Risk Assessment Report

for the

SCG Secure Cloud System

Version 1.2

June 1, 2016

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

SCG Secure Cloud System Risk Assessment Report

The Risk Assessment Report for the SCG Secure Cloud system must be approved by the SCG President, the Vice President of Administration, the Information Technology Director, and the Program Manager. The undersigned acknowledge that they have reviewed the SCG Secure Cloud System Risk Assessment Report and agree with the information presented in this document. This document will be reviewed annually and any changes to security planning procedure deemed necessary will be coordinated with, and approved by, the undersigned or their designated representatives.

6/1/16

Beverly J. Campbell
President

DATE

Stacy E. Philipson

6/1/16

Stacy E. Philipson
Vice President of Administration

DATE

6/1/16

Chuck C. Lee
Director of Information Technology

DATE

Susie Warner

6/1/16

Susie Warner
Program Manager

DATE

Document Information and Revision History

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

Document Revision and History			
Revision	**Date**	**Author**	**Comments**
0.9	2/20/15	Identity Management Enterprise Architecture, LLC (IMEA)	Initial draft developed; transferred information from outdated template.
1.0	3/18/15	IMEA	Added assessment results.
1.1	3/18/15	Beverly Campbell	Minor revisions throughout document.
1.2	6/1/16	Chuck Lee, Beverly Campbell	Minor revisions throughout document.

Distribution List			
Name	**Title**	**Office**	**Phone No.**
Beverly Campbell	President	SCG Gaithersburg	(301) 670-4990
Chuck Lee	IT Director	SCG Gaithersburg	(301) 670-4990
Stacy Philipson	Vice President of Administration	SCG Gaithersburg	(301) 670-4990
Susie Warner	Program Manager	SCG Gaithersburg	(301) 670-4990

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

Table of Contents

List of Tables

List of Figures

Executive Summary

The National Institute of Diabetes and Digestive and Kidney Diseases (NIDDK) recognizes the best, most up-to-date health information is without value unless it is pertinent and accessible to the people it is meant to serve. SCG has been tasked to conduct a risk assessment of the SCG Secure Cloud system for the purpose of assessment and authorization (A&A) of the SCG Secure Cloud (SCGSC) system under *NIDDK Information Security Program Policy.* This Risk Assessment Report, in conjunction with the System Security Plan, assesses the use of resources and controls to eliminate and/or manage vulnerabilities that are exploitable by threats internal and external to NIDDK. The successful completion of the A&A process results in a formal Authorization to Operate the SCG Secure Cloud system.

The scope of this risk assessment effort was limited to the security controls applicable to the SCG Secure Cloud system's environment relative to its conformance with the minimum *NIDDK Information Technology (IT) Security Program.* These baseline security requirements address security controls in the areas of computer hardware and software, data, operations, administration, management, information, facility, communication, personnel, and contingency.

The SCG Secure Cloud system risk assessment was conducted in accordance with the methodology described in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-30, *Revision 1, Guide for Conducting Risk Assessments.* The methodology used to conduct this risk assessment is qualitative, and no attempt was made to determine any annual loss expectancies, asset cost projections, or cost-effectiveness of security safeguard recommendations.

The risk assessment of the SCG Secure Cloud system identified 314 observations. These controls can be considered as observations in the areas of Management, Operational, and Technical Security. Observations are weaknesses that may be exploited by a threat or group of threats. These observations can be mitigated by following the recommended safeguards. Safeguards are security features and controls that, when added to or included in the information technology environment, mitigate the risk associated with the operation to manageable levels. Forty-one (41) observations were rated **High**, 36 were rated **Medium**, and 237 were rated as **Low**. A list of the observations and recommended safeguards is found in Appendix B: SCGSC Security Scan Results and Appendix C: SCGSC Plan of Action and Milestones of this report.

The overall SCG Secure Cloud system security categorization is rated as **Moderate** in accordance with Federal Information Processing Standards 199 (FIPS 199).

The following risk ratings were used in this assessment:

- **High Risk.** It is likely that exploitation of a given vulnerability by a threat will severely and adversely affect SCGSC tangible and intangible resources, which will impede the overall mission and purpose of SCGSC, or the reputation or interests of SCG, Inc. and the NIDDK. This level of risk indicates a strong need for corrective measures and actions, and a plan must be developed to incorporate these actions within a reasonable period.

- **Medium Risk.** It is likely that exploitation of the identified vulnerability by a threat will moderately affect SCGSC, indicating the loss of some tangible assets or resources, which could impede the overall mission and purpose of SCGSC, or the reputation or interests of the NIDDK. This level of risk indicates that corrective actions are needed, and a plan must be developed to incorporate these actions within a reasonable period.

- **Low Risk.** The identified weaknesses may be subject to exploitation by a threat, but the probability of exploitation is low and the impact would be minor. This level of risk indicates that management should be cautioned and corrective measures applied where required.

Forty-one (41) High, 36 Medium, and 237 Low observations were determined for SCGSC.

1. Introduction

1.1 Purpose

The Risk Assessment Report (RAR) provides the SGC, Inc., management with an assessment of the adequacy of the management, operation, and technical security controls that are currently in place to secure SCGSC. This RAR identifies threats and vulnerabilities applicable to SCGSC. It is based on the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-30, *Revision 1, Guide for Conducting Risk Assessments*. It also evaluates the likelihood that an identified vulnerability can be exploited, assesses the impact associated with these threats and vulnerabilities, and identifies the overall risk level.

This RAR documents the consideration of risks resulting from the incorporation of information systems into the mission and business processes of the SCG, Inc. and the NIDDK.[1] The RAR will help SCG, Inc. management understand the security posture of SCGSC and any residual risks.

1.2 Mission

The mission of the SCG Secure Cloud system is to provide the infrastructure for the best, most up-to-date, pertinent health information and make it accessible to the people it is meant to serve. The SCG Secure Cloud system directly supports the mission of the National Institute of Diabetes and Digestive and Kidney Diseases (NIDDK), which is to conduct and support medical research and research training and to disseminate science-based information on diabetes and other endocrine and metabolic diseases; digestive diseases, nutritional disorders, and obesity; and kidney, urologic, and hematologic diseases, to improve people’s health and quality of life.

NIDDK conducts, supports, and coordinates research on many of the most serious diseases affecting public health. NIDDK cannot provide medical advice for individuals. The information provided using the SCG Secure Cloud system as the information platform is informed by NIDDK research, reviewed by doctors, and provided to help the public and health professionals understand more about the diseases and conditions. The NIDDK is part of the National Institutes of Health (NIH), the medical research agency of the United States.

[1] NIST SP 800-39, Managing Information Security Risk: An Organizational Perspective provides guidelines for managing risk to organizational operations, organizational assets, individuals, other organizations, and the Nation resulting from the operation and use of information systems. NIST SP 800-39 is the flagship document in the series of FISMA-related publications developed by NIST and provides a structured, yet flexible approach for managing that portion of risk resulting from the incorporation of information systems into the mission and business processes of organizations. (See http://csrc.nist.gov/publications/PubsSPs.html.)

1.3 Scope

The scope of this risk assessment included assessment of the system's use of resources and controls (implemented or planned) to eliminate and/or manage vulnerabilities exploitable by threats internal and external to the SCG Secure Cloud system. If exploited, these vulnerabilities could result in:

- Unauthorized disclosure of data.
- Unauthorized modification to the system, its data, or both.
- Denial of service, access to data, or both to authorized users.

This Risk Assessment Report evaluates the **confidentiality** (protection from unauthorized disclosure of system and data information), **integrity** (protection from improper modification of information), and **availability** (loss of system access) of the system. Recommended security safeguards will allow management to make decisions about security-related initiatives.

1.4 Structure

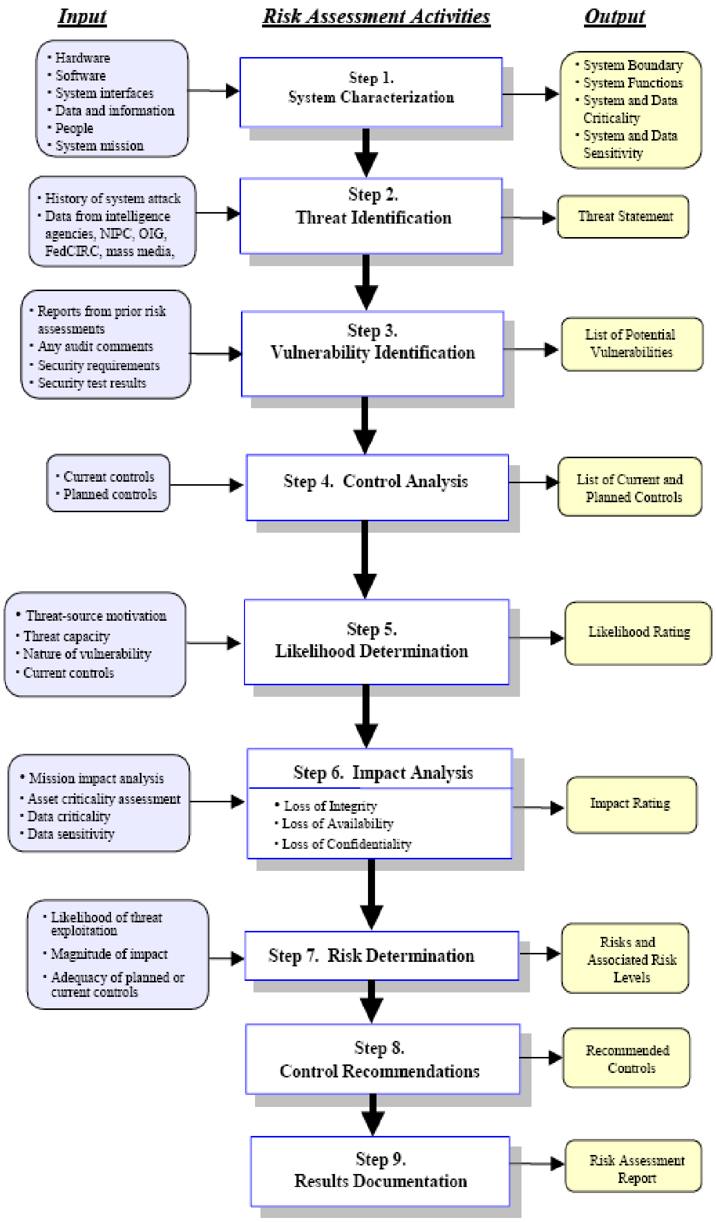
This document is divided into five sections. Section 1 is the introduction. The remainder of the document consists of the following sections:

- Section 2 describes the risk assessment approach used by the independent risk assessment team.
- Section 3 describes the risk assessment methodology used by the independent risk assessment team.
- Section 4 describes the characteristics of SCGSC, including the hardware, software, connectivity, criticality, data, and SCGSC users.
- Section 5 contains the threat statement, including threat categories, threat sources, and threat actions. It also provides an analysis of the observations in the management, operational and technical security domains.

2. Risk Assessment Approach

As **Error! Reference source not found.** shows, the independent risk assessment team’s risk assessment approach involved nine major steps, which are illustrated below.

Figure 1. Risk Assessment Approach



The approach used to perform the risk assessment for the SCGSC system was developed by the independent risk assessment team with reference to the NIST SP 800-30.

The level of risk was assessed by evaluating all collected risk-related attributes regarding threats, vulnerabilities, assets and resources, current controls, and the associated likelihood that a vulnerability could be exploited by a potential threat and the impact (e.g., magnitude of loss resulting from such exploitation).

The assessment is broad in scope and evaluates security vulnerabilities affecting confidentiality, integrity, and availability. The assessment recommends appropriate security safeguards, permitting management to make knowledge-based decisions about security-related initiatives. The methodology addresses the following types of controls:

- Management Controls: Management of the information technology (IT) security system and the management and acceptance of risk.
- Operational Controls: Security methods focusing on mechanisms implemented and executed primarily by people (as opposed to systems), including all aspects of physical security, media safeguards, and inventory controls.
- Technical Controls: Hardware and software controls providing automated protection to the system or applications. (Technical controls operate within the technical system and applications.)

2.1 Determine System Review Boundaries

Determining system boundaries involves determining which system components are included within this specific review. It outlines the limitations and allows the independent risk assessment team to focus on applicable hardware, software, and information data within these boundaries.

2.2 Gather Information

To gather information relevant to the system, the following techniques were used:

- **Questionnaires.** Questionnaires about security controls in place or controls planned for the system were developed. The questionnaires were distributed to appropriate personnel and management staff within the designated agency.
- **On-site Interviews and Observations.** On-site interviews with appropriate technical support and management staff were conducted to gather useful information pertaining to the system. On-site interviews also permitted the independent risk assessment team to observe, assess, and gather security information on management, operational, and technical controls that are currently in place or planned.

- **Document Review.** The independent risk assessment team reviewed client-provided policy, security, and system-related documentation pertaining to the system. The documentation provided information about security controls that are in place or planned for in the future implementation.
- **Use of Automated Scanning Tools.** Although the initial risk assessment did not entail the use of automated scanning tools, future risk assessments could include the use of automated scanning tools, such as a network-mapping tool, to collect information on security controls that are currently in place.
- **Performance of the ST&E or Security Controls Assessment (SCA).** The ST&E or SCA provides for an in-depth degree of system testing that verifies a system's adherence to the security controls as set forth in NIST SP 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*.

2.3 Assess Risk

Following the collection of system characterization information, the process of assessing risk began by determining system-specific threats based on the system operations, configuration, information, and geographical location. The independent risk assessment team determined that a system-specific list of potential threats could exploit identified vulnerabilities of the SCGSC system operational environment. After threats were outlined, system safeguards and vulnerabilities were identified. Once the safeguards and vulnerabilities were identified, the independent risk assessment team determined the likelihood of the specific vulnerabilities being exploited by the system-specific threats. Finally, the impact to the system, and system resources was determined, in the event the vulnerability should be exploited.

2.4 Document Results

Once the threats and vulnerabilities were identified, risks were assessed, and recommended safeguards were established. The independent risk assessment team documented the results in this document. This overall risk assessment report describes the threats and vulnerabilities, measures the risks, and determines the impact of any exploited vulnerabilities. This report is useful to senior management and system owners in understanding the risks and allocating the necessary resources to correct or reduce potential damages.

3. Risk Assessment Methodology

The methodology described below is based on a qualitative approach to assessing risk; thus, no numerical values are calculated, rather a rating of high, medium, or low was assigned based on established definitions, analysis of the system and provided information, and the expertise of the independent risk assessment team. The independent risk assessment team developed the methodology used to perform the risk assessment for SCGSC through use of the guidelines outlined in the NIST SP 800-30, which provides a foundation for an effective risk management program for federal organizations that process sensitive information.

The SCGSC system risk assessment enables management to make informed risk-based business decisions without the use of complex mathematical formulas. The risk assessment methodology involved the steps displayed in **Error! Reference source not found.**.

The level of risk is determined by evaluating the following factors:

- All collected risk-related attributes related to threats, vulnerabilities, assets and resources, and current controls,
- The associated likelihood that a vulnerability could be exploited by a potential threat,
- The impact if a vulnerability was exploited (e.g., magnitude of loss resulting from such exploitation).

3.1 Characterize the System

This step consists of reviewing system documentation and conducting interviews to gather important information necessary to develop the system characterization, such as:

- Organization’s mission,
- Operations of the organization,
- Policies of the organization or system,
- Processes of the organization,
- Operating environment of the organization or system,
- Organization's security posture,
- Functional requirements,
- Physical and procedural security controls,
- System security controls,
- System security requirements,
- System security architecture,
- Online electronic transactions, and/or
- Information storage and flows.

The information collected was reviewed and analyzed to gain an overall understanding of the functionality of SCGSC and to capture the system interfaces, type of data processed and stored, system criticality and data sensitivity levels, and users.

3.2 Identify Threats

The system characterization developed in Step 1, **Error! Reference source not found.**, was used to identify and develop a realistic list of potential threat sources that are applicable specifically to the SCGSC system. A threat source is defined as any circumstance or event with the potential to cause harm to an information system. Advisories, interviews, incident reports, and other sources were also used as resources to determine potential threats. Examples of threat sources are categorized and provided in Table 1.

Table 1. Threat Sources

Threat	Impact
Natural	
Flooding	Flooding of the computer room and support areas from sources external to the building (e.g., mudslides).
Earthquake	An earthquake causing structural damage to the facility and surrounding area.
Lightning Strikes	Severe lightning can cause structural damage to the facility or the system.
Severe Storm	Facility and/or surrounding area damage due to snowstorms, sandstorms, hail, monsoons, dust storms, or lightning not directly associated with other natural threats.
Hurricane/Typhoon	Damage to facility and/or surrounding area due to hurricanes or typhoons.
Tornado	Buildings and/or facilities can be damaged as a result of tornados.
Water Spouts	Tornados occurring over water can result in structural damage or collapse.
Sinkholes	Depression in a land surface can cause destruction of a facility.
Volcano	Eruption and debris (e.g., ash, lava) can cause damage or destruction to a facility.
Environmental and Physical	
Fire	Can include large fires (e.g., those that trigger the fire suppression system, if the site is so equipped, or require the involvement of trained firefighters) and small fires (e.g., those extinguishable with a hand-held extinguisher).
Temperature	Lack of temperature control can cause system degradation or malfunction of system parts.
Humidity	Too high or too low levels of humidity can cause system parts to malfunction.
Power Instability	Long- and short-term power failure associated with power outages, brownouts, and power fluctuations.
Liquid Leakage	Liquid leakage resulting in flooding of the computer room and support areas from an internal source (e.g., broken water or sewage pipes or activated fire suppression system).
Loss of Communication Medium	Loss of physical communication capabilities (e.g., cable break).
Human	
Accidental System Damage	The unintentional destruction or degradation of any system and/or component including spilling of beverages (e.g., coffee, soda, and water).
Theft	Acquisition of data, hardware, and software by unauthorized individuals.

Threat	Impact
Eavesdropping	An unauthorized individual connecting to, or tapping, voice or data transmissions to gain access to the message content for the purpose of reviewing it.
Sabotage/Vandalism	The deliberate destruction or degradation of any system and/or component.
Improper Handling of Sensitive Information	The failure of authorized individuals to handle sensitive information (e.g., Privacy Act, Sensitive But Unclassified (SBU), For Official Use Only (FOUO), or proprietary, Limited Official Use) in accordance with applicable policies and procedures, possibly compromising the information.
Resource Misuse and Abuse	The unauthorized use of any asset for a purpose other than originally intended.
Social Engineering	A method of obtaining information to be used for compromising a system (e.g., a password) from an individual rather than by breaking into the system. Social engineering can be used over an extended period of time to maintain a continuing stream of information and help from unsuspecting users.
Unauthorized External Access	The ability and opportunity of an external source to obtain information, or physical access to facilities, without proper authorization or clearance.
Unauthorized Internal Access	The ability and opportunity of an internal source to obtain information, or physical access to facilities, without proper authorization or clearance.
Terrorism	Destruction of any system by means of information warfare, system attack, system penetration, or system tampering.
Impersonation	Misinterpretation of human or cyber identity.
Falsified Input	Deliberately inputting inaccurate data or information into a system to cause corruption of data.
Interception	Capturing unauthorized data for malicious intent.
Bribery	Offering money or something of value to gain system access.
Hacking	Gaining unauthorized system access.

3.2.1 *Threat Sources*

Human threat sources are the most common threats to exploit vulnerabilities. Environmental threat sources can also be manipulated to exploit vulnerabilities. For example, a disgruntled employee could cause damage to a facility by accessing and rupturing an external plumbing pipe, thereby causing leakage or flooding. A list of potential human threat sources would include the following:

- Insiders—includes any authorized user (e.g., government agency employee, contractor, business partner) who is either poorly trained, disgruntled, dishonest, malicious, negligent, attempting unauthorized system access and/or exceeding system privilege to gain unauthorized access to the system;
- Contractors and subcontractors—includes system developers, technical support staff, security officers, and other support personnel;
- Former contractors and subcontractors—includes former contractor personnel with previous system access;

- Maintenance staff—includes facility maintenance staff, telecommunications service personnel, and other maintenance teams;
- Former employees—employees who have separated from service (e.g., retired, resigned);
- Unauthorized external users—public Internet users, criminals, terrorists, and intruders (hackers and crackers), who attempt to access internal networks.

3.3 Identify Vulnerabilities and Safeguards

During this step, the independent risk assessment team used the system characterization and other information gathered from documentation and interviews to evaluate the weaknesses associated with SCGSC and developed a list of potential vulnerabilities. Existing security controls or safeguards currently in place for SCGSC also were identified.

As part of identifying vulnerabilities, the independent risk assessment team reviewed the System Security Plan and the specific implementation of the controls from NIST SP 800-53, Revision 4. This exercise was performed to determine if the identified weaknesses were previously documented and have planned or compensating controls already in place to mitigate the vulnerabilities.

3.4 Assess Risk

The risk assessment process encompassed the following subtasks:

- Determining the likelihood of the identified system-specific threats exploiting a specific identified vulnerability;
- Determining the impact to system operations and information should a threat exploit the specific identified vulnerability;
- Determining the overall risk for the specific identified vulnerability.

The following equation summarizes how risk was determined for each observation:

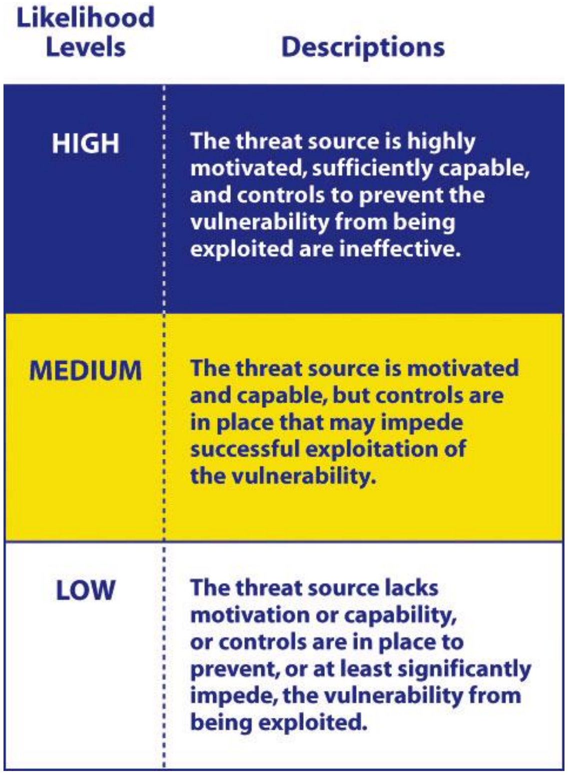
Figure 2. Risk Score

Risk = Likelihood x Impact

3.4.1 Likelihood

Likelihood was determined by considering threats and vulnerabilities. The likelihood that vulnerability will be exploited by a threat was assessed and described as High, Medium, or Low. Factors that govern the likelihood of threat exploitation include threat capability, frequency of threat occurrence, and effectiveness of current countermeasures. The descriptions shown in were used to determine the likelihood level for the threat/vulnerability pair.

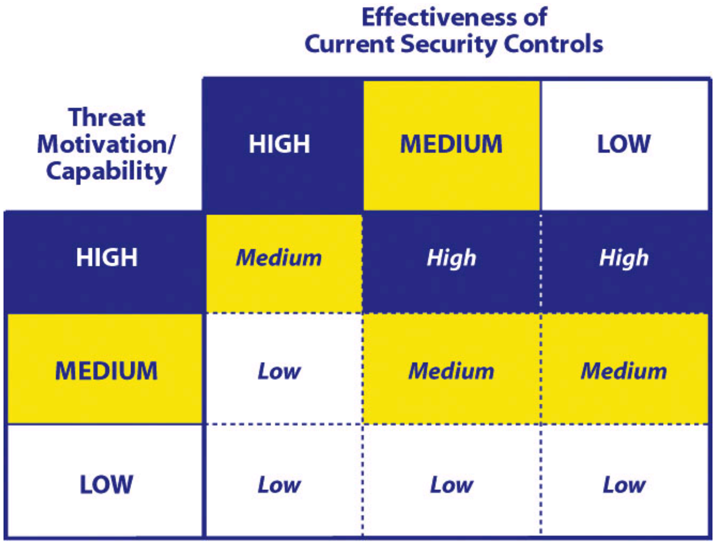
Figure 3. Likelihood Descriptions



Likelihood Levels	Descriptions
HIGH	The threat source is highly motivated, sufficiently capable, and controls to prevent the vulnerability from being exploited are ineffective.
MEDIUM	The threat source is motivated and capable, but controls are in place that may impede successful exploitation of the vulnerability.
LOW	The threat source lacks motivation or capability, or controls are in place to prevent, or at least significantly impede, the vulnerability from being exploited.

Once the threat capability and countermeasure effectiveness were assessed for each threat/vulnerability pair, the matrix shown in **Error! Reference source not found.** was used to determine the overall likelihood of the threat exploiting the vulnerability.

Figure 4. Likelihood Matrix



	Effectiveness of Current Security Controls		
Threat Motivation/ Capability	HIGH	MEDIUM	LOW
HIGH	*Medium*	*High*	*High*
MEDIUM	*Low*	*Medium*	*Medium*
LOW	*Low*	*Low*	*Low*

3.4.2 Impact

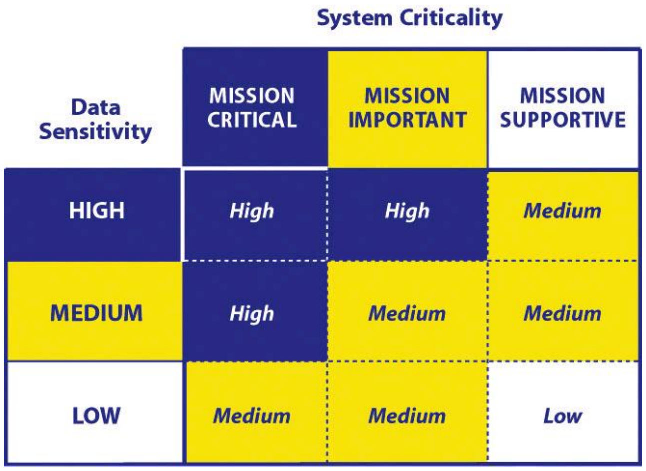
Impact refers to the magnitude of potential harm that may be caused by threat exploitation. Impact is determined by the value of the resource at risk, both in terms of its inherent (replacement) value and its importance (criticality) to NIDDK's mission. The criticality and sensitivity of both the system and data are useful guides for assessing the potential impact of an exploited vulnerability. **Error! Reference source not found.** provides a description for each level of impact.

Figure 5. Impact Descriptions

Impact Levels	Descriptions
HIGH	Exploitation of the vulnerability – (1) may result in the costly loss of major tangible assets or resources; (2) may significantly violate, harm, or impede NIDDK's mission, reputation, or interest; or (3) may result in human death or serious injury.
MEDIUM	Exploitation of the vulnerability – (1) may result in the costly loss of tangible assets or resources; (2) may violate, harm, or impede NIDDK's mission, reputation, or interest; or (3) may result in human injury.
LOW	Exploitation of the vulnerability – (1) may result in the loss of some tangible assets or resources; or (2) may noticeably affect NIDDK's mission, reputation, or interest.

Based on system criticality and information sensitivity, the matrix shown in **Error! Reference source not found.** can be used to determine the impact. The level of impact equals the intersection of the system criticality and information sensitivity values. For example, suppose the system criticality level is mission important (MI) and the data sensitivity level is High, based on the impact matrix in **Error! Reference source not found.**, the impact level would be High.

Figure 6. Impact Matrix

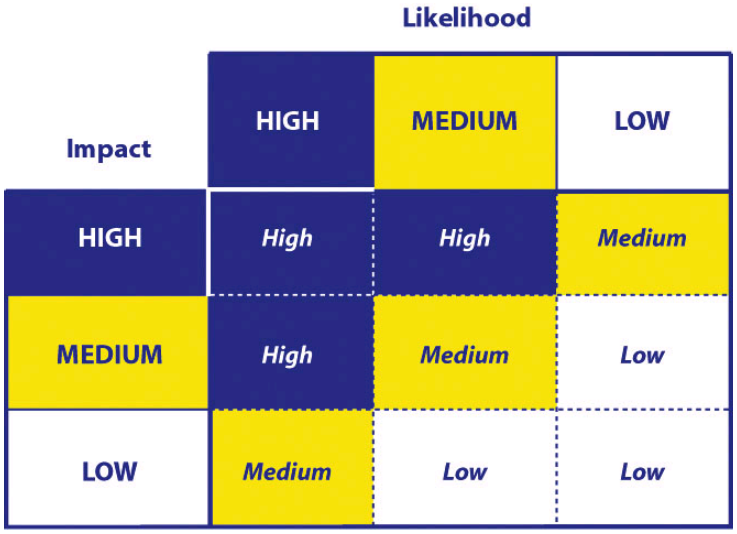


	System Criticality		
Data Sensitivity	MISSION CRITICAL	MISSION IMPORTANT	MISSION SUPPORTIVE
HIGH	*High*	*High*	*Medium*
MEDIUM	*High*	*Medium*	*Medium*
LOW	*Medium*	*Medium*	*Low*

3.4.3 Risk

After evaluating likelihood and impact, the independent risk assessment team employed a risk scale matrix with the ratings of High, Medium, and Low to determine the degree or level of risk to which a system, facility, or procedure might be exposed if a vulnerability were exploited. The level of risk equals the intersection of the likelihood and impact values. For example, suppose the likelihood level is High and the impact level is Low for the threat/vulnerability pair. Based on the risk matrix shown in **Error! Reference source not found.**, there would be a Medium risk level.

Figure 7. Risk Level



	Likelihood		
Impact	HIGH	MEDIUM	LOW
HIGH	*High*	*High*	*Medium*
MEDIUM	*High*	*Medium*	*Low*
LOW	*Medium*	*Low*	*Low*

3.5 Determine Risk Mitigation Strategies

Once the risk assessment phase was complete, the independent risk assessment team evaluated the observations and determined risk mitigation strategies that best suited SCGSC. The observations are provided in Appendix B, and risk mitigation strategies are documented here and in Appendix C: SCGSC Plan of Action and Milestones.

4. System Characterization

This section provides a detailed description of the system being reviewed and establishes the boundaries of the review. The description of the system also provides details on the system environment. The review boundaries detail system components and capabilities within and outside the boundaries established. Furthermore, this section examines the criticality and sensitivity of the system and data processed. The information provided within this section was gathered from document reviews, observation, and on-site interviews with the following personnel:

- Beverly Campbell, SCG President
- Chuck Lee, Information Technology Director

4.1 Descriptions and Purpose

The SCG Secure Cloud system supports the development and communications of health information that improves public health and quality of life. The SCGSC system provides Support for National Information Clearinghouses and Campaign-Focused Programs for the NIDDK Office of Communications and Public Liaison, in Bethesda, Maryland. The SCGSC system 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 SCG Secure Cloud system is housed in a secure office building in Gaithersburg, MD. SCG has the entire second floor of the building plus a suite on the seventh floor where the system is located. There is controlled access to SCG's offices and the SCGSC 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 identical host servers consisting that are HP ProLiant DL360 Gen9 – Xeon E5-2620V3 2.4 GHz, 80 GB RAM, 900 GB HD, RAID5 running VMWare VSphere ESXi 6.0 update 2. Within this virtualized host environment, the system is running four virtual machines (VMs): VM 1 (SCSQL-PROD), VM 2 (SCCOLDSHARE-PROD), VM 3 (SCFSMO), and VM 4 (3PL). These VMs are stored on a 4 TB Network Attached Storage (NAS), HPE 1450 NAS. The operating system for all virtual servers is Windows 2008 R2 Enterprise (x64). They all are joined to a single domain (SCGSC.COM) except VM 4. VM 4 is a standalone server. The VMs have Symantec Endpoint Protection Suite 2015 for protection against viruses and intrusions. In addition, VM 1 has SQL Server 2012 Standard (x64) and is a local secondary DNS Server. VM 2 has IIS 7, ColdFusion 9 and SharePoint Foundation

2010 and is the web server where the public can access the websites. VM 3 is the domain controller and holds Active Directory, DNS, and the Kiwi Syslog. Microsoft Dynamics NAV runs on VM 4. SCG Secure Cloud system has four switches—Cisco 2960 Manageable Switch, Netgear FS524S (unmanaged switch), Netgear GS108 (unmanaged switch), and Cisco SG110D-08 (unmanaged switch). There is one firewall—Cisco 5512-X. External to the SCGSC, there are two tape backup devices—Tandberg StorageLoader LTO-6 Tape Autoloader and Tandberg StorageLoader LTO-4 Tape Autoloader. These 2 devices are attached to 2 separate physical servers to perform backup jobs. The external IP address for VM 2 is 63.146.253.40.

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.

4.2 Review Boundaries

SCG Secure Cloud is a standalone system that does not interconnect with any information systems or services.

SCGSC does not use eAuthentication; therefore, a risk assessment for electronic transactions is not required for this document.

4.2.1 Access Control

SCG Secure Cloud is a standalone system. Access control is enforced through Active Directory, requiring privileged users to authenticate into the system before being granted access.

4.3 Criticality of System and Sensitivity of Information

System criticality and sensitivity is determined by the adverse effect that a security event could have on the system, and how it impacts the integrity, availability, and confidentiality of the system. The criticality criteria are shown in **Error! Reference source not found.**.

Figure 8. Criticality Criteria

MC Mission Critical	MI Mission Important	MS Mission Supportive
Automated information resources whose failure would preclude the NIDDK from accomplishing its core business operations	Automated information resources whose failure would not preclude the NIDDK from accomplishing its core business processes in the short term (few hours), but would cause failure in the mid to long term (few hours to few weeks)	Automated information resources whose failure would not preclude the NIDDK from accomplishing its core business processes in the short to long term (few hours to few weeks), but would have an impact on the effectiveness or efficiency of day-to-day

🟦	🟨	operations

This system/application has a FIPS199 Security Categorization of Moderate. It requires protection to safeguard data and information from unauthorized modification, and/or ensure that the organization's services are available to meet mission requirements. Impact Levels of High, Moderate, and Low were determined for the categories of confidentiality, availability, integrity, and classification defined in Table 2.

Table 2. Classification Levels

Category	Definition	This System's Level
Confidentiality:	The system contains information that requires protection from unauthorized disclosure. Unauthorized disclosure of this information may adversely impact the consumer confidence level of NIKDD.	Moderate
Availability:	The system contains information or provides services that must be available on a timely basis to meet mission requirements or to avoid substantial losses.	Moderate
Integrity:	The system contains information that must be protected from unauthorized, unanticipated, or unintentional modification.	Moderate
Classification:	The highest classification for this system:	**Moderate**

SCGSC was evaluated using the following methodology to determine SCGSC's criticality. System criticality is determined based on how integral the system is in conducting the mission of the NIKDD. The system is categorized using one of three criteria (i.e., Mission Critical [MC], Mission Important [MI], or Mission Supportive [MS]). Criteria definitions are provided in **Error! Reference source not found.**.

NIST SP 800-60 defines automated information resources, whose failure would not preclude NIDDK from accomplishing core business operations in the short to long term (few hours to a few weeks), but would have an impact on the effectiveness or efficiency of day-to-day operations, as being mission supportive. The SCGSC system contains the name and address data provided by individuals ordering items from the clearinghouses, but the failure of the SCGSC system would not preclude the NIDDK from accomplishing its core business processes in the short to long term (few hours to few weeks), but would have an impact on the effectiveness or efficiency of day-to-day operations. Consequently, SCGSC is considered Mission Supportive.

4.4 Data Description

SCGSC was determined to contain Sensitive But Unclassified Information (SBU) and contains the following information types:

- Health Care and Practitioner Information Type (M/M/L)
- Personal Identity and Authentication Information Type (M/M/M)

Upon examination of each information type, it was determined that the special considerations that could impact determination would not apply for the information types. As such, the Security Categorization (SC) for SCGSC is **Moderate**.

SCGSC collects the name and address of users that request a publication or document identified in the online catalog on the web site. As a result, the SP 800-60, Personal Identity and Authentication Information Type with impact levels as follows: Confidentiality: M, Integrity: M, and Availability: M, have been added to the sensitivity impact level. The overall sensitivity level for SCGSC is Moderate.

5. System Threat Environment

This section describes the specific threat environment for the system being reviewed. The threat sources described in Section 3 are natural, environmental/physical, and human. The threat sources applicable to the SCGSC environment are listed below.

5.1 System Threat Description

Based on the system characterization, the system criticality, and data sensitivity levels determined for SCGSC, a realistic list of potential natural, environmental/physical, and human threats were determined. Advisories, interviews, incident reports, and other sources were also used as resources to determine potential threats. The threat sources pertaining to the SCGSC are human threats, environmental threats, and natural threats. These threats could exploit the SCGSC's technical security and program management support weaknesses and cause unauthorized data modification, unauthorized data disclosure, unauthorized data destruction, and/or denial of services. The SCGSC is a mission-important system; therefore, failures could potentially impact the ability of NIDDK to accomplish its core business operations from a few hours to a few weeks.

5.1.1 System Threat Identification

The specific natural, physical and environmental, and human threats applicable to the SCGSC System are listed in the following sections. The natural threat sources were determined based on the geographical and environmental location of FSIS. Potential threat agents can exploit vulnerabilities based on the human threat sources listed below.

5.2 Natural Threats

Based on the geographical location of the system, the types of natural threats that are applicable to the environment are tornados, wildfires, and hurricanes.

5.3 Human Threats

Human threats that are applicable to the SCGSC environment include personnel whose employment has been terminated, disgruntled employees, unauthorized users, computer criminals, terrorists, and negligent persons. However, the greatest threats in this category are computer-based, including computer viruses/malware, and intrusions. This threat is constant and has the potential to be virulent. The remaining types of man-made threats that are likely (with a probability of occurrence of Moderate or higher) and applicable to SCGSC are: administrative errors, disgruntled employee or citizen, human error/omission, management error/omission, substance abuse, theft of assets, and unauthorized access to client system. Factors that govern the likelihood of threat exploitation include threat capability, frequency of threat occurrence, and effectiveness of current countermeasures. For this reason, continuous monitoring of all controls (managerial, operational, and technical) provides a major component in making likelihood determinations about threats. Continuous monitoring of the agreed-upon milestones to mitigate the risks are reportable to NIH and HHS for the POA&M. The POA&M will be used by the ISSO to monitor the successful completion of the milestones.

5.4 Risk Assessment Results

This section presents the results of the risk assessment performed for the SCGSC System. Each identified threat, which could exploit vulnerability, was documented. The System Security Plan specifically developed for the SCGSC system allowed for the testing of general security requirements and system-specific security requirements. The System Security Plan requirements and existing technical and procedural countermeasures that might mitigate the risks to the SCGSC system environment were considered when assigning the risk level to each observation. The presentation of each observation consists of the following:

- Statement of the observation;
- Description of the current environment in relation to the observation;
- An assessment of the likelihood that a vulnerability will be exploited by a threat;
- An assessment of how the vulnerability can be exploited;
- The impact on the SCGSC System upon successful exploitation of a vulnerability;
- An overall assessment of the level of risk to the SCGSC System based on the threat and vulnerability assessment;
- A recommendation of countermeasures that would reduce the risk.

Risk levels are rated as high, medium, or low. Related or similar observations are grouped together for discussion purposes. Risks to the SCGSC system were evaluated in the management, operational, and technical security domains.

5.5 Management Controls

Management controls focus on the management of the IT security system and the management of risk for a system. There are techniques and concerns that are normally addressed by management. There were 42 observations in the area of management controls. The management observations are identified in the form of POAMs in Appendix C.

5.6 Operational Controls

The operational controls address security methods focusing on mechanisms primarily implemented and executed by people (as opposed to systems). These controls are put in place to improve the security of a particular system (or group of systems). Often, they require technical or specialized expertise and rely upon management activities as well as technical controls. There are **152** observation in operational security. The operational controls are identified in the form of POAMs in Appendix C.

5.7 Technical Controls

Technical controls focus on security controls that the computer system executes. The controls can provide automated protection for unauthorized access or misuse, facilitate detection of security violations, and support security requirements for applications and data. There were a total of **122** observations in technical security. Seventy nine (79) of those observations were the results of the system scan. The SCGSC Scan results are listed in Appendix B. The scan solutions provided must be analyzed and a decision made as to whether to implement the solution or determine if the implementation will cause a disruption to the system and therefore not to implement the solution.

Appendix A: Acronyms

A&A	Assessment and Authorization
FOUO	For Official Use Only
ID	Identification
IT	Information Technology
MC	Mission Critical
MI	Mission Important
MS	Mission Supportive
NIST	National Institute of Standards and Technology
POA&M	Plan of Action and Milestones
SBU	Sensitive But Unclassified
SCA	Security Controls Assessment
SP	Special Publication
ST&E	Security Test and Evaluation

Appendix B: SCGSC Security Scan Results

Appendix C: SCGSC Plan of Action and Milestones