



The Scientific Consulting Group, Inc.

Incident Response Policy and Plan

for the

SCG Secure Cloud System

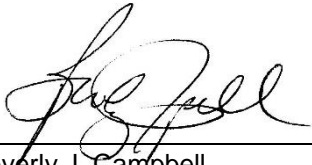
Version 1.5

June 14, 2016

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

Incident Response Policy and Plan Approval

The Incident Response Policy and Plan must be approved by the SCG President/Business Owner and the Information Technology (IT) Director. The undersigned acknowledge that they have reviewed the SCG Secure Cloud Incident Response Policy and Plan and agree with the information presented in this document. The SCG President and IT Director will review this Incident Response Policy Plan annually and revise the plan as necessary to address system/organizational changes or problems encountered during plan implementation, execution, or testing. Any changes to the Incident Response Policy and Plan will be coordinated with, and approved by, the undersigned or their designated representatives.



Beverly J. Campbell
President

6/14/16

DATE



Chuck C. Lee
IT Director

6/14/16

DATE

Document Information and Revision History

Document Owners	
SCG Information Technology Director	
Name	Chuck Lee
Contact Number	(301) 670-4990; (301) 366-3273 (Cell)
E-mail Address	clee@scgcorp.com
SCG President	
Name	Beverly J. Campbell
Contact Number	(301) 670-4990; (301) 461-1109 (Cell)
E-mail Address	bcampbell@scgcorp.com

Document Revision and History			
Revision	Date	Author	Comments
1.0	1/30/15	K. Martinez	Detailed outline
1.1	2/4/15	B. Campbell/C. Lee	Draft Plan
1.2	2/26/15	B. Campbell	Minor revisions to document
1.3	2/28/15	B. Campbell	Minor revisions to document
1.4	4/20/16	B. Campbell	Revisions to document
1.5	6/14/16	B. Campbell	Revisions to 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

Preface.....	1
1. Purpose.....	2
2. Scope.....	3
3. Applicability	3
4. Exceptions	3
5. Consequences of Non-Compliance	3
6. Maintenance	3
7. Definitions	4
8. Incident Response Policy.....	5
8.1 Incident Response Training and Testing.....	5
8.2 Incident Handling, Monitoring, Reporting, and Assistance	5
8.3 Incident Response Plan	6
8.4 Audience	7
8.5 Responsibilities	7
9. Incident Response Plan	7
9.1 The Requirements for Incident Response.....	7
9.2 Objectives and Effectiveness Targets	8
9.3 Organization and Structure	9
9.4 Roles and Responsibilities	10
9.4 Guidance and Procedures.....	13
9.4.1 Preparation/Pre-Incident Actions.....	14
9.4.2 Detection and Analysis/Incident Recognition.....	16
9.4.3 Incident Response Containment, Eradication, and Recovery.....	24
9.4.4 Post-Incident Activities	29
9.5 Vulnerability Management.....	31
9.6 Information Dissemination Control	32
9.7 Incident Response Plan Compliance Requirements	33
9.8 Testing, Training, and Exercise (TT&E)	33
9.9 Incident Response Plan Maintenance	33
9.10 Distribution/Access List	34
Appendix A: HHS/NIH and SCG Incidence Response Policy and Procedures	35

Appendix B: Reporting Formats	36
Appendix C: Incident Response Team Contact List	38
Appendix D: NIDDK Contacts	39
Appendix E: Glossary	40
Appendix F: Incident Response Log	42
Appendix G: Acronyms.....	43

List of Figures

Figure 1. Incident Response Procedure Model	10
---	----

List of Tables

Table 1. Performance Metrics of the SCG IRT	8
Table 2. Roles and Responsibilities	10
Table 3. Incident Handling Checklist	20
Table 4. Incident Procedures by Priority Level	24
Table 5. Actions Taken to Manage SCGSC Vulnerability.....	31

Preface

SCG was founded in 1991 with a vision of harnessing leading-edge technologies to develop innovative solutions and quality products that improve our health and protect our environment. From our first contracts to support the National Cancer Institute's Division of Cancer Prevention and the U.S. Environmental Protection Agency's Office of Research and Development, we have remained true to our vision. Over the past 20 years, we have expanded our staff and capabilities, gained new clients, and worked diligently to constantly improve the quality of our services. As SCG grew, so did our reputation for quality and integrity. Since 1991, we have been awarded more than 375 contracts to provide health and environmental consulting services to a variety of government and private clients. We now have more than 50 talented, professional staff members who offer our clients a diverse base of experience and expertise in health and environmental sciences.

Commitment to meeting our clients' needs is the key to SCG's success. Our mission is to assist our clients in meeting their goals and fulfilling their responsibilities of safeguarding human health and maintaining a safe and healthy environment. We have cultivated longstanding working relationships with many clients because we go beyond understanding how our clients are organized and function to learn about the challenges they face and the constraints they must work under, whether it is budget reductions, security issues, complicated reporting requirements, legislative mandates, resource realignments, or others. We perform with the ultimate impact in mind, always seeking to enhance the mission of the agencies and programs that we support.

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

- Support for the Information Requests for NIDDK Clearinghouses and Several Campaign-Focused Programs and Exhibit Support;
- Support for Content Development and Maintenance for Multiple Health Information Products; Support for Printing, Print on Demand Services;
- Support for Materials Receipt, Storage, and Dissemination, Integrated Tracking System;
- Support Services for NIDDK's Digital Channels Including Website Development and Website Usability Testing;
- Campaign Support for numerous NIDDK Health Campaigns including: NKDEP, Weight-Control Information Network's Sisters Together Campaign, Celiac

Disease Awareness and Bowel Control Awareness Campaigns, and NDEP; Conference/Exhibit Logistics and Meeting Support;

- Market Research and Evaluation Services for OCPL Programs; and
- Message Promotion Services.

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

NIDDK is one of the Institutes of the National Institutes of Health (NIH) in Bethesda, Maryland. NIH is part of Department of Health and Human Services (HHS). The Incident Response Plan will make clear that the SCG Secure Cloud system is an Infrastructure as a Service (IaaS) being contracted by NIDDK. NIDDK will be the interface to NIH incident response personnel, as NIH is the interface to HHS. This document establishes a unified approach for handling security incidents that incorporates those principles of interactions.

1. Purpose

The purpose of the SCGSC Incident Response Policy and Plan is to provide the policy that defines the incident response requirements and mechanisms to be implemented for the SCGSC and to identify incident handling and response procedures to resolve and recover from a security incident involving the SCGSC system. SCG is required by NIDDK (through NIH and HHS security policy) to establish an Incident Response Team (IRT) to respond to computer attacks. These computer attacks may be directed against the SCG Secure Cloud system or other systems that impact the SCGSC including environmental control systems and perimeter control systems.

SCG has established a successful incident response capability with our Information Technology (IT) group. SCG has established clear procedures for prioritizing the handling of incidents and effective methods of collecting, analyzing, and reporting data associated with these incidents.

This document provides the incident response policy and detailed incident response procedures for implementation within SCG for the SCG Secure Cloud system. The requirements outlined in this document are **mandatory**, and are designed to standardize incident handling and reporting for the SCGSC system.

2. Scope

This document provides policy, mitigation strategies, and responses to intentional or inadvertent information security incidents affecting the confidentiality, integrity, and availability of the SCG Secure Cloud system. It also provides procedures for the expected actions to respond to computer security incidents. The scope includes coordination among the IRT and the NIDDK Information System Security Officer (ISSO) regarding common incidents across the SCGSC system.

The document does not address physical disruptions to, or the loss of, information, information systems, or networks as a result of disasters impacting the information infrastructure. These non-cyber events and responses are covered in the SCG Secure Cloud System Contingency Plan (CP) and Disaster Recovery Plan (DRP).

3. Applicability

The provisions and guidelines of this plan apply to the SCG Secure Cloud and all SCG personnel who support information security incident response for the SCGSC system. These include, but are not limited to, system administrators, developers, and information security personnel.

4. Exceptions

Exceptions to this policy must be formally documented with a valid business justification and submitted to the SCG President and IT Director for review. All requests will have their potential business and security risks identified, analyzed, and determined to be either acceptable or unacceptable. When the President and IT Director determine the risks are acceptable, they may approve the request and document the exception in a revision or an appendix to this document.

5. Consequences of Non-Compliance

Given the importance that proper implementation of this Incident Response Plan holds for mission performance and readiness, failure to comply with this policy and execute the provisions of this plan through negligence or willful disregard may result in adverse administrative or disciplinary action. Subject to applicable laws and regulations, all applicable entities found in violation of this policy are subject to further actions/discussions by SCG's Human Resources Department. Failure to comply with the incident response policy and plan for the SCGSC could result in loss of access to the SCGSC system, disciplinary action, employment termination, or prosecution depending on the circumstances.

6. Maintenance

SCG is responsible for updating this document and all supporting documents, procedures, standards, and guidelines at least annually and after any significant change, including:

- Policy or rules change
- Approver or policy owner leaves the company or changes roles
- Significant change to the definitions
- Introduction of new systems/hardware
- Identification and remediation of security vulnerabilities
- Regulatory changes
- Changes to the risk profile.

7. Definitions

An *event* is any observable transmission of information within a system or network. Examples of events include a user connecting to a file share, a server receiving a request for a web page, a user sending e-mail, and a firewall blocking a connection attempt. *Adverse events* are events with negative consequences, such as system crashes, packet floods, unauthorized use of system privileges, unauthorized access to sensitive data, and execution of malware that destroys data. This plan addresses only adverse events that are computer security-related, not those caused by natural disasters, power failures, etc.

An *incident* is any violation event that compromises the confidentiality, integrity, or availability of an information system. Examples of incidents are:

- An attacker commands a botnet to send high volumes of connection requests to a web server, causing it to crash.
- Users are tricked into opening a “quarterly report” sent via e-mail that is actually malware; running the tool has infected their computers and established connections with an external host.
- An attacker obtains sensitive data and threatens that the details will be released publicly if the organization does not pay a designated sum of money.
- A user provides or exposes sensitive information to others through peer-to-peer file sharing services.

A computer incident is an indication of an attempted or achieved unauthorized entry and/or information attack on a SCG Secure Cloud system or network. Information incidents by categories include:

- Network penetration
- Root or user account compromise
- Denial of service
- Website defacing
- Malicious code and virus
- Probes and scans

- Password access
- Other (incidents not applicable to above categories).

8. Incident Response Policy

This section specifies the incident response requirements, mechanisms, and provisions that are to be applied within the SCGSC system.

8.1 Incident Response Training and Testing

- A formal Incident Response program must be implemented for the SCGSC system. It is the responsibility of the IT Director to train personnel in incident response roles and responsibilities. Incident response training must be conducted on an annual basis for refresher purposes. **(IR-2.1)**
- In order to determine the effectiveness of its incident response capability, SCG must test the incident response capability for the information system on an annual basis using defined tests and/or exercises that are in accordance with NIST SP 800-61. The testing results of the incident response exercise must be documented. **(IR-3.1)**
- It is the responsibility of the IT Director to define and document the types of tests or exercises that are in accordance with NIST SP 800-61. Furthermore, it is the responsibility of the IT Director to provide test plans to the NIDDK on an annual basis. Test plans must be approved and accepted by the NIDDK ISSO *prior* to testing. **(IR-3.1)**

8.2 Incident Handling, Monitoring, Reporting, and Assistance

- As part of the incident handling capability, mechanisms must be in place to address each of the following phases **(IR-4.1.a)**:
 - Preparation
 - Detection and analysis
 - Containment
 - Eradication
 - Recovery
- It is the responsibility of the IT Director to coordinate incident handling activities with contingency planning activities. **(IR-4.1.b)**
- For ongoing incident handling activities, lessons learned must be incorporated into all incident response procedures, training, and tests/exercises. Changes must be implemented accordingly. **(IR-4.1.c.)**
- Automated mechanisms must be implemented to support the incident handling process. **(IR-4.1.1)**

- Mechanisms must be in place to track and document information system security incidents. **(IR-5.1)**
- Personnel are required to report all suspected security incidents to IT Director and Program Manager within the time periods that align with the US-CERT incident reporting timelines as specified in the NIST SP 800-61. Personnel must also report security incident information to designated authorities. **(IR-6.1)**
- Automated mechanisms must be in place to support the reporting of security incidents. **(IR-6.1.1)**
- To support the handling and reporting of security incidents, it is the responsibility of the IT Director to provide incident response support resource for users of the information system. **(IR-7.1)**
- Automated mechanisms must be implemented to increase the availability of incident response-related information and support. **(IR-7.1.1)**
- SCG must implement a direct, cooperative relationship between its incident response capability and external providers of the SCGSC system protection capability. Furthermore, the SCG Incident Response Team members must be identified to the external providers. **(IR-7.1.2)**

8.3 Incident Response Plan

- A formal Incident Response Plan must be developed that:
 - Provides SCG with a roadmap for implementing its incident response capability;
 - Describes the structure and organization of the incident response capability;
 - Provides a high-level approach for how the incident response capability fits into the overall organization;
 - Meets the unique requirements of the organization, which relate to mission, size, structure, and functions;
 - Defines reportable incidents;
 - Provides metrics for measuring the incident response capability within SCG;
 - Defines the resources and management support needed to effectively maintain and mature an incident response capability; and
 - Is reviewed and approved by the SCG IT Director and President. **(IR-8.1.a)**
- The Incident Response Plan must be distributed to the SCG employees who are responsible for incident response for the SCGSC system and the NIDDK system owner and ISSO. **(IR-8.1.b)**

- The Incident Response Plan must be reviewed on an annual basis and whenever there are changes to the information system environment or problems encountered during plan implementation, execution and testing. **(IR-8.1.c/IR-8.1.d)**
- It is the responsibility of the IT Director to communicate incident response plan changes to SCG employees involved in incident response for the SCGSC and the NIDDK system owner and ISSO. **(IR-8.1.e)**

8.4 Audience

The audience is SCG employees involved with incident response for the SCGSC system.

8.5 Responsibilities

The following table identifies who within SCG is responsible for developing and implementing and approving the incident response policy. The following definitions apply:

- **Responsible Parties** – the persons responsible for developing and implementing the policy.
- **Approver** – the person or persons required to approve the final policy implementation or amendment.

Policy	Responsible Parties	Responsibilities	Approver
Incident Response Policy	IT Director, Program Manager, System Owner, and ISSO	Support and approve the policy	SCG President and IT Director
	Incident Response Team	Develop, implement, and maintain the policy at least annually	SCG President and IT Director
	IT Director	Enforces the policy and communicates any changes	SCG President
	SCG Employees	Acknowledge and comply with policy	IT Director and Program Manager

9. Incident Response Plan

9.1 The Requirements for Incident Response

In accordance with National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Rev. 4, HHS defines a computer security incident as “a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard computer security practices.” If you suspect an information security

or privacy related incident, please contact your OPDIV Chief Information Security Officer or the HHS Computer Security Incident Response Center (HHS CSIRC). The HHS CSIRC can be reached at [HHS CSIRC@hhs.gov](mailto:HHS-CSIRC@hhs.gov) or 866-646-7514.

These requirements for incident response and reporting are part of the federal government's effort to attain the goals outlined in Presidential Decision Directive 63 (PDD 63).

The following documents establish or provide the basis for computer incident response:

- Presidential Decision Directive 63, *Critical Infrastructure Protection*
- Office of Management and Budget's (OMB) Circular No. A-130, Appendix III
- Federal Information Processing Standards (FIPS) 200, *Minimum Security Requirements for Federal Information and Information Systems*, March 2006
- OMB Memorandum M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*, May 2007
- HHS – Policy for IT Security and Privacy Incident Reporting and Response 4/05/2010

9.2 Objectives and Effectiveness Targets

SCG's IRT has been established to protect and defend the SCG Secure Cloud system against intrusive, abusive, and destructive behavior from both internal and external sources. To meet this goal, the objectives, and target performance metrics of the SCG IRT and this plan are listed in Table 1.

Table 1. Performance Metrics of the SCG IRT

No.	Objective	Target
1.	Proactively prepare for and practice the implementation of incident response process.	Exercise the IRP annually, or when significant personnel turnover in key positions has occurred.
2.	Identify incidents rapidly.	Recognize and identify an incident or event within one (1) hour of the appearance of suspicious indicators.
3.	Initiate comprehensive record-keeping immediately to ensure critical observations and technical details are captured to support analytical needs.	System users, the IRT and system administrators initiate an incident response log upon recognition of any suspicious activity. System administrators begin documenting and capturing system/network activity upon recognition of suspicious behavior reported by a user.
4.	Rapidly report available details to the HHS CSIRC and NIDDK ISSO and notify interfacing systems and network owners of suspected events and incidents.	The IRT notifies the HHS Computer Security Incident Response Center (HHS CSIRC) and NIDDK Information System Security Officer (ISSO) within one (1) hour after the incident

No.	Objective	Target
		and issues an initial Incident Report in accordance with reporting timelines provided in the HHS' Policy for IT Security and Privacy Incident Reporting and Response.
5.	Help users and component elements limit the duration of the incident.	The IRT provides immediate guidance to users reporting suspicious activity, and follows up by providing specific mitigation instructions within one (1) hour of receipt of HHS CSIRC guidance.
6.	Minimize operational impacts from the loss or compromise of information, applications, systems, and networks.	Minimal loss of mission capability.
7.	Develop systematic incident response procedures to promote effective recovery.	Review and update the IRP and incorporate lessons learned from incidents and IRP exercises.
8.	Carefully consider operational requirements along with forensic and legal requirements in the development of mitigation actions.	Minimal compromise and minimal loss of data required for technical analysis unless IRT determines potentially serious operational consequences could result.
9.	Immediately acknowledge and act on, as appropriate, HHS CSIRC requests for data.	Report compliance within the specified time period in the required format.

9.3 Organization and Structure

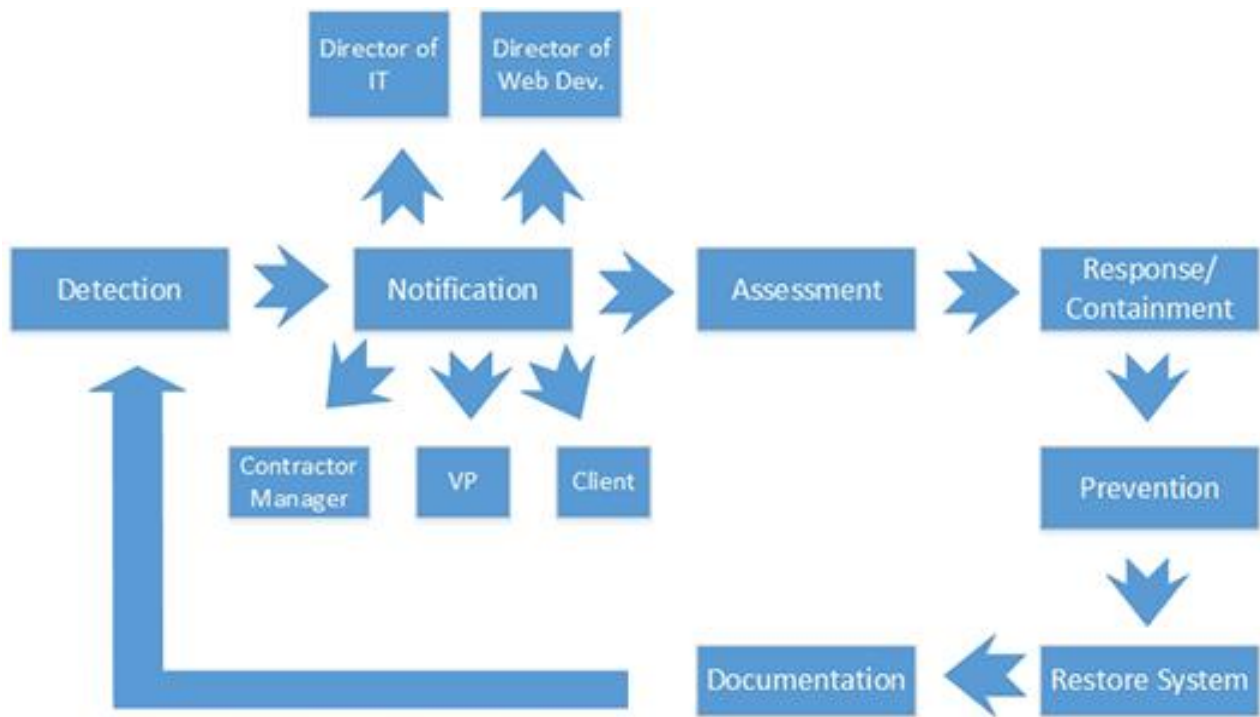
The IRT personnel for the SCG Secure Cloud system consist of the IT Director, Web Development Director, Program Manager, Vice President of Administration, IT Systems Specialists, and the SCG President. Members of our IRT have excellent technical skills, including system administration, network administration, cybersecurity, programming, web development, IT troubleshooting, crisis management, and intrusion detection and remediation. In addition, every team member has good problem-solving skills and critical-thinking abilities. Our team includes at least one highly proficient person in each major area of technology (e.g., commonly attacked operating systems and applications), as well as experience in network intrusion detection and malware analysis. If necessary, SCG will bring in technical specialists who are not normally part of the IRT to address an incident. SCG's incident response procedure model is presented in Figure 1.

The strong performance of the SCG IRT has allowed it to establish a solid incident handling and security foundation. The program is focused on not only sustaining the current maturity and effectiveness, but making forward progress and significant improvement by incorporating the latest guidance and best practices. SCG's incident handling procedures continue to evolve to meet cybersecurity challenges and incorporate NIH/HHS requirements.

Contact information for personnel involved in incident response resides in the SCG IT Director's office. The contact information also is available in the Vice President of Administration's office. In addition to the updated point of contact list, SCG also maintains (electronic and hardcopy) the SCGSC Incident Response Plan in both of

these locations. A hardcopy of the plan also is maintained in the SCG Secure Cloud system server room and an electronic version is stored on the server.

Figure 1. Incident Response Procedure Model



9.4 Roles and Responsibilities

The roles and responsibilities for incident response have been identified and are shown in Table 2.

Table 2. Roles and Responsibilities

Role	Responsibilities
IRT Manager/IT Director	<ul style="list-style-type: none"> Implements and maintains the Incident Response Plan. Coordinates incident response activities at SCG and with the NIH/HHS. Ensures the IRP supports incident response process. Works with HHS CSIRC/NIDDK ISSO to execute an IRP test annually. Updates the IRP to incorporate lessons learned. Develops incident management mitigation strategies. Manages all SCG related incidents throughout the incident response lifecycle. Identifies all incidents relating to the SCG Secure Cloud system.

Role	Responsibilities
	<ul style="list-style-type: none"> • Reviews and edits incident description. • Researches and collects pertinent information relating to the incident if Privacy Officer (PO) decides further research is needed. • Ensures the incident is closed. • Initiates an Incident Response Log (see Appendix E) when an event is suspect. • Ensures documentation of all incidents supports technical analysis and legal evidentiary requirements. • Develops and implements incident management mitigation strategies. • Assesses the operational impacts of incidents. • Provides subject matter expertise for guiding specific mitigation and response actions. The individuals assigned to this role will depend upon the type of incident and potential impact. Assignment will be made by the IRT for each specific incident. • Takes containment actions up to and including the immediate shut down of the system to prevent further intrusion or damage to the SCG Secure Cloud system or agency system or other department network or resources. • Makes a determination on the value/sensitivity of the data to the agency mission in concert with the SCG President, Vice President of Administration, and Program Manager. Collaboratively develop a damage determination based on an analysis of the incident. • Prioritizes SCG IT resources to respond to specific incident in coordination with the SCG Security Team. • Documents and distributes "lessons learned" from the incident, upon incident closure • Ensures all incident reports are completed and follow the formats and timeframes outlined in the HHS/NIH incident response policy. • Ensures that the IRT and NIDDK Project Officer has the current names, phone numbers, and e-mail addresses of the personnel responsible for incident handling at SCG. • Ensures the system is tested to determine that vulnerabilities have been corrected or adequately mitigated prior to release into production. • Assigns staff to examine the compromised system to determine what changes occurred to the system and removes all unknown code and software from the compromised system. • Records all events/incidents reported in the SCG Secure Cloud system IRP log.
Vice President of Administration	<ul style="list-style-type: none"> • Receives reports of security events/incidents. • Reports all events/incidents to the SCG President and senior managers and appropriate staff.

SCG Secure Cloud Incident Response Policy and Plan

Role	Responsibilities
	<ul style="list-style-type: none"> Provides the IRT Manager guidance and instructions from SCG senior management.
System Administrators	<ul style="list-style-type: none"> Communicate with the IRT on proper mitigation strategies.
Developers/Users	<ul style="list-style-type: none"> Report all suspicious computer events/incidents to the IT Director. Coordinate and cooperate with the IRT. Complete the annual security and privacy awareness training as required.
SCG President/ Business Owner	<ul style="list-style-type: none"> Approves the incident handling scope within SCG. Ensures incident response personnel are assigned, trained, and understand their responsibilities in the organization incident response process. Provides adequate resources for incident response and support to enable SCG to comply with HHS/NIH and federal requirements. Oversees development of procedures for monitoring, reviewing, approving, and closing incidents. Confirms that procedures for reporting and responding to incidents are documented, and implemented to comply with federal government and SCG policy. Ensures procedures are developed that include mitigation actions necessary to safeguard agency systems/information assets. Takes disciplinary and other appropriate actions to prevent future incidents.
Privacy Officer	<p>In the case of Personal Identifiable Information (PII) incidents, the Privacy Officer:</p> <ul style="list-style-type: none"> Determines if IRT research is needed to deem an incident as a PII breach. Determines if an incident is classified as a PII breach. Provides guidance to SCG on how to mitigate incidents. Decides if a notification letter should be provided and provides letter to subject of PII breach. Determines if any monitoring should be offered and notifies HHS CSIRC when offers have been issued. Performs a privacy analysis to determine if individual privacy data have been compromised. If so, determines the extent of the damage and advises IRT.
HHS Computer Security Incident Response Center (CSIRC)	<ul style="list-style-type: none"> Receives primary notice of a potential incident from within or outside of HHS. Receives and processes Final HHS Containment Report. Confirms incident is closed.
System Owner	<ul style="list-style-type: none"> Acts in partnership with SCG to ensure data protection for the SCGSC system, interacting with the IRT on incident response.

Sensitive But Unclassified/Sensitive Security Information – Disseminate on a Need-To-Know Basis Only

Role	Responsibilities
	<ul style="list-style-type: none"> Provides guidance on the value/sensitivity of the data to NIDDK's mission. Works with the IRT to collaboratively develop a damage determination based on an analysis of the incident. Verifies that incident response personnel in their respective groups understand their responsibilities in the incident handling process. Ensures that SCG's IRT takes actions with guidance from the NIDDK ISSO and Privacy Officer to effectively assess, contain, and recover from SCGSC computer security (CS) incidents. Confirms that incident handling actions taken are in accordance with established policies and procedures including incident close out. Advises and assists as needed the SCG IRT in the assessment and containment actions, as necessary.
SCG Secure Cloud IT Systems Staff	<ul style="list-style-type: none"> Verifies systems have been adequately patched/updated with security controls prior to resumption of normal operations. Conducts system scans in coordination with the IRT. Ensures adequate security controls and countermeasures are in place or implemented. Develops and maintains written procedures for orderly system startup and shutdown. Requests approval from the IRT to return compromised systems/applications to operational status. Ensures compromised systems/applications remain offline and disconnected from the network until approval is received. Takes mitigation and countermeasure actions to prevent incident recurrences by adding procedures or updated parameters/systems. Rebuilds the compromised systems as needed. Preserves and protects the evidence compiled as a result of the investigation or research and ensures forensic evidence has been maintained. Assists in any research or investigation required to determine the extent of any damage done or the impact of the incident/event on the SCGSC system.

9.4 Guidance and Procedures

The incident response process has several phases (new guidance from NIST 800-61, Revision 2, published August 2012). The initial phase involves establishing and training an IRT, and acquiring the necessary tools and resources. During the preparation phase, attempts are made to limit the number of incidents that will occur by selecting and implementing a set of controls based on the results of risk assessments.

Residual risk, however, will inevitably persist after controls are implemented. Therefore, detection of security breaches is necessary to alert the organization whenever incidents occur. In keeping with the severity of the incident, the impact of the incident can be mitigated by containing it and ultimately recovering from it. During this phase, activity often cycles back to detection and analysis. For example, while eradicating a malware incident the organization should investigate to see if additional hosts are infected by malware. After the incident is adequately handled, a report should be issued that details the cause and cost of the incident and the steps that should be taken to prevent future incidents. This section describes the major phases of the incident response process—preparation, detection and analysis, containment, eradication and recovery, and post-incident activity.

9.4.1 Preparation/Pre-Incident Actions

Incident response methodologies typically emphasize preparation. The IT Division should not only establish an incident response capability so the organization is ready to respond to incidents, but also prevent incidents by ensuring systems, networks, and applications are sufficiently secure. At SCG, the IT Division is typically responsible for incident prevention, which is fundamental to the success of the incident response program.

This section provides basic advice on preparing to handle incidents and on preventing incidents.

Preparing to Handle Incidents

The following actions will be taken as part of this plan to attain the best possible defensive posture in advance of future cyber probes or attacks:

- The provisions of the IRP will be incorporated into the security awareness training program to familiarize all personnel with the plan and their responsibilities if a cyber-incident occurs, or a request from the HHS CSIRC/NIH/NIDDK is received.
- The IRT will review current administrative, operational, and support standard operating procedures (SOPs), policies, procedures, and standards to ensure consistency with the provision of the IRP and to identify any new arrangements needed.
- The IT Division will verify and test to ensure all HHS CSIRC/NIH/NIDDK tasks affecting SCGSC applications, systems, or networks have been applied.
- The SCG President/Business Owner and IT Director will plan for the augmentation of the IRT to cover incidents of extended duration.
- Legal counsel will be consulted if necessary regarding protecting the chain of custody of evidence if an incident occurs.

SCG has created its IT Division to be the central point for incident response for the company and to coordinate with the HHS CSIRC/NIH.

Preventing Incidents

Keeping the number of incidents reasonably low is very important to protect the SCG Secure Cloud system. If security controls are insufficient, higher volumes of incidents may occur, overwhelming the IRT. This can lead to slow and incomplete responses, which translate to a larger negative impact (e.g., more extensive damage, longer periods of service and data unavailability).

At SCG, the IT Division is responsible for securing resources and advocating sound security practices. The SCG IT Division is able to identify problems that the organization is otherwise not aware of and plays a key role in risk assessment and training by identifying gaps. The following provides a brief overview of some of the main recommended practices implemented by the IT Division for securing networks, systems, and applications:

- **Risk Assessments.** Periodic assessments of systems and applications should determine what risks are posed by combinations of threats and vulnerabilities. This should include understanding the applicable threats, including organization-specific threats. Each risk should be prioritized, and the risks can be mitigated, transferred, or accepted. Another benefit of conducting assessments regularly is that critical resources are identified, allowing staff to emphasize monitoring and response activities for those resources.
- **Host Security.** All hosts should be hardened appropriately using standard configurations, such as Federal Desktop Core Configuration (FDCC) and United States Government Configuration Baseline (USGCB). In addition to keeping each host properly patched, hosts should be configured to follow the principle of least privilege. Users should have only the privileges necessary for performing their authorized tasks. Hosts should have auditing enabled and should log significant security-related events. The security of hosts and their configurations should be continuously monitored.
- **Network Security.** The network perimeter should be configured to deny all activity that is not expressly permitted. This includes securing all connection points, such as virtual private networks (VPNs), closing of open ports, and dedicated connections to other organizations.
- **Malware Prevention.** Software to detect and stop malware should be deployed throughout the organization. Malware protection should be deployed at the host level (e.g., server and workstation operating systems), the application server level (e.g., e-mail server, web proxies), and the application client level (e.g., e-mail clients, instant messaging clients).
- **User Awareness and Training.** Users should be made aware of policies and procedures regarding appropriate use of networks, systems, and applications. Applicable lessons learned from previous incidents also should be shared with users so they can see how their actions could affect the organization. Improving user awareness regarding incidents should reduce the frequency of incidents. IT

staff should be trained so they can maintain their networks, systems, and applications in accordance with the organization's security standards.

9.4.2 Detection and Analysis/Incident Recognition

The most important first step is to recognize that an incident may be unfolding. Early recognition allows a rapid and informed identification of the nature and scope of the incident. The earlier mitigation strategies can be applied, the more likely they are to be successful. While incidents and events can present a variety of "symptoms," some of the most common are:

- Website defacement
- Denial of service or unwanted disruption of service caused by activities such as an e-mail-blitz, more commonly called "Spamming"
- Execution of malicious code (Virus, Worm, Trojan Horse)
- Attempts (either failed or successful) to gain unauthorized access to a system, or its data (e.g., unsuccessful log-on attempts)
- Access compromises, such as:
 - Unauthorized use of a system for the processing or storage of data (e.g., unexplained output on a screen or a printer)
 - Unauthorized use of another user's account
 - Unauthorized use of system privileges
 - Suspicious entries in a system/network account
 - Unexplained new user accounts
 - Unexplained changes in system files
 - Unexplained attempts to write to system files
 - Unexplained modifications to, or deletions of, data, file lengths, file dates, especially in system .EXE files
 - Unexplained file names
 - Unexplained new files
 - Unusual usage patterns or time of use profiles.

SCG uses Cisco Intrusion Prevention System (IPS), Symantec Endpoint Protection Suite Enterprise, and Kiwi Syslog to prevent, detect, and analyze incidents. The Cisco IPS is the SCGSC system's first line of defense for managing vulnerability. It protects against intrusions, viruses, and other attacks. The firewall is configured to update automatically to maximize system protection. When an intrusion, virus, or other attack is detected, an e-mail notice is sent to the IT Director, who notifies the other IRT members. The IRT will assess the threat and the IT Director will take remedial action as necessary. Symantec Endpoint Protection provides another layer of protection for the

SCGSC system. Symantec Endpoint Protection monitors intrusions, network security, and viruses and other malware. Once detected, an e-mail is sent to the IT Director, who will notify the other IRT members. The IRT will assess the threat and propose remedial action as necessary. Symantec quarantines suspicious items until the IT Director takes remedial action.

Attack Vectors

Incidents can occur in countless ways, so it is infeasible to develop step-by-step instructions for handling every incident. SCG is generally prepared to handle any incident but is focused on being prepared to handle incidents that use common attack vectors. SCG has developed and continues to develop many SOPs for identification and response for incident types (see Appendix A). Different types of incidents merit different response strategies. The attack vectors listed below are not intended to provide definitive classification for incidents; rather, they simply list common methods of attack, which can be used as a basis for defining more specific handling procedures:

- **External/Removable Media:** An attack executed from removable media or a peripheral device—for example, malicious code spreading onto a system from an infected USB flash drive.
- **Attrition:** An attack that employs brute force methods to compromise, degrade, or destroy systems, networks, or services (e.g., a Distributed Denial of Service [DDoS] intended to impair or deny access to a service or application; a brute force attack against an authentication mechanism, such as passwords, CAPTCHAS, or digital signatures).
- **Web:** An attack executed from a website or Web-based application—for example, a cross-site scripting attack used to steal credentials or a redirect to a site that exploits browser vulnerability and installs malware.
- **E-mail:** An attack executed via an e-mail message or attachment—for example, exploit code disguised as an attached document or a link to a malicious website in the body of an e-mail message.
- **Impersonation:** An attack involving replacement of something benign with something malicious—for example, spoofing, man in the middle attacks, rogue wireless access points, and SQL injection attacks all involve impersonation.
- **Improper Usage:** Any incident resulting from violation of an organization's acceptable usage policies by an authorized user, excluding the above categories; for example, a user installs file sharing software, leading to the loss of sensitive data; or a user performs illegal activities on a system.
- **Loss or Theft of Equipment:** The loss or theft of a computing device or media used by the organization, such as a laptop, Smartphone, or authentication token.

Signs of an Incident

The most challenging part of the incident response process is accurately detecting and assessing possible incidents, determining whether an incident has occurred and, the type, extent, and magnitude of the problem. What makes this so challenging is a combination of three factors:

- Incidents may be detected through many different means, with varying levels of detail and fidelity. Automated detection capabilities include network-based and host-based intrusion prevention systems (IPS), antivirus software, and log analyzers. Incidents also may be detected through manual means, such as problems reported by users. Some incidents have overt signs that can be easily detected, whereas others are almost impossible to detect.
- The volume of potential signs of incidents is typically low for SCG systems. It would be uncommon for SCG to receive dozens of intrusion detection sensor alerts per day.
- A wide array of specialized technical knowledge of and extensive experience with SCG infrastructure are necessary for proper and efficient analysis of incident-related data.

Signs of an incident fall into one of two categories:

- Precursors – A precursor is a sign that an incident may occur in the future.
- Indicators – An indicator is a sign that an incident may have occurred or may be occurring now.

Most attacks do not have any identifiable or detectable precursors from the target's perspective. If precursors are detected, the IT Division may have an opportunity to prevent the incident by altering its security posture to save a target from attack. At a minimum, the IT Division can monitor activities involving the target more closely.

Examples of precursors are:

- Web server log entries that show the usage of a vulnerability scanner.
- An announcement of a new exploit that targets a vulnerability of SCG's server.
- A threat from a group stating it will attack the organization.

While precursors are relatively rare, indicators are all too common. Too many types of indicators exist to exhaustively list them, but some examples include:

- A network intrusion detection sensor alerts when a buffer overflow attempt occurs against a database server.
- Antivirus software alerts when it detects that a host is infected with malware.
- A System Administrator sees a filename with unusual characters.
- A host records an auditing configuration change in its log.

- An application logs multiple failed login attempts from an unfamiliar remote system.
- A network administrator notices an unusual deviation from typical network traffic flows.

Incident Analysis

Incident detection and analysis would be simpler if every precursor or indicator were guaranteed to be accurate; unfortunately, this is not the case. For example, user-provided indicators, such as a complaint of a server being unavailable, often are incorrect. Intrusion detection systems may produce false positives or incorrect indicators. The IRT works quickly to analyze and validate each incident, following a pre-defined process and documenting each step taken. When the IT Division believes an incident has occurred, the team rapidly performs an initial analysis to determine the incident's scope, such as which network, system, or applications are affected; who or what originated the incident; and how the incident is occurring (e.g., what tools or attack methods are being used, what vulnerabilities are being exploited). The initial analysis should provide enough information for the IRT to prioritize subsequent activities, such as containment of the incident and deeper analysis of the effects of the incident. Escalation procedures are built into this process.

Performing the initial analysis and validation is challenging. The following recommendations for making incident analysis easier and more effective, are incorporated in SCG's incident handling procedures:

- Profile networks and systems
- Understand normal behaviors
- Create a log retention policy
- Perform event correlation
- Keep all host clocks synchronized
- Maintain and use a knowledge base of information
- Use internet search engines for research
- Run packet sniffers to collect additional data
- Filter the data
- Seek assistance from others.

SCG's incident handling checklist is provided in Table 3.

Table 3. Incident Handling Checklist

No.	Action	Completed
Detection and Analysis		
1.	Determine whether an incident has occurred	
1.1	Analyze the precursors and indicators	
1.2	Look for correlating information	
1.3	Perform research (e.g., search engines, knowledge base)	
1.4	Once incident confirmed, begin documenting the investigation and gathering evidence	
2.	Prioritize handling the incident based on the relevant factors (functional impact, information impact, recoverability effort, etc.)	
3.	Report the incident to the internal personnel and NIDDK ISSO and other personnel	
Containment, Eradication, and Recovery		
4.	Acquire, preserve, secure, and document evidence	
5.	Contain the incident	
6.	Eradicate the incident	
6.1	Identify and mitigate all vulnerabilities that were exploited	
6.2	Remove malware, inappropriate materials, and other components	
6.3	If more affected hosts are discovered (e.g., new malware infections), repeat the Detection and Analysis steps (1.1, 1.2) to identify all other affected hosts, then contain (5) and eradicate (6) the incident for them	
7.	Recover from the incident	
7.1	Return affected systems to an operationally ready state	
7.2	Confirm that the affected systems are functioning normally	
7.3	If necessary, implement additional monitoring to look for future related activity	
Post-Incident Activity		
8.	Create a follow-up report	
9.	Hold a lessons learned meeting and document lessons learned in incident response report.	

Incident Documentation

The IT Division, when it suspects that an incident has occurred, immediately starts recording all facts regarding the incident. Documenting system events, conversations, and observed changes in files leads to a more efficient, more systematic, and less error-prone handling of the problem. Every step taken, from the time the incident was

detected, to its final resolution is documented. Every document regarding the incident is dated and entered into the IT Division incident handling file. Information of this nature also can be used as evidence in a court of law if legal prosecution is pursued.

The IT Division maintains records about the status of incidents, along with other pertinent information. The records are located on the SCG Secure Cloud system server and backed up daily. Adequate recordkeeping and tracking of incidents helps to ensure incidents are handled and resolved in a timely manner. The issue tracking system contains information on the following:

- The current status of the incident (new, in progress, forwarded for investigation, resolved, etc.)
- A summary of the incident
- Indicators related to the incident
- Other incidents related to this incident
- Actions taken by all incident handlers on this incident
- Chain of custody, if applicable
- Impact assessments related to the incident
- Contact information for other involved parties (e.g., business owner, system administrators)
- A list of evidence gathered during the incident investigation
- Comments from IRT
- Next steps to be taken (e.g., rebuild the host, upgrade an application).

The IT Division safeguards incident data and restricts access to them because they often contain sensitive information. Some examples are data on exploited vulnerabilities, recent security breaches, and users that may have performed inappropriate actions. Only authorized personnel and the IT Division should have access to the incident database. Incident communications (e.g., e-mails) and documents are password protected or encrypted so only authorized personnel can read them.

Incident Prioritization

Prioritizing the handling of the incident is perhaps the most critical decision point in the incident handling process. Incidents should not be handled on a first-come, first-served basis as a result of resource limitations. Instead, handling is prioritized based on the relevant factors, such as the following:

- Functional impact of the incident.
- Information impact of the incident.

- Recoverability from the incident.

Combining the functional impact to the SCGSC system and the impact to its information determines the business impact of the incident. For example, a distributed denial of service attack against a public Web server may temporarily reduce the functionality for users attempting to access the server, whereas unauthorized root-level access to a public Web server may result in the exfiltration of personally identifiable information (PII), which could have a long-lasting impact on the organization's reputation.

The recoverability from the incident determines the possible responses the IT Division may take when handling the incident. An incident with a high functional impact that requires low effort for recovery is an ideal candidate for immediate action from the team. The IT Division prioritizes the response to each incident based on its estimate of the business impact caused by the incident and the estimated efforts required to recover from the incident.

SCG can best quantify the effect of its own incidents because of its situational awareness.

Incident Notification/Incident Reporting

When an incident is analyzed and prioritized, the IRT Manager notifies the appropriate individuals so that all who need to be involved will play their roles. During incident handling, the IRT Manager provides status updates to certain parties, even in some cases the entire organization. The IRT plans and prepares several communication methods, including out-of-band methods (e.g., in person, paper), and selects the methods that are appropriate for a particular incident. Possible communication methods include: e-mail, website (internal, external, or portal), telephone calls, in person (e.g., daily briefings), voice mailbox greeting (e.g., set up a separate voice mailbox for incident updates and update the greeting message to reflect the current incident status), and paper (e.g., post notices on bulletin boards and doors, hand out notices at all entrance points).

SCG follows the procedures defined by HHS CSIRC for the different Priority Levels for an incident (see Table 4).

The high level procedures for the IRT are as follows:

1. Provide a verbal or written initial report to NIDDK ISSO and HHS CSIRC within one (1) hour after discovery/detection of a Priority Level 1 incident. The following are examples of Level 1 incidents:
 - Root compromise
 - User compromise
 - Denial of service/distributed denial of service attacks (no matter how successful or unsuccessful)
 - Website defacements

- a. Provide a written preliminary incident report to the NIDDK ISSO and HHS CSIRC within 24 hours containing as much information as possible.
 - b. Provide a written final report to the NIDDK ISSO and HHS CSIRC within 10 working days of the resolution of an incident.
 - c. In cases where incident resolution is expected to take more than 30 days, provide a status report to the NIDDK ISSO and HHS CSIRC every 10 days.
2. Provide an initial report to the NIDDK ISSO and HHS CSIRC within one (1) hour after discovery/detection of Priority Level 2 incidents, including:
 - User compromise
 - Successful virus/worm infection
 - Successful introduction of a virus/worm into a network
 - Scanning of classified or critical systems
 - a. Provide a written preliminary incident report to the NIDDK ISSO and HHS CSIRC within 24 hours containing as much information as possible.
 - b. Provide a written final report to the NIDDK ISSO and HHS CSIRC within 10 working days of the resolution of an incident.
 - c. In cases where incident resolution is expected to take more than 30 days, provide a status report to the NIDDK ISSO and HHS CSIRC every 10 days.
3. Report Priority Level 3 incidents on a weekly basis. The following are examples of Level 3 incidents:
 - Scanning of unclassified, non-critical systems
 - Detection and elimination of malicious logic before infestation
4. Report Priority Level 4 incidents on a monthly basis. The following are examples of Level 4 incidents:
 - Misuse of resources
 - Spam e-mail
 - Fraudulent e-mail
 - Social Engineering
5. Provide reports to the NIDDK ISSO and HHS CSIRC in response to OMB/Federal Computer Incident Response Center (FedCIRC) vulnerability management and patch installation data calls by the due date and time.
6. Report incidents involving loss or compromise of PII to the NIDDK ISSO, in addition to HHS CSIRC.

Table 4. Incident Procedures by Priority Level

Priority Level Incident Examples			
<u>Priority Level 1</u>	<u>Priority Level 2</u>	<u>Priority Level 3</u>	<u>Priority Level 4</u>
Examples: <ul style="list-style-type: none"> • Root compromise • User compromise • All successful or unsuccessful DoS/DDoS attacks • Website defacement 	Examples: <ul style="list-style-type: none"> • User compromise • Successful virus/worm infection • Successful introduction of a virus/worm into a network • Scanning of classified or critical systems 	Examples: <ul style="list-style-type: none"> • Scanning of unclassified, non-critical systems • Detection and elimination of malicious logic before infestation 	Examples: <ul style="list-style-type: none"> • Misuse of resources • Spam e-mail • Fraudulent e-mail • Social engineering

Incident Procedures	Priority Level			
	1	2	3	4
Provide a verbal or written initial report to HHS CSIRC/NIDDK ISSO within one (1) hour after discovery/detection of an incident.	✓	✓		
Provide a written preliminary incident report to HHS CSIRC/NIDDK ISSO within 24 hours, containing as much information as possible.	✓	✓		
Provide a written final report to HHS CSIRC/NIDDK ISSO within 10 working days of the resolution of an incident.	✓	✓		
In cases where incident resolution is expected to take more than 30 days, provide a status report to HHS CSIRC/NIDDK ISSO every 10 days.	✓	✓		
Report incidents on a weekly basis.			✓	
Report incidents on a monthly basis.				✓
Provide reports to HHS CSIRC/NIDDK ISSO in response to OMB/FedCIRC vulnerability management and patch installation data calls by the due date and time.	✓	✓	✓	✓
Report incidents involving loss or compromise of classified information to the NIDDK ISSO, in addition to HHS CSIRC.	✓	✓	✓	✓

9.4.3 Incident Response Containment, Eradication, and Recovery

Choosing a Containment Strategy

Containment is important before an incident overwhelms resources or increases the damage. Most incidents require containment, which is an important consideration early

in the course of handling each incident. Containment provides time for developing a tailored remediation strategy. An essential part of containment is decision-making (e.g., shut down a system, disconnect it from a network, and disable certain functions). Such decisions are much easier to make if there are predetermined strategies and procedures for containing the incident. SCG has defined acceptable risks in dealing with incidents and developed strategies accordingly.

Containment strategies vary based on the type of incident. For example, the strategy for containing an e-mail-borne malware infection is quite different from that of a network-based DDoS attack. SCG has created separate containment strategies for each major incident type, with criteria documented clearly to facilitate decision-making. Criteria for determining the appropriate strategy include:

- Potential damage to and theft of resources
- Need for evidence preservation
- Service availability (e.g., network connectivity, services provided to external parties)
- Time and resources needed to implement the strategy
- Effectiveness of the strategy (e.g., partial containment, full containment)
- Duration of the solution (e.g., emergency workaround to be removed in 4 hours, temporary workaround to be removed in 2 weeks, permanent solution).

SCG is using Cisco IPS and Symantec Endpoint Protection Suite to block and contain incidents affecting the SCGSC system. The Cisco IPS is the SCGSC system's first line of defense for managing vulnerability. It protects against intrusions, viruses, and other attacks. The firewall is configured to update automatically to maximize system protection. When an intrusion, virus, or other attack is detected, an e-mail notice is sent to the IT Director, who notifies the other members of the IRT. The IRT will assess the threat and the IT Director will take remedial action as necessary. Symantec Endpoint Protection provides another layer of protection for the SCGSC system. Symantec Endpoint Protection monitors intrusions, network security, and viruses and other malware. Once detected, an e-mail is sent to the IT Director, who will assess the threat and propose remedial action as necessary. Symantec quarantines suspicious items until the IT Director takes remedial action.

Evidence Gathering and Handling

Although the primary reason for gathering evidence during an incident is to resolve the incident, it also may be needed for legal proceedings. In such cases, it is important to clearly document how all evidence, including compromised systems, has been preserved. Evidence should be collected according to procedures that meet all applicable laws and regulations that have been developed from previous discussions with legal staff and appropriate law enforcement agencies, so all evidence can be admissible in court. In addition, evidence should be accounted for at all times; whenever evidence is transferred from person to person, chain of custody forms should detail the

transfer and include each party's signature. A detailed log should be kept for all evidence, including but not limit to the following:

- Identifying information (e.g., the location, serial number, model number, hostname, media access control (MAC) addresses, and Internet Protocol (IP) addresses of a computer).
- Name, title, and phone number of each individual who collected or handled the evidence during the investigation.
- Time and date (including time zone) of each occurrence of evidence handling.
- Locations where the evidence was stored.

Collecting evidence from computing resources presents some challenges. It is generally desirable to acquire evidence from a system of interest as soon as one suspects an incident may have occurred. Many incidents cause a dynamic chain of events to occur; an initial system snapshot may do more good in identifying the problem and its source than most other actions that can be taken at this stage. From an evidentiary standpoint, it is much better to get a snapshot of the system as-is rather than doing so after incident handlers, system administrators, and others have inadvertently altered the state of the machine during the investigation. Users and system administrators should be made aware of the steps they should take to preserve evidence. See NIST SP 800-86, *Guide to Integrating Forensic Techniques into Incident Response*, for additional information on preserving evidence.

Identifying the Attacking Hosts

During incident handling, the IT Director and SCG President and others sometimes want to, or need to, identify the attacking host or hosts. Although this information can be important, the IRT generally stays focused on containment, eradication, and recovery. Identifying an attacking host can be a time-consuming and futile process that can prevent a team from achieving its primary goal, which is minimizing the business impact. The following items are the most commonly performed activities for attacking host identification:

1. Validating the attacking host's IP address;
2. Researching the attacking host through search engines;
3. Using incident databases; and
4. Monitoring possible attacker communication channels.

Eradication and Recovery

After an incident has been contained, eradication may be necessary to eliminate components of the incident, such as deleting malware and disabling breached user accounts, as well as identifying and mitigating all vulnerabilities that were exploited. During eradication, it is important to identify all affected hosts within the organization so

they can be remediated. For some incidents, eradication is either not necessary or is performed during recovery.

In recovery, administrators restore systems to normal operation, confirm the systems are functioning normally, and (if applicable) remediate vulnerabilities to prevent similar incidents. Recovery may involve such actions as restoring systems from clean backups, rebuilding systems from scratch, replacing compromised files with clean versions, installing patches, changing passwords, and tightening network perimeter security (e.g., firewall rule sets, boundary router access control lists). Higher levels of system logging or network monitoring are often part of the recovery process. Once a resource is successfully attacked, it often is attacked again, or other resources within the organization are attacked in a similar manner.

Activating the Incident Response Team

Containment, eradication, and recovery should be done in a phased approach so that remediation steps are prioritized. For SCGSC incidents, the following occurs:

1. **Identify the IRT Manager.** Usually, the IT Director leads the incident response but he could delegate the responsibility to a member of his team. The IRT Manager needs to have as broad a view as possible of the environment in which the incident occurred, and should be trained in incident response procedures.
2. **Identify an incident has occurred or is occurring.** The IRT Manager verifies the situation is not the result of a simple mistake. Do not rush through the procedures. Instead, follow all of the steps of the procedures, and take precautions to prevent destruction or corruption of evidence that may be needed to support criminal prosecution.
3. **Verbally report the incident to the HHS CSIRC/NIDDK ISSO.** The IRT Manager is the person at SCG who is responsible for verbally reporting the incident to the HHS CSIRC/NIDDK ISSO. Notifications should be limited to those who have a legitimate need to know.
4. **Determine the nature and scope of the incident.** Ask questions (who, what, when, where) and take good notes. Timestamp all notes. Use a stitched binder to record notes so that it is easy to verify that no notes have been lost or misplaced.
 - a. Look for modifications to system software and configuration files.
 - b. Look for tools installed by the intruder.
 - c. Check other local systems for modification.
 - d. Check remote systems for modifications.
 - e. Notify HHS CSIRC to check for systems at other sites that may be involved.
5. **Maintain and secure all evidence.** Identify and properly secure all evidence to maintain its validity in court. Keep a log of everyone who has access to the evidence.

- 6. Maintain a low profile.** Send a small onsite team to secure the area, ask questions, and review the information from the identification phase. Avoid tipping off the attacker. Maintain standard procedures and avoid looking for the attacker with obvious methods.
- 7. Isolate the system.** In some cases, taking the system offline may be a serious step because of the importance of its services. The need to continue important services should be weighed against the potential harm that can arise from the security incident. Therefore, the decision to isolate the system must be made at the appropriate management level. The decision should come after careful examination of system logs to determine if the attack is external or internal and to evaluate the risks of continuing operation. Whether the system is isolated or not, appropriate actions shall be taken to contain the attack and prevent further attacks.
- 8. Backup the system.** If possible, use two different backup methods. The information obtained from backing up the system may be used as evidence. Therefore, the backup media should be previously unused to avoid suggestions that it could be faulty. Log the original backup media properly as evidence. Include the following:
 - a. Registers, cache contents
 - b. Memory contents
 - c. State of network connections
 - d. State of running processes
 - e. Contents of the storage media
 - f. Contents of removable and backup media.
- 9. Protect the chain of custody of the backup data.** Store the data in a secure location. Keep a record of the individuals who have touched each piece of evidence. The record should include the date, time, and locations of where the evidence is stored.
- 10. Resolve the problem and return the system to normal operating status.** The following are steps that may be taken to eradicate the problem:
 - a. Understand the cause of the incident.
 - b. Determine the vulnerability that the intruder used to enter the system.
 - c. Load a clean, uncontaminated operating system.
 - d. Install appropriate software to ensure the incident will not reoccur.
 - e. Apply all the latest patches.
 - f. Remove any unnecessary services.
 - g. Install a file integrity assessment tool.

- h. Assess nearby computers on same network segment to ensure the problem did not spread to other computers.
- i. Verify the system has returned to its normal operating condition.
- j. Monitor the system to ensure no “back doors” were left undetected.

If the problem cannot be solved by the IRT, contact HHS CSIRC/NIDDK ISSO for technical assistance.

9.4.4 Post-Incident Activities

Lessons Learned

One of the most important parts of incident response is the one most often omitted: learning and improving. Each IRT should evolve to reflect new threats, improved technology, and lessons learned. Holding a “lessons learned” meeting with all involved parties after a major incident, can be extremely helpful in improving security measures and the incident handling process itself. Multiple incidents can be covered in a single “lessons learned” meeting. This meeting provides a chance to achieve closure with respect to an incident by reviewing what occurred, what was done to intervene, and how well intervention worked. The meeting should be held within several days of the end of the incident. Questions to be answered in the meeting include:

- Exactly what happened, and at what times?
- How well did staff and management perform in dealing with the incident? Were the documented procedures followed? Were they adequate?
- What information was needed sooner?
- Were any steps or actions taken that might have inhibited the recovery?
- What would the IRT, IT staff, and management do differently the next time a similar incident occurs?
- How could information sharing with other organizations have been improved?
- What corrective actions can prevent similar incidents in the future?
- What precursors or indicators should be watched for in the future to detect similar incidents?
- What additional tools or resources are needed to detect, analyze, and mitigate future incidents?

Small incidents need limited post-incident analysis, with the exception of incidents performed through new attack methods that are of widespread concern and interest. After serious attacks have occurred, it is usually worthwhile to hold post-mortem meetings that cross team and organizational boundaries to provide a mechanism for information sharing. The primary consideration in holding such meetings is ensuring the right people are involved, and the IT Director usually calls these meetings. The IT Director invites people who have been involved in the incident that is being analyzed,

but also considers who should be invited for the purpose of facilitating future cooperation.

The success of such meetings also depends on the agenda. Collecting input about expectations and needs (including suggested topics to cover) from participants before the meeting, increases the likelihood that the participants' needs will be met. In addition, establishing rules of order before or during the start of a meeting can minimize confusion and discord. Having one or more moderators who are skilled in group facilitation can yield a high payoff. Finally, it also is important to document the major points of agreement and action items and to communicate them to parties who could not attend the meeting.

Lessons learned meetings provide other benefits as well. Reports from these meetings are good material for training new team members by showing them real examples of how more experienced team members respond to incidents. Updating incident response policies and procedures is another important part of the lessons learned process. Post-mortem analysis of the way an incident was handled often will reveal a missing step or an inaccuracy in a procedure, providing impetus for change. Because of the changing nature of information technology and changes in personnel, the IRT should review all related documentation and procedures for handling incidents at designated intervals.

Another important post-incident activity is creating a follow-up report for each incident, which can be quite valuable for future use (if needed). The report provides a reference that can be used to assist in handling similar incidents. Creating a formal chronology of events (including time-stamped information, such as log data from systems) is important for legal reasons, as is creating a monetary estimate of the amount of damage the incident caused. This estimate may become the basis for subsequent prosecution activity by entities, such as the U.S. Attorney General's office. Follow-up reports should be kept for a period of time, as specified in record retention policies.

Using Collected Incident Data

Lessons learned activities should produce a set of objective and subjective data regarding each incident. Over time, the collected incident data should be useful in several capacities. The data, particularly the total hours of involvement and the cost, may be used to justify additional funding of the IRT. A study of incident characteristics may indicate systemic security weaknesses and threats, as well as changes in incident trends.

The incident data can be put back into the risk assessment process, ultimately leading to the selection and implementation of additional controls. Another good use of the data is measuring the success of the IRT. If incident data are collected and stored properly, they should provide several measures of the success (or at least the activities) of the IRT. Incident data also can be collected to determine if a change to incident response capabilities causes a corresponding change in the team's performance (e.g., improvements in efficiency, reductions in costs). Furthermore, organizations that are

required to report incident information will need to collect the necessary data to meet their requirements.

With HHS CSIRC guidance, SCG has decided what incident data to collect based on reporting requirements and on the expected return on investment from the data (e.g., identifying a new threat and mitigating the related vulnerabilities before they can be exploited). Some of the metrics for incident-related data include: number of incidents handled, time per incident, objective assessment of each incident (location, category), and subjective assessment of each incident.

Evidence Retention

SCG follows HHS CSIRC guidance for how long evidence from an incident should be retained.

9.5 Vulnerability Management

The IT Director will implement the appropriate procedures to ensure proper actions are taken for the success of our Vulnerability Management Program for the SCG Secure Cloud system. The actions to be taken to manage vulnerability are described in Table 5.

Although the SCG Secure Cloud system does not connect to any HHS/NIH/NIDDK systems, the IT Director will review HHS CSIRC Security Alerts, Product Security Bulletins, and Virus Bulletins to keep abreast of the security measures, types of attacks, potential vulnerabilities and other developments in cybersecurity. The IT Director will review and take actions where needed to ensure the SCG Secure Cloud system is protected against serious vulnerabilities.

HHS CSIRC Alerts provide notification about critical new vulnerabilities that pose an immediate threat and contain instructions on how to mitigate these vulnerabilities. HHS CSIRC Product Security Bulletins and Security Broadcasts provide notification of vulnerabilities or potential vulnerability issues of lesser impact than a Security Alert. Virus Bulletins provide warnings about serious viruses that have either been found within the Department's systems or are in the wild and could infect Department computer systems if protections are not implemented.

Table 5. Actions Taken to Manage SCGSC Vulnerability

Item	Actions
Cisco ASA 5512-X Firewall	<ul style="list-style-type: none">• The Cisco firewall is the SCG Secure Cloud system's first line of defense for managing vulnerability. It protects against intrusions, viruses, and other attacks. The firewall is configured to update automatically to maximize system protection. When an intrusion, virus, or other attack is detected, an e-mail notice is sent to the IT Director, who notifies the other IRT members. The IRT will assess the threat and take remedial action as necessary.• The IT Director will take any corrective actions deemed necessary by the IRT.

Item	Actions
	<ul style="list-style-type: none"> The IT Director will notify the IRT members and the NIDDK ISSO that the corrective actions have been applied or justify why they could not be applied within 30 days or less.
Symantec Endpoint Protection Suite Enterprise 2015	<ul style="list-style-type: none"> Symantec Endpoint Protection provides another layer of protection for the SCG Secure Cloud system. The system is equipped with Symantec Endpoint Protection, which monitors intrusions, network security, and viruses and other malware. Once detected, an e-mail is sent to the IT Director, who notifies the other IRT members. The IRT will assess the threat and propose remedial action as necessary. The IT Director will take any corrective actions deemed necessary by the IRT. The IT Director will notify the IRT that the corrective actions have been applied or justify why they could not be applied within 30 days or less.
HHS CSIRC Security Alerts	<ul style="list-style-type: none"> The IT Division will review and evaluate the information in the Alert and will determine if action needs to be taken to protect the SCG Secure Cloud system. Any corrective actions will be applied as soon as possible. The IT Director will confirm compliance or justify why the corrective action could not be applied within 30 days or less.
HHS CSIRC Virus Bulletins	<ul style="list-style-type: none"> The IT Division will review and evaluate the information in the bulletin and determine if action needs to be taken to protect the SCG Secure Cloud system. The IT Division will identify and implement preventative actions, if needed. The IT Director will report any action taken or explain why the preventative action was not applicable.

9.6 Information Dissemination Control

Because incident reports reveal sensitive information about the vulnerabilities, capacity to respond, and operational readiness, rules for dissemination and handling controls are necessary.

All incident-related materials and documents are to be marked Sensitive But Unclassified (SBU), at a minimum.

The HHS CSIRC is responsible for releasing incident response and associated information within the HHS/NIH community and SCG's IT Director is responsible for releasing incident response and associated information within the SCG community.

9.7 Incident Response Plan Compliance Requirements

Given the importance that proper implementation of this Incident Response Plan holds for mission performance and readiness, failure to execute the provisions of this plan through negligence or willful disregard may result in adverse administrative or disciplinary action.

9.8 Testing, Training, and Exercise (TT&E)

SCG is required to conduct Testing, Training, and Exercise (TT&E) events periodically, following organizational or system changes, the issuance of new TT&E guidance, or as otherwise needed. In addition, SCG personnel accessing the SCGSC or other federal government systems are required to complete annual computer security and awareness training. Execution of TT&E events assists SCG in determining the plan's effectiveness, and that all personnel know what their roles are in the conduct of each step outlined in the plan. TT&E events will be held annually and as needed after system changes are implemented or new guidance is issued. The annual TT&E events will address contingency planning, incident response, and disaster recovery.

The importance of having IT personnel trained to fulfill their roles and responsibilities, have plans exercised to validate their effectiveness, and have systems tested to ensure their operability has been recognized by SCG.

The terms "test" and "exercise" are used interchangeably based on generic definitions, but they are given specific, different meanings with NIST, so "test-exercise" may be documented for both. Minimum documentation requirements for each test and/or exercise include a test and/or exercise plan and test and/or exercise after-action report (AAR). Additional documentation may be required to adequately document TT&E events based on the specific situation. The lessons learned from TT&E events and actual incident responses will be incorporated into the policies and procedures for incident response, disaster recovery, and contingency planning.

The SCG IT Division will be responsible for the coordination of training. A key element in the successful implementation of this procedure is ensuring all of the SCG IT personnel are capable of handling incidents as prescribed by procedures documented in the various plans for the SCGSC system.

As new employees join SCG and are assigned to support the SCGSC, the IT Division will provide these procedures in written form and familiarize them with the proper procedures through training and hands-on demonstrations within one (1) month of assuming an incident response role or responsibility. Each trainee must demonstrate the capability to handle incidents that might arise. Training will be conducted as needed when changes are implemented to the system and annually thereafter.

9.9 Incident Response Plan Maintenance

This plan will be distributed to SCG employees by the IT Director and it will be reviewed at least once every year and updated as necessary by the IT Director and IRT. All updates to this document will be reviewed and distributed using the methodology

defined herein. As stated above, the lessons learned from TT&E events and actual incident responses will be incorporated into the policies and procedures for incident response, disaster recovery, and contingency planning.

9.10 Distribution/Access List

An electronic copy of the IRP is stored in the offices of the IT Director and the Vice President of Administration. The IRP also is posted on the SCG Intranet (in read-only format) to permit easy access by SCGSC staff. The IRP log documenting incident response is stored on the SCG Secure Cloud system server and tape backup of the log is made daily. Authorization and access to the IRP log is controlled by the Microsoft Access Control List.

The IRT Manager controls access to the IRP log and ensures that technical staff responsible for content and responding to an incident have access.

Appendix A: HHS/NIH and SCG Incidence Response Policy and Procedures

This plan complies with the following federal and Departmental policies:

- HHS Policy for Responding to Breaches of Personally Identifiable Information
- HHS IRM Policy for Prevention, Detection, Removal and Reporting of Malicious Software
- Federal Information Security Management Act (FISMA), P.L. 107-347, Title III, December 2002.
- NIST SP 800-34 (Revision 1), *Incident Planning Guide for Federal Information Systems*, May 2010.
- NIST SP 800-53 (Revision 3), *Recommended Security Controls for Federal Information Systems*, August 2009 (Errata as of May 1, 2010).
- NIST SP 800-61 (Revision 2), *Incident Handling*, August 2012.
- NIST SP 800-86, *Guide to Integrating Forensic Techniques into Incident Response*.
- OMB, Circular A-130, Appendix III, Transmittal Memorandum #4, *Management of Federal Information Resources*, November 2000.

This plan also references and includes information from all SCG policies and SOPs. The following SOP goes into more detail on how the Incident Response activities will be performed:

- SCG Incident Handling Standard Operating Procedure (SOP)

Appendix B: Reporting Formats

SCG maintains current reporting formats and keeps these current based on our interaction with the HHS CSIRC/NIDDK ISSO. The IRT has both electronic and hardcopies of the SCGSC Incident Response Plan and incident handling procedures. The plan also is available as a PDF file on the SCG Intranet. The incident report will include the following elements:

- Contact Information for the Incident Reporter
 - Name
 - Role
 - Organizational unit (e.g., department, division, team) and affiliation
 - Email address
 - Phone number
 - Location (e.g., mailing address, office room number)
- Contact Information for the Incident Manager
 - Name
 - Role
 - Organizational unit (e.g., department, division, team) and affiliation
 - Email address
 - Phone number
 - Location (e.g., mailing address, office room number)
- Incident Details
 - Status change date/timestamps (including time zone): when the incident started, when the incident was discovered/detected, when the incident was reported, when the incident was resolved/ended, etc.
 - Physical location of the incident (e.g., city, state)
 - Current status of the incident (e.g., ongoing attack)
 - Source/cause of the incident (if known), including hostnames and IP addresses
 - Description of the incident (e.g., how it was detected, what occurred)
 - Description of affected resources (e.g., networks, hosts, applications, data), including systems' hostnames, IP addresses, and function
 - If known, incident category, vectors of attack associated with the incident, and indicators related to the incident (traffic patterns, registry keys, etc.)
 - Prioritization factors (functional impact, information impact, recoverability, etc.)
 - Mitigating factors (e.g., stolen laptop containing sensitive data was using full disk encryption)

- Response actions performed (e.g., shut off host, disconnected host from network)
 - Other organizations contacted (e.g., software vendor)
- General Comments
- Incident Handler Data Elements
 - Current Status of the Incident Response
 - Summary of the Incident
 - Incident Handling Actions
 - ✓ Log of actions taken by all handlers
 - ✓ Contact information for all involved parties
 - ✓ List of evidence gathered
 - Incident Manager Comments
 - Cause of the Incident (e.g., misconfigured application, unpatched host)
 - Cost of the incident
 - Business Impact of the Incident

Appendix C: Incident Response Team Contact List

Name and Title	Phone Numbers	Email Address
Chuck Lee, IT Director	301-670-4990 (W) 301-366-3273 (C) 301-637-4355 (H)	chuck@scgcorp.com
Kenny Ying Lee, IT Systems Specialist	301-670-4990 (W) 315-956-7796 (C)	ylee@scgcorp.com
John Bernheimer, IT Systems Specialist	301-670-4990 (W) 410-428-1330 (C)	jbernheimer@scgcorp.com
Ric Blackman, Web Development Director	301-670-4990 (W) 301-529-0760 (C)	rblackman@scgcorp.com
Adam Mann, Web Developer	301-670-4990 (W) 301-717-3273 (C)	amann@scgcorp.com
Susie Warner, Program Manager	301-670-4990 (W) 301-366-3217 (C) 301-355-4388 (H)	swarner@scgcorp.com
Stacy Philipson, Vice President of Administration	301-670-4990 (W) 301-742-5954 (C) 301-363-5707 (H)	sphilipson@scgcorp.com
Beverly Campbell, President	301-670-4990 (W) 301-461-1109 (C) 540-887-9829 (H)	bcampbell@scgcorp.com

The IT Director maintains the Contact List for the IRT in the table above. These names are kept in electronic and hardcopy in the offices of the IT Director and Vice President of Administration. The contact information also is available on the SCG Secure Cloud system server.

Appendix D: NIDDK Contacts

NIDDK System Owner: Dana Sheets, Digital Engagement Lead, Office of Communications and Public Liaison (OCPL), NIDDK/NIH, 301-496-7059, sheetsdm@mail.nih.gov

NIDDK Information Systems Security Officer (ISSO) Contact: Warren Herder, Information Systems Security Officer, Computer Technology Branch, NIDDK/NIH, 301-443-9292, herderjw@niddk.nih.gov

NIDDK Authorizing Official/Designated Approving Authority Contact (AO/DAA): Chandan Sastry, IT Director and CIO, Computer Technology Branch, NIDDK/NIH, 301-496-9555, sastrych@mail.nih.gov

NIDDK Privacy Officer: Kelly Yager, Management Analyst, Office of Management and Policy Analysis, NIDDK/NIH, 301-594-3056, kelly.yager@nih.gov.

Appendix E: Glossary

Breach (as it relates to protected health information [PHI]) — The unauthorized acquisition, access, use, or disclosure of protected health information, which compromises the security or privacy of such information, except where an unauthorized person to whom such information is disclosed would not reasonably have been able to retain such information. (Defined in the American Recovery and Reinvestment Act of 2009)

Breach (as it relates to PII) — The loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons other than authorized users and for an other than authorized purpose have access or potential access to personally identifiable information, whether physical or electronic. (Defined in OMB M-07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information)

Incident — The act of violating an explicit or implied security policy. Of course, this definition relies on the existence of a security policy that, while generally understood, varies among organizations. Incidents include but are not limited to:

- attempts (either failed or successful) to gain unauthorized access to a system or its data
- unwanted disruption or denial of service
- the unauthorized use of a system for the processing or storage of data; and
- changes to system hardware, firmware, or software characteristics without the owner's knowledge, instruction, or consent. (US-CERT)

Information — Any communication or representation of knowledge such as facts, data, or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual forms. (Defined in OMB Circular A-130, Transmittal Memorandum #4, Management of Federal Information Resources, 6(a))

Information Technology Resources — These resources include but are not limited to: personal computers and related peripheral equipment and software, network and Web servers, telephones, facsimile machines, photocopiers, Internet connectivity and access to internet services, e-mail and, for the purposes of this policy, office supplies. It includes data stored in or transported by such resources for HHS purposes.

Information System — A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. (Defined in NIST SP 800-53, Recommended Security Controls for Federal Information Systems, Appendix B)

Protected Health Information (PHI) — “Individually identifiable health information” held or transmitted by a covered entity or its business associate, in any form or media, whether electronic, paper, or oral. “Individually identifiable health information” is information, including demographic data, that relates to:

- The individual’s past, present, or future physical or mental health or condition;
- The provision of health care to the individual; or
- The past, present, or future payment for the provision of health care to the individual that identifies the individual or for which there is a reasonable basis to believe it can be used to identify the individual. Individually identifiable health information includes many common identifiers (e.g., name, address, birth date, Social Security number).

The HIPAA Privacy Rule excludes from protected health information employment records that a covered entity maintains in its capacity as an employer and education and certain other records subject to, or defined in, the Family Educational Rights and Privacy Act, 20 U.S.C. §1232g. (Defined in the HIPAA Privacy Rule)

Personally Identifiable Information (PII) — Information that can be used to distinguish or trace an individual's identity, such as their name, Social Security number, biometric records, etc., alone, or when combined with other personal or identifying information that is linked or linkable to a specific individual, such as date and place of birth, mother’s maiden name, etc. (Defined in OMB M-07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information)

Privacy — The appropriate use of personal information. (Defined in the International Association of Privacy Professionals site glossary)

Privacy Incident — An incident that involves personally identifiable information or protected health information. (US-CERT)

Appendix F: Incident Response Log

Description of Incident:					
Date/Time Detected:					
Date/Time IRT Mobilized:					
Activities Undertaken	Date & Time Initiated	Date & Time Completed	IRT Member Responsible	Problems Encountered, Resolution, & Outcome	Follow-on Action Required

Appendix G: Acronyms

CIO	Chief Information Officer
CP	Contingency Plan
CS	Computer Security
CSIRC	Computer Security Incident Response Center
DDoS	Distributed Denial of Service
DoS	Denial of Service
FDCC	Federal Desktop Core Configuration
FedCIRC	Federal Computer Incident Response Center
FIPS	Federal Information Processing Standard
FISMA	Federal Information Security Management Act
HHS	Health and Human Services
HIPAA	Health Insurance Portability and Accountability Act
IP	Internet Protocol
IRP	Incident Response Plan
IRT	Incident Response Team
ISSO	Information System Security Officer
IT	Information Technology
MAC	Media Access Control
NDEP	National Diabetes Education Program
NIDDK	National Institute of Diabetes and Digestive and Kidney Diseases
NIH	National Institutes of Health
NIST	National Institute of Standards and Technology
NKDEP	National Kidney Disease Education Program
OCPL	Office of Communications and Public Liaison

OMB	Office of Management and Budget
OPDIV	Operating Division
PDD	Presidential Decision Directive
PHI	Protected Health Information
PII	Personally Identifiable Information
PO	Privacy Officer
SBU	Sensitive But Unclassified
SOP	Standard Operating Procedure
SP	Special Publication
TT&E	Testing, Training & Exercise
US-CERT	United States Computer Emergency Readiness Team
USGCB	United States Government Configuration Baseline
VPNs	Virtual Private Networks