

SPG 2810.2
December, 2001

**John C. Stennis Space Center
Information Technology (IT) Security
Incident Reporting and Handling Procedure**



National Aeronautics and
Space Administration

John C. Stennis Space Center
Stennis Space Center, MS 39529-6000

| | | |
|---|------------------------------------|-------------|
| Stennis Procedures and Guidelines | SPG 2810.2 | Basic |
| | <i>Number</i> | <i>Rev.</i> |
| | Effective Date: December 31, 2001 | |
| | Expiration Date: December 31, 2006 | |
| Page ii of v | | |
| Responsible Office: RA00/Center Operations Directorate | | |
| SUBJECT: SSC ITS Incident Reporting and Handling Procedure | | |

TABLE OF CONTENTS

| | |
|--|----|
| PREFACE | iv |
| P1. PURPOSE | iv |
| P2. APPLICABILITY | iv |
| P3. AUTHORITY | iv |
| P4. REFERENCES | v |
| P5. MEASUREMENTS | v |
| P6. CANCELLATION | v |
| CHAPTER 1. INTRODUCTION | 1 |
| 1.1 Requirement for IT Security and Incident Reporting | 1 |
| 1.2 Philosophy and Accountability | 1 |
| 1.3 Purpose and Scope of Guideline | 1 |
| CHAPTER 2. ROLES AND RESPONSIBILITIES | 2 |
| 2.1 Center Director | 2 |
| 2.2 SSC Chief Information Officer (CIO) | 2 |
| 2.3 SSC Directors and Chiefs | 2 |
| 2.4 System Computer Security Officials (CSO) | 2 |
| 2.5 SSC Line Managers | 3 |
| 2.6 SSC Chief of Security | 3 |
| 2.7 IT Security Manager | 3 |
| 2.8 SSC Incident Response Team | 3 |
| 2.9 System Administrator(s) | 4 |
| 2.10 SSC Employee(s) | 4 |
| CHAPTER 3. CATEGORIZING INCIDENTS FOR REPORTING | 5 |
| 3.1 Rationale | 5 |
| 3.2 System Compromise | 5 |
| 3.3 Information Compromise | 5 |
| 3.4 Unauthorized Access | 6 |
| 3.5 Denial of Service | 6 |
| 3.6 Misuse of Information Technology Resources | 7 |
| 3.7 Hostile Probe | 7 |
| 3.8 Other IT Security Concerns | 7 |
| CHAPTER 4. SECURITY INCIDENT RECOGNITION | 8 |
| 4.1 Introduction | 8 |
| 4.2 Incidents Related to Computer Files | 8 |
| 4.3 Incidents Related to User Accounts | 8 |
| 4.4 Incidents Related to Application Software | 9 |
| 4.5 Incidents Related to Physical Areas | 9 |
| 4.6 Incidents Related to Viruses | 9 |

| | | |
|---|------------------|-------------------|
| Stennis Procedures and Guidelines | SPG 2810.2 | Basic |
| | <i>Number</i> | <i>Rev.</i> |
| | Effective Date: | December 31, 2001 |
| | Expiration Date: | December 31, 2006 |
| Page iii of v | | |
| Responsible Office: RA00/Center Operations Directorate | | |
| SUBJECT: SSC ITS Incident Reporting and Handling Procedure | | |

| | |
|---|----|
| 4.7 Incidents Related to Misuse..... | 9 |
| CHAPTER 5. PROCESSES AND PROCEDURES..... | 11 |
| 5.1 Introduction | 11 |
| 5.2 Reporting IT Security Incidents | 11 |
| c. External (non-SSC) Source..... | 11 |
| 5.2.1 System User Incident Reports..... | 11 |
| 5.2.2 Reports by System Administrators | 12 |
| 5.2.3 Reports from External Sources of Incidents Arising from SSC Misuse..... | 12 |
| 5.3 Incident Response and Initial Determination | 13 |
| 5.4 IRT Assessment and Investigation | 14 |
| 5.5 Returning Equipment to Service | 16 |
| APPENDIX A: ACRONYMS AND DEFINITIONS..... | 18 |
| <u>Acronyms</u> | 18 |
| <u>Definitions</u> | 19 |
| ATTACHMENT A: SSC INCIDENT RESPONSE TEAM..... | 24 |
| ATTACHMENT B: SSC INCIDENT REPORTING FORM..... | 27 |

| | | |
|---|------------------------------------|-------------|
| Stennis Procedures and Guidelines | SPG 2810.2 | Basic |
| | <i>Number</i> | <i>Rev.</i> |
| | Effective Date: December 31, 2001 | |
| | Expiration Date: December 31, 2006 | |
| Responsible Office: RA00/Center Operations Directorate | | |
| SUBJECT: SSC ITS Incident Reporting and Handling Procedure | | |

PREFACE

P1. PURPOSE

SPD 2810.1 establishes Stennis Space Center (SSC) policy for Information Technology (IT) Security at Stennis Space Center. SPG 2810.2 provides the procedures and guidelines for implementing and administering the IT Security Program. This document supplements provisions of the SSC IT Security Program implemented by SPG 2810.2 and defines the process and procedure for reporting and handling of security incidents by SSC personnel.

P2. APPLICABILITY

This procedure is applicable to all National Aeronautics and Space Administration (NASA) and NASA contractor employees at SSC as well as all facilities, resources, and personnel under a contract from NASA/SSC at a college, university, or research facility.

P3. AUTHORITY

- a. 40 U.S.C. 759 note, the Computer Security Act, P.L. 100-235, as amended.
- b. 42 U.S.C. 2451, et. seq., the National Aeronautics and Space Act of 1958, as amended.
- c. 18 U.S.C. 799, et. seq., Violation of regulations of National Aeronautics and Space Administration.
- d. 5 U.S.C. 552, et. seq., the Freedom of Information Act, as implemented by 14 CFR 1201.
- e. 5 U.S.C. 552a, the Privacy Act, P.L. 93-579, as amended.
- f. 40 U.S.C. 1401, et. seq., Section 808 of Public Law 104-208, the Clinger-Cohen Act of 1996 [renaming, in pertinent part, the Information Technology Management Reform Act (ITMRA), Division E of Public Law 104-106].
- g. 50 U.S.C. 2401-2420, the Export Administration Act of 1979, as amended, as implemented by the Export Administration Regulations, 15 CFR Part 730-774.
- h. 18 U.S.C. 2510, et. seq., the Electronic Communications Privacy Act, as amended.
- i. 44 U.S.C. 2510, et. seq., the Paperwork Reduction Act of 1995, P.L. 104-13, as amended.
- j. Executive Order No. 12958, Classified National Security Information of May 18, 1995.

| | | |
|---|------------------------------------|-------------|
| Stennis Procedures and Guidelines | SPG 2810.2 | Basic |
| | <i>Number</i> | <i>Rev.</i> |
| | Effective Date: December 31, 2001 | |
| | Expiration Date: December 31, 2006 | |
| Responsible Office: RA00/Center Operations Directorate | | |
| SUBJECT: SSC ITS Incident Reporting and Handling Procedure | | |

k. Executive Order No. 13011, Federal Information Technology of July 16, 1996.

l. OMB Circular No. A-130, Management of Federal Information Resources.

P4. REFERENCES

This instruction is implemented in accordance with requirements of the documents listed below. The latest version of these documents applies unless otherwise indicated.

- a. NPD 2810.1, Security of Information Technology.
- b. NPG 2810.1, Security of Information Technology.
- c. NPD 1600.2, NASA Security Policy.
- d. NPG 1620.3, Security Procedures and Guidelines.

P5. MEASUREMENTS

The effectiveness of this SPG will be evaluated using the documentation generated in response to an incident. In addition, incident metrics are to be reported to the Principal Center for Information Technology Security (PCITS) on a quarterly basis.

P6. CANCELLATION

NONE

Mark Craig
Acting Director

DISTRIBUTION

SDL
NODIS

| | | |
|---|------------------|-------------------|
| Stennis Procedures and Guidelines | SPG-2810.2 | Basic |
| | <i>Number</i> | <i>Rev.</i> |
| | Effective Date: | December 31, 2001 |
| | Expiration Date: | December 31, 2006 |
| | | Page 1 of 28 |
| Responsible Office: RA00/Center Operations Directorate | | |
| SUBJECT: SSC ITS Incident Reporting and Handling Procedure | | |

CHAPTER 1. INTRODUCTION

1.1 Requirement for IT Security and Incident Reporting

NASA NPG 2810.1 describes the NASA IT Security Program, providing direction designed to ensure that safeguards for the protection of the integrity, availability, and confidentiality of IT resources (e.g., data, information, applications, and systems) are integrated into and support the mission of NASA.

1.2 Philosophy and Accountability

Part of the underlying philosophy for the NASA IT Security Program is that all of NASA's information is considered valuable and sensitive to some degree and that everyone is responsible for helping to ensure that IT resources are not exposed to undue risks. While managers and others in key positions are accountable for preserving the security of IT resources, everyone who uses IT resources bears some responsibility for ensuring that integrity, availability, and confidentiality are not compromised.

Inherent to the protection of NASA's IT resources is the prompt recognition, reporting, and remediation of IT Security Incidents. Prompt interception of real or suspected IT Security Incidents minimizes potential impacts to IT resources and provides insight for more effective risk management.

1.3 Purpose and Scope of Guideline

This guideline specifically:

- a. Defines and implements SSC requirements for reporting and handling IT Security incidents
- b. Identifies the structure, roles, relationships, and responsibilities for managing and mitigating incidents
- c. Provides the methodologies, processes and procedures for all personnel to follow if a real or suspected incident occurs.

The roles, relationships, and responsibilities for managing the SSC IT Security Program and for reporting and mitigating IT Security Incidents are described in Chapter 2. Chapter 3 provides guidance for categorizing incidents and summarizes NASA reporting requirements. Chapter 4 provides instruction on recognizing incidents and the detailed processes and procedures to be used for incident reporting, handling, and investigation. Supplemental information is provided in Appendices and Attachments to this document. Acronyms and definitions are provided in Appendix A.

| | | |
|---|------------------|-------------------|
| Stennis Procedures and Guidelines | SPG-2810.2 | Basic |
| | <i>Number</i> | <i>Rev.</i> |
| | Effective Date: | December 31, 2001 |
| | Expiration Date: | December 31, 2006 |
| | | Page 2 of 28 |
| Responsible Office: RA00/Center Operations Directorate | | |
| SUBJECT: SSC ITS Incident Reporting and Handling Procedure | | |

CHAPTER 2. ROLES AND RESPONSIBILITIES

2.1 Center Director

The SSC Center Director has oversight responsibilities for ensuring that an effective IT Security Program is established and maintained for SSC. To ensure compliance with Federal, NASA, and SSC IT Security Directives, the Center Director appoints (in writing) a Center IT Security Manager (C-ITSM).

2.2 SSC Chief Information Officer (CIO)

The SSC CIO is responsible for establishing an effective and economical Information Resource Management (IRM) Program that defines the design and operation of the SSC information infrastructure (such as networks, electronic mail applications, servers, and electronic forms). The CIO has been delegated the functional responsibility by the Center Director for the SSC IT Security Program. The CIO shall assure that the computer infrastructure has built-in recovery features (availability), provides adequate baseline protections (confidentiality), and protects data from modifications (integrity).

2.3 SSC Directors and Chiefs

The Directors of SSC Directorates and Chiefs of SSC Staff elements (including program/project organizations and staff officers) who report directly to the SSC Director, are responsible for designating (in writing) a Computer Security Official (CSO) for each IT system identified in the organization. The Directors of SSC Directorates and Chiefs of SSC Staff elements are responsible for establishing IT security in their organizations.

2.4 System Computer Security Officials

System CSO's are responsible for the SSC IT Security Program for their systems. They serve as the critical communication link to and from their organizations for all IT security matters. They serve as the organization's representative to the C-ITSM and represent the organization line managers on security matters. The CSO is responsible for reporting suspected and actual IT security incidents to the C-ITSM and line management. The CSO establishes management controls and a communications process to ensure that the organization's implementation of IT security is consistent with mission needs and SSC policies and guidance.

| | | |
|---|------------------|-------------------|
| Stennis Procedures and Guidelines | SPG-2810.2 | Basic |
| | <i>Number</i> | <i>Rev.</i> |
| | Effective Date: | December 31, 2001 |
| | Expiration Date: | December 31, 2006 |
| | | Page 3 of 28 |
| Responsible Office: RA00/Center Operations Directorate | | |
| SUBJECT: SSC ITS Incident Reporting and Handling Procedure | | |

2.5 SSC Line Managers

SSC Line Managers are responsible for overall IT security for their systems. They ensure that a properly trained System Administrator (SA) is assigned as the focal point for the security of each system or application and report suspected IT security incidents.

2.6 SSC Chief of Security

The Center Chief of Security (CCS) is responsible for providing oversight, guidance, and approval authority for projects conducting classified activities. The CCS assists the C-ITSM and Office of Inspector General (OIG) in investigations of security incidents as required.

2.7 IT Security Manager

The C-ITSM is responsible for overall IT Security program implementation, administration and operations. The C-ITSM is responsible for responding to IT security incidents and reporting of incidents to SSC management, the PCITS, and/or the NASA Automated Systems Incident Response Center (NASIRC) depending on the type of incident.

The C-ITSM is responsible for establishing a core team of technically oriented personnel for first-line response, investigation, and reporting of security incidents or suspected incidents. The C-ITSM will identify or appoint other resources as appropriate to fully resolve security incidents from incident investigation through recovery actions. The C-ITSM will maintain and distribute a contact list of core SSC Incident Response Team (IRT) members. An IRT key contact list is provided in the attachments to this document for reference. The list will be updated as needed.

2.8 SSC Incident Response Team

The SSC IRT is composed of NASA and/or contractor personnel as identified by the C-ITSM are responsible for investigating all security incidents and reporting any findings to the C-ITSM. The designated TTSC IT Security Liaison serves as a key contact of the IRT for incident reporting and supports the C-ITSM in the conduct of SSC IT Security activities. The IRT will interview all individuals associated with reported incidents and gather all available information, reports, system logs, and documentation associated with incidents and provide an incident assessment report to the C-ITSM for determination of further action and/or criminal investigation.

| | | |
|---|------------------|-------------------|
| Stennis Procedures and Guidelines | SPG-2810.2 | Basic |
| | <i>Number</i> | <i>Rev.</i> |
| | Effective Date: | December 31, 2001 |
| | Expiration Date: | December 31, 2006 |
| Page 4 of 28 | | |
| Responsible Office: RA00/Center Operations Directorate | | |
| SUBJECT: SSC ITS Incident Reporting and Handling Procedure | | |

2.9 System Administrator(s)

The SA is responsible for monitoring system logs and system activity to identify suspicious activity that might indicate a security incident. The SA of an affected system is responsible for reporting incidents to the C-ITSM and providing any assistance and system access requested by the IRT. The SA is also responsible for taking any necessary action to prevent the spread of a virus.

2.10 NASA Network Manager

The NASA Network Manager is responsible for analyzing network intrusion detection systems in the event of an incident. The NASA Network Manager provides the SSC Incident Response Team with log files relevant to the attack or suspected attack.

2.11 ODIN Network Administrator

The ODIN Network Administrator works with the SSC Incident Response Team during an IT Security incident. The ODIN Network Administrator is responsible for analyzing the firewall systems and providing networking information necessary to fully respond to an incident.

2.12 SSC ODIN Help Desk

The SSC ODIN Help Desk is responsible for notifying the SSC Incident Response Team when a suspected incident is reported to the SSC ODIN Help Desk. Responsibility is for notification of the SSC Incident Response Team is for 24 hours per day, 7 days a week coverage.

2.13 SSC Employee(s)

Each SSC employee should be aware of possible suspicious activity, be able to recognize a security incident, and is responsible for notifying the C-ITSM or the IRT if they have discovered or think they have discovered a security incident. Upon discovery of an incident, employees should record pertinent details associated with the incident for submitting the report to the appropriate authority.

| | | |
|---|------------------|-------------------|
| Stennis Procedures and Guidelines | SPG-2810.2 | Basic |
| | <i>Number</i> | <i>Rev.</i> |
| | Effective Date: | December 31, 2001 |
| | Expiration Date: | December 31, 2006 |
| Page 5 of 28 | | |
| Responsible Office: RA00/Center Operations Directorate | | |
| SUBJECT: SSC ITS Incident Reporting and Handling Procedure | | |

CHAPTER 3. CATEGORIZING INCIDENTS FOR REPORTING

3.1 Rationale

Defining and tracking categories of incidents provides statistical data that can assist management in allocating resources to improve the IT security posture of the Agency and its Centers. The C-ITSM is responsible for reporting the incident category to PCITS quarterly. To understand the nature and extent of threats to IT resources, NASA has defined the following seven categories of incidents, based upon severity to the system. Further definition is provided in following paragraphs.

- a. System compromise
- b. Information compromise
- c. Unauthorized access
- d. Denial of service
- e. Misuse
- f. Hostile probes
- g. Other IT Security concerns.

3.2 System Compromise

The following are acts that represent a system compromise.

- a. Any account or application that has system privileges is used without prior authorization or approval.
- b. A weakness in the system is successfully exploited, and access is gained to accounts with system privileges.
- c. A valid account is used to increase its own privileges and is successfully exploited to gain access to accounts with system privileges.

3.3 Information Compromise

The following are acts that represent an information compromise:

- a. A valid account is used without authorization, and access is gained to password files, data, applications, or accounts that are protected or restricted, but access is not gained to accounts with system privileges.

| | | |
|---|------------------|-------------------|
| Stennis Procedures and Guidelines | SPG-2810.2 | Basic |
| | <i>Number</i> | <i>Rev.</i> |
| | Effective Date: | December 31, 2001 |
| | Expiration Date: | December 31, 2006 |
| Responsible Office: RA00/Center Operations Directorate | | Page 6 of 28 |
| SUBJECT: SSC ITS Incident Reporting and Handling Procedure | | |

- b. A weakness in the system is successfully exploited and is successfully used to gain access to password files, data, applications, or accounts that are protected or restricted, but access is not gained to accounts with system privileges.
- c. The physical theft of assets provides access to password files, protected or restricted data, licensed applications or software, or restricted applications, software, or code.

3.4 Unauthorized Access

The following are acts that represent unauthorized access:

- a. A valid account is used without authorization, but access is not gained to password files, data, applications, or accounts that are protected or restricted outside of the account's authorizations.
- b. A weakness in the system is successfully exploited, but access is not gained to data, applications, accounts with system privileges or password files, or accounts that are protected or restricted outside the exploited function's authorization.

3.5 Denial of Service

The following are acts that represent a denial of service:

- a. A system's ability to perform its normal functions is impaired due to its being inundated with activity originating from one or more sources.
- b. Resources, such as power, network access, or routing tables, are deliberately modified to cause a system to not be able to perform its normal functions.
- c. Malicious code interferes with a system to a significant degree. (Malicious code includes, but is not limited to, viruses, Java applets, ActiveX, trojan horses, logic bombs, worms, unauthorized scripts, daemons, or similar programs.)
- d. Assets have been physically taken or destroyed, but no password files, protected or restricted data, applications, restricted software, or code were compromised.

| | | |
|---|------------------|-------------------|
| Stennis Procedures and Guidelines | SPG-2810.2 | Basic |
| | <i>Number</i> | <i>Rev.</i> |
| | Effective Date: | December 31, 2001 |
| | Expiration Date: | December 31, 2006 |
| | | Page 7 of 28 |
| Responsible Office: RA00/Center Operations Directorate | | |
| SUBJECT: SSC ITS Incident Reporting and Handling Procedure | | |

3.6 Misuse of Information Technology Resources

The following are acts that represent the misuse of IT resources:

- a. An authorized account is used in violation of Federal laws, NASA, or SSC policies regarding proper use of IT resources.
- b. Resources or privileges higher than those allocated or assigned are obtained without authorization.
- c. Unlicensed software or applications are installed.

3.7 Hostile Probe

The following are acts that represent a hostile probe:

- a. Exploits are run against a system that would, if successful, have resulted in a system compromise, information compromise, or unauthorized access.
- b. Exploits are run against a system that would, if successful, have impaired the system's ability to perform its normal functions.
- c. Illicit information gathering or attempted gathering is directed against one or more systems.

3.8 Other IT Security Concerns

Questionable events that do not fit into the other categories, include suspicious network activity, excessive junk mailing, chain letters, mail spoofing, or hoaxes that are determined by the C-ITSM to be of concern.

| | | |
|---|------------------|-------------------|
| Stennis Procedures and Guidelines | SPG-2810.2 | Basic |
| | <i>Number</i> | <i>Rev.</i> |
| | Effective Date: | December 31, 2001 |
| | Expiration Date: | December 31, 2006 |
| Responsible Office: RA00/Center Operations Directorate | | Page 8 of 28 |
| SUBJECT: SSC ITS Incident Reporting and Handling Procedure | | |

CHAPTER 4. SECURITY INCIDENT RECOGNITION

4.1 Introduction

It is not always possible to look at a computer system and tell what has occurred. Without analysis, computer crimes, maintenance problems, and operator errors often look alike. If in doubt, contact the SA for assistance. Some of the more common symptoms and indicators of security incidents are identified in the following paragraphs.

4.2 Incidents Related to Computer Files

The following are indicators of possible IT Security breaches related to computer files:

- a. Files that should be accessible to a user are suddenly unavailable.
- b. Files have been edited, though no changes should have occurred.
- c. Files appear, disappear, or undergo significant and unexpected changes in size.

4.3 Incidents Related to User Accounts

Indicators of security incidents related to user accounts include:

- a. User accounts appear or disappear from the system without the knowledge or consent of the SA.
- b. A user's password has been changed without the user's knowledge or involvement.
- c. An employee's account suddenly becomes active, but the employee is not present to use it and the employee is known not to be using it remotely.
- d. System logs record numerous unsuccessful logon attempts to a given user's account, but the user is not the one who attempted the logons.
- e. Parts or all of the system logs are missing, or logs appear altered.
- f. System logs indicate successful logons to a user's account but are at odd hours for that user.

| | | |
|---|------------------|-------------------|
| Stennis Procedures and Guidelines | SPG-2810.2 | Basic |
| | <i>Number</i> | <i>Rev.</i> |
| | Effective Date: | December 31, 2001 |
| | Expiration Date: | December 31, 2006 |
| | | Page 9 of 28 |
| Responsible Office: RA00/Center Operations Directorate | | |
| SUBJECT: SSC ITS Incident Reporting and Handling Procedure | | |

4.4 Incidents Related to Application Software

A common indicator of a security breach associated with application software includes but is not necessarily limited to:

- a. Application software has been modified, but changes have not been approved.
- b. Application software does not produce expected output or does not execute properly.

4.5 Incidents Related to Physical Areas

Compromises of a physical nature may indicate a breach of IT Security. These may include:

- a. Output of a sensitive nature that would normally be handled carefully is found in printer trays or left uncontrolled in the work area.
- b. Unauthorized personnel are discovered in the work area.

4.6 Incidents Related to Viruses

Viruses present a very real threat to IT Security and may be subtle in their destructive capacity. Some common indicators of virus infiltration include:

- a. Files that should be accessible to a user are suddenly unavailable.
- b. Files have been edited, though no changes should have occurred.
- c. Files appear, disappear, or undergo significant and unexpected changes in size.
- d. The system displays strange messages or mislabels files and directories.
- e. The system becomes inaccessible (e.g., it will not boot properly).
- f. Data on the system hard drive are no longer available.

4.7 Incidents Related to Misuse

- a. An authorized account is used in violation of Federal laws, NASA, or SSC policies regarding proper use of IT resources such as maintaining or conducting an outside business; advertising goods or services for sale for monetary or personal gain; or participating in Chat Rooms, News Groups, or similar activities where the posting will be seen by the public.

| | | |
|---|------------------|-------------------|
| Stennis Procedures and Guidelines | SPG-2810.2 | Basic |
| | <i>Number</i> | <i>Rev.</i> |
| | Effective Date: | December 31, 2001 |
| | Expiration Date: | December 31, 2006 |
| | | Page 10 of 28 |
| Responsible Office: RA00/Center Operations Directorate | | |
| SUBJECT: SSC ITS Incident Reporting and Handling Procedure | | |

- b. Resources or privileges higher than those allocated or assigned are obtained without authorization.
- c. Unlicensed software or applications are discovered on system.
- d. Inappropriate (racist or sexually explicit) material and files are discovered on system.
- e. Sending chain letters, personal mass mailing, hoaxes, or harassing messages.

| | | |
|---|------------------|-------------------|
| Stennis Procedures and Guidelines | SPG-2810.2 | Basic |
| | <i>Number</i> | <i>Rev.</i> |
| | Effective Date: | December 31, 2001 |
| | Expiration Date: | December 31, 2006 |
| Responsible Office: RA00/Center Operations Directorate | | Page 11 of 28 |
| SUBJECT: SSC ITS Incident Reporting and Handling Procedure | | |

CHAPTER 5. PROCESSES AND PROCEDURES

5.1 Introduction

The SSC IT Security Incident and Handling Procedure encompasses four phases of activity, each with unique guidelines and requirements.

- a. Reporting IT Security Incidents
- b. Incident Response and Assessment
- c. Criminal Investigation
- d. Returning the System to Use

The processes and procedures to be used in each phase are described in the following paragraphs.

5.2 Reporting IT Security Incidents

Security incidents or suspected incidents may be discovered and reported by:

- a. System Users
- b. System Administrators
- c. External (non-SSC) Source

The following procedures are required and used for reporting IT security incidents.

5.2.1 System User Incident Reports

The System Users community will follow the steps below if they have discovered or think they have discovered a security incident.

1. Immediately notify the C-ITSM at extension 8-2249, the CCS at extension 8-2003, and the SSC Test and Technical Services Contractor (TTSC) IT Security Liaison at extension 8-1245 and await assistance.
2. Notify the SA of the affected system and await assistance. For Program Support Computer System (PSCS) software or systems, call extension 8-2116. If it is an Outsourcing Desktop Initiative for NASA (ODIN) Desktop System, contact the Help desk at extension 8-2525.

| | | |
|---|------------------|-------------------|
| Stennis Procedures and Guidelines | SPG-2810.2 | Basic |
| | <i>Number</i> | <i>Rev.</i> |
| | Effective Date: | December 31, 2001 |
| | Expiration Date: | December 31, 2006 |
| | | Page 12 of 28 |
| Responsible Office: RA00/Center Operations Directorate | | |
| SUBJECT: SSC ITS Incident Reporting and Handling Procedure | | |

3. Leave the equipment alone. Do not try to process, insert, or delete any information on the affected system.
4. After reporting, do not discuss or release information about the security incident without consulting the C-ITSM or the direction of the IRT.

5.2.2 Reports by System Administrators

SAs will follow the steps below if suspicious activity that might indicate a security incident is identified while monitoring system logs and system activity or in response to requests for assistance by system users.

1. Immediately notify the C-ITSM at extension 8-2249, the CCS at extension 8-2003, and the SSC TTSC IT Security Liaison at extension 8-1245 and await assistance.
2. Leave the equipment alone. Do not try to process, insert, or delete any information on the affected system, hardware, or software.
3. Do not try to track or catch the intruder. Record pertinent details of incident or suspected incident for provision to appropriate authorities such as: date, time, location; software, hardware, or system involved; identifying characteristics of incident; suspected perpetrators.
4. If a virus begins to execute and it appears that the virus is damaging files, immediately shut down the system by turning off the power and call for assistance.
5. After reporting, do not discuss or release information about the security incident without consulting the C-ITSM or the direction of the IRT.

5.2.3 Reports from External Sources of Incidents Arising from SSC Misuse

When a member of the SSC community is notified from an external (non-SSC) source of a detected or suspected penetration, or attempted penetration of an external computer arising from a SSC source, the following steps will be followed:

1. Immediately notify the C-ITSM at extension 8-2249, the CCS at extension 8-2003, the TTSC IT Security Liaison at extension 8-1245, and the Help Desk at extension 8-2525 and await assistance or instruction.
2. Record the name and contact information of the notifier and pertinent details of the incident for provision to the appropriate authority. Do not try to track or catch the intruder.
3. Do not discuss or release information about the security incident without consulting the C-ITSM or the direction of the IRT.

| | | |
|---|------------------|-------------------|
| Stennis Procedures and Guidelines | SPG-2810.2 | Basic |
| | <i>Number</i> | <i>Rev.</i> |
| | Effective Date: | December 31, 2001 |
| | Expiration Date: | December 31, 2006 |
| | | Page 13 of 28 |
| Responsible Office: RA00/Center Operations Directorate | | |
| SUBJECT: SSC ITS Incident Reporting and Handling Procedure | | |

5.3 Incident Response and Initial Determination

Upon receiving notification of a IT security incident or a suspected incident, the C-ITSM and/or TTSC IT Security Liaison will contact the individual who reported the suspected incident and the SA of the system to:

- a. Gather all pertinent information
- b. Make an initial determination if an actual security incident occurred.

After a full review, if it is determined that a security incident did not occur, the incident is closed. If it is determined that a security incident did occur, the following steps should be followed.

1. The C-ITSM or TTSC IT Security Liaison will notify the appropriate IRT members of the incident.
2. The C-ITSM or TTSC IT Security Liaison will notify the Organizational CSO, the Line Manager, and SA of the affected or suspected system. They will be instructed that the IRT is responding to the incident and the infected or attacked systems will be turned over to the IRT.
3. The C-ITSM or TTSC IT Security Liaison will notify the ODIN Network Administrator and the NASA Network Manager of the security incident and provide the name and IP address of the affected or suspected system.
4. The C-ITSM Manager or TTSC IT Security Liaison will notify all SSC SAs by encrypted e-mail of the computer systems involved in the incident.
5. The C-ITSM or TTSC IT Security Liaison will notify the SSC CIO, Center Director, OIG, and the CCS that an IT security incident has occurred and that a preliminary report will be available within 24 hours.
6. The C-ITSM or TTSC IT Security Liaison will report the incident to NASIRC, encrypted, except for the misuse of IT resources and for previously known viruses unless the virus caused a major impact and might affect other Centers. See Attachment B for an example of the SSC IT Security Incident Reporting Form.

| | | |
|---|------------------|-------------------|
| Stennis Procedures and Guidelines | SPG-2810.2 | Basic |
| | <i>Number</i> | <i>Rev.</i> |
| | Effective Date: | December 31, 2001 |
| | Expiration Date: | December 31, 2006 |
| | | Page 14 of 28 |
| Responsible Office: RA00/Center Operations Directorate | | |
| SUBJECT: SSC ITS Incident Reporting and Handling Procedure | | |

5.4 IRT Assessment and Investigation

The IRT will use the following procedure for collecting and compiling IT security incident information:

1. The IRT will interview all individuals who have information about the incident and collect any or all of the following:
 - Two disk “image” verified backups of the disk or disks on the system (e.g., those created using the “dd” UNIX command)
 - Any applicable audit trails or system logs
 - Any exception reports (i.e., summaries of security-relevant events extracted from more extensive system logs)
 - Any available system monitoring reports
 - An account with system privileges to examine the system
 - Any available documentation that will help the IRT assess the affected system and its connectivity.

2. The IRT will conduct a preliminary investigation and prepare a preliminary report for delivery to the C-ITSM within 24 hours. The IRT will also initiate corrective or remediative actions. The preliminary report must contain at a minimum the following information regarding each of the computer systems involved:
 - Incident Category
 - Date and time of the incident notification
 - Identification of the person providing the incident notification
 - Date and time of the incident
 - Description of the sequence of events that led to the discovery of the incident
 - Name and NASA property number of the SSC computer system and identification of any non-SSC computer system
 - Location of the computer system (building number and room number)
 - Type of computer system
 - Operating system (name and version)
 - Cognizant organization
 - Identification of the computer system manager
 - Primary function of the computer system
 - Classification of the computer system (sensitivity level and configuration)
 - Method of penetration or virus infection, if known

| | | |
|---|------------------|-------------------|
| Stennis Procedures and Guidelines | SPG-2810.2 | Basic |
| | <i>Number</i> | <i>Rev.</i> |
| | Effective Date: | December 31, 2001 |
| | Expiration Date: | December 31, 2006 |
| Responsible Office: RA00/Center Operations Directorate | | Page 15 of 28 |
| SUBJECT: SSC ITS Incident Reporting and Handling Procedure | | |

- Preliminary estimate of damage, if available, and/or potential for damage
 - Immediate corrective actions taken.
3. Upon receipt of the IRT investigative report, the C-ITSM will prepare and distribute a preliminary report to the CIO, Center Director, Public Affairs Office (PAO), CCS, and the Line Manager with responsibility for the computer system involved.
 4. The C-ITSM will determine whether the incident is a computer crime. If there is doubt about the possible criminality of these incidents, the C-ITSM will consult with the CCO, the local OIG or NASA Headquarters IG Computer Crimes Division.
 5. If the incident is confirmed to be a computer crime, the C-ITSM will report the incident to the NASA OIG.
 6. The C-ITSM will consult with the CCS and OIG regarding appropriate evidence handling procedures.
 7. The C-ITSM, TTSC Security Liaison, IRT, TTSC IT Security Team, and affected line managers will assist the OIG in investigating, monitoring, and gathering evidence necessary to identify and prosecute individuals committing computer crimes.
 8. The Center Director will decide, after coordinating with the OIG whether to control/terminate incidents, when in their judgement, SSC's mission, its customers, its reputation, or its assets are in jeopardy, or to allow incidents to continue in order to collect information related to possible prosecution of attackers.
 9. If the incident involves computer misuse and a computer crime has not occurred, the C-ITSM will refer the incident to the appropriate line manager and/or Human Resources Office for appropriate action if the incident involves Civil Servants. If the incident involves contractor personnel, the cognizant Contracting Officer's Technical Representative (COTR) and Contract Manager will be notified for appropriate action.
 10. The IRT and C-ITSM will complete the detailed investigation and prepare a summary report. The summary report must contain at a minimum the following information regarding each of the computer systems involved:
 - Incident Category
 - Date and time of the incident notification
 - Identification of the person providing the incident notification
 - Date and time of the incident
 - Description of the sequence of events that led to the discovery of the incident

| | | |
|---|------------------|-------------------|
| Stennis Procedures and Guidelines | SPG-2810.2 | Basic |
| | <i>Number</i> | <i>Rev.</i> |
| | Effective Date: | December 31, 2001 |
| | Expiration Date: | December 31, 2006 |
| | | Page 16 of 28 |
| Responsible Office: RA00/Center Operations Directorate | | |
| SUBJECT: SSC ITS Incident Reporting and Handling Procedure | | |

- Name and NASA property number of the SSC computer system and identification of any non-SSC computer system
- Location of the computer system (building number and room number)
- Type of computer system
- Operating system (name and version)
- Cognizant organization
- Identification of the computer system manager
- Primary function of the computer system
- Classification of the computer system (sensitivity level and configuration)
- Detailed description of the incident, including interviews and statements, evidence collected, tests, analyses, the identification of the persons or computer perpetrating the incident, and conclusion
- Final estimate of damage
- Identification of remediation requirements and plans to correct the deficiencies.

11. The C-ITSM will distribute the summary report to the CIO, Center Director, PAO, CCS, and the Line Manager with responsibility for the computer system involved.

12. The C-ITSM, with concurrence from the CIO, will determine if information on the incident is to be released to other agencies at SSC and if necessary, prepare the information for release.

5.5 Returning Equipment to Service

The C-ITSM will return equipment to service as quickly as possible following an incident. In most cases, equipment will be returned to service the same day. The type and scope of each incident will determine the timeframe required to return the affected systems to service. The underlying vulnerability that caused the incident to occur must be identified and removed or mitigated prior to returning a system to service.

If the equipment was compromised by an unauthorized user, the hard drive must be completely reformatted in order to remove any trojan programs or “back doors” that the unauthorized user may have left on the system. The operating system should be reinstalled from the distribution media and only data files (and source code) should be restored from the backup media. In the case of a computer virus, worm, or trojan horse infection, follow the instructions posted on the anti-virus software manufacturer’s web site for irradiating the virus from the equipment. If there is no known method of irradiating the equipment, the same method as used for a system compromise should be performed. If the incident involves misuse, the associated files and applications should be deleted from the system.

| | | |
|---|------------------|-------------------|
| Stennis Procedures and Guidelines | SPG-2810.2 | Basic |
| | <i>Number</i> | <i>Rev.</i> |
| | Effective Date: | December 31, 2001 |
| | Expiration Date: | December 31, 2006 |
| | | Page 17 of 28 |
| Responsible Office: RA00/Center Operations Directorate | | |
| SUBJECT: SSC ITS Incident Reporting and Handling Procedure | | |

Usually, the line manager will use threat information from the C-ITSM, CCS, and OIG to decide whether a system will be removed from service, patched, or remain in service. In some cases, the risk to other systems will mandate that risk-reduction action take precedence over returning the system to operational status. On rare occasions, if the seriousness of an incident warrants it, equipment may be removed from the area and held as evidence.

| | | |
|---|------------------|-------------------|
| Stennis Procedures and Guidelines | SPG-2810.2 | Basic |
| | <i>Number</i> | <i>Rev.</i> |
| | Effective Date: | December 31, 2001 |
| | Expiration Date: | December 31, 2006 |
| Page 18 of 28 | | |
| Responsible Office: RA00/Center Operations Directorate | | |
| SUBJECT: SSC ITS Incident Reporting and Handling Procedure | | |

APPENDIX A: ACRONYMS AND DEFINITIONS

Acronyms

| | |
|--------|--|
| CCS | Center Chief of Security |
| CIO | Chief Information Officer |
| C-ITSM | Center IT Security Manager |
| COTR | Contracting Officer's Technical Representative |
| CSO | Computer Security Official |
| IG | Inspector General |
| IRM | Information Resource Management |
| IRT | Incident Response Team |
| IT | Information Technology |
| ITMRA | Information Technology Management Reform Act |
| LAN | Local Area Network |
| NASA | National Aeronautics and Space Administration |
| NASIRC | NASA Automated Systems Incident Response Center |
| NPD | NASA Policy Directive |
| NPG | NASA Procedures and Guidelines |
| OIG | Office of Inspector General |
| ODIN | Outsourcing Desktop Initiative for NASA |
| PAO | Public Affairs Office |
| PCITS | Principal Center for Information Technology Security |
| PSCS | SSC Program Support Computer System |
| SA | System Administrator |
| SPD | Stennis Policy Directive |
| SPG | Stennis Procedures and Guidelines |
| SSC | Stennis Space Center |
| TTSC | Test and Technical Services Contractor |

| | | |
|---|------------------|-------------------|
| Stennis Procedures and Guidelines | SPG-2810.2 | Basic |
| | <i>Number</i> | <i>Rev.</i> |
| | Effective Date: | December 31, 2001 |
| | Expiration Date: | December 31, 2006 |
| | | Page 19 of 28 |
| Responsible Office: RA00/Center Operations Directorate | | |
| SUBJECT: SSC ITS Incident Reporting and Handling Procedure | | |

Definitions

ACCESS - The ability to obtain or change information or data. Within a system, “access” is the interaction between a subject (e.g., person, process, or device) and an object (e.g., record, file, program, or device) that results in the flow of information from one to the other. The nature or type of access can be read, write, execute, append, modify, delete, and create.

APPLICATION - A set of computer commands, instructions, and procedures used to cause a computer to process a specific set of information. Application software does not include operating systems, generic utilities, or similar software that are normally referred to as “system software.”

AVAILABILITY - The state wherein information, data, and systems are in the place needed by the user, at the proper time, and in the form that the user requests.

COMPUTER CRIME - The use of system(s), software, or network(s) to deliberately commit criminal activities, which may include, but are not limited to, the compromise of system privileges (e.g., root access), compromise of information protected by law (e.g., International Traffic in Arms Regulations, Privacy Act Data, procurement sensitive data), denial of service of major IT resources, child pornography, and malicious destruction of NASA data and/or information.

CONFIDENTIALITY - Holding sensitive data in confidence such that distribution is limited to those individuals or organizations with an established need to know.

CONTROLS - Protective measures used to improve security by reducing risks, also known as “safeguards,” “countermeasures,” or “security features.”

CRITICAL SYSTEM FILES - Those that are necessary in order for a system to perform regular tasks, including boot-ups, network logon(s), and all other normal standard operations.

DAEMON - A UNIX process that runs in the background in support of other processes that users may invoke using different commands. Daemons are usually active as long as the system is active. Typically, they do “housekeeping” on a computer.

DATA OWNER - The individual (organizational line manager) responsible for the confidentiality, integrity, and availability of a specific set of data. This individual is responsible for making judgments and decisions on behalf of the organization with regard to the data’s information category level, criticality, use, protection, and sharing. Typically, this individual is a member of the organization directly supported by the data. Often this individual maintains the data and ensures its accuracy. All data have a data owner.

| | | |
|---|------------------|-------------------|
| Stennis Procedures and Guidelines | SPG-2810.2 | Basic |
| | <i>Number</i> | <i>Rev.</i> |
| | Effective Date: | December 31, 2001 |
| | Expiration Date: | December 31, 2006 |
| | | Page 20 of 28 |
| Responsible Office: RA00/Center Operations Directorate | | |
| SUBJECT: SSC ITS Incident Reporting and Handling Procedure | | |

DENIAL OF SERVICE - A type of malicious attack that causes the interruption and/or stoppage of regular ongoing IT system activities.

ENCRYPTION - Any procedure used in cryptography to convert plain text into cipher text in order to prevent anyone other than the intended recipient from reading that data.

GOVERNMENT INFORMATION - Knowledge or facts created, collected, processed, disseminated, or disposed of both by and for the Federal Government.

HOSTILE PROBES -The act of using one or more systems to scan targeted systems or networks with intent to conduct or to gather information for unauthorized activities. They are often targeted against networks (LAN's) rather than single stand-alone systems. They may return information that may provide information on system vulnerabilities.

"IMAGE" BACKUPS - A dump of the entire contents of a system's disk media. For example, in UNIX a command is used to make an image (exact copy) of the "system" disk. The disks must be physically identical for this to work. The command "dd" copies the specified input file to the specified output with possible conversions.

INFORMATION - Any communication or reception of knowledge, such as facts, data, or opinions, including numerical, graphic, or narrative forms, whether oral or maintained in any medium, such as computerized databases, paper microfilm, tapes, disk, memory chips, RAM, ROM, microfiche, communication lines, and display terminals.

INFORMATION COMPROMISE - That which occurs when information has been made available to person(s) and/or systems(s) who are not the intended audience. Compromises usually occur when a system has been successfully hacked into (i.e., security controls have been compromised).

INFORMATION TECHNOLOGY (IT) - Hardware and software operated by a Federal agency or by a contractor of a Federal agency or other organization that processes information on behalf of the Federal government to accomplish a Federal function, regardless of the technology involved, whether by computers, telecommunications systems, automatic data processing equipment, or other.

INFORMATION TECHNOLOGY (IT) RESOURCES - Data and information; computers, ancillary equipment, software, firmware, and similar products; facilities that house such resources; services, including support services; and related resources used for the acquisition, storage, manipulation, management, movement, control, display, switching, interchange,

| | | |
|---|------------------|-------------------|
| Stennis Procedures and Guidelines | SPG-2810.2 | Basic |
| | <i>Number</i> | <i>Rev.</i> |
| | Effective Date: | December 31, 2001 |
| | Expiration Date: | December 31, 2006 |
| | | Page 21 of 28 |
| Responsible Office: RA00/Center Operations Directorate | | |
| SUBJECT: SSC ITS Incident Reporting and Handling Procedure | | |

transmission, or reception of data. This includes telecommunication systems, network systems, and human resources. (Also called Automated Information Resources.)

INFORMATION TECHNOLOGY (IT) SECURITY INCIDENT - An adverse event or situation associated with a system which poses a threat to the integrity, availability, or confidentiality of data or systems and that results in a failure of security controls; an attempted, suspected, or actual compromise of information; or the waste, fraud, abuse, loss, or damage of Government property or information.

INTEGRITY - The state that exists when computerized data is the same as that in source documents or has been correctly computed from source data and has not been exposed to accidental or malicious alteration or destruction.

LOGIC BOMBS - A resident computer program that triggers the perpetuation of an unauthorized act when particular states of the system are realized.

LOGON - The identification and authentication sequence that authorizes a user's access to a computer. Conversely, "logoff" is the sequence that terminates user access to the system.

MALICIOUS CODE - Computer program instructions created with the intent of malice or unauthorized acts towards the targeted system(s) and may be written in many computer languages, including but not limited to, C, C++, Visual Basic, Assembly Language, and Java.

MISUSE - The use of computer systems and or facilities that do not comply with Center or Agency guidelines, standards, and/or policies.

OFFICIAL BUSINESS USE - The use of Government property, such as computers and facilities, for conducting business in accordance with official policies and procedures of the respective Government agency.

PASSWORD - A protected word, phrase, or a string of symbols that is used to authenticate the identity of a user. When associated with a particular user ID, it is considered proof of authentication to use the capabilities associated with that user ID.

PROPER USE - The use of Government property in accordance with the policies, procedures, and guidance specified by the respective Government agency.

SYSTEM - An interconnected set of information resources under the same management control which shares common functionality and requires the same level of security controls. Normally includes hardware, software, information, data, applications, telecommunication systems, network communications systems, and people.

| | | |
|---|------------------|-------------------|
| Stennis Procedures and Guidelines | SPG-2810.2 | Basic |
| | <i>Number</i> | <i>Rev.</i> |
| | Effective Date: | December 31, 2001 |
| | Expiration Date: | December 31, 2006 |
| | | Page 22 of 28 |
| Responsible Office: RA00/Center Operations Directorate | | |
| SUBJECT: SSC ITS Incident Reporting and Handling Procedure | | |

SYSTEM COMPROMISE - A situation in which a system has been accessed by an individual who is not authorized to conduct such activities. Usually this is the result of some exploited vulnerability of the system.

SYSTEM LOGS - Records that contain information about various activities including, but not limited to, logon information, root-privileged processes, and network connection(s) information. They are usually kept in order to investigate system functionality issues and intrusion or probe attempts. Also referred to as “journals” or “audit logs.”

SYSTEM PRIVILEGES - Unlimited access to a system by yielding all commands and permissions of files. Someone with system privileges can modify the computer’s operating system, system audit logs, system configurations, account privileges, account passwords, data files, software, or applications; add or delete accounts; install or delete software and applications; or alter the system’s security controls outside those abilities normally authorized for an individual’s account. (System privileges are equivalent to root privileges on UNIX Operating Systems.)

THREATS - An indication of impending danger or harm. Within the context of IT security, they may be viewed as perceived potential dangers and are events or circumstances, whether internal or external, that have the potential to cause harm to a system or to its associated applications or information.

TRAP DOOR - Pieces of code written into applications or operating systems to grant programmers access to programs without having to go through the normal methods of access authentication. They are used primarily by programmers for debugging or monitoring code that is in development and are also referred to as “back doors.”

TROJAN CODE - Programming code developed to perform a task while using functions and/or displays to make it seem as if it is running other tasks. The program appears to be doing what the user wants, but it is doing something else entirely.

TROJAN HORSE - A computer program with an apparently (or actually) useful function that contains additional (hidden) functions that surreptitiously exploit the legitimate authorizations of the invoking process.

UNAUTHORIZED ACCESS - The accessing of system(s) and/or processes using methods that are not approved or certified by the system and/or SAs.

| | | |
|---|------------------|-------------------|
| Stennis Procedures and Guidelines | SPG-2810.2 | Basic |
| | <i>Number</i> | <i>Rev.</i> |
| | Effective Date: | December 31, 2001 |
| | Expiration Date: | December 31, 2006 |
| | | Page 23 of 28 |
| Responsible Office: RA00/Center Operations Directorate | | |
| SUBJECT: SSC ITS Incident Reporting and Handling Procedure | | |

USER IDENTIFICATION (USER ID) - A unique character string used in a computer to identify a user which is not normally protected as private/privileged information, but is normally unique within the system.

VIRUS - Self-propagating software that parasitically attaches itself to authorized software and has three functional components: mission, trigger, and self-propagation. It is capable of doing anything that software can do, both good and bad, once it is activated in a system.

VULNERABILITY - A weakness in a system or software application that could be exploited to compromise security processes or controls that protect the system and the information it handles.

| | | |
|---|------------------|-------------------|
| Stennis Procedures and Guidelines | SPG-2810.2 | Basic |
| | <i>Number</i> | <i>Rev.</i> |
| | Effective Date: | December 31, 2001 |
| | Expiration Date: | December 31, 2006 |
| | | Page 26 of 28 |
| Responsible Office: RA00/Center Operations Directorate | | |
| SUBJECT: SSC ITS Incident Reporting and Handling Procedure | | |

Tommy Spiers (NT)

Office: 228-688-1973
Home: 601-798-8100
Pager: 1-800-759-8888, PIN # 1432062

| | | |
|---|------------------|-------------------|
| Stennis Procedures and Guidelines | SPG-2810.2 | Basic |
| | <i>Number</i> | <i>Rev.</i> |
| | Effective Date: | December 31, 2001 |
| | Expiration Date: | December 31, 2006 |
| Responsible Office: RA00/Center Operations Directorate | | |
| SUBJECT: SSC ITS Incident Reporting and Handling Procedure | | |

ATTACHMENT B: SSC INCIDENT REPORTING FORM

| | | |
|--|---|--|
| STENNIS SPACE CENTER INCIDENT REPORTING FORM | | Time of Incident Notification: |
| Incident Category (Check all that apply) <input type="checkbox"/> System Compromise <input type="checkbox"/> Information Compromise <input type="checkbox"/> Unauthorized Access <input type="checkbox"/> Denial of Service <input type="checkbox"/> Misuse <input type="checkbox"/> Hostile Probes <input type="checkbox"/> Other IT concerns | | Date of Incident Notification: Name of the person reporting the incident: <hr style="width: 80%; margin: 5px 0;"/> System Administrator: <hr style="width: 80%; margin: 5px 0;"/> |
| Date of the incident: | Time of the incident: | |
| Description of the sequence of events that led to the discovery of the incident: | | |
| Name and NASA property number of the SSC computer system and identification of any non-SSC computer system (include IP number): | | |
| Location of the computer system (building number and room number): | Type of computer system: | Operating system (including ver.): |
| Cognizant organization: | Primary function of the computer system: | |
| Identification of the computer system manager: | Classification of the computer system (sensitivity level and configuration): | |

| | | |
|---|------------------|-------------------|
| Stennis Procedures and Guidelines | SPG-2810.2 | Basic |
| | <i>Number</i> | <i>Rev.</i> |
| | Effective Date: | December 31, 2001 |
| | Expiration Date: | December 31, 2006 |
| Responsible Office: RA00/Center Operations Directorate | | Page 28 of 28 |
| SUBJECT: SSC ITS Incident Reporting and Handling Procedure | | |

Method of Penetration or Virus Infection, if known:

Source Host Names and IP Addresses of Attackers:

Description of Sensitive Information Involved:

Affected Machine(s) System Administrator and Phone Number:

Additional Comments:

Report Prepared by:

Date of Report: