



**The Scientific Consulting Group, Inc.**

# **System and Information Integrity Policy and Procedures**

for the

## **SCG Secure Cloud System**

*Version 1.3*

*May 19, 2016*

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

## System and Information Integrity Policy and Procedures Approval

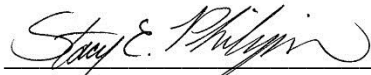
The System and Information Integrity Policy and Procedures for the SCG Secure Cloud system must be approved by the SCG President, the Vice President of Administration, and the Information Technology Director. The undersigned acknowledge that they have reviewed the SCG Secure Cloud System and Information Integrity Policy and Procedures and agree with the information presented in this document. The SCG President and Information Technology (IT) Director will review the System and Information Integrity Policy and Procedures at least once every three (3) years and revise the plan to address system/organizational changes or changes to policy or procedures. Any changes to the document will be coordinated with, and approved by, the undersigned or their designated representatives.



Beverly J. Campbell  
President

5/19/16

DATE



Stacy E. Philipson  
Vice President of Administration

5/19/16

DATE



Chuck C. Lee  
Director of Information Technology

5/19/16

DATE

## Document Information and Revision History

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

Document Revision and History			
Revision	Date	Author	Comments
1.0	2/16/15	B. Campbell	Draft Policy
1.1	2/22/15	C. Berry	Added additional controls for a Moderate system; updated references; made minor modifications
1.2	2/23/15	B. Campbell/C. Lee	Minor modifications to document
1.3	5/19/16	B. Campbell	Minor modifications throughout document

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

## Table of Contents

<b>1. Purpose and Distribution .....</b>	<b>1</b>
<b>2. Scope .....</b>	<b>1</b>
<b>3. Intent .....</b>	<b>1</b>
<b>4. Policy .....</b>	<b>1</b>
4.1 SI-1 System and Information Integrity Procedures .....	1
4.2 SI-2 Flaw Remediation .....	1
4.3 SI-3 Malicious Code Protection .....	1
4.4 SI-4 Information System Monitoring .....	1
4.5 SI-5 Security Alerts, Advisories, and Directives .....	2
4.6 SI-7 Software, Firmware, and Information Integrity .....	2
4.7 SI-8 Spam Protection .....	2
4.8 SI-9 Information Input Restrictions .....	3
4.9 SI-10 Information Input Validation .....	3
4.10 SI-11 Error Handling .....	3
4.11 SI-12 Information Output Handling and Retention .....	4
<b>5. Procedures .....</b>	<b>4</b>
5.2 SI-3 – Malicious Code Protection .....	9
5.3 SI-4 – Information System Monitoring .....	11
5.4 SI-5 – Security Alerts, Advisories, and Directives .....	12
5.5 SI-7 – Software and Information Integrity .....	13
5.6 SI-8 – Spam Protection .....	14
5.7 SI-9 – Information Input Restrictions .....	14
5.8 SI-10 – Information Input Validation .....	14
5.9 SI-11 – Error Handling .....	15
5.10 SI-12 – Output Handling and Retention .....	16
<b>6. Roles and Responsibilities .....</b>	<b>16</b>
<b>Appendix A: References .....</b>	<b>0</b>

## **1. Purpose and Distribution**

This document establishes the SCG Secure Cloud System and Information Integrity Policy and Procedures for managing risks from system flaws/vulnerabilities, malicious code, unauthorized code changes, and inadequate error handling through the establishment of an effective system and information integrity program. The system and information integrity program helps SCG implement security best practices with regard to system configuration, security, and error handling.

This document is distributed to the IT personnel who are responsible for and have access to the SCGSC system as well as the SCG President, Vice President of Administration, and Program Manager. The document is posted in a read-only format on the SCG Intranet to facilitate access by SCG employees responsible for the SCGSC.

## **2. Scope**

The policy and procedures in this document are applicable to the SCG Secure Cloud system, which was developed and is operated by SCG to support the National Institute of Diabetes and Digestive and Kidney Diseases (NIDDK). All SCG employees, contractors, vendors, or others who use SCG Secure Cloud IT resources are responsible for reading and adhering to this policy and these procedures.

## **3. Intent**

The SCG Secure Cloud System and Information Integrity policy serves to be consistent with best practices associated with organizational information security management. It is the intention of this policy to establish a system and information integrity capability throughout SCG to help the organization implement security best practices with regard to SCGSC system configuration, security, and error handling.

## **4. Policy**

SCG has chosen to adopt the System and Information Integrity principles established in NIST SP 800-53 "System and Information Integrity," Control Family guidelines, as the official policy for this domain. The following sections in this document outline the System and Information Integrity standards that constitute SCG Secure Cloud system policy. All SCG employees, subcontractors, consultants, vendors, and others supporting or using the SCG Secure Cloud system are bound to this policy, and must develop or adhere to a program plan that demonstrates compliance with the policy and standards documented.

### **4.1 SI-1 System and Information Integrity Procedures**

SCG must develop, adopt, or adhere to a formal, documented system and information integrity **policy** that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.

## **4.2 SI-2 Flaw Remediation**

SCG must:

- Identify, report, and correct information system flaws.
- Test software updates related to flaw remediation for effectiveness and potential side effects on organizational information assets before installation.
- Incorporate flaw remediation into the organizational configuration management process.
- Install security-relevant software and firmware updates within 30 days of the release of the updates.
- Employ automated mechanisms periodically to determine the state of information system components with regard to flaw remediation.

## **4.3 SI-3 Malicious Code Protection**

SCG must:

- Employ malicious code protection mechanisms at information asset entry and exit points and at workstations, servers, or mobile computing devices (e.g., e-mail, removable media, and malicious websites) on the network to detect and eradicate malicious code.
- Update malicious code protection mechanisms (including signature definitions) whenever new releases are available in accordance with organizational configuration management policy and procedures.
- Configure malicious code protection mechanisms (e.g., real-time scans, periodic scans, malicious code detection) to protect company information systems and assets.
- Address the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the information asset.
- Manage malicious code protection mechanisms centrally.  
Update malicious code protection mechanisms automatically.

## **4.4 SI-4 Information System Monitoring**

SCG must:

- Monitor events on the information asset and detect information asset attacks.
- Identify unauthorized use of the information assets.
- Deploy monitoring devices (1) strategically within the information asset to collect organization-determined essential information, and (2) at ad-hoc locations within the system to track specific types of transactions of interest to the organization.
- Heighten the level of information asset monitoring activity whenever there is an 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.

- Obtain legal opinion with regard to information asset monitoring activities in accordance with applicable federal laws, directives, policies, or regulations.
- Employ automated tools to support near real-time analysis of events.
- Ensure the system monitors inbound and outbound communications traffic frequently for unusual or unauthorized activities or conditions.
- Ensure the system alerts the IT Director when the following indications of compromise or potential compromise occur: Any unusual activities.
- Use NIST SP 800-61, Revision 2; SP 800-83, Revision 1; SP 800-92; and SP 800-94 as guidance on incident handling, responding to detecting malware-based attacks, computer security log management, and intrusion detection and prevention system.

#### **4.5 SI-5 Security Alerts, Advisories, and Directives**

SCG must:

- Receive information asset security alerts, advisories, and directives from designated external organizations on an ongoing basis.
- Generate internal security alerts, advisories, and directives as deemed necessary.
- Disseminate security alerts, advisories, and directives to SCG IT staff; also disseminate critical alerts/advisories/directives to the system owner, Program Manager, and stakeholders, as appropriate.
- Implement security directives in accordance with established time frames, or notify the System Owner and Program Manager of the degree and reason for noncompliance.

#### **4.6 SI-7 Software, Firmware, and Information Integrity**

SCG must:

- Detect unauthorized changes to software within the information asset.
- Ensure the system performs an integrity check of all Microsoft Windows updates and Symantec Endpoint Protection updates at startup and during manual check once a month.
- Incorporate the detection of unauthorized intrusion with IPS and Symantec alerts with sensitivity categorized as anything above "Warning" into the organizational incident response capability.

#### **4.7 SI-8 Spam Protection**

SCG must:

- Employ spam protection mechanisms at information asset entry and exit points and at workstations, servers, or mobile computing devices on the network to detect and take action on unsolicited messages transported by e-mail, e-mail attachments, web accesses, or other common means. In addition, SCG must update spam protection mechanisms (including signature definitions) when new releases are available in accordance with organizational configuration management policy and procedures.
- Centrally manage spam protection mechanisms.
- Automatically update spam protection mechanisms.

#### **4.8 SI-9 Information Input Restrictions**

SCG must:

- Restrict the capability to input information to the system to authorized personnel.

#### **4.9 SI-10 Information Input Validation**

SCG must:

- Configure the system to check the validity of information inputs and verify validation as part of system testing.
- Configure the system to check all arguments or input data strings submitted by users, external process, or untrusted internal processes.
- Put rules in place to check the valid syntax and semantics of information system inputs (e.g., character length, numerical range, acceptable values) to verify that inputs match specified definitions for format and content.
- Configure the system to perform the following input validations: type checks, format and syntax checks, and parameter and character validity checks.
- Ensure that invalid inputs or error statements do not give the user sensitive data, storage locations, database names, or information about the system's architecture.

#### **4.10 SI-11 Error Handling**

SCG must:

- Configure the system to Identify potentially security-relevant error conditions.
- Generate error messages that provide information necessary for corrective actions without revealing company sensitive information in error logs and administrative messages that could be exploited by adversaries.
- Reveal error messages only to authorized personnel.



#### 4.11 SI-12 Information Output Handling and Retention

SCG must handle and retain both information within and output from the SCG Secure Cloud system in accordance with applicable federal laws, directives, policies, regulations, standards, and operational requirements.

### 5. Procedures

#### 5.1 SI-2 – Flaw Remediation

SCG shall identify, report, and correct information system flaws.

**Note:** *Flaws include errors in software, as well as errors in configuration settings for information systems. Flaw remediation encompasses installing software patches, service packs, and hot fixes, as well as making changes to configuration settings. Vulnerability mitigation also can involve removing software or disabling functions, ports, protocols, and/or services.*

An inventory of the SCG Secure Cloud system and components must be collected and maintained in order to determine which hardware equipment, operating systems, and software applications are in operation.

Flaw remediation must be incorporated into SCG's configuration management process. Refer to the Configuration Management Plan for requirements on configuration management.

The Configuration Management Plan must include a plan for managing patches and vulnerability that addresses the following:

- All SCGSC equipment, operating system, and software applications must be included.
- The criteria for implementing flaw remediation must be defined with respect to threat level, risk of compromise, and consequences of compromise.
- The responsible party for monitoring and coordinating with each vendor for patch release support must be designated.
- The responsible party for testing patches must be identified and coordinated.
- Information security patches shall be installed in accordance with the Configuration Management Plan.

Security sources for vulnerability announcements (i.e., both patch and non-patch remediation) and emerging threats that correspond to the software within the information system's inventory must be monitored.

- The following sources must be monitored by subscription or on a daily basis where subscription is not available:
  - United States Computer Emergency Readiness Team (US-CERT) National Cyber Alert System (signed up for automatic alerts)
  - Vendor and developer sites (signed up for automatic alerts)

- Other third-party alert systems (searched periodically as needed)
- When new devices are added to the inventory, the following sites must be accessed to ensure that the latest patches and versions are currently used and installed:
  - US-CERT National Cyber Alert System
  - NIST National Vulnerability Database (NVD)
  - Vendor and developer sites
  - Other third-party sites

Information systems containing software affected by recently announced software flaws (and potential vulnerabilities resulting from those flaws) must be reported to designated organizational officials with information security responsibilities (i.e., IT Director). Serious vulnerabilities that pose escalated risk should be reported to the SCG President, Program Manager, and, if appropriate, the NIDDK Information System Security Officer.

Vulnerability and remediation information must be disseminated to system administrator and security personnel. Standard e-mail distribution lists must be established.

The system administrator must be instructed or trained on how to apply vulnerability and configuration management remediations. Notifications of vulnerabilities and remediations must contain instructions on how to apply them, if automated mechanisms are not used.

Vulnerabilities and remediation actions must be prioritized, and their priority order must be based on the individual vulnerability criticality or severity ratings.

- Priorities must be established based on the source's assessment of severity or criticality as high, moderate/medium, or low.
- US-CERT's established criticality takes priority.
- The next highest priority available from the following sources must be used unless SCG has established a different priority based on the application of NIST's Common Vulnerability Scoring System (CVSS) Calculator:
  - Vendor web sites and mailing lists
  - Third-party web sites
  - Vulnerability scanner
  - Vulnerability databases
  - Enterprise patch management tools
  - Other notification tools
- Source severity assessments other than those established by US-CERT may be modified in accordance with detailed knowledge of criteria specific to SCG, by using NIST's CVSS Calculator, provided the criteria, ratings, and results are documented and retained for the record and the alteration is noted in the alert.

- NIST's CVSS Calculator must be used to establish priority as follows:
  - Vulnerabilities must be labeled "Low" severity if they have a CVSS base score of 0.0–3.9.
  - Vulnerabilities must be labeled "Medium" severity if they have a base CVSS score of 4.0–6.9.
  - Vulnerabilities must be labeled "High" or "Critical" severity if they have a CVSS base score of 7.0–10.0.

A database of remediations that need to be applied to the SCG Secure Cloud resources must be created and maintained. Vulnerability remediation must be monitored.

Software updates related to flaw remediation, (including patches, services packs, and hot fixes) must be tested before installation for effectiveness and potential side effects on the SCG Secure Cloud system.

- The level and timing of testing may vary and depend on risk to the information system and priority of the remediation.
  - Fixes for vulnerabilities ranked high or critical must be tested as soon as possible but no later than 2 business days.
  - Fixes for vulnerabilities ranked moderate or medium must be tested within 7 business days.
  - Complete testing of fixes for low priority vulnerabilities must be completed within 30 days.
- Existing change management procedures must be used for testing low priority remediations and, when possible, for testing patches and configuration modifications of moderate/medium priority vulnerabilities.
- The flaw remediation process must be centrally managed and software updates must be installed automatically.
- The software code for all patches, service packs, hot fixes, etc., must be verified before testing or installation.
  - A vendor authentication mechanism (e.g., cryptographic checksums, Pretty Good Privacy [PGP] signatures, digital certificates) must be used to ensure the authenticity of the code.
  - The code must be scanned for viruses using the most current virus signature database.
  - A search must be performed to learn what experiences others have had in installing or using the patch.
- All remediation changes must be tested on non-production systems prior to implementation on all agency-standard IT products and configurations in order to reduce or eliminate the following:

- Unintended consequences
- Alteration of security settings
- Enabling of default user accounts that had been disabled
- Resetting of default passwords for user accounts
- Enabling of services and functions that had been disabled
- Non-security changes, such as new functionality
- Testing of patches must ensure that patches are installed in the required sequence and any removal of any previous security patch is not unintended.
- Testing must include checking all related software to ensure that it is operating correctly.
- Testing must include a selection of systems that accurately represent the configuration of the system in deployment.
  - Testing of remediations must be conducted on IT components that use standardized configurations. Images of standard configurations must be used on test systems or within virtual machines on test systems that can expedite the testing process.
  - Non-standard IT products that have been approved for use on SCG Secure Cloud must be tested using approved configurations.

Based on the results of testing, it must be considered whether any significant disadvantages outweigh the benefits of installing a patch and whether remediation should be delayed. If the potential negative consequences are significant, then the following must be considered:

- Waiting until the vendor releases a newer patch that corrects the major issues.
- The ability to “undo” or uninstall a patch.

**Note:** *Even when the “undo” option is provided, the uninstall process does not always return the system to its previous state, which requires a documented fix.*

- Delay of high or moderate/medium priority remediation must be approved by the IT Director and ISSO, with appropriate documentation of rationale and mitigation measures.

A schedule for the release and implementation of patches, service packs, and hot fixes must be developed by the IT Director in coordination with individual system security personnel. The patch release schedule must be developed using a risk-based decision that is in compliance with pre-defined criteria (i.e., threat level, risk of compromise, and consequences of compromise) outlined in the Flaw and Vulnerability Management Plan.

Security-relevant software updates (e.g., patches, service packs, and hot fixes) must be installed promptly by SCG IT security personnel.

- The requirements for testing and consideration of significant negative consequences of the remediation must still apply.

- Flaws discovered during security assessments, continuous monitoring, incident response activities, or information system error handling also must be addressed expeditiously.
- The priority of the vulnerability must determine how promptly the remediation is implemented.
  - Vulnerabilities ranked high or critical must be mitigated and reported to the ISSO within 2 business days after testing is completed.
  - Vulnerabilities ranked moderate/medium must be mitigated and reported to the ISSO within 7 business days after testing is completed.
  - Vulnerabilities ranked low must be mitigated within 30 days.
- Automated deployment of patches to SCGSC IT devices using appropriate patch management tools must be performed.
  - SCG's standard tools for automated patch deployment and installation must be used.
  - When automated mechanisms are not available, feasible, or appropriate, manual patch installation and remediation must be performed.
- Automated tools acquired to support vulnerability and configuration management remediation actions must be selected based on the following order of priority:
  - Tools that implement, support, and are validated by NIST to conform to the Security Content Automation Protocol (SCAP)
  - Tools that are pursuing or have a corporate commitment to conformance with NIST validation of SCAP
  - Tools that readily integrate with other SCAP-validated tools
  - Commercial tools that lack SCAP validation, in the absence of validated tools
  - Tools developed in house that readily integrate with SCAP-validated tools

Vulnerability and flaw remediation actions must be tracked and verified.

- Appropriate automated tools and methods include, but are not limited to, the following:
  - Patch deployment tool database
  - Network and host vulnerability scanning
  - Configuration management tool
- Where automated tools are not feasible, installation must be verified by manual methods, including, but not limited to the following:
  - Inspecting the configuration by, for example, viewing Basic Input/Output System (BIOS) boot screen, "Help – About" or other available and appropriate verification mechanism for the hardware, operating system, or application

- Reviewing files or configuration settings that the remediation was intended to correct to ensure that they have been changed as stated in the vendor's documentation or instructions
  - Reviewing patch logs
- Verification must not employ exploit procedures (e.g., a penetration test) or code to exploit any vulnerabilities without written authorization and approval from the SCGSC's Authorizing Official (AO).
  - Exploit methods such as penetration testing may be used without authorization and approval only on test systems in a test environment.
- The accomplishment of procedures contained in US-CERT guidance and Information Assurance Vulnerability Alerts must be verified.

When flaw remediation and vulnerability mitigation activities are completed, the following actions must occur: (1) the inventory of the system and components must be updated to reflect current software versions and configurations; and (2) stakeholders, including but not limited to the NIDDK ISSO, must be notified.

NIST SP 800-40, Revision 3, Guide to Enterprise Patch Management Technologies must be used as guidance on security patch installation and patch management.

## **5.2 SI-3 – Malicious Code Protection**

Malicious code protection mechanisms must be employed at information system entry and exit points (e.g., firewalls, web servers, proxy servers, remote-access servers).

Malicious code protection mechanisms must be configured to block at gateways and quarantine at host, validate quarantined code before releasing to user, clean quarantined malware as appropriate.

Standard malicious code protection software deployed on the servers must be configured to adhere to the following:

- The SCGSC servers must be scanned for malicious code on a continuous basis.
- Malicious code protection software must be updated concurrently with releases of updates provided by the vendor of the software. Updates should be tested and/or approved according to SCG requirements.

Malicious code protection mechanisms must be used to detect and eradicate malicious code (e.g., viruses, worms, Trojan horses, spyware) that is:

- Transported by e-mail, e-mail attachments, web accesses, removable media (e.g., Universal Serial Bus [USB] devices, diskettes or compact disks), or other common means.
- Inserted through the exploitation of information system vulnerabilities.
- Encoded in various formats (e.g., UUENCODE, Unicode) or contained within a compressed file.

Malicious code protection mechanisms (including signature definitions) must be updated whenever new releases are available and in accordance with SCG Secure Cloud configuration management policy, procedures, and standards.

- As applicable, the malicious code protection software must be supported under a vendor Service Level Agreement (SLA) or maintenance contract that provides frequent updates of malicious code signatures and profiles.
- Refer to the Configuration Management Procedures for requirements on configuration management.

Malicious code protection mechanisms must be configured to:

- Perform periodic scans of the information system daily and real-time scans of files from external sources as the files are downloaded, opened, or executed in accordance with SCG security policy.
- Block and quarantine malicious code and send alert to an administrator in response to malicious code detection.

The following elements must be addressed during vendor and product selection and when tuning the malicious code protection software:

- The receipt of false positives during malicious code detection and eradication.
- The resulting potential impact on the availability of the information.

**Note:** *A variety of technologies and methods exist to limit or eliminate the effects of malicious code attacks. Pervasive configuration management and strong software integrity controls may be effective in preventing execution of unauthorized code. In addition to commercial off-the-shelf software, malicious code also may be present in custom-built software. This could include, for example, logic bombs, back doors, and other types of cyber attacks that could affect organizational missions and business functions.*

In situations where traditional malicious code protection mechanisms are not capable of detecting malicious code in software (e.g., logic bombs, back doors), SCG must rely instead on other risk mitigation measures to include, for example, secure coding practices, trusted procurement processes, configuration management and control, and monitoring practices to help ensure that software does not perform functions other than those intended.

NIST SP 800-83, Revision 1, Guide to Malware Incident Prevention and Handling for Desktops and Laptops, and current anti-malware vendor guidance must be used as guidance when implementing malicious code protection.

The SCGSC System Security Plan (SSP) shall adopt a defense-in-depth strategy that integrates firewalls, screening, routers, wireless intrusion detection systems, antivirus software, encryption, and strong authentication management to ensure information security solutions and secure connections to external interfaces are consistently enforced.

For moderate and high information systems (the SCGSC is a moderate information system):

- Malicious code protection mechanisms must be centrally managed. Central management must include server-based solutions, not client-based. The server-based solution must automatically check for and push out updates.
- The information system must automatically update malicious code protection mechanisms (including signature definitions).
- The information system must be configured to prevent non-privileged users from circumventing malicious code protection capabilities.

### **5.3 SI-4 – Information System Monitoring**

Events on the information system must be monitored in accordance with defined monitoring objectives and information system attacks must be detected.

**Note:** *Information system monitoring includes external and internal monitoring. External monitoring includes the observation of events occurring at the system boundary (i.e., part of perimeter defense and boundary protection). Internal monitoring includes the observation of events occurring within the system (e.g., within internal organizational networks and system components). Information system monitoring capability is achieved through a variety of tools and techniques (e.g., intrusion detection systems, intrusion prevention systems, malicious code protection software, audit record monitoring software, network monitoring software).*

Unauthorized use of the system must be identified.

Events on the information system must be monitored in accordance with the SSP.

The granularity of information collected must be determined based upon SCG monitoring objectives and the capability of the information system to support such activities.

SCG shall obtain legal opinion with regard to information system monitoring activities in accordance with applicable federal laws, Executive Orders, directives, policies, or regulations.

SCG shall heighten the level of information system monitoring activity whenever there is an indication of increased risk to SCG Secure Cloud operations, assets, personnel, other organizations, or the Nation based on law enforcement information, intelligence information, or other credible sources of information.

The information system must be configured to monitor inbound and outbound communications for unusual or unauthorized activities or conditions including, but not limited to:

- Internal traffic that indicates the presence of malicious code within an information system or propagating among system components.



- The unauthorized export of information.
- Attack signatures.
- Signaling to an external information system.
- Localized, targeted, and network-wide events.

Evidence of malicious code must be used to identify potentially compromised SCGSC components.

Automated tools must be employed to support near real-time analysis of events.

The SCGSC must be configured to provide a near real-time alert when indications of compromise or potential compromise occur from the following sources:

- Audit records.
- Input from malicious code protection mechanisms.
- Intrusion detection and prevention mechanisms.
- Boundary protection devices, such as firewalls, gateways, and routers.

The SCGSC must be configured to prevent non-privileged users from circumventing intrusion detection and prevention capabilities.

NIST SP 800-61, Revision 2, Computer Security Incident Handling must be used as guidance on responding to attacks through various types of security technologies.

NIST SP 800-83, Revision 1, must be used as guidance on responding to detecting malware-based attacks.

NIST SP 800-92, Guide to Computer Security Log Management must be used as guidance on monitoring and analyzing computer security event logs.

NIST SP 800-94, Guide to Intrusion Detection and Prevention Systems (IDPS) must be used as guidance on intrusion detection and prevention.

#### **5.4 SI-5 – Security Alerts, Advisories, and Directives**

The IT Director shall receive information system security alerts, advisories, and directives from designated external organizations on an ongoing basis.

Internal security alerts, advisories, and directives must be generated, as deemed necessary.

Security alerts, advisories, and directives must be disseminated to appropriate IT security personnel. Information system and security personnel shall check for security alerts, advisories, and directives on an ongoing basis. All security alerts, advisories, and directives must be from reputable sources (i.e., vendors, manufacturers, government agencies, ISSO).

Security directives must be implemented in accordance with established time frames, or the degree of noncompliance must be reported to the ISSO.

**Note:** *Security alerts and advisories are generated by US-CERT to maintain situational awareness across the federal government. Security directives are issued by OMB or other designated organizations with the responsibility and authority to issue such directives. Compliance with security directives is essential due to the critical nature of many of these directives and the potential immediate adverse effects on organizational operations and assets, individuals, other organizations, and the Nation should the directives not be implemented in a timely manner.*

The types of actions to be taken in response to security alerts/advisories must be documented.

The IT Director and his team shall take appropriate actions in response to security alerts/advisories.

The IT Director shall maintain a repository of the alerts and advisories, including related communications (i.e., responses, questions, concerns) from other IT security personnel.

The IT Director shall maintain contact with special interest groups (e.g., information security forums) that:

- Facilitate sharing of security-related information (e.g., threats, vulnerabilities, and latest security technologies).
- Provide access to advice from security professionals.
- Improve knowledge of security best practices.

NIST SP 800-40, Revision 3 must be used as guidance on monitoring and distributing security alerts and advisories.

## **5.5 SI-7 – Software and Information Integrity**

The SCGSC must be configured to detect unauthorized changes to software and information.

Integrity is verified by reviewing system logs to monitor unauthorized access and changes to the system and looking for evidence of information tampering, errors, and omissions.

Good software engineering practices must be employed on the SCGSC with regard to commercial off-the-shelf integrity mechanisms and tools must be used to automatically monitor the integrity of the information. The mechanism used should be able to provide a means to determine the date and time a resource was last modified or accessed depending on sensitivity.

SCG shall assess the integrity of the SCGSC system using BIOS diagnostic tests (memory, hard drive, etc.) to verify firmware integrity. 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.

## **5.6 SI-8 – Spam Protection**

Spam protection mechanisms must be employed at information systems entry and exit points (e.g., firewalls, web servers, proxy servers) and at workstations, servers, or mobile computing devices on the network.

Spam protection mechanisms are centrally managed.

Spam protection mechanisms must be used to detect and take action on unsolicited messages transported by e-mail, e-mail attachments, web accesses, or other common means.

Spam protection mechanisms (including signature definitions) must be updated when new releases are available. Updates are implemented in accordance with SCGSC configuration management policy and procedures.

Spam protection mechanisms must be configured to perform the following:

- Maintain a list of authorized Internet Protocol (IP) addresses or ensure authorized sources will always be allowed.
- Block a list of senders that have been verified as sending spam.
- Allow users to tag or block suspected spam messages that were not detected by the spam mechanism.

SCG shall give consideration to using spam protection software products from multiple vendors (e.g., using one vendor for boundary devices and servers and another vendor for workstations).

## **5.7 SI-9 – Information Input Restrictions**

The capability to input information to the SCGSC must be restricted to authorized personnel.

**Note:** *Restrictions on organizational personnel authorized to input information to the information system may extend beyond the typical access controls employed by the system and include limitations based on specific operational/project responsibilities.*

## **5.8 SI-10 – Information Input Validation**

The SCGSC must be configured to check the validity of information inputs. The checks for input validation must be verified as part of system testing.

The SCGSC must be configured to check all arguments or input data strings submitted by users, external processes, or untrusted internal processes.

- The information system must validate all values that originate externally to the application program itself, including arguments, environment variables, and information system parameters.
- The information system must trust only reliable external entities that have been identified by authorized SCG personnel.

Rules for checking the valid syntax and semantics of SCGSC inputs (e.g., character set, length, numerical range, acceptable values) must be in place to verify that inputs match specified definitions for format and content.

The information system must be configured to perform the following input validations:

- Type checks – Checks to ensure that the input is, in fact, a valid data string and not any other type of object.
  - This includes validating that input strings contain no inserted executable content or active content that can be mistakenly interpreted as instructions to the system, including, but not limited to, Trojan horses, malicious code, metacode, metadata, or metacharacters, Hypertext Markup Language (HTML), Extensible Markup Language (XML), JavaScript, Structured Query Language (SQL) statements, shell script, and streaming media.
  - Inputs passed to interpreters must be prescreened to prevent the content from being unintentionally interpreted as commands.
- Format and syntax checks – Checks to verify that data strings conform to defined formatting and syntax requirements for that type of input.
- Parameter and character validity checks – Checks to verify that any parameters or other characters entered, including format parameters for routines that have formatting capabilities, have recognized valid values.
  - Any parameters that have invalid values must be rejected and discarded.
  - Web server applications must be configured to prohibit invalid data from web clients in order to mitigate web application vulnerabilities including, but not limited to, buffer overflow, cross-site scripting, null byte attacks, SQL injection attacks, and HTTP header manipulation.

Invalid inputs or error statements must not give the user sensitive data, storage locations, database names, or information about the application or SCGSC's architecture.

## **5.9 SI-11 – Error Handling**

The SCGSC must be configured to identify potentially security-relevant error conditions.

The structure and content of error messages must be carefully considered by information system personnel. The criticality or severity level of error messages for the SCGSC must be determined.

The SCGSC must be configured to reveal error messages only to authorized personnel. System error messages must be revealed only to authorized personnel (e.g., system administrators, maintenance personnel).

Error messages generated by the SCGSC must provide information necessary for corrective actions without revealing sensitive information (e.g., home addresses) or potentially harmful information in error logs and administrative messages that could be exploited by adversaries.

- Error messages revealed to users must not include file pathnames or system architecture information.
- Alert error messages revealed to the administrator must include file pathnames or system architecture information and must be written to the application's error log and audit trail.

The extent to which the SCGSC is able to identify and handle error conditions must be guided by operational requirements.

The SCGSC's error-handling mechanisms must enable the administrator to configure the application to gracefully terminate processes, when appropriate in response to various errors and failures.

### **5.10 SI-12 – Output Handling and Retention**

Both information within and output from the SCGSC must be handled and retained in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements.

Output handling and retention requirements must cover the full life cycle of the information, which in some cases, may extend beyond the disposal of the information system.

- Records with expired retention periods must be disposed of in accordance with NIDDK guidance.
- When information (either electronic or printed) no longer becomes necessary, the media must be destroyed in accordance with the media protection procedures and standards found in the Media Protection Policy and Procedures.

SCG shall ensure that all personnel receive security awareness training on the proper handling and protection of information outputs. The SCGSC Contingency Plan, Disaster Recovery Plan, and Security Awareness and Training Policy and Procedures contain requirements on security awareness training.

## **6. Roles and Responsibilities**

The IT Director and SCG President are responsible for establishing and enforcing the SCGSC System and Information Integrity Policy and Procedures. The IT Director and SCG President review the policies and procedures periodically to ensure they are up to date and adequate for managing risks from system flaws/vulnerabilities, malicious code,

unauthorized code changes, and inadequate error handling. The IT Director is responsible for implementing the system and information integrity program to ensure that SCG is using security best practices with regard to SCGSC system configuration, security, and error handling.

The IT Director is responsible for:

- Developing and maintaining an inventory of the SCG Secure Cloud system and its components that identifies the hardware equipment, operating systems, and software applications in operation.
- Monitoring and coordinating with each vendor for software patch release support.
- Installing and testing software patches, service packs, and hot fixes for the SCGSC.
- Making changes to configuration settings for flaw remediation.
- Removing software or disabling functions, ports, protocols, and/or services as necessary.
- Ensuring that information security patches are installed in accordance with the SCGSC Configuration Management Plan.
- Monitoring security sources for vulnerability announcements (i.e., both patch and non-patch remediation) and emerging threats that correspond to the software within the SCGSC's inventory.
- Reporting information systems containing software affected by recently announced software flaws (and potential vulnerabilities resulting from those flaws) to designated officials (i.e., SCG President, Vice President of Administration, Program Manager, NIDDK ISSO, and NIDDK System Owner) with information security responsibilities.
- Disseminating vulnerability and remediation information to system administrator and security personnel.
- Training/instructing personnel on how to apply vulnerability and configuration management remediations.
- Prioritizing vulnerabilities and remediation actions in priority order based on the individual vulnerability criticality or severity ratings.
- Creating and maintaining a database of remediations that need to be applied to the SCG Secure Cloud resources.
- Monitoring vulnerability remediation.
- Testing software updates related to flaw remediation (including patches, services packs, and hot fixes) for effectiveness and potential side effects on the SCG Secure Cloud system before installation.
- Assessing whether any significant disadvantages outweigh the benefits of installing a patch and whether remediation should be delayed, based on the testing.

- Developing a schedule for the release and implementation of patches, service packs, and hot fixes in coordination with system security personnel.
- Supervising prompt installation of all security-relevant software updates (e.g., patches, service packs, and hot fixes) SCGSC IT security personnel.
- Tracking and verifying vulnerability and flaw remediation actions.
- Updating the inventory of system and components when flaw remediation and vulnerability mitigation activities are completed to reflect current software versions and configurations, and notifying appropriate officials that activities are completed.
- Employing malicious code protection mechanisms at information system entry and exit points (e.g., firewalls, web servers, proxy servers, remote-access servers).
- Configuring malicious code protection to block at gateways and quarantine at host, validating quarantined code before releasing to user, and cleaning quarantined malware as appropriate.
- Deploying standard malicious code protection software on the SCGSC servers that is configured to scan for malicious code on a continuous basis and ensuring that update releases are tested and installed promptly.
- Updating malicious code protection mechanisms whenever new releases are available and in accordance with SCG Secure Cloud configuration management policy, procedures, and standards.
- Configuring malicious code protection mechanisms to perform periodic scans of the SCGSC system daily and real-time scans of files from external sources as the files are downloaded, opened, or executed in accordance with SCG security policy.
- Configuring malicious code protection mechanisms to block and quarantine malicious code and send an alert to an administrator in response to malicious code detection.
- Conducting internal and external Information system monitoring through a variety of tools and techniques (e.g., intrusion detection systems, intrusion prevention systems, malicious code protection software, audit record monitoring software, network monitoring software).
- Ensuring that events on the SCGSC are monitored in accordance with the SSP.
- Configuring the SCGSC to provide a near real-time alert when indications of compromise or potential compromise occur, and to prevent non-privileged users from circumventing intrusion detection and prevention capabilities.
- Checking for/receiving information system security alerts, advisories, and directives from designated external organizations on an ongoing basis; generating internal security alerts, advisories, and directives, as deemed necessary; and disseminating security alerts, advisories, and directives to appropriate IT security personnel.

- Implementing security directives in accordance with established time frames, or reporting the degree of noncompliance to the ISSO.
- Documenting the types of actions to be taken in response to security alerts/advisories and leading the team to take the appropriate actions in response to security alerts/advisories.
- Maintaining a repository of the security alerts and advisories, including related communications (i.e., responses, questions, concerns) from other IT security personnel.
- Maintaining contact with special interest groups (e.g., information security forums) that share security-related information (e.g., threats, vulnerabilities, and latest security technologies), provide advice to security professionals, and improve knowledge of security best practices.
- Configuring the SCGSC to detect unauthorized changes to software and information.
- Reviewing system logs to monitor unauthorized access and changes to the system and looking for evidence of information tampering, errors, and omissions.
- Ensuring that good software engineering practices are employed on the SCGSC with regard to commercial off-the-shelf integrity mechanisms and that tools are used to automatically monitor the integrity of the information.
- Assessing the integrity of the SCGSC system using BIOS diagnostic tests (memory, hard drive, etc.) to verify firmware integrity. Using the Windows Error-Checking tool to verify the integrity of the Windows operating system, and automatically fix performance issues and file and system errors. Performing these integrity checks monthly and following any security-related events.
- Ensuring that spam protection mechanisms are employed at SCGSC entry and exit points, are centrally managed, and are effective for detection and protection.
- Updating spam protection mechanisms when new releases are available and implementing them in accordance with SCGSC configuration management policy and procedures.
- Selecting spam protection software products from multiple vendors.
- Ensuring that the capability to input information to the SCGSC is restricted to authorized personnel.
- Configuring the SCGSC to check the validity of information inputs, and verifying the checks for input validation as part of system testing.
- Configuring the SCGSC to identify potentially security-relevant error conditions, ensuring that error messages are revealed only to authorized personnel, and provide information necessary for corrective actions without revealing sensitive information or potentially harmful information.
- Ensuring that the information within and output from the SCGSC is handled and retained in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements.



- Ensuring that all personnel responsible for the SCGSC receive security awareness training on the proper handling and protection of information outputs.

## **Appendix A: References**

The following references illustrate public laws that have been issued on the subject of information security and should be used to demonstrate SCG responsibilities associated with protection of the SCG Secure Cloud system.

- United States Department of Commerce National Institute for Standards and Technology (NIST) Special Publication 800-53, Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations, April 2013.
- United States Department of Commerce National Institute for Standards and Technology (NIST) Special Publication 800-100, Information Security Handbook: A Guide for Manager, October 2006.
- United States Department of Commerce National Institute for Standards and Technology (NIST) Special Publication 800-40, Revision 3, Guide to Enterprise Patch Management Technologies”, July 2013.
- United States Department of Commerce National Institute for Standards and Technology (NIST) Special Publication 800-83, Revision 1, Guide to Malware Incident Prevention and Handling for Desktops and Laptops, July 2013.
- United States Department of Commerce National Institute for Standards and Technology (NIST) Special Publication 800-61, Revision 2 Computer Security Incident Handling Guide, April 2012.
- United States Department of Commerce National Institute for Standards and Technology (NIST) Special Publication 800-92, Guide to Computer Security Log Management, September 2006.
- United States Department of Commerce National Institute for Standards and Technology (NIST) Special Publication 800-94, Guide to Intrusion Detection and Prevention Systems (IDPS), February 2007.
- United States Department of Commerce National Institute for Standards and Technology (NIST) Special Publication 800-45, Guidelines on Electronic Mail Security, February 2007.