SORNs], Privacy Act Statements, or Computer Matching Agreements [CMAs]).</td><td>
<table>
<tr><th>Status</th><th></th><th>Type</th><th></th></tr>
<tr><td>In Place</td><td>X</td><td>Common</td><td>X</td></tr>
<tr><td>Planned</td><td></td><td>Hybrid</td><td></td></tr>
<tr><td>In Place and Planned</td><td></td><td>System Specific</td><td></td></tr>
<tr><td>Not Applicable</td><td></td><td colspan="2"></td></tr>
</table>
</td></tr>
</table>

The NIDDK Privacy statement located on the NIH/NIDDK website identifies the purposes for which PII is collected. The SCGSC system collects only the name and address of users who order documents through the clearinghouse. This information is protected using 128-bit Secure Socket Layer (SSL) protocol. This information is not shared.

23. Accountability, Audit, and Risk Management (AR)

This family enhances public confidence through effective controls for governance, monitoring, risk management, and assessment to demonstrate that organizations are complying with applicable privacy protection requirements and minimizing overall privacy risk.

The status of accountability, audit, and risk management controls for the SCGSC system is as indicated in the following table:

<table>
<tr><th>Control Number</th><th>Description of Control</th><th>Control Status/Type</th></tr>
<tr><td>AR-1</td><td>Governance and Privacy Program: The organization:
a. Appoints a Senior Agency Official for Privacy (SAOP) accountable for developing, implementing, and maintaining a Department-wide governance and privacy program to ensure compliance with all applicable laws and regulations regarding the collection, use, maintenance, sharing, and disposal of PII by programs and information systems;

Note: The HHS SAOP must govern and manage all privacy requirements; however, HHS may appoint other privacy officials and points of contact to support the SAOP so that HHS complies with laws, regulations, and OMB memoranda. These other officials and points of contact may assist with executing items (b)-(f) of this section.

b. Monitors federal privacy laws and policy for changes that affect the privacy program;
c. Allocates organization-defined budget and staffing resources sufficient to implement and operate the organization-wide privacy program;</td><td>
<table>
<tr><th>Status</th><th></th><th>Type</th><th></th></tr>
<tr><td>In Place</td><td>X</td><td>Common</td><td></td></tr>
<tr><td>Planned</td><td></td><td>Hybrid</td><td></td></tr>
<tr><td>In Place and Planned</td><td></td><td>System Specific</td><td>X</td></tr>
<tr><td>Not Applicable</td><td></td><td colspan="2"></td></tr>
</table>
</td></tr>
</table>

	d. Develops a strategic organizational privacy plan for implementing applicable privacy controls, policies, and procedures; e. Develops, disseminates, and implements operational privacy policies and procedures that govern the appropriate privacy and security controls for programs, information systems, or technologies involving PII; and f. Updates privacy plan, policies, and procedures in accordance with SAOP direction, but at least every two (2) years.	
HHS appoints a Senior Agency Official for Privacy who governs and manages all privacy requirements.		

AR-2	**Privacy Impact and Risk Assessment:** The organization: a. Documents and implements a privacy risk management process that assesses privacy risk to individuals resulting from the collection, sharing, storing, transmitting, use, and disposal of PII; and b. Conducts Privacy Impact Assessments (PIAs) for information systems, programs, or other activities that pose a privacy risk in accordance with applicable law, OMB policy, or any existing organizational policies and procedures.	Status		Type	
		In Place	X	Common	
		Planned		Hybrid	
		In Place and Planned		System Specific	X
		Not Applicable			
HHS requires PIAs to be conducted on all information systems early in the system development life cycle. A PIA questionnaire for the SCGSC system was completed, submitted to, and approved by NIDDK.					

AR-3	**Privacy Requirements for Contractors and Service Providers:** The organization: a. Establishes privacy roles, responsibilities, and access requirements for contractors and service providers; b. Includes privacy requirements in contracts and other acquisition-related documents; and c. Reviews, every two (2) years, a random sample of agency contracts that provide for the maintenance of a system of records on behalf of the agency to accomplish an agency function, in order to ensure that the contracts include clauses that make all requirements of the Privacy Act apply to the system and that	Status		Type	
		In Place	X	Common	
		Planned		Hybrid	
		In Place and Planned		System Specific	X
		Not Applicable			

	make the criminal penalty provisions of the Privacy Act apply to the contractor or service provider and its personnel.	
HHS establishes privacy roles, responsibility, and access requirements for contractors and service providers. These requirements are included in all acquisition-related documents and random samples of contracts are reviewed every two (2) years to ensure that pertinent clauses are included.		

AR-4	**Privacy Monitoring and Auditing:** The organization: a. Monitors and audits privacy controls and internal privacy policy at least every 365 days to ensure effective implementation; and b. Documents, tracks, and ensures mitigation of corrective actions identified through monitoring or auditing.	Status		Type	
		In Place	X	Common	X
		Planned		Hybrid	
		In Place and Planned		System Specific	
		Not Applicable			
The HHS SAOP coordinates privacy monitoring and auditing with Departmental and OpDiv information security and privacy officials. (See HHS-OCIO Policy for Information Systems Security and Privacy at http://www.hhs.gov/ocio/policy/policydocs/hhs-ocio-2011-0003_is2p.doc.)					

AR-5	**Privacy and Awareness Training:** The organization: a. Develops, implements, and updates a comprehensive privacy training and awareness strategy aimed at educating and informing personnel about their privacy responsibilities and procedures; b. Administers basic privacy training at least annually and targeted, role-based privacy training annually for personnel having responsibility for PII or for activities that involve PII; and c. Ensures that personnel certify (manually or electronically) acceptance of responsibilities for privacy requirements at least every 365 days.	Status		Type	
		In Place	X	Common	X
		Planned		Hybrid	
		In Place and Planned		System Specific	
		Not Applicable			
All SCG staff with access to the SCGSC must complete the NIH Information Security and Privacy Awareness Training every 365 days (http://irtsectraining.nih.gov/). All personnel are required to certify acceptance of their privacy responsibilities at least every 365 days.					

AR-6	**Privacy Reporting:** The organization develops, disseminates, and updates reports to the OMB, Congress, and other oversight bodies, as appropriate, to demonstrate accountability with specific statutory and regulatory privacy program mandates, and to senior management and other personnel with responsibility for monitoring privacy program progress and compliance.	Status		Type	
		In Place	X	Common	X
		Planned		Hybrid	
		In Place and Planned		System Specific	
		Not Applicable			
The HHS SOAP provides this information annually in response to statutory and regulatory requirements, as appropriate.					

AR-7	**Privacy Enhanced System Design and Development:** The organization designs information systems to support privacy by automating privacy controls to the extent feasible, integrating and meeting privacy requirements throughout the EPLC, and incorporating privacy concerns into reviews of significant changes to HHS systems, networks, physical environments, and other agency infrastructures. The organization also conducts periodic reviews of systems to determine the need for updates to maintain compliance with the Privacy Act, the organization's privacy policy, and any other legal or regulatory requirements.	Status		Type	
		In Place	X	Common	X
		Planned		Hybrid	
		In Place and Planned		System Specific	
		Not Applicable			
The HHS SOAP provides automated tools to support the Privacy Program.					

AR-8	**Accounting of Disclosure:** The organization: a. Keeps an accurate accounting of disclosures of PII held in each system of records under its control, including: 1. Date, nature, and purpose of each disclosure of a record; and 2. Name and address of the person or agency to which the disclosure was made; b. Retains the accounting of disclosures for the life of the record or five (5) years after the disclosure is made, whichever is longer; and c. Makes the accounting of disclosures available to the person named in the record upon request.	Status		Type	
		In Place	X	Common	X
		Planned		Hybrid	
		In Place and Planned		System Specific	
		Not Applicable			

The HHS SAOP maintains an accurate accounting of disclosures of PII held in each system of records under its control. In the event of a disclosure of PII, SCG would notify the NIDDK ISSO and System Owner, and provide them with a detailed record of the event to ensure accurate accounting of disclosures of PII.

24. Data Quality and Integrity (DI)

This family enhances public confidence that any PII collected and maintained by organizations is accurate, relevant, timely, and complete for the purpose for which it is to be used, as specified in public notices.

The status of data quality and integrity controls for the SCGSC system is as indicated in the following table:

Control Number	Description of Control	Control Status/Type
DI-1	**Data Quality:** The organization: a. Confirms to the greatest extent practicable upon collection or creation of PII, the accuracy, relevance, timeliness, and completeness of that information; b. Collects PII directly from the individual to the greatest extent practicable; c. Checks for, and corrects as necessary, any inaccurate or outdated PII used by its programs or systems at an at least every 365 days; and d. Issues guidelines for maximizing the quality, utility, objectivity, and integrity of disseminated information.	Status: In Place X; Planned; In Place and Planned; Not Applicable Type: Common X; Hybrid; System Specific
All PII is entered directly by the user requesting the NIDDK publication, SCG does not create or verify the accuracy of the information. The information is used only to facilitate the delivery of the requested material and the data are purged from the SCGSC every 30 days. There is no use of the data by programs or other systems.		

DI-2	**Data Integrity and Data Integrity Board:** The organization: a. Documents processes to ensure the integrity of PII through existing security controls; and b. Establishes a Data Integrity Board (DIB) to oversee organizational Computer Matching Agreements and to ensure that those agreements comply with the computer matching provisions of the Privacy Act.	Status: In Place X; Planned; In Place and Planned; Not Applicable Type: Common X; Hybrid; System Specific

SCG has documented processes and procedures for ensuring the integrity of PII in the SCGSC through various security controls. The HHS Data Integrity Board oversees organizational Computer Matching Agreements and ensures that those agreements comply with the computer matching provisions of the Privacy Act.

25. Data Minimization and Retention (DM)

This family helps organizations implement the data minimization and retention requirements to collect, use, and retain only PII that is relevant and necessary for the purpose for which it was originally collected. Organizations retain PII for only as long as necessary to fulfill the purpose(s) specified in public notices and in accordance with a National Archives and Records Administration (NARA)-approved record retention schedule.

The status of data minimization and retention controls for the SCGSC system is as indicated in the following table:

Control Number	Description of Control	Control Status/Type
DM-1	**Minimization of Personally Identifiable Information:** The organization: a. Identifies the minimum PII elements that are relevant and necessary to accomplish the purpose of collection (and where a collection of certain PII requires legal authorization, HHS shall ensure that such collection is legally authorized); b. Limits the collection and retention of PII to the minimum elements identified in the notice and, when the collection of PII is made directly from the subject individual, limits its purposes to those for which the individual has provided consent to the extent permitted by law; and c. Conducts an initial evaluation of PII holdings and establishes and follows a schedule for regularly reviewing those holdings at least every 365 days to ensure that only PII identified in the notice is collected and retained, and that the PII continues to be necessary to accomplish its purpose.	Status: In Place X; Planned; In Place and Planned; Not Applicable Type: Common X; Hybrid; System Specific

The SCGSC collects names, addresses, and phone numbers of individuals who request NIDDK publications from the catalog. This is the minimum amount of information needed to fulfill the requests. No legal authorization is required for collection of this information. The purpose of the PII is limited to this single use and data are purged from the system every 30 days. SCG reviews the need to collect the PII annually to verify that it is necessary to support that task of distributing NIDDK publications to requestors. The PII to be collected by the SCGSC was determined by NIDDK and the previous contractors that supported the NIDDK clearinghouses.

DM-2	**Minimization of Personally Identifiable Information:** The organization: a. Retains each collection of PII for the minimum time period, specified by the Records Management Officer to fulfill the purpose(s) identified in the notice or as required by law; b. Disposes of, destroys, erases, and/or anonymizes the PII, regardless of the method of storage, in accordance with a National Archives and Records Administration (NARA) approved record retention schedule and in a manner that prevents loss, theft, misuse, or unauthorized access; and c. Uses organization-defined techniques or methods to ensure secure deletion or destruction of PII (including originals, copies, and archived records).	Status / Type

Status		Type	
In Place	X	Common	
Planned		Hybrid	
In Place and Planned		System Specific	X
Not Applicable			

The SCGSC system retains PII for a maximum of 30 days as the system is purged of all records on a monthly basis. Records are destroyed in accordance with the methods used in NIST SP 800-88, Rev1, Guidelines for Media Sanitization.

DM-3	**Minimization of Personally Identifiable Information:** The organization: a. Develops procedures that minimize the use of PII for testing, training, and research; and b. Implements controls to protect PII used for testing, training, and research.	Status / Type

Status		Type	
In Place	X	Common	
Planned		Hybrid	
In Place and Planned		System Specific	X
Not Applicable			

No PII is used for the purposes of testing, training, and research for the SCGSC. Dummy records are created for such purposes.

26. Individual Participation and Redress (IP)

This family addresses the need to make individuals active participants in the decision-making process regarding the collection and use of their personally identifiable information (PII). By providing individuals with access to PII and the ability to have their PII corrected or amended, as appropriate, the controls in this family enhance public confidence in organizational decisions made based on the PII.

The status of individual participation and redress controls for the SCGSC system is as indicated in the following table:

<table>
<tr><th>Control Number</th><th>Description of Control</th><th>Control Status/Type</th></tr>
<tr><td>IP-1</td><td>Consent: The organization:
a. Provides means, where feasible and appropriate, for individuals to authorize the collection, use, maintaining, and sharing of PII prior to its collection;
b. Provides appropriate means for individuals to understand the consequences of decisions to approve or decline the authorization of the collection, use, dissemination, and retention of PII;
c. Obtains consent, where feasible and appropriate, from individuals prior to any new uses or disclosure of previously collected PII; and
d. Ensures that individuals are aware of and, where feasible, consent to all uses of PII not initially described in the public notice that was in effect at the time the organization collected the PII.</td><td><table><tr><th>Status</th><th></th><th>Type</th><th></th></tr><tr><td>In Place</td><td>X</td><td>Common</td><td>X</td></tr><tr><td>Planned</td><td></td><td>Hybrid</td><td></td></tr><tr><td>In Place and Planned</td><td></td><td>System Specific</td><td></td></tr><tr><td>Not Applicable</td><td></td><td colspan="2"></td></tr></table></td></tr>
<tr><td colspan="3">HHS provides individuals appropriate notice of the purposes of the PII collection or technology use and a means for individuals to consent to the activity. This information is available in the NIDDK Privacy Statement posted on the NIH/NIDDK website, which is linked on the Catalog website.</td></tr>
</table>

<table>
<tr><td>IP-1 (1)</td><td>Mechanisms Supporting Itemized or Tiered Consent: The organization implements mechanisms to support itemized or tiered consent for specific uses of data.</td><td><table><tr><th>Status</th><th></th><th>Type</th><th></th></tr><tr><td>In Place</td><td>X</td><td>Common</td><td>X</td></tr><tr><td>Planned</td><td></td><td>Hybrid</td><td></td></tr><tr><td>In Place and Planned</td><td></td><td>System Specific</td><td></td></tr><tr><td>Not Applicable</td><td></td><td colspan="2"></td></tr></table></td></tr>
</table>

Where appropriate HHS provides individuals with itemized choices as to whether they wish to be contacted for any of a variety of purposes. See the NIDDK Privacy Statement posted on the NIH/NIDDK website and linked on the Catalog website.

IP-2	**Individual Access:** The organization: a. Provides individuals the ability to have access to their PII maintained in its system(s) of records; b. Publishes rules and regulations governing how individuals may request access to records maintained in a Privacy Act system of records; c. Publishes access procedures in SORNs; and d. Adheres to Privacy Act requirements and OMB policies and guidance for the proper processing of Privacy Act requests.	Status / Type

Status		Type	
In Place	X	Common	
Planned		Hybrid	
In Place and Planned		System Specific	X
Not Applicable			

The PII collected in the SCGSC system is entered by the user requesting a publication. The user has the ability to review the name and address information entered into the system. All data are purged from the system every 30 days. The information is not used for any other purpose.

IP-3	**Redress:** The organization: a. Provides a process for individuals to have inaccurate PII maintained by the organization corrected or amended, as appropriate; and b. Establishes a process for disseminating corrections or amendments of the PII to other authorized users of the PII, such as external information-sharing partners and, where feasible and appropriate, notifies affected individuals that their information has been corrected or amended.	Status / Type

Status		Type	
In Place	X	Common	
Planned		Hybrid	
In Place and Planned		System Specific	X
Not Applicable			

Because the PII in the SCGSC is not retained beyond a maximum of 30 days and is used solely for the one-time purpose of distributing the requested publication, there is no process required to allow users to correct inaccurate information. No corrections or amendments of PII are disseminated.

IP-4 (1)	**Response Times:** The organization: a. Acknowledges complaints, concerns, or questions from individuals within 10 working days; b. Completes review of requests within 30 working days of receipt, unless unusual or exceptional circumstances preclude completing action by that time; and c. Responds to any appeal as soon as possible, but no later than 30 working days after receipt of the appeal unless the appeal authority can show good cause to extend the response period.	Status: In Place X; Planned; In Place and Planned; Not Applicable Type: Common; Hybrid; System Specific X
All requests for publications are processed rapidly (usually within 1 to 2 days). Any complaints received from users regarding the failure to receive a publication or the excessive time it took to receive a publication are reported to the NIDDK Project Officer and documented in the monthly progress report prepared by SCG. All complaints are addressed the same day or the next business day (e.g., resending a requested publication that never arrived at the destination).		

27. Security (SE)

This family supplements the security controls in Appendix F to ensure that technical, physical, and administrative safeguards are in place to protect PII collected or maintained by organizations against loss, unauthorized access, or disclosure, and to ensure that planning and responses to privacy incidents comply with OMB policies and guidance. The controls in this family are implemented in coordination with information security personnel and in accordance with the existing NIST Risk Management Framework.

The status of security controls for the SCGSC system is as indicated in the following table:

Control Number	Description of Control	Control Status/Type
SE-1	**Inventory of Personally Identifiable Information:** The organization: a. Establishes, maintains, and updates at least every 365 days an inventory that contains a listing of all programs and information systems identified as collecting, using, maintaining, or sharing PII; and b. Provides each update of the PII inventory to the CIO or information security official at least every 365 days to support the establishment	Status: In Place X; Planned; In Place and Planned; Not Applicable Type: Common X; Hybrid; System Specific

	of information security requirements for all new or modified information systems containing PII.	
HHS maintains an inventory that contains a listing of all programs and systems that have been identified as collecting, using, maintaining, or sharing PII. This inventory is updated every 365 days.		

SE-2	**Privacy Incident Response:** The organization: a. Develops and implements a Privacy Incident Response Plan; and b. Provides an organized and effective response to privacy incidents in accordance with the HHS Privacy Incident Response Plan.	Status		Type	
		In Place	X	Common	X
		Planned		Hybrid	
		In Place and Planned		System Specific	
		Not Applicable			
HHS requires that all privacy incidents be reported in accordance with the HHS Privacy Incident Response Plan.					

28. Transparency (TR)

This family ensures that organizations provide public notice of their information practices and the privacy impact of their programs and activities.

The status of transparency controls for the SCGSC system is as indicated in the following table:

Control Number	Description of Control	Control Status/Type			
TR-1	**Privacy Notice:** The organization: a. Provides effective notice to the public and to individuals regarding: (i) its activities that impact privacy, including its collection, use, sharing, safeguarding, maintenance, and disposal of PII; (ii) authority for collecting PII; (iii) the choices, if any, individuals may have regarding how the organization uses PII and the consequences of exercising or not exercising those choices; and (iv) the ability to request access and have PII amended or corrected if necessary; b. Describes: (i) the PII the organization collects and the purpose(s) for which it collects that information; (ii) how the organization uses PII internally; (iii) whether the organization shares	Status		Type	
		In Place	X	Common	X
		Planned		Hybrid	
		In Place and Planned		System Specific	
		Not Applicable			

	PII with external entities, the categories of those entities, and the purposes for such sharing; (iv) whether individuals have the ability to consent to specific uses or sharing of PII and how to exercise any such consent; (v) how individuals may obtain access to PII; and (vi) how the PII will be protected; and c. Revises its public notices to reflect changes (such as the use or collection of information by the website or system) in practice or policy that affect PII or changes in its activities that impact privacy, before or as soon as practicable after the change.	
HHS provides effective notice to the public regarding its activities that affect the public. By virtue of its clarity, readability, and comprehensiveness, individuals are able to understand how an organization uses PII generally and, where appropriate, to make an informed decision prior to providing PII to an organization. The NIDDK website Privacy Statement provides this information.		

TR-1 (1)	**Real-Time or Layered Notice:** The organization provides real-time and/or layered notice when it collects PII.	Status / Type In Place: X; Common: Planned; Hybrid: In Place and Planned; System Specific: X Not Applicable
The NIDDK Privacy notice link appears on the Catalog website to provide individuals with a summary of the NIDDK privacy policy at the time of collection.		

TR-2	**System of Records Notices and Privacy Act Statements:** The organization, through the HHS Privacy Act Officer, OpDiv Privacy Contacts, and the HHS Office of General Counsel: a. Publishes SORNs in the Federal Register, subject to required oversight processes, for systems containing PII; b. Keeps SORNs current; and c. Includes Privacy Act Statements on its forms that collect PII, or on separate forms that can be retained by individuals, to provide additional formal notice to individuals from whom the information is being collected.	Status / Type In Place: X; Common: X Planned; Hybrid: In Place and Planned; System Specific: Not Applicable
The HHS Privacy Act Officer provides system of record notices and privacy act statements.		

TR-2 (1)	**Public Website Publication:** The organization publishes SORNs on its public website.	Status: In Place X; Planned; In Place and Planned; Not Applicable Type: Common X; Hybrid; System Specific
The HHS SAOP publishes SORNs on the public website.		

TR-3	**Dissemination of Privacy Program Information:** The organization: a. Ensures that the public has access to information about its privacy activities and is able to communicate with its SAOP/Chief Privacy Officer (CPO); and b. Ensures that its privacy practices are publicly available through organizational websites or otherwise.	Status: In Place X; Planned; In Place and Planned; Not Applicable Type: Common X; Hybrid; System Specific
HHS/NIDDK discloses publicly the use of third-party websites and applications (TPWAs) and web measurement and customization technologies used on HHS websites. This information is listed in the NIDDK Privacy Statement.		

29. Use Limitation (UL)

This family ensures that organizations only use personally identifiable information (PII) either as specified in their public notices, in a manner compatible with those specified purposes, or as otherwise permitted by law. Implementation of the controls in this family will ensure that the scope of PII use is limited accordingly.

The status of use limitation controls for the SCGSC system is as indicated in the following table:

Control Number	Description of Control	Control Status/Type
UL-1	**Internal Use:** The organization uses PII internally only for the authorized purpose(s) identified in the Privacy Act and/or in public notices.	Status: In Place X; Planned; In Place and Planned; Not Applicable Type: Common X; Hybrid; System Specific

HHS ensures that PII is only used for legally authorized purposes and in a manner compatible with uses identified in the Privacy Act and/or public notices.

UL-2	**Information Sharing with Third Parties:** The organization: a. Shares PII externally, only for the authorized purposes identified in the Privacy Act and/or described in its notice(s) or for a purpose that is compatible with those purposes; b. Where appropriate, enters into Memoranda of Understanding, Memoranda of Agreement, Letters of Intent, Computer Matching Agreements, or similar agreements, with third parties that specifically describe the PII covered and specifically enumerate the purposes for which the PII may be used; c. Monitors, audits, and trains its staff on the authorized sharing of PII with third parties and on the consequences of unauthorized use or sharing of PII; and d. Evaluates any proposed new instances of sharing PII with third parties to assess whether the sharing is authorized and whether additional or new public notice is required.	Status		Type	
		In Place	X	Common	X
		Planned		Hybrid	
		In Place and Planned		System Specific	
		Not Applicable			

The HHS SAOP (in coordination with the NIDDK SOP) and legal counsel review and approve any proposed external sharing of PII, including with other public, international, or private sector entities, for consistency with uses described in the existing organizational public notice(s). The SCGSC system does not share any subscriber information.

Appendix A: References

NIST SP 800-12, “An Introduction to Computer Security: The NIST Handbook”

NIST SP 800-18, Rev. 1 “Guide for Developing Security Plans for Federal Information Systems”

NIST SP 800-23, “Guidelines to Federal Organizations on Security Assurance and Acquisition/Use of Tested/Evaluated Products”

NIST SP 800-27, Rev A, “Engineering Principles for Information Technology Security (A Baseline for Achieving Security)”

NIST SP 800-28, Version 2 “Guidelines on Active Content and Mobile Code”

NIST SP 800-30, Rev. 1 “Guide for Conducting Risk Assessments”

NIST SP 800-34, Rev. 1 “Contingency Planning Guide for Federal Information Systems”

NIST SP 800-35, “Guide to Information Technology Security Services”

NIST SP 800-36, “Guide to Selecting Information Technology Security Products”

NIST SP 800-37, Rev. 1, “Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach”

NIST SP 800-40, Rev. 3 “Guide to Enterprise Patch Management Technologies”

NIST SP 800-46, Rev. 1 “Guide to Enterprise Telework and Remote Access Security”

NIST SP 800-47, “Security Guide for Interconnecting Information Technology Systems”

NIST SP 800-48, Rev. 1 “Guide to Securing Legacy IEEE 802.11 Wireless Networks”

NIST SP 800-50, “Building an Information Technology Security Awareness and Training Program”

NIST SP 800-53, Rev 4, “Security and Privacy Controls for Federal Information Systems and Organizations”

NIST SP 800-53A, Rev. 4, “Assessing Security and Privacy Controls in Federal Information Systems and Organization: Building Effective Security Assessment Plans”

NIST SP 800-56A, Rev. 2 “Recommendation for Pair-Wise Key-Establishment Schemes Using Discrete Logarithm Cryptography”

NIST SP 800-57, “Recommendation on Key Management”

NIST SP 800-60, Rev. 1 “Guide for Mapping Types of Information and Information Systems to Security Categories”

NIST SP 800-61, Rev. 2 “Computer Security Incident Handling Guide”

NIST SP 800-63 -2, “Electronic Authentication Guideline”

NIST SP 800-64, Rev. 2 “Security Considerations in the System Development Life Cycle”

NIST SP 800-65, “Integrating IT Security into the Capital Planning and Investment Control Process”

NIST SP 800-66, Rev. 1 “An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule”

NIST SP 800-88, Rev. 1 “Guidelines for Media Sanitization”

Appendix B: Acronyms

AO	Authorizing Official
CIO	Chief Information Officer
CIRT	Computer Incident Response Team
COTS	Commercial Off-The-Shelf
DAA	Designated Approving Authority
DNS	Domain Name Systems
E-MAIL	Electronic Mail
FIPS	Federal Information Processing Standard
FISMA	Federal Information Security Management Act of 2002
HHS	Department of Health and Human Services
HIPPA	Health Insurance Portability and Accountability Act of 1996
IP	Internet Protocol
ISO	Information Security Officer
ISSO	Information System Security Officer
IT	Information Technology
LAN	Local Area Network
NIDDK	National Institute of Diabetes and Digestive and Kidney Diseases
NIH	National Institutes of Health
NIST	National Institute of Standards and Technology
OI&T	Office of Information & Technology
OIG	Office of Inspector General
OMB	Office of Management and Budget
PO	Privacy Officer
SCGSC	SCG Secure Cloud
SSP	System Security Plan

Appendix C: Glossary

Access Control	Security control designed to permit authorized access to an AIS.
Accreditation	The official management decision given by a senior agency official to authorize operation of an information system and to explicitly accept the risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals, based on the implementation of an agreed-upon set of security controls.
Accreditation Boundary	All components of an information system to be accredited by an authorizing official and excludes separately accredited systems, to which the information system is connected.
Accreditation Package	The evidence provided to the authorizing official to be used in the security accreditation decision process. Evidence includes, but is not limited to: (i) the system security plan; (ii) the assessment results from the security certification; and (iii) the plan of action and milestones.
Accrediting Authority	See Authorizing Official.
Adequate Security [OMB Circular A-130, Appendix III]	Security commensurate with the risk and the magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information.
Agency	See Executive Agency.
Application [OMB Circular A-130, Appendix III]	The use of information resources (information and information technology) to satisfy a specific set of user requirements.
Assessment Method	A focused activity or action employed by an assessor for evaluating a particular attribute of a security control.
Assessment Procedure	A set of activities or actions employed by an assessor to determine the extent to which a security control is implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.

ATO	Authority to Operate. Authority granted by the AO to operate the information system, resulting in Accreditation of the system.
Audit Trail	A record showing who has accessed a computer system and what operations he or she has performed during a given period of time. Audit trails are useful both for maintaining security and for recovering lost transactions.
Authentication	Verification of the identity of a user, user device, or other entity, or the integrity of data stored, transmitted, or otherwise exposed to unauthorized modification in an AIS.
Authenticity	The property of being genuine and being able to be verified and trusted; confidence in the validity of a transmission, a message, or message originator. See authentication.
Authorization	See Accreditation.
Authorize Processing	See Accreditation.
Authorizing Official	Official with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals.
Authorizing Official Designated Representative	Individual selected by an authorizing official to act on their behalf in coordinating and carrying out the necessary activities required during the security certification and accreditation of an information system.
Automated Information System(s) (AIS)	An assembly of computer hardware, software and/or firmware configured to collect, create, communicate, compute, disseminate, process, store, and/or control data or information.
Availability [44 U.S.C., Sec. 3542]	Ensuring timely and reliable access to and use of information.

Certification	A comprehensive assessment of the management, operational, and technical security controls in an information system, made in support of security accreditation, to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.
Certification Agent	The individual, group, or organization responsible for conducting a security certification.
Chief Information Officer [44 U.S.C., Sec. 5125(b)]	Agency official responsible for: (i) Providing advice and other assistance to the head of the executive agency and other senior management personnel of the agency to ensure that information technology is acquired and information resources are managed in a manner that is consistent with laws, Executive Orders, directives, policies, regulations, and priorities established by the head of the agency; (ii) Developing, maintaining, and facilitating the implementation of a sound and integrated information technology architecture for the agency; and (iii) Promoting the effective and efficient design and operation of all major information resources management processes for the agency, including improvements to work processes of the agency.
Ciphertext	Form of cryptography in which the plaintext is made unintelligible to anyone who intercepts it by a transformation of the information itself, based on some key.
Common Security Control	Security control that can be applied to one or more agency information systems and has the following properties: (i) the development, implementation, and assessment of the control can be assigned to a responsible official or organizational element (other than the information system owner); and (ii) the results from the assessment of the control can be used to support the security certification and accreditation processes of an agency information system where that control has been applied.

Confidentiality [44 U.S.C., Sec. 3542]	Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.
Configuration Control [CNSS Inst. 4009]	Process for controlling modifications to hardware, firmware, software, and documentation to ensure the information system is protected against improper modifications prior to, during, and after system implementation.
COTS Software	Commercial Off The Shelf Software – software acquired by government contract through a commercial vendor. This software is a standard product, not developed by a vendor for a particular government project.
Countermeasures [CNSS Inst. 4009]	Actions, devices, procedures, techniques, or other measures that reduce the vulnerability of an information system. Synonymous with security controls and safeguards.
Default	A value or setting that a device or program automatically selects if you do not specify a substitute.
Designated Approving (Accrediting) Authority	See Authorizing Official.
Dial-up	The service whereby a computer terminal can use the telephone to initiate and effect communication with a computer.
Encryption	The process of making information indecipherable to protect it from unauthorized viewing or use, especially during transmission or storage. Encryption is based on an algorithm and at least one key. Even if the algorithm is known, the information cannot be decrypted without the key(s).
Executive Agency [41 U.S.C., Sec. 403]	An executive department specified in 5 U.S.C., Sec. 101; a military department specified in 5 U.S.C., Sec. 102; an independent establishment as defined in 5 U.S.C., Sec. 104(1); and a wholly owned Government corporation fully subject to the provisions of 31 U.S.C., Chapter 91.
Facsimile	A document that has been sent, or is about to be sent, via a fax machine.

Federal Information System [40 U.S.C., Sec. 11331]	An information system used or operated by an executive agency, by a contractor of an executive agency, or by another organization on behalf of an executive agency.
Firewall	A system or combination of systems that enforces a boundary between two or more networks.
Gateway	A bridge between two networks.
General Support System [OMB Circular A-130, Appendix III]	An interconnected set of information resources under the same direct management control that shares common functionality. It normally includes hardware, software, information, data, applications, communications, and people.
Hardware	Refers to objects that you can actually touch, like disks, disk drives, display screens, keyboards, printers, boards, and chips.
IATO	Interim Authority to Operate. A temporary ATO, valid for a limited time until ATO can be achieved.
Identification	The process that enables recognition of a user described to an AIS.
Information [FIPS 199]	An instance of an information type.
Information Owner [CNSS Inst. 4009]	Official with statutory or operational authority for specified information and responsibility for establishing the controls for its generation, collection, processing, dissemination, and disposal.
Information Resources [44 U.S.C., Sec. 3502]	Information and related resources, such as personnel, equipment, funds, and information technology.
Information Security [44 U.S.C., Sec. 3542]	The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.
Information Security Policy [CNSS Inst. 4009]	Aggregate of directives, regulations, rules, and practices that prescribes how an organization manages, protects, and distributes information.

Information System [44 U.S.C., Sec. 3502] [OMB Circular A-130, Appendix III]	A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.
Information System Owner (or Program Manager) [CNSS Inst. 4009, Adapted]	Official responsible for the overall procurement, development, integration, modification, or operation and maintenance of an information system.
Information System Security Officer [CNSS Inst. 4009, Adapted]	Individual responsible to the senior agency information security officer, authorizing official, or information system owner for ensuring the appropriate operational security posture is maintained for an information system or program.
Information Technology [40 U.S.C., Sec. 1401]	Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency. For purposes of the preceding sentence, equipment is used by an executive agency if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency which: (i) requires the use of such equipment; or (ii) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. The term information technology includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources.
Information Type [FIPS 199]	A specific category of information (e.g., privacy, medical, proprietary, financial, investigative, contractor sensitive, security management), defined by an organization or in some instances, by a specific law, Executive Order, directive, policy, or regulation.
Integrity [44 U.S.C., Sec. 3542]	Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.
Internet	A global network connecting millions of computers. As of 1999, the Internet has more than 200 million users worldwide, and that number is growing rapidly.

Intranet	A network based on TCP/IP protocols (an internet) belonging to an organization, usually a corporation, accessible only by the organization's members, employees, or others with authorization. An intranet's Web sites look and act just like any other Web sites, but the firewall surrounding an intranet fends off unauthorized access.
Intrusion Detection	Pertaining to techniques, which attempt to detect intrusion into a computer or network by observation of actions, security logs, or audit data. Detection of break-ins or attempts either manually or via software expert systems that operate on logs or other information available on the network.
LDAP	Short for Lightweight Directory Access Protocol, a set of protocols for accessing information directories. LDAP is based on the standards contained within the X.500 standard, but is significantly simpler. An unlike X.500, LDAP supports TCP/IP, which is necessary for any type of Internet access.
Least Privilege	The process of granting users only those accesses they need to perform their official duties.
Local Area Network	A short-haul data communications systems that connects AIS devices in a building or group of buildings within a few square miles, including (but not limited to) workstations, front end processors, controllers, switches, and gateways.
Major Application [OMB Circular A-130, Appendix III]	An application that requires special attention to security due to the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application.
Major Information System [FISMA]	An information system that requires special management attention because of its importance to an agency mission; its high development, operating, or maintenance costs; or its significant role in the administration of agency programs, finances, property, or other resources.
Management Controls	Security methods that focus on the management of the computer security system and the management of risk for a system.

Management Controls [NIST SP 800-18]	The security controls (i.e., safeguards or countermeasures) for an information system that focus on the management of risk and the management of information system security.
Minor Application	An application, other than a major application, that requires attention to security due to the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application. Minor applications are typically included as part of a general support system.
Modem	An electronic device that allows a microcomputer or a computer terminal to be connected to another computer via a telephone line.
National Security Information	Information that has been determined pursuant to Executive Order 12958 as amended by Executive Order 13292, or any predecessor order, or by the Atomic Energy Act of 1954, as amended, to require protection against unauthorized disclosure and is marked to indicate its classified status.
National Security System [44 U.S.C., Sec. 3542]	Any information system (including any telecommunications system) used or operated by an agency or by a contractor of an agency, or other organization on behalf of an agency— (i) the function, operation, or use of which involves intelligence activities; involves cryptologic activities related to national security; involves command and control of military forces; involves equipment that is an integral part of a weapon or weapons system; or is critical to the direct fulfillment of military or intelligence missions (excluding a system that is to be used for routine administrative and business applications, for example, payroll, finance, logistics, and personnel management applications); or, (ii) is protected at all times by procedures established for information that have been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept classified in the interest of national defense or foreign policy.
Network	Two or more systems connected by a communications medium; a network is composed of a communications medium and all components attached to that medium whose responsibility is the transference of information.

Non-repudiation [CNSS Inst. 4009]	Assurance that the sender of information is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so neither can later deny having processed the information.
Operating System	The most important program that runs on a computer. Every general-purpose computer must have an operating system to run other programs. Operating systems perform basic tasks, such as recognizing input from the keyboard, sending output to the display screen, keeping track of files and directories on the disk, and controlling peripheral devices such as disk drives and printers.
Operational Controls	Security methods that focus on mechanisms that primarily are implemented and executed by people (as opposed to systems).
Operational Controls [NIST SP 800-18]	The security controls (i.e., safeguards or countermeasures) for an information system that primarily are implemented and executed by people (as opposed to systems).
Parity	The quality of being either odd or even. The fact that all numbers have a parity is commonly used in data communication to ensure the validity of data. This is called parity checking.
Password	Protected/private character string used to authenticate an identity or to authorize access to data.
PBX	Short for private branch exchange, a private telephone network used within an enterprise. Users of the PBX share a certain number of outside lines for making telephone calls external to the PBX.
Peripheral Device	Any external device attached to a computer. Examples of peripherals include printers, disk drives, display monitors, keyboards, and mice.
PFSS	Patient Financial Services System
Plan of Action and Milestones [OMB Memorandum 02-01]	A document that identifies tasks needing to be accomplished. It details resources required to accomplish the elements of the plan, any milestones in meeting the tasks, and scheduled completion dates for the milestones.

Port	An interface on a computer to which you can connect a device.
Port Protection Device	A device that authorizes access to the port itself, often based on a separate authentication independent of the computer's own access control functions.
Potential Impact [FIPS 199]	Low: The loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals. Moderate: The loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals. High: The loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.
RADIUS	Short for Remote Authentication Dial-In User Service, an authentication and accounting system used by many Internet Service Providers (ISPs). When you dial in to the ISP you must enter your username and password. This information is passed to a RADIUM server, which checks that the information is correct, and then authorizes access to the ISP system.
Real Time	Occurring immediately. Real time can refer to events simulated by a computer at the same speed that they would occur in real life.
Remote Access	The hookup of a remote computing device via communication lines such as ordinary phone lines or wide area networks to access network applications and information.
Risk [NIST SP 800-30]	The level of impact on agency operations (including mission, functions, image, or reputation), agency assets, or individuals resulting from the operation of an information system given the potential impact of a threat and the likelihood of that threat occurring.

Risk Assessment [NIST SP 800-30]	The process of identifying risks to agency operations (including mission, functions, image, or reputation), agency assets, or individuals by determining the probability of occurrence, the resulting impact, and additional security controls that would mitigate this impact. Part of risk management, synonymous with risk analysis, and incorporates threat and vulnerability analyses.
Risk Management [NIST SP 800-30]	The process of managing risks to agency operations (including mission, functions, image, or reputation), agency assets, or individuals resulting from the operation of an information system. It includes risk assessment; cost-benefit analysis; the selection, implementation, and assessment of security controls; and the formal authorization to operate the system. The process considers effectiveness, efficiency, and constraints due to laws, directives, policies, or regulations.
Router	An interconnection device that is similar to a bridge but serves packets or frames containing certain protocols. Routers link LANs at the network layer.
Safeguards [CNSS Inst. 4009, Adapted]	Protective measures prescribed to meet the security requirements (i.e., confidentiality, integrity, and availability) specified for an information system. Safeguards may include security features, management constraints, personnel security, and security of physical structures, areas, and devices. Synonymous with security controls and countermeasures.
Security Accreditation	See Accreditation.
Security Authorization	See Accreditation.
Security Category [FIPS 199]	The characterization of information or an information system based on an assessment of the potential impact that a loss of confidentiality, integrity, or availability of such information or information system would have on organizational operations, organizational assets, or individuals.

Security Controls [FIPS 199]	The management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information.
Security Impact Analysis	The analysis conducted by an agency official, often during the continuous monitoring phase of the security certification and accreditation process, to determine the extent to which changes to the information system have affected the security posture of the system.
Security Incident	An adverse event in a computer system or the threat of such an event occurring.
Security Objective	Confidentiality, integrity, or availability.
Security Plan	See System Security Plan.
Security Requirements [CNSS Inst. 4009, Adapted]	Types and levels of protection necessary for equipment, data, information, applications, and facilities to meet laws, Executive Orders, directives, policies, or regulations.
Senior Agency Information Security Officer	Official responsible for carrying out the Chief Information Officer responsibilities under FISMA and serving as the Chief Information Officer's primary liaison to the agency's authorizing officials, information system owner s, and information system security officers.
Separation of Duties	A process that divides roles and responsibilities so that a single individual cannot subvert a critical process.
Server	The control computer on a local area network that controls software access to workstations, printers, and other parts of the network.
Smart Card	A credit-card-sized device with embedded microelectronics circuitry for storing information about an individual. This is not a key or token, as used in the remote access authentication process.
Software	Computer instructions or data. Anything that can be stored electronically is software.
Software Copyright	The right of the copyright owner to prohibit copying and/or issue permission for a customer to employ a particular computer program.

SPAM	To crash a program by overrunning a fixed-site buffer with excessively large input data. Also, to cause a person or newsgroup to be flooded with irrelevant or inappropriate messages.
Subsystem	A major subdivision or component of an information system consisting of information, information technology, and personnel that performs one or more specific functions.
System	See Information System.
System Security Plan [NIST SP 800-18]	Formal document that provides an overview of the security requirements for the information system and describes the security controls in place or planned for meeting those requirements.
System-specific Security Control	A security control for an information system that has not been designated as a common security control.
TCP/IP	Transmission Control Protocol/Internet Protocol. The suite of protocols the Internet is based on.
Technical Controls	Security methods consisting of hardware and software controls used to provide automated protection to the system or applications. Technical controls operate within the operating system and applications.
Technical Controls [NIST SP 800-18, Adapted]	The security controls (i.e., safeguards or countermeasures) for an information system that are primarily implemented and executed by the information system through mechanisms contained in the hardware, software, or firmware components of the system.
Technical Security Policy	Specific protection conditions and/or protection philosophy that express the boundaries and responsibilities of the AIS product in supporting the information protection policy control objectives and countering expected threats.
Telecommunications	Any transmission, emission, or reception of signals, writing, images, sound or other data by cable, telephone lines, radio, visual or any electromagnetic system.

Threat [CNSS Inst. 4009, Adapted]	Any circumstance or event with the potential to adversely impact agency operations (including mission, functions, image, or reputation), agency assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.
Threat Agent	See Threat Source.
Threat Assessment [CNSS Inst. 4009]	Formal description and evaluation of threat to an information system.
Threat Source [NIST SP 800-30]	Either: (i) intent and method targeted at the intentional exploitation of a vulnerability; or (ii) a situation and method that may accidentally trigger a vulnerability. Synonymous with threat agent.
Trojan Horse	Any program designed to do things that the user of the program did not intend to do or that disguises its harmful intent. A program that installs itself while the user is making an authorized entry; and, then are used to break-in and exploit the system.
User	Any person who is granted access privileges to a given AIS.
User Interface	The part of an application that the user works with. User interfaces can be text-driven, such as DOS, or graphical, such as Windows.
User Representative	An individual that represents the operational interests of the user community and serves as the liaison for that community throughout the system development life cycle of the information system.
Virus	A self-propagating Trojan horse (a program that surreptitiously exploits the security/integrity of a program), composed of a mission component, a trigger component, and a self-propagating component.
Vulnerability	A weakness in automated system security procedures, technical controls, environmental controls, administrative controls, internal controls, etc., that could be used as a threat to gain unauthorized access to information or disrupt critical processing.

Vulnerability [CNSS Inst. 4009, Adapted]	Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.
Vulnerability Assessment [CNSS Inst. 4009]	Formal description and evaluation of the vulnerabilities in an information system.
Wide Area Network	A physical or logical network that provides capabilities for a number of independent devices to communicate with each other over a common transmission-interconnected topology in geographic areas larger than those served by local area networks.

Appendix D: SCG Secure Cloud System Rules of Behavior

NIH IT RULES OF BEHAVIOR

I understand, accept, and agree to the following terms and conditions that apply to my access to, and use of, information, including sensitive information, or information systems of the National Institutes of Health (NIH).

1. GENERAL RULES OF BEHAVIOR

a. I understand that when I use any Government information system, I have NO expectation of Privacy in NIH records that I create or in my activities while accessing or using such information system.

b. I understand that authorized NIH personnel may review my conduct or actions concerning NIH information and information systems, and take appropriate action. Authorized NIH personnel include my supervisory chain of command as well as NIH system administrators and Information Security Officers (ISOs). Appropriate action may include monitoring, recording, copying, inspecting, restricting access, blocking, tracking, and disclosing information to authorized Office of Inspector General (OIG), NIH, and law enforcement personnel.

c. I understand that the following actions are prohibited: unauthorized access, unauthorized uploading, unauthorized downloading, unauthorized changing, unauthorized circumventing, or unauthorized deleting information on NIH systems, modifying NIH systems, unauthorized denying or granting access to NIH systems, using NIH resources for unauthorized use on NIH systems, or otherwise misusing NIH systems or resources. I also understand that attempting to engage in any of these unauthorized actions is also prohibited.

d. I understand that such unauthorized attempts or acts may result in disciplinary or other adverse action, as well as criminal, civil, and/or administrative penalties. Depending on the severity of the violation, disciplinary or adverse action consequences may include: suspension of access privileges, reprimand, suspension from work, demotion, or removal. Theft, conversion, or unauthorized disposal or destruction of Federal property or information may also result in criminal sanctions.

e. I understand that I have a responsibility to report suspected or identified information security incidents (security and privacy) to my Operating Unit's Information Security Officer (ISO), Privacy Officer (PO), and my supervisor as appropriate.

f. I understand that I have a duty to report information about actual or possible criminal violations involving NIH programs, operations, facilities, contracts or information systems to my supervisor, any management official or directly to the OIG, including reporting to the OIG Hotline. I also understand that I have a duty to immediately report

to the OIG any possible criminal matters involving felonies, including crimes involving information systems.

g. I understand that the NIH National Rules of Behavior do not and should not be relied upon to create any other right or benefit, substantive or procedural, enforceable by law, by a party to litigation with the United States Government.
h. I understand that the NIH National Rules of Behavior do not supersede any local policies that provide higher levels of protection to NIH's information or information systems. The NIH National Rules of Behavior provide the minimal rules with which individual users must comply.

i. **I understand that if I refuse to sign this NIH National Rules of Behavior as required by NIH policy, I will be denied access to NIH information and information systems. Any refusal to sign the NIH National Rules of Behavior may have an adverse impact on my employment with the Department.**

2. SPECIFIC RULES OF BEHAVIOR

a. I will follow established procedures for requesting access to any NIH computer system and for notification to the NIH OPDIV and the ISO when the access is no longer needed.

b. I will follow established NIH information security and privacy policies and procedures.

c. I will use only devices, systems, software, and data, which I am authorized to use, including complying with any software licensing or copyright restrictions. This includes downloads of software offered as free trials, shareware or public domain.

d. I will only use my access for authorized and official duties, and to only access data that is needed in the fulfillment of my duties except as provided for in NIH security documents. I also agree that I will not engage in any activities prohibited as stated in section 1c.

e. I will secure NIH sensitive information **in all areas** (at work and remotely) and in any form (e.g., digital, paper etc.), to include mobile media and devices that contain sensitive information, and I will follow the mandate that all NIH sensitive information must be in a protected environment at all times or it must be encrypted (using FIPS 140-2 approved encryption). If clarification is needed whether or not an environment is adequately protected, I will follow the guidance of the local NIH OPDIV.

f. I will properly dispose of NIH sensitive information, either in hardcopy, softcopy or electronic format, in accordance with NIH policy and procedures.

g. I will not attempt to override, circumvent or disable operational, technical, or management security controls unless expressly directed to do so in writing by authorized NIH staff.

h. I will not attempt to alter the security configuration of government equipment unless authorized. This includes operational, technical, or management security controls.

i. I will protect my verify codes and passwords from unauthorized use and disclosure and ensure I utilize only passwords that meet the NIH minimum requirements for the systems that I am authorized to use and are contained in NIH security documents.

j. I will not store any passwords/verify codes in any type of script file or cache on NIH systems.

k. I will ensure that I log off or lock any computer or console before walking away and will not allow another user to access that computer or console while I am logged on to it.

l. I will not misrepresent, obscure, suppress, or replace a user's identity on the Internet or any NIH electronic communication system.

m. I will not auto-forward e-mail messages to addresses outside the NIH network.

n. I will comply with any directions from my supervisors, NIH system administrators and information security officers concerning my access to, and use of, NIH information and information systems or matters covered by these Rules.

o. I will ensure that any devices that I use to transmit, access, and store NIH sensitive information outside of a NIH protected environment will use FIPS 140-2 approved encryption (the translation of data into a form that is unintelligible without a deciphering mechanism). This includes laptops, thumb drives, and other removable storage devices and storage media (CDs, DVDs, etc.).

p. I will obtain the approval of appropriate management officials before releasing NIH information for public dissemination.

q. I will not host, set up, administer, or operate any type of Internet server on any NIH network or attempt to connect any personal equipment to a NIH network unless explicitly authorized **in writing** by my local CIO and I will ensure that all such activity is in compliance with Federal and NIH policies.

r. I will not attempt to probe computer systems to exploit system controls or access NIH sensitive data for any reason other than in the performance of official duties. Authorized penetration testing must be approved in writing by the NIH CIO.

s. I will protect Government property from theft, loss, destruction, or misuse. I will follow NIH policies and procedures for handling Federal Government IT equipment and will sign for items provided to me for my exclusive use and return them when no longer required for NIH activities.

t. I will only use virus protection software, anti-spyware, and firewall/intrusion detection software authorized by the NIH on NIH equipment or on computer systems that are connected to any NIH network.

u. If authorized, by waiver, to use my own personal equipment, I must use NIH approved virus protection software, anti-spyware, and firewall/intrusion detection software and ensure the software is configured to meet NIH configuration requirements. My local CIO will confirm that the system meets NIH configuration requirements prior to connection to NIH's network.

v. I will never swap or surrender NIH hard drives or other storage devices to anyone other than an authorized OI&T employee at the time of system problems.

w. I will not disable or degrade software programs used by the NIH that install security software updates to NIH computer equipment, to computer equipment used to connect to NIH information systems, or to create, store or use NIH information.

x. I agree to allow examination by authorized OI&T personnel of any personal IT device [Other Equipment (OE)] that I have been granted permission to use, whether remotely or in any setting to access NIH information or information systems or to create, store or use NIH information.

y. I agree to have all equipment scanned by the appropriate facility IT Operations Service prior to connecting to the NIH network if the equipment has not been connected to the NIH network for a period of more than three weeks.

z. I will complete mandatory periodic security and privacy awareness training within designated timeframes, and complete any additional required training for the particular systems to which I require access.

aa. I understand that if I must sign a non-NIH entity's Rules of Behavior to obtain access to information or information systems controlled by that non-NIH entity, I still must comply with my responsibilities under the NIH National Rules of Behavior when accessing or using NIH information or information systems. However, those Rules of Behavior apply to my access to or use of the non-NIH entity's information and information systems as a NIH user.

bb. I understand that remote access is allowed from other Federal government computers and systems to NIH information systems, subject to the terms of NIH and the host Federal agency's policies.

cc. I agree that I will directly connect to the NIH network whenever possible. If a direct connection to the NIH network is not possible, then I will use NIH-approved remote access software and services. I must use NIH-provided IT equipment for remote access when possible. I may be permitted to use non–NIH IT equipment [Other Equipment (OE)] only if a NIH-CIO-approved waiver has been issued and the equipment is configured to follow all NIH security policies and requirements. I agree that NIH officials may examine such devices, including an OE device operating under an approved waiver, at any time for proper configuration and unauthorized storage of NIH sensitive information.

dd. I agree that I will not have both a NIH network connection and any kind of non-NIH network connection (including a modem or phone line or wireless network card, etc.) physically connected to any computer at the same time unless the dual connection is explicitly authorized in writing by my local CIO.

ee. I agree that I will not allow NIH sensitive information to reside on non-NIH systems or devices unless specifically designated and approved in advance by the appropriate NIH official (supervisor), and a waiver has been issued by the NIH's CIO. I agree that I will not access, transmit or store remotely any NIH sensitive information that is not encrypted using NIH approved encryption.

ff. I will obtain my NIH supervisor's authorization, in writing, prior to transporting, transmitting, accessing, and using NIH sensitive information outside of NIH's protected environment.

gg. I will ensure that NIH sensitive information, in any format, and devices, systems and/or software that contain such information or that I use to access NIH sensitive information or information systems are adequately secured in remote locations, e.g., at home and during travel, and agree to periodic NIH inspections of the devices, systems or software from which I conduct access from remote locations. I agree that if I work from a remote location pursuant to an approved telework agreement with NIH sensitive information that authorized OI&T personnel may periodically inspect the remote location for compliance with required security requirements.

hh. I will protect sensitive information from unauthorized disclosure, use, modification, or destruction, including using encryption products approved and provided by the NIH to protect sensitive data.

ii. I will not store or transport any NIH sensitive information on any portable storage media or device unless it is encrypted using NIH approved encryption.

jj. I will use NIH-provided encryption to encrypt any e-mail, including attachments to the e-mail that contains NIH sensitive information before sending the e-mail. I will not send any e-mail that contains NIH sensitive information in an unencrypted form. NIH

sensitive information includes personally identifiable information and protected health information.

kk. I may be required to acknowledge or sign additional specific or unique rules of behavior in order to access or use specific NIH systems. I understand that those specific rules of behavior may include, but are not limited to, restrictions or prohibitions on limited personal use, special requirements for access or use of the data in that system, special requirements for the devices used to access that specific system, or special restrictions on interconnections between that system and other IT resources or systems.

ACKNOWLEDGEMENT AND ACCEPTANCE

a. I acknowledge that I have received a copy of these Rules of Behavior.

b. I understand, accept, and agree to comply with all terms and conditions of these Rules of Behavior.

_____	_____
[Print or type your full name]	Signature
_____	
Date	
_____	_____
Office Phone	Position Title

Appendix E: Information System Media

As required by the Media Protection (MP) control family, organizations must physically control and restrict access to information system media. The term “information system media” includes, but is not limited to, the types and examples listed in the table below. Applicable restrictions are listed in the far-right columns, depending on the FIPS 199 security classification of the system that uses the media.

Media Type	Examples	Restrictions		
		Low	Moderate	High
Hard Copy Storage	• Paper • Microforms	--	Depends on sensitivity and whether PII is present.	
Mobile Devices	• Laptops • Cell phones and smart phones (e.g., iPhone, Android, BlackBerry) • E-readers (e.g., Kindle) • Tablets (e.g., iPad)	Government-furnished devices must be encrypted, with waivers being required for any exceptions. Personally-owned devices must adhere to OpDiv-defined policies. All devices must implement OpDiv-defined identification and authentication controls.		
Equipment	• Photocopiers • Printers • Fax machines • Multifunction machines	--	If it contains a storage device, media disposal and sanitization rules apply. Consult SP 800-88 for more information.	
Legacy Magnetic Media	• Magnetic tapes (e.g., backup tapes) • ATA and SCSI hard drives • Floppy disks • ZIP drives	--	Not allowed unless they can be stored in OpDiv-defined controlled environments.	
Peripherally Attached Storage	• Removable hard drives • Locally attached hard drives (attached via USB, Firewire, etc.)	Personally-owned devices in this category are prohibited.		
Optical Media	• Compact Discs (CDs) • Digital Video Discs (DVDs) • Blu-ray	--	All discs must be encrypted.	
Flash-Based Storage Devices	• USB removable media (e.g., thumb drives, memory sticks) • Memory cards (e.g., SD, SDHC, MMC, Compact Flash) • ATA Solid State Drives (SSDs) • SCSI Solid State Drives (SSDs) • PCI Express Devices • Embedded Flash on Boards and Devices	Personally-owned devices in this category are prohibited.		
RAM and ROM-Based Storage Devices	• Dynamic Random Access Memory (DRAM) • Electronically Alterable PROM (EAPROM) • Electronically Erasable PROM (EEPROM)	Personally-owned devices in this category are prohibited.		

Appendix F: Risk Assessment

SCG Secure Cloud System Risk Assessm

Appendix G: Configuration Management Plan

SCGSC Configuration Mana

Appendix H: Contingency Plan

SCGSC Contingency Plan_v1.4.pdf

Appendix I: Incident Response Plan

SCGSC Incident Response Plan v1.3.

Appendix J: Privacy Impact Assessment

NIDDK Catalog - HHS IT System PIA A

Appendix K: Security Controls to Related References/ Publications/Directives

CONTROLS NUMBER	CONTROL NAME	RELATED NIST PUBLICATIONS	RELATED FISMA/HIPAA/ GUIDANCE
AC-1	Access Control Policy and Procedures	FIPS 200, 201-1; NIST Special Publications 800-12, 800-14, 800-19, 800-36, 800-41, 800-44, 800-45, 800-46, 800-66, 800-100	*HIPAA 164.306* *FISMA 12.0* *Memo*, August 2, 2006, National Deployment of the PIV Process
AC-11	Session Lock	No references available.	*HIPAA 164.312a1* *HIPAA 164.312a2* *HIPAA 164.312d* *FISMA 15.1.1* *FISMA 15.2.2*
AC-12	Session Lock	No references available.	*HIPAA 164.312a1* *HIPAA 164.312a2* *HIPAA 164.312d* *FISMA 15.1.1* *FISMA 15.2.2*
AC-14	Permitted Actions without Identification or Authentication	No references available.	
AC-17	Remote Access	FIPS 201-1; NIST Special Publications 800-24, 800-44, 800-45, 800-46, 800-58, 800-68, 800-73, 800-76. 800-77, 800-78, 800-87, 800-96	*HIPAA 164.308a4iiB HIPAA 164.308a4iiC HIPAA 164.312e FISMA 6.2.4* *FISMA 8.2* *FISMA 15.1* *FISMA 16.1* Memo, Aug 2, 2006, *National Deployment of the PIV Process*
AC-18	Wireless Access	NIST Special Publications 800-46, 800-48, 800-58, 800-97	*HIPAA 164.308a4iiB* *HIPAA 164.308a4iiC HIPAA 164.312e FISMA 6.2.4* *FISMA 8.2* *FISMA 15.1* *FISMA 16.1*
AC-19	Access Control for Mobile Devices	No references available.	*FISMA 7.3*
AC-2	Account Management	NIST Special Publications 800-12, 800-43, 800-66	*HIPAA 164.308a4iiB, HIPAA 164.308a4iiC HIPAA 164.312b* *HIPAA 164.312e* *FISMA 6.2.4* *FISMA 8.2*

CONTROLS NUMBER	CONTROL NAME	RELATED NIST PUBLICATIONS	RELATED FISMA/HIPAA/ GUIDANCE
			FISMA 15.1 *FISMA 16.1* *FISMA 17.1.1*
AC-20	Use of External Information Systems	NIST Special Publications 800-46, 800-77	
AC-22	Publicly Accessible Content	No references available.	
AC-3	Access Enforcement	FIPS 201-1; NIST Special Publications 800-12, 800-19, 800-66, 800-68, 800-73, 800-76, 800-78, 800-87, 800-95, 800-96, 800-98	*HIPAA 164.308a4iiB HIPAA 164.308a4iiC HIPAA 164.312e* *FISMA 6.2.4* *FISMA 8.2* *FISMA 15.1* *FISMA 16.1*
AC-4	Information Flow Enforcement	NIST Special Publications 800-41, 800-77, 800-82	*38 USC 7332,* *HIPAA 164.308a4iiB HIPAA 164.308a4iiC* *HIPAA 164.312e FISMA 6.2.4* *FISMA 8.2* *FISMA 15.1* *FISMA 16.1*
AC-5	Separation of Duties	NIST Special Publication 800-66, 800-98	*HIPAA 164.308a3ii HIPAAii HIPAA 164.308a3iiA HIPAA 164.308a4ii HIPAA 164.308a4iiB HIPAA 164.308a4iiC HIPAA 164.312e,* *FISMA 6.1.1* *FISMA 6.2.4* *FISMA 8.2* *FISMA 15.1* *FISMA 16.1*
AC-6	Least Privilege	NIST Special Publications 800-12, 800-19, 800-28 800-66, 800-68, 800-69, 800-81, 800-83	
AC-7	Unsuccessful Login Attempts	NIST Special Publication 800-68	*HIPAA 164.312a1* *HIPAA 164.312a2* *HIPAA 164.312d* *FISMA 15.1.1* *FISMA 15.2.2*
AC-8	System Use Notification	No references available.	*Public Law 99-474* *HIPAA 164.310b*
AT-1	Security Awareness and Training Policy and Procedures	FIPS 200; NIST Special Publications 800-12, 800-14, 800-50, 800-66, 800-100	*HIPAA 164.306* *FISMA 12.0*

CONTROLS NUMBER	CONTROL NAME	RELATED NIST PUBLICATIONS	RELATED FISMA/HIPAA/ GUIDANCE
AT-2	Security Awareness Training	NIST Special Publications 800-50, 800-66	*Computer Security Act of 1987 HIPAA 164.308a5 FISMA 13.0 C.F.R. Part 5 Subpart C (5 C.F.R 930.301) Executive Order 13587*
AT-3	Role-Based Security Training	NIST Special Publications 800-16, 800-40, 800-50, 800-66	*Computer Security Act of 1987 HIPAA 164.308a5 FISMA 13.0*
AT-4	Security Training Records	NIST Special Publications 800-50	*HIPAA 164.308a5 FISMA 13.0*
AU-1	Audit and Accountability Policy and Procedures	FIPS 200; NIST Special Publications 800-12, 800-14, 800-44, 800-57, 800-66, 800-72, 800-92, 800-100	*HIPAA 164.306, FISMA 12.0*
AU-11	Audit Record Retention	NIST Special Publication 800-92	
AU-12	Audit Generation	No references available.	
AU-2	Audit Events	NIST Special Publications 800-12, 800-44, 800-45, 800-66, 800-68, 800-72, 800-83, 800-92, 800-94	*HIPAA 164.312b FISMA 17.1.1*
AU-3	Content of Audit Records	NIST Special Publications 800-12, 800-19, 800-92, 800-94	*HIPAA 164.312b FISMA 17.1.1*
AU-4	Audit Storage Capacity	NIST Special Publications 800-68, 800-92	*HIPAA 164.312b FISMA 17.1.1*
AU-5	Response to Audit Processing Failures	NIST Special Publications 800-83, 800-92	*HIPAA 164.312b FISMA 17.1.1*
AU-6	Audit Review, Analysis, and Reporting	NIST Special Publications 800-12, 800-42, 800-44, 800-45, 800-83, 800-92, 800-94	*HIPAA 164.312b FISMA 17.1.1*
AU-7	Audit Reduction and Report Generation	NIST Special Publications 800-12, 800-44, 800-92	*HIPAA 164.312b FISMA 17.1.1*
AU-8	Time Stamps	NIST Special Publications 800-92, 800-94	
AU-9	Protection of Audit Information	NIST Special Publications 800-12, 800-19, 800-45, 800-72, 800-92, 800-94	*HIPAA 164.312b FISMA 17.1.1*
CA-1	Security Assessment and Authorization	FIPS 200; NIST Special Publications 800-12, 800-14, 800-23, 800-37, 800-53A, 800-66, 800-79, 800-100	*OMB Circular A-130 HIPAA 164.306 FISMA 12.0*

CONTROLS NUMBER	CONTROL NAME	RELATED NIST PUBLICATIONS	RELATED FISMA/HIPAA/ GUIDANCE
	Policies and Procedures		
CA-2	Security Assessments	NIST Special Publications 800-17, 800-20, 800-22, 800-23, 800-35, 800-36, 800-37, 800-53A, 800-55, 800-66, 800-76, 800-79	
CA-3	System Interconnections	NIST Special Publications 800-18, 800-47, 800-66	*OMB Circular A-130 Appendix III* *HIPAA 162.308a8, HIPAA 64.308a8b1, FISMA 3.2* *FISMA 3.2.9* *FISMA 4. 0* *FISMA 12.2.3* *FISMA 12.2.5*
CA-5	Plan of Action and Milestones	NIST Special Publications 800-18, 800-30, 800-37, 800-65	*HIPAA 162.308a8* *FISMA 3.2* *FISMA 4. 0* *FISMA 12.2.5*
CA-6	Security Authorization	NIST Special Publications 800-37, 800-66, 800-79	
CA-7	Continuous Monitoring	NIST Special Publications 800-37, 800-42, 800-53A, 800-79 800-85A, 800-85B	*HIPAA 162.308a8, FISMA 3.2* *FISMA 4. 0* *FISMA 12.2.5*
CA-9	Internal Systems Connections		
CM-1	Configuration Management Policy and Procedures	FIPS 200; NIST Special Publications 800-12, 800-14, 800-37, 800-100	*HIPAA 164.306* *FISMA 12.0*
CM-10	Software Usage Restrictions	No references available	
CM-11	User Installed Software	No references available	
CM-2	Baseline Configuration	NIST Special Publications 800-35, 800-40, 800-82	*FISMA 3.1.4* *FISMA 10.0*
CM-3	Configuration Change Control	No references available.	*FISMA 3.1.4* *FISMA 10.0*
CM-4	Security Impact Analysis	NIST Special Publication 800-83	*FISMA 3.1.4* *FISMA 10.0*
CM-5	Access Restrictions for Change	No references available.	*HIPAA 164.312c1* *HIPAA 164.312c2* *FISMA 3.1.4* *FISMA 10.0*
CM-6	Configuration Settings	NIST Special Publications 800-40, 800-43, 800-44, 800-45, 800-46, 800-48, 800-54, 800-68, 800-70, 800-81, 800-82, 800-83	*FISMA 3.1.4* *FISMA 10.0*

CONTROLS NUMBER	CONTROL NAME	RELATED NIST PUBLICATIONS	RELATED FISMA/HIPAA/ GUIDANCE
CM-7	Least Functionality	NIST Special Publications 800-81, 800-83	*FISMA 3.1.4* *FISMA 10.0*
CM-8	Information System Component Inventory	NIST Special Publications 800-35, 800-40	*FISMA 3.1.4* *FISMA 10.0*
CM-9	Configuration Management Plan	NIST Special Publications 800-128	
CP-1	Contingency Planning Policy and Procedures	FIPS 200; NIST Special Publications 800-12, 800-14, 800-34, 800-66, 800-84, 800-100	*HIPAA 164.308a7i* *HIPAA 164.308a7iiC FISMA 9.0* *FISMA 12.1.8*
CP-10	Information System Recovery and Reconstitution	NIST Special Publications 800-21, 800-24, 800-34, 800-43, 800-44, 800-57, 800-81, 800-83, 800-98	*HIPAA 164.308a7i* *FISMA 9.0* *FISMA 12.1.8*
CP-2	Contingency Plan	NIST Special Publications 800-12, 800-14, 800-34, 800-66	*HIPAA 164.308a7i* *HIPAA 164.308a7iiC FISMA 9.0* *FISMA 12.1.8*
CP-3	Contingency Training	NIST Special Publications 800-34, 800-50, 800-84	*HIPAA 164.308a7i* *FISMA 9.0* *FISMA 12.1.8*
CP-4	Contingency Plan Testing	NIST Special Publications 800-12, 800-34, 800-56, 800-66, 800-84	*HIPAA 164.308a7i* *HIPAA 164.308a7iiD, FISMA 9.0,* *FISMA 12.1.8*
CP-6	Alternate Storage Site	NIST Special Publication 800-34	*HIPAA 164.308a7i* *FISMA 9.0* *FISMA 12.1.8*
CP-7	Alternate Processing Site	NIST Special Publication 800-34	*HIPAA 164.308a7i* *FISMA 9.0* *FISMA 12.1.8*
CP-8	Telecommunications Services	NIST Special Publications 800-13, 800-34	*HIPAA 164.308a7i* *FISMA 9.0* *FISMA 12.1.8*
CP-9	Information System Backup	NIST Special Publications 800-21, 800-25, 800-34, 800-41, 800-43, 800-44, 800-45, 800-57, 800-69	*HIPAA 164.308a7i* *FISMA 9.0* *FISMA 12.1.8*
IA-1	Identification and Authentication Policy and Procedures	FIPS 190, FIPS 200, FIPS 201-1; NIST Special Publications 800-12, 800-14, 800-25, 800-36, 800-44, 800-45, 800-46, 800-63, 800-73, 800-76, 800-87, 800-100	*HIPAA 164.306* *FISMA 12.0*
IA-2	Identification and Authentication	FIPS 201-1; NIST Special Publications 800-12, 800-24, 800-44,	*HIPAA 164.312a2i* HIPAA 164.312a5iiD

CONTROLS NUMBER	CONTROL NAME	RELATED NIST PUBLICATIONS	RELATED FISMA/HIPAA/ GUIDANCE
	(Organizational Users)	800-46, 800-68, 800-69, 800-73, 800-76, 800-78, 800-87, 800-96, 800-97	
IA-3	Device Identification and Authentication	NIST Special Publications 800-48, 800-52, 800-72, 800-73, 800-77, 800-81, 800-96, 800-97	
IA-4	Identifier Management	FIPS 201-1; NIST Special Publications 800-66, 800-72, 800-73, 800-78, 800-87, 800-96	
IA-5	Authenticator Management	FIPS 190, 201-1; NIST Special Publications 800-25, 800-32, 800-63, 800-66, 800-68, 800-73, 800-76, 800-77, 800-78, 800-87, 800-96	
IA-6	Authenticator Feedback	NIST Special Publication 800-72	*HIPAA 164.312a1* *HIPAA 164.312a2* *HIPAA 164.312d* *FISMA 15.1.1* *FISMA 15.2.2*
IA-7	Cryptographic Module Authentication	FIPS 140-2; NIST Special Publications 800-73, 800-78, 800-87	
IA-8	Identification and Authentication (Non-Organizational Users)	FIPS Publication 201; NIST Special Publications 800-63, 800-116	OMB Memoranda 04-04, 11-11, 10-06-2011; FICAM Roadmap and Implementation Guidance; National Strategy for Trusted Identities in Cyberspace; Web: idmanagement.gov.
IR-1	Incident Response Policy and Procedures	FIPS 200; NIST Special Publications 800-12, 800-14, 800-61, 800-66, 800-86, 800-83, 800-84, 800-100	*HIPAA 164.308a6ii* *FISMA 14.0*
IR-2	Incident Response Training	NIST Special Publications 800-50, 800-61, 800-84	*HPM 589A4-349* *HIPAA 164.308a6ii* *FISMA 14.0*
IR-3	Incident Response Testing	NIST Special Publication 800-61, 800-84	*HIPAA 164.308a6ii* *FISMA 14.0*
IR-4	Incident Handling	NIST Special Publications 800-36, 800-61, 800-83, 800-86, 800-92, 800-94, 800-101	
IR-5	Incident Monitoring	NIST Special Publication 800-61	*HIPAA 164.308a6ii* *FISMA 14.0*
IR-6	Incident Reporting	NIST Special Publication 800-61	*HIPAA 164.308a6ii* *FISMA 14.0*

CONTROLS NUMBER	CONTROL NAME	RELATED NIST PUBLICATIONS	RELATED FISMA/HIPAA/ GUIDANCE
IR-7	Incident Response Assistance	NIST Special Publication 800-61	
IR-8	Incident Response Plan	NIST Special Publication 800-61	
MA-1	System Maintenance Policy and Procedures	FIPS 200; NIST Special Publications 800-12, 800-14, 800-34, 800-88, 800-100	*FISMA 3.1.4* *FISMA 10.0*
MA-2	Controlled Maintenance	NIST Special Publication 800-24	*FISMA 3.1.4* *FISMA 10.0*
MA-3	Maintenance Tools	No references available.	*FISMA 3.1.4* *FISMA 10.0*
MA-4	Nonlocal Maintenance	NIST Special Publication 800-77	*FISMA 3.1.4* *FISMA 10.0*
MA-5	Maintenance Personnel	No references available.	*FISMA 3.1.4* *FISMA 10.0*
MA-6	Timely Maintenance	No references available.	*FISMA 3.1.4* *FISMA 10.0*
MP-1	Media Protection Policy and Procedures	FIPS 200; NIST Special Publications 800-12, 800-14, 800-66, 800-72, 800-88, 800-100	*HIPAA 164.306* *FISMA 12.0*
MP-2	Media Access	NIST Special Publication 800-72	*HIPAA 164.308a5i164.310c* *HIPAA 164.310a2ii* *FISMA 7.1* *FISMA 7.2.1* *FISMA 8.2* *FISMA 10.1*
MP-3	Media Marking	No references available.	*Appendix E* *HIPAA 164.308a5i164.310c*
MP-4	Media Storage	NIST Special Publications 800-66, 800-88, 800-92	*HIPAA 164.308a7i*
MP-5	Media Transport	NIST Special Publications 800-57, 800-72, 800-92	*HIPAA, Privacy Act,* *HIPAA 164.308a5i164.310c*
MP-6	Media Sanitization	NIST Special Publications 800-24, 800-36, 800-66, 800-88, 800-98	*NARA 36 CPR 1228.58,* *HIPAA 164.310d1* *HIPAA 164.310d2i* *FISMA 8.2.0, 3.2.11 – 3.2.13*
PE-1	Physical and Environmental Protection Policy and Procedures	FIPS 200; NIST Special Publications 800-12, 800-14, 800-66, 800-100	*HIPAA 164.306* *FISMA 12.0*
PE-10	Emergency Shutoff	No references available.	*HIPAA 164.308a7iiC, HIPAA 164.310a2i* *FISMA 7.1.12 – 7.1.19*
PE-11	Emergency Power	NIST Special Publication 800-58	
PE-12	Emergency Lighting	No references available.	

CONTROLS NUMBER	CONTROL NAME	RELATED NIST PUBLICATIONS	RELATED FISMA/HIPAA/ GUIDANCE
PE-13	Fire Protection	NIST Special Publication 800-12	*HIPAA 164.308a7iiC HIPAA 164.310a2i* *FISMA 7.1.12 – 7.1.19*
PE-14	Temperature and Humidity Controls	No references available.	*HIPAA 164.308a7iiC, HIPAA 164.310a2i,* *FISMA 7.1.12 – 7.1.19*
PE-15	Water Damage Protection	No references available.	*HIPAA 164.308a7iiC HIPAA 164.310a2i* *FISMA 7.1.12 – 7.1.19*
PE-16	Delivery and Removal	No references available.	
PE-17	Alternate Work Site	No references available.	
PE-2	Physical Access Authorizations	No references available.	*HIPAA 164.301a2ii* *HIPAA 164.310a2iii HIPAA 64.308a7iiB HIPAA 164.310a1* *HIPAA 164.310a2ii* *FISMA 7.1* *FISMA 7.2.1* *FISMA 8.2* *FISMA 10.1*
PE-3	Physical Access Control	NIST Special Publications 800-12, 800-24, 800-66, 800-73, 800-76, 800-78, 800-82, 800-96, 800-98	*NFPA 75 Standard for the Protection of Information Technology Equipment; Chapter 5; 5.5 Penetrations of Fire-Resistant-Rated Enclosures.* *HIPAA 164.301a2ii* *HIPAA 164.310a2iii HIPAA 164.308a7iiB HIPAA 164.310a1* *HIPAA 164.310a2ii* *FISMA 7.1* *FISMA 7.2.1* *FISMA 8.2* *FISMA 10.1*
PE-4	Access Control for Transmission Medium	NIST Special Publications 800-12, 800-58	*HIPAA 164.308a5i164.310c*
PE-5	Access Control for Output Devices	No references available.	*HIPAA 164.308a5i164.310c*
PE-6	Monitoring Physical Access	No references available.	*HIPAA 164.310a2ii* *FISMA 7.1* *FISMA 7.2.1* *FISMA 8.2* *FISMA 10.1*

CONTROLS NUMBER	CONTROL NAME	RELATED NIST PUBLICATIONS	RELATED FISMA/HIPAA/ GUIDANCE
PE-8	Visitor Access Records	No references available.	*HIPAA 164.310a2ii* *FISMA 7.1* *FISMA 7.2.1* *FISMA 8.2* *FISMA 10.1*
PE-9	Power Equipment and Power Cabling	No references available.	*HIPAA 164.308a7iiC, HIPAA 164.310a2i,* *FISMA 7.1.12 – 7.1.19*
PL-1	Security Planning Policy and Procedures	FIPS 200; NIST Special Publications 800-12, 800-14, 800-18, 800-42, 800-65, 800-66, 800-100	*HIPAA 164.312c* *HIPAA 164.308a5iiD FISMA 5.0* *FISMA 3.2.8* *FISMA 3.2.10* *FISMA 12.2.1*
PL-2	System Security Plan	FIPS 199, 200; NIST Special Publications 800-12, 800-14, 800-18, 800-19, 800-21, 800-25, 800-27, 800-30, 800-32, 800-33, 800-34, 800-37, 800-40, 800-41, 800-44, 800-45, 800-57, 800-58, 800-64, 800-81	*HIPAA 164.312c* *HIPAA 164.308a5iiD FISMA 5.0* *FISMA 3.2.8* *FISMA 3.2.10* *FISMA 12.2.1*
PL-4	Rules of Behavior	NIST Special Publications 800-45, 800-46, 800-48, 800-89	*OMB Circular A-130 Appendix III,* *HIPAA 164.308a3i* *FISMA 4.1.3* *FISMA 13.1.1*
PL-8	Rules of Behavior	No References Available	
PS-1	Personnel Security Policy and Procedures	FIPS 200; NIST Special Publications 800-12, 800-14, 800-66, 800-100	*HIPAA 164.308a3* *FISMA 6.0*
PS-2	Position Risk Designation	NIST Special Publication 800-12	*5 CFR sections 732.102* *HIPAA 164.308a3* *FISMA 6.0*
PS-3	Personnel Screening	NIST Special Publication 800-12	*HIPAA 164.308a3* *HIPAA 164.308a3iiB* *HIPAA 164.314a1* *FISMA 6.0*
PS-4	Personnel Termination	NIST Special Publications 800-12, 800-14, 800-66	
PS-5	Personnel Transfer	NIST Special Publication 800-12	*HIPAA 164.308a3* *HIPAA 64.308a3ii* *FISMA 6.0*
PS-6	Access Agreements	No references available.	
PS-7	Third-Party Personnel Security	No references available.	*HIPAA 164.308a3* *HIPAA 164.314a1* *FISMA 6.0*
PS-8	Personnel Sanctions	NIST Special Publication 800-66	

CONTROLS NUMBER	CONTROL NAME	RELATED NIST PUBLICATIONS	RELATED FISMA/HIPAA/ GUIDANCE
RA-1	Risk Assessment Policy and Procedures	FIPS 200; NIST Special Publications 800-12, 800-14, 800-30, 800-37, 800-66, 800-100	*Appendix D page 7*
RA-2	Security Categorization	FIPS 199; NIST Special Publications 800-30, 800-37, 800-40, 800-59, 800-60, 800-66	*OMB Circular A-130*
RA-3	Risk Assessment	NIST Special Publications 800-12, 800-13, 800-14, 800-19, 800-23, 800-24, 800-25, 800-28, 800-30, 800-32, 800-34, 800-37, 800-40, 800-42, 800-44, 800-45, 800-46, 800-48, 800-53A, 800-54, 800-60, 800-63, 800-65, 800-66, 800-82, 800-94, 800-98	
RA-5	Vulnerability Scanning	NIST Special Publications 800-24, 800-36, 800-37, 800-40, 800-42, 800-44, 800-45, 800-46, 800-51, 800-83, 800-94	*HIPAA 164.308a1i*
SA-1	System and Services Acquisition Policy and Procedures	FIPS 200; NIST Special Publications 800-12, 800-14, 800-35, 800-36, 800-64, 800-65, 800-66, 800-100	*HIPAA 164.306* *FISMA 12.0*
SA-10	Developer Configuration Management	No references available.	
SA-11	Developer Security Testing and Evaluation	NIST Special Publications 800-76, 800-85A, 800-85B	
SA-2	Allocation of Resources	NIST Special Publications 800-35, 800-64, 800-65	*FISMA 3.1.2*
SA-3	System Develop Life Cycle	NIST Special Publications 800-12, 800-14, 800-21, 800-27, 800-30, 800-34, 800-35, 800-64, 800-97, 800-98	
SA-4	Acquisition Process	NIST Special Publications 800-23, 800-36, 800-64, 800-94	
SA-5	Information System Documentation	No references available.	
SA-8	Security Engineering Principles	NIST Special Publications 800-27, 800-33	
SA-9	External Information System Services	NIST Special Publications 800-35, 800-66	
SC-1	System and Communications	FIPS 200; NIST Special Publications 800-12, 800-14, 800-28, 800-100	*HIPAA 164.306* *FISMA 12.0*

CONTROLS NUMBER	CONTROL NAME	RELATED NIST PUBLICATIONS	RELATED FISMA/HIPAA/ GUIDANCE
	Protection Policy and Procedures		
SC-10	Network Disconnect	NIST Special Publication 800-46	
SC-12	Cryptographic Key Establishment and Management	FIPS 140-2; NIST Special Publications 800-12, 800-21, 800-52, 800-56, 800-57, 800-58, 800-73, 800-77, 800-97	
SC-13	Cryptography Protection	FIPS 140-2, 180-2, 186-2, 190, 197 198, 201-1; NIST Special Publications 800-12, 800-17, 800-20, 800-21, 800-22, 800-29, 800-38A, 800-38B, 800-38C, 800-38D, 800-67, 800-78, 800-90	
SC-15	Collaborative Computing Devices	No references available.	
SC-17	Public Key Infrastructure Certificates	FIPS 201; NIST Special Publications 800-15, 800-25, 800-32, 800-36, 800-56, 800-57, 800-89	
SC-18	Mobile Code	NIST Special Publication 800-28	
SC-19	Voice Over Internet Protocol	NIST Special Publication 800-58	*HIPAA 164.308a4iiB HIPAA 164.308a4iiC* *HIPAA 164.312e, FISMA 6.2.4* *FISMA 8.2* *FISMA 15.1* *FISMA 16.1*
SC-2	Application Partitioning	NIST Special Publication 800-19	
SC-20	Secure Name/Address Resolution Service (Authoritative Source)	NIST Special Publications 800-32, 800-81	
SC-21	Secure Name/Address Resolution Service (Recursive or Caching Resolver)	NIST Special Publication 800-81	

CONTROLS NUMBER	CONTROL NAME	RELATED NIST PUBLICATIONS	RELATED FISMA/HIPAA/ GUIDANCE
SC-22	Architecture and Provisioning for Name/Address Resolution Service	NIST Special Publication 800-81	
SC-23	Session Authenticity	NIST Special Publications 800-52, 800-54, 800-77, 800-95	
SC-3	Security Function Isolation	NIST Special Publication 800-81	
SC-4	Information in Shared Resources	No references available.	
SC-5	Denial of Service Protection	NIST Special Publications 800-44, 800-54, 800-68, 800-81, 800-94, 800-95	
SC-7	Boundary Protection	NIST Special Publications 800-28, 800-36, 800-41, 800-44, 800-46, 800-54, 800-58, 800-70, 800-77, 800-82, 800-83	
SC-8	Transmission Integrity	FIPS 198; NIST Special Publications 800-44, 800-45, 800-49, 800-52, 800-57, 800-54, 800-58, 800-66, 800-77, 800-81, 800-95, 800-97	
SI-1	System and Information Integrity Policy and Procedures	FIPS 200; NIST Special Publications 800-12, 800-14, 800-66, 800-94, 800-100	*HIPAA 164.306* *FISMA 12.0*
SI-10	Information Input Validation	NIST Special Publications 800-44, 800-57	
SI-11	Error Handling	No references available.	
SI-12	Information Handling and Retention	No references available.	*FISMA 7.1* *FISMA 7.2.1* *FISMA 8.2* *FISMA 10.1*
SI-16	Memory Protection	No references available.	
SI-2	Flaw Remediation	NIST Special Publications 800-28, 800-40, 800-43, 800-51, 800-83	*HIPAA 164.312c2* *FISMA 11.0*
SI-3	Malicious Code Protection	NIST Special Publications 800-19, 800-36, 800-42, 800-45, 800-69, 800-83, 800-94	*HIPAA 164.312c1* *HIPAA 164.312c2* *FISMA 11.0*

CONTROLS NUMBER	CONTROL NAME	RELATED NIST PUBLICATIONS	RELATED FISMA/HIPAA/ GUIDANCE
SI-4	Information System Monitoring	NIST Special Publications 800-36, 800-40, 800-42, 800-44 800-48, 800-83, 800-92, 800-94	*HIPAA 164.312c1* *HIPAA 164.312c2* *FISMA 11.0*
SI-5	Security Alerts and Advisories	NIST Special Publications 800-40, 800-51, 800-61	*HIPAA 164.312c1* *HIPAA 164.312c2* *FISMA 11.0*
SI-7	Software, Firmware, and Information Integrity	NIST Special Publications 800-19, 800-44, 800-57, 800-66, 800-94	
SI-8	Spam Protection	NIST Special Publication 800-45	