Information Security Handbook

Incident Response and Management: NASA Information Security Incident Management

ITS-HBK-2810.09-02
Effective Date: 20110824
Expiration Date: 20130824
Responsible Office: OCIO/Deputy CIO for Information Technology Security

Contents

1.0 Introduction **1**
2.0 Incident Management Lifecycle Overview **2**
3.0 Definition and Categorizations **3**
3.1 Definition of Incident 3
3.2 Categorizations 3
3.3 Indicators 3
3.4 Priority 3
3.5 Dispositions 4
4.0 Incident Management Roles and Responsibilities **5**
4.1 Overview 5
4.2 Core Incident Response Team Roles 5
Center Privacy Manager (CPM) *5*
Forensic Analyst (FA) *5*
Incident Response Manager (IRM) *6*
IT Technician (IT) *7*
Network Incident Analyst (NIA) *7*
Technical Investigator (TI) *7*
4.3 Auxiliary Incident Response Roles 8
Information System Security Official (ISSO) *8*
Subject Matter Expert (SME) *8*
4.4 Related Roles/Organizations 8
Center Chief Counsel *8*
Center Human Resources Employee Relations *8*
Center Public Affairs Office *8*
Computer Security Official (CSO) *8*
Contracting Officer (CO)/ Contracting Officer's Technical Representative (COTR) *8*
Incident Reporter *9*
Information System Owner (ISO) *9*
NASA Information Systems Network (NISN) Network Operations Center (NOC) *9*
NASA Security Operations Center (NASA SOC) *9*
Office of the Inspector General (OIG) *9*
Office of Protective Services (OPS) *9*
Senior Agency Official for Privacy (SAOP) *9*
System Administrator/Service Provider *9*
United States Computer Emergency Response Team (US-CERT) *9*
4.5 Incident Response Team 9
5.0 Incident Management Lifecycle **12**
5.1 Overview 12
5.2 Incident Preparation 12
5.3 Incident Identification 12
a. Reporting a Suspected Incident *12*
b. Initial Response *13*
c. Categorizing and Prioritizing Incidents *13*
d. Additional Requirements for Specific Classes of Compromised Data *13*
5.4 Incident Containment 13
a. Overview of Incident Containment *13*
b. Selection of a Containment Strategy *13*
5.5 Incident Eradication 14
a. Overview of Incident Eradication *14*
b. Guidelines for Incident Eradication *14*
5.6 Incident Recovery 14
a. Overview of Incident Recovery *14*
b. Selection Requirements for System Recovery *14*

c. Framework for Incident Recovery *14*
5.7 Incident Follow-Up 16
a. Overview of Incident Follow-Up *16*
b. Post-Incident Analysis *16*
c. Post-Incident Report *16*
d. Revising Policies, Procedures, and Security Plans *16*
5.8 Incident Documentation 17
5.9 Incident Analysis 17
a. Overview of Incident Analysis *17*
b. Identifying Artifacts *17*
c. Protecting Artifacts *17*
5.10 Incident Communication 17
a. Overview of Incident Communication *17*
b. Communication Channels *17*
c. Communication Logs *17*
6.0 Incident Management Framework 18
6.1 Overview 18
6.2 Incident Tracking 18
6.3 The Incident Management Process Flow 18
6.4 Mapping the IM Process Flow to the IM Roles 20
7.0 References 21
Appendix A – Acronyms 22
Appendix B – Unauthorized Access Use Case 24
Handling Unauthorized Access Incidents 24
Initial Action 24
Identification 24
Containment 25
Eradication/Recovery 25
Post-Incident Activities 25
Appendix C – Malicious Code Use Case 26
Handling Malicious Code Outbreaks 26
Initial Action 26
Identification 26
Containment 27
Eradication/Recovery 27
Post-Incident Activities 27
Appendix D – Use Case for Inappropriate Use 28
Handling Inappropriate Usage Incidents 28
Initial Action 28
Identification 28
Containment, Eradication, Recovery 29
Post-Incident Activities 29
Appendix E – Denial of Service Use Case 30
Handling Denial of Service Attacks 30
Initial Action 30
Identification 30
Containment 32
Eradication/Recovery 33
Post-Incident Activities 33
Appendix F – Extra Discussion 34
Selection of a Containment Strategy 34
Cryptographic Hashes 34
Overview of Live Host Analysis 34
a. Information Collected During Live Host Analysis *35*
b. Dead Host Analysis *35*

c. Malware Analysis *36*
Selection Requirements for System Recovery 36
Benefits of Incident Follow-Up 37
Incident Response Procedure Analysis 37
Incident Response Cost Analysis 37
Appendix G - Incident Indicators by Category 39
Appendix H – Quantified Approach for Incident Prioritization 42
Appendix I – Procedures for Breach of Personally Identifiable Information (PII) 45
Applicable Documents 45
Personally Identifiable Information Defined 45
Handling Breach of Personally Identifiable Information 45
Breach of Personally Identifiable Information Process 46
Step 1: Initial Investigation and Determination *46*
Step 2: Initial Mitigation *47*
Step 3: Breach Risk Assessment *47*
Step 4(a): External Mitigation Recommendation *48*
Step 4(b): Breach Notification Recommendation *49*
Additional Considerations 51
Communications Plan/ Notification Plan 51
Multi-Center Breach 52
Post Incident Closure 52
Post Incident Follow-Up 52
General Process Flow 53
Sample Notification Letters 54

Distribution:

NODIS

Approved

Valarie Burks

Valarie Burks
Deputy Chief Information Officer for
Information Technology Security

8-24-11

Date

Change History

Change Number	Date	Change Description
1.0	08/24/2011	Initial Draft

1.0 Introduction

This handbook is designed to help NASA better manage Information Security risks, provide guidance when operating under abnormal circumstances, and to streamline response during an Information Security incident. This handbook presents two abstract models for systematically handling Information Security incidents:

- The Incident Management Lifecycle, which characterizes the continuous effort to identify, analyze and contain incidents, recover from them, and improve security as a set of sequential phases and perpetual parallel activities; and
- The Incident Management Framework, which is a collection of practices and tools for prioritization, categorization, tracking, assignment, documentation, and communication to ensure that incident response activities are organized and that composure, is maintained.

This handbook strives to provide a practical strategy for responding to and managing incidents so as to achieve consistent and cost-efficient outcomes across NASA.

This handbook defines:

- What constitutes an Information Security incident;
- The various categories of incidents;
- Structured approaches to prioritizing incidents;
- Useful dispositions for determining a course of action and documenting the results of analysis;
- Roles and responsibilities for incident responders and those they interface with; and
- References for additional guidance and provides used cases for response examples.

Each of the following sections is designed to provide direction, at a high level, on how to manage an incident at NASA. Some sections have a collection of discussions that may provide beneficial background to the reader on a given subject. These discussions are outlined in Appendix F.

2.0 Incident Management Lifecycle Overview

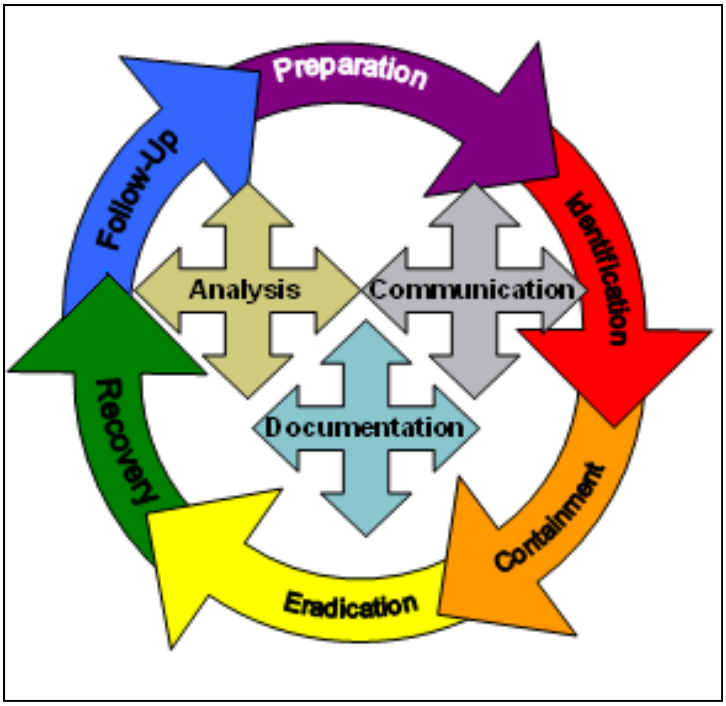


Figure 1 – The Incident Management Lifecycle

Information Security Incident Management at NASA is a lifecycle approach, represented by Figure 1 – The Incident Management Lifecycle, and is composed of serial phases (Preparation, Identification, Containment, Eradication, Recovery, and Follow-Up) and of ongoing parallel activities (Analysis, Communication, and Documentation). This lifecycle is derived from many standardized incident response processes such as those published by NIST and other authorities. The following are descriptions of those actions that comprise the NASA Incident Management Lifecycle:

- **Preparation:** Maintaining and improving incident response capabilities;
- **Identification:** Confirming, categorizing, scoping, and prioritizing suspected incidents;
- **Containment:** Minimizing loss, theft of information, or service disruption;
- **Eradication:** Eliminating the threat;
- **Recovery:** Restoring computing services quickly and securely; and
- **Follow-Up:** Assessing response to better handle future incidents through utilization of reports, "Lessons Learned" and after-action activities, or mitigation of exploited weaknesses to prevent similar incidents from occurring in the future.

Cross-cutting elements present throughout the Incident Management Lifecycle:

- **Communication:** Notifying appropriate internal and external parties and maintaining situational awareness;
- **Analysis:** Examining available data to support decision-making throughout the incident management lifecycle; and
- **Documentation:** Recording and time-stamping all evidence discovered, information, and actions taken from Identification through Follow-Up.

3.0 Definition and Categorizations

3.1 Definition of Incident

An Information Security incident is an adverse event or situation associated with electronic and non-electronic information that poses a threat to the integrity, availability, or confidentiality of that system. An Information Security incident results in the following:

- A failure of NASA information or Information Security controls;
- The waste, fraud, abuse, loss, or damage of NASA resources or information; and/or
- A violation or imminent threat of violation of NASA information protection and IT policies.

3.2 Categorizations

Table 1 contains the various types of Information Security incidents that may threaten an IT infrastructure.

Name	Description
Unauthorized Access	When an individual or entity gains logical or physical access without permission to a federal agency network, system, application, data, or other resource.
Denial of Service (DoS)	An attack that successfully prevents or impairs the normal authorized functionality of networks, systems or applications by exhausting resources. This activity includes being the victim or participating in the DoS.
Malicious Code	Successful installation of malicious software (e.g., virus, worm, Trojan horse, or other code-based malicious entity) that infects an operating system or application. Agencies are NOT required to report malicious logic that has been successfully quarantined by antivirus (AV) software.
Improper (or Inappropriate) Usage	When a person violates acceptable computing policies.
Suspected PII Breach	If an incident involves personally identifiable information (PII) a breach is reportable by being merely **Suspected**. (Suspected PII incidents can be resolved by confirmation of a non-PII determination.)
Suspected Loss of Sensitive Information	When an incident involves a suspected loss of sensitive information (not PII) that occurred as a result of Unauthorized Access, Malicious Code, or Improper (or Inappropriate) Use, but the cause or extent of which is not known.

Table 1 - Incident Categorizations

3.3 Indicators

Indicators to aid in appropriately categorizing an incident can be found in Appendix G –Incident Indicators by Category.

3.4 Priority

When multiple incidents occur simultaneously, the most serious or highest potential impact incidents should be handled first. The determination of incident priority is performed by the Incident Response Manager (IRM) based on knowledge of the incident and the affected device(s).

By default, all incidents are considered to have a Medium priority. An incident may be demoted to Low or promoted to High priority based upon the judgment of the IRM. Some factors to consider when determining priority include the following:

- The incident categorization (Section 3.2) -- the more severe the incident, the higher the priority;
- Whether sensitive information may be involved, i.e., sensitive Personally Identifiable Information (PII), Sensitive But Unclassified (SBU), ITAR; and

- The information system classification, e.g., FIPS 199 categorization, and the anticipated level of impact to the system or mission.

Some environments may want to apply a quantified approach which can be found in more detail in Appendix H.

3.5 Dispositions

An incident can be resolved in one of several ways. The most common incident resolutions are listed below in Table 2.

Incident	
Confirmed	*An incident has been **Confirmed** and response is underway according to the IM framework.*
Deferred	*A confirmed incident may be **Deferred*** due to resource constraints, or information type.
Unidentified	*A confirmed incident* involving an asset which cannot be located may be resolved as ***Unidentified.***
Transferred	*A confirmed incident may be **Transferred*** to OIG, OSPP, or another organization for further investigation.
Not An Incident	
Insufficient Data	When insufficient data is available to explain an ambiguous (i.e., not definitively hostile or benign) indicator, the incident may be dispositioned as ***Insufficient Data.***
Faulty Indicator	A false positive where an investigation reveals that the source indicator used as the basis for incident detection was a ***Faulty Indicator***.
Misconfiguration	A false positive where an event that appeared to be malicious activity was subsequently disproven and determined to be a ***Misconfiguration*** (malfunction) of a system.
Scan/Probe	Reconnaissance activity which ***Scanned*** or ***Probed*** for the presence of a vulnerability which may be later exploited to gain unauthorized access.
Failed	A ***Failed*** attempt to gain unauthorized access, conduct a denial of service, install malicious code, or misuse an IT resource, typically because a security control prevented it from succeeding.
Refuted	Any other circumstance where a suspected incident was determined to not be an incident and was ***Refuted***.
Duplicate	
Duplicate	*An incident may be a **Duplicate*** of another record in the Incident Management System, and should be merged with the existing workflow.

Table 2 - Incident Dispositions

4.0 Incident Management Roles and Responsibilities

4.1 Overview

This section describes the Incident Management roles and responsibilities as they relate to the phases of the Incident Management Lifecycle. Oversight responsibilities and delegation of authority from the NASA Chief Information Officer (CIO) through the Senior Agency Information Security Official (SAISO) and the Center Chief information Security Officer (CISO) is defined in NPR 2810.1 and is not further discussed within this document.

4.2 Core Incident Response Team Roles

The Permanent Incident Response Roles, outlined below, are functional in nature (i.e. duties are attached to a particular person or title, as opposed to actual or full time positions). Best practices indicate that it is a sound idea to assign IM roles across multiple individuals. However there is no prohibition to assigning several of these roles to a single individual.[1]

Center Privacy Manager (CPM)

The Center Privacy Manager's functional role is to make the determination of whether protected information (i.e., sensitive PII) may be involved in an incident. At some centers the CPM may also be the CISO. The CPM may delegate this incident responsibility to an individual who has the desired background. If sensitive information is not involved in the incident the CPM has no further responsibilities on the Incident Response Team.

Responsibilities:

- Determine if sensitive PII is involved, and CPM shall remain engaged in the incident management processes throughout the lifecycle of the incident.
- Determines the sensitivity of the information that the IRM determines is involved in the incident.
- Performs breach responsibilities as outlined in Appendix I of this Handbook, if sensitive information is involved.

Desired Background:

- Knowledgeable of privacy laws, and NASA privacy policies, procedures, and handbooks.
- A deep understanding of what is protected information.
- A deep understanding of protected information breach response.

Desirable certifications:

- Certified Information Privacy Professional/Government (CIPP/G) issued by the International Association of Privacy Professionals (IAPP)

Forensic Analyst (FA)

The Forensic Analyst's functional role is to receive guidance from the Technical Investigator and provides detailed forensic analysis of collected information and media. This is a highly specialized role.

Responsibilities:

- Analyzes information gathered by the IT Technician and/or Network Incident Analyst to evaluate a particular incident.
- Performs forensic analysis of media to determine information regarding the incident exploitation vector, activities on the system, system characteristics, etc.
- Generates a detailed forensic report identifying findings.

[1] The roles definitions leave open the appropriate staffing plan for a Center, Program, or Project. As future capabilities become available, it may be appropriate for an IRM to obtain services for one or more of the roles from an Agency resource. For example, the SOC provides network intrusion analysts for the wide area network, while several centers maintain complimentary capabilities. OCIO has also established a limited capability to provide forensics analysis to the Agency. As the NASA incident response processes mature, the IT Technician is a good area in which to consider re-tasking desktop technicians. For example, a system administrator could be trained to serve as an IT Technician; if the IT Technician were to encounter something unexpected, the Technical Investigator would provide or obtain support.

Desired background:

- Knowledgeable of computer hardware, including accessing and removing internal components such as hard drives.
- A deep understanding of forensic analysis software.
- A deep understanding of computer forensics.

Desirable certifications:

- SANS GIAC Forensics Analyst (GCFA)

Incident Response Manager (IRM)

This role is designated by the CISO or an Information System Owner (ISO). The Incident Response Manager is the primary function for tracking and managing incidents within the area of **defined** responsibility. In general, the IRM is designated by the CISO. For information systems requiring additional support, the ISO may appoint a system-specific IRM with the concurrence of the responsible SAISO/CISO. The SAISO/CISO will ensure the appropriate inclusion of the system-level IRM into the incident management processes.

The NASA Office of the Chief Information Officer (OCIO) will designate an IRM for Agency-level issues. The Agency IRM may direct other IRMs as required to coordinate incident response activities across the Agency.

Responsibilities:

- Ensures all incidents in area of responsibility are appropriately handled by cultivating more rapid and systematic detection, promoting situational awareness, and overseeing incident responders' efforts to minimize loss or service disruption, quickly and efficiently restore computing services, and ensure weaknesses that were exploited are mitigated.
- Ensures all incidents are appropriately reported, prioritized, categorized, tracked, assigned, and documented in the Incident Management System (IMS), incorporating impact and damage assessments.
- Ensures all incidents are promptly and thoroughly contained.
    - Includes authority to unilaterally take action to protect NASA's assets, e.g., suspend network access to a system or account, coordinated to the extent practical with the cognizant service or information system owner.
- Ensures that all follow-up activities are conducted, e.g. work to strengthen security controls, or weaknesses, that allowed the incident to occur.
- Ensures the ISO and ISSO are appropriately involved in the handling of the incident, specifically in assessing impacts of containment, eradication, and recovery.
    - Works with the ISO, ISSO, CISO, and CIO, among others.
- Engages the CPM immediately if there is suspicion, however slight, of sensitive or non-sensitive PII.
- Ensures incident response is conducted in compliance with the Incident Management Lifecycle and Incident Management Framework, emphasizing a continuous effort to contain and recover from incidents while incrementally improving security and employing a collection of tools to ensure that incident response activities are organized and that composure is maintained.
- Ensures technical investigators are assigned and fully supported throughout the Incident Management Lifecycle, and that they have performed an adequate analysis of the incident.
- When a data compromise is suspected to involve specific information types outlined in section 5.3d, collaborate with the appropriate subject matter expert (SME) to determine whether such data has actually been compromised. The IRM shall defer to the SMEs determination of compromised data is part of the specified type.
    - When one of the specific information types is involved, ensures that all necessary steps are being performed to use Information Security system capabilities to contain, control, and mitigate the potential risks of a breach and prevent any further unauthorized access to, or use of, the information.
- Refers Information Security incidents that are determined to be computer crimes immediately to the OIG for investigation.
- Supports the OIG for investigation of computer crimes as requested by the OIG.

Desired background:

- Knowledgeable in general Information Security issues and implementations.
- Knowledgeable in NASA Information Security policies.
- A deep understanding of the NASA Incident Management Lifecycle and associated processes.
- Excellent communications skills.
- DOD Secret clearance.

Desirable certifications:

- SANS GIAC Incident Handler (GCIH)
- ISC2 Certified Information System Security Professional (CISSP)
- ISACA Certified Information System Manager (CISM)

IT Technician (IT)

The IT Technician's functional role is to collect the necessary information from a system involved in an incident. The IT Technician takes guidance from and provides incident artifacts to the Technical Investigator.

Responsibilities:

- Gathers incident artifacts in accordance with incident response processes.

Desired background:

- Knowledgeable of computer hardware, including accessing and removing internal components such as hard drives.

Desirable certifications:

- CompTIA A+

Network Incident Analyst (NIA)

This role is designated by the NASA Security Operations Center (SOC) or, for center level monitoring, by the CISO. The Network Incident Analyst generally provides the first notification of an incident and thereby starts the incident management process which commonly results in the activation of an incident response process.

Responsibilities:

- Reviews events from a variety of information sources to identify incidents.
- Reports detected incidents in a prompt and timely manner using the established processes.

Desired background:

- Sufficient technical knowledge to evaluate events and determine when an Information Security incident has occurred.
- Familiarity with detection tools and information sources (e.g., Intrusion Detection Systems [IDSs], log-correlation.).
- Familiarity with the Agency processes for incident management.

Desirable certifications:

- SANS GIAC Intrusion Analyst (GCIA)

Technical Investigator (TI)

The Technical Investigator role is designated by the CISO, or as delegated, by the IRM. The TI serves as the primary technical focal point to track all aspects of one or more incidents, leads the analysis to determine the scope and entry vector of the incident, and assists the operations staff in the eradication and recovery of incidents. In general, a TI is needed for organizations with a local incident response capability. One or more TIs will function at the Agency level, as determined by the CIO, to address widespread incidents.

Responsibilities:

- Ensures all relevant information necessary to understand the incident is gathered in accordance with NASA incident management and response processes.
    - e.g., affected systems, asset information, vulnerability information, system configurations, IDS, logs, console reviews, memory dumps, forensic analysis, etc.
- Analyzes the gathered information to understand the scope of the incident.
- Assists the affected organization in ensuring the incident has been successfully eradicated.
- Assists the affected organization in ensuring the affected system is restored successfully to full operational status.
- Provides guidance to the IT Technicians and organization staff.
- Ensures a technical summary of the incident is prepared.

  - At a minimum, this will include the incident root cause(s), exploitation vector, and steps taken to address the incident.
- Ensures the IT Technicians are appropriately collecting incident artifacts.

Desired background:

- Knowledgeable in general Information Security issues and implementations.
- Knowledgeable in NASA Information Security policies.
- A deep understanding of the NASA Incident Management Lifecycle and associated processes.
- Excellent communications skills.
- A deep understanding of technical security issues and intrusion attributes.
- DOD Secret clearance.

Desirable certifications:

- SANS GIAC Incident Handler (GCIH)
- SANS GIAC Forensics Analyst (GCFA)

4.3 Auxiliary Incident Response Roles

Information System Security Official (ISSO)

The ISSO will assist in developing containment and remediation strategies, which minimize impact to an information system. Further reference to the roles and responsibilities of the ISSO can be found in current version of NPR 2810.

Subject Matter Expert (SME)

The SME will provide details about system configuration, architecture, implemented controls and other technical details which may impact the IM process. Some instances may require consulting a SME in order to take appropriate action.

4.4 Related Roles/Organizations

Center Chief Counsel

The Center Chief Counsel, or designee, advises on legal issues and reviews proposed breach notification materials for legal sufficiency.

Center Human Resources Employee Relations

The Center Human Resources Employee Relations advises the CPM in situations where disciplinary action may be taken against a civil servant.

Center Public Affairs Office

The Center Public Affairs Office advises the CPM on and reviews proposed notification materials and approaches.

Computer Security Official (CSO)

The CSO serves as a liaison between Information Security roles such as the IRM and organizational line management.

Contracting Officer (CO)/ Contracting Officer's Technical Representative (COTR)

The CO/COTR is responsible for ensuring that the proper security language is in included in a contractor's contract. The CO/COTR is responsible for influencing contractor performance, ensuring that contractor personnel follow all NASA Information Security policies, and that proper corrective actions are taken should the severity of an Information Security incident warrant the contractor to do so.

In situations where breached sensitive information was in the custody of a NASA contractor and being maintained on NASA's behalf, or where the information breached was information in NASA's custody about NASA contractors, the CO/COTR serves as the interface to the contractor and the CPM.

Incident Reporter
The Incident Reporter can be any NASA personnel, contractor, volunteer, or third party. Upon suspecting an Information Security incident, the Incident Reporter is responsible for contacting the NASA SOC.

Information System Owner (ISO)
The ISO evaluates the criticality of the system according to FIPS 199 and is responsible for eradication and recovery phases of the Incident Management Lifecycle. Often this responsibility is delegated to persons whom have an appropriate knowledge base, such as a System Administrator, or ISSO. Further reference to the roles and responsibilities of the ISO can be found in NPR 2810.

NASA Information Systems Network (NISN) Network Operations Center (NOC)
The NASA SOC works with the NISN NOC to provide agency-level capabilities for network-level containment.

NASA Security Operations Center (NASA SOC)
The NASA SOC is the central coordination and analysis facility for Information Security incidents. The NASA SOC provides agency-level incident tracking and network security monitoring. Some IR roles may be filled by staff of the NASA SOC.

Office of the Inspector General (OIG)
The NASA OIG may contact the Technical Investigator, or other IM roles, for information concerning OIG investigations into suspected criminal activity.

Office of Protective Services (OPS)
NASA OPS may contact the Technical Investigator, or other IM roles, for information concerning OPS investigations into counterintelligence activity.

Senior Agency Official for Privacy (SAOP)
The SAOP is the Agency CIO and is responsible for approving recommended actions and breach notification plans when multiple centers are impacted. The SAOP advises Agency Management on the situation and progress as appropriate.

System Administrator/Service Provider
A service provider will generally be responsible for implementing containment and remediation strategies, e.g., by removing a compromised machine from the network and rebuilding it. An example of this may be a contract IT Security Point of Contact.

United States Computer Emergency Response Team (US-CERT)
The SOC must report all security incidents to US-CERT after discovering the incident.

4.5 Incident Response Team

At the onset of an incident, an Incident Response Team (IRT) is assembled whose membership is commensurate to the severity and scope of the incident. The IRT will typically include the CISO or designee, the IRM, Technical Investigator, and can be augmented by other Incident Response members, such as a CPM, as required.

Below, Figure 2 demonstrates how parallel incident response teams may be operated, including use of different technical disciplines as required by the incident specifics.

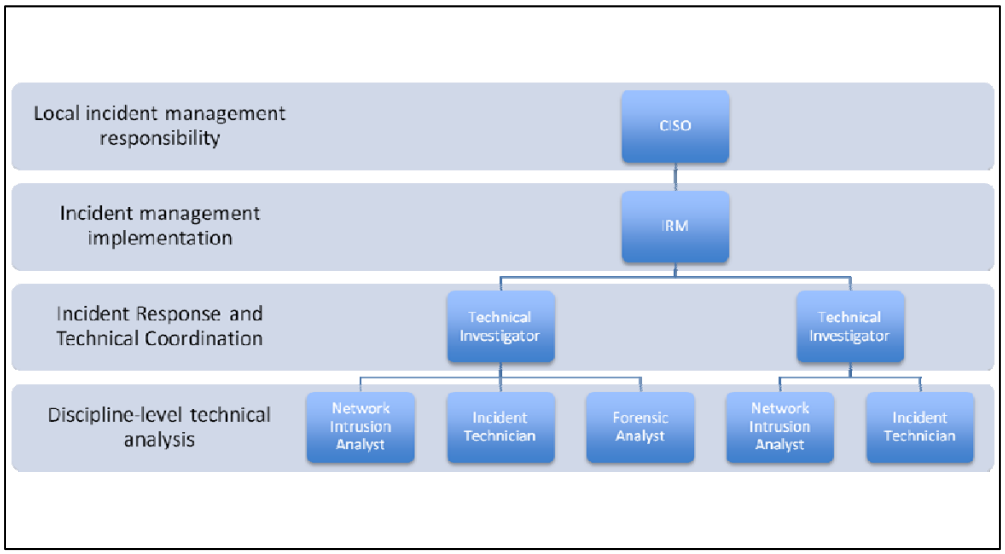


Figure 2 - Permanent Roles Notional Local View

Figure 3 demonstrates how the Agency IRM role may be utilized to manage widespread incidents.

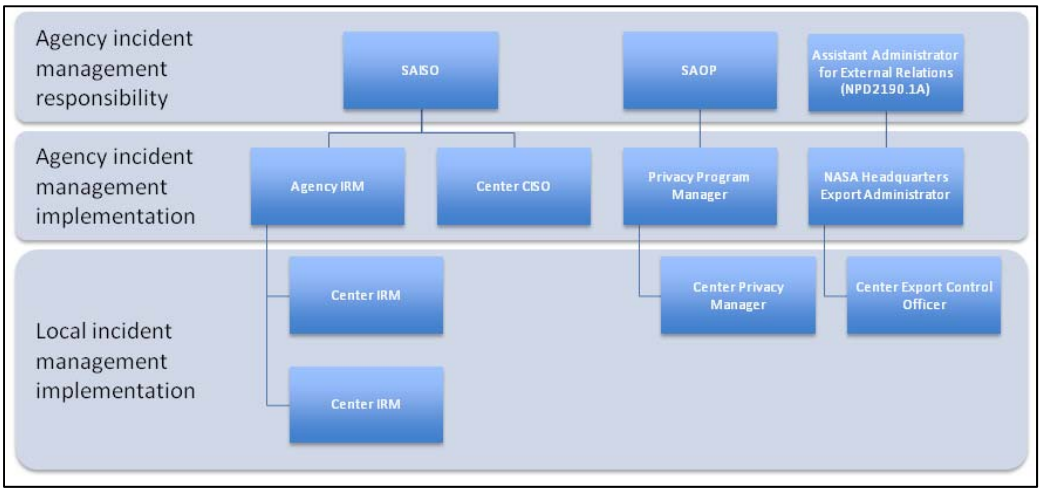


Figure 3 - Permanent Roles Notional Agency View

Figure 4 depicts which functional roles supporting incident response are filled at the Agency's various organizational levels. Where functional roles are defined as "Required" or "Optional", it denotes the requirement for the role to be staffed at that organizational level, but not necessarily the requirement for that role to participate in every incident that organization responds to (e.g., the Center Privacy Manager functional role must be staffed within every Center, but the Center Privacy Manager is not required to participate in response to Center incidents which do not involve PII).

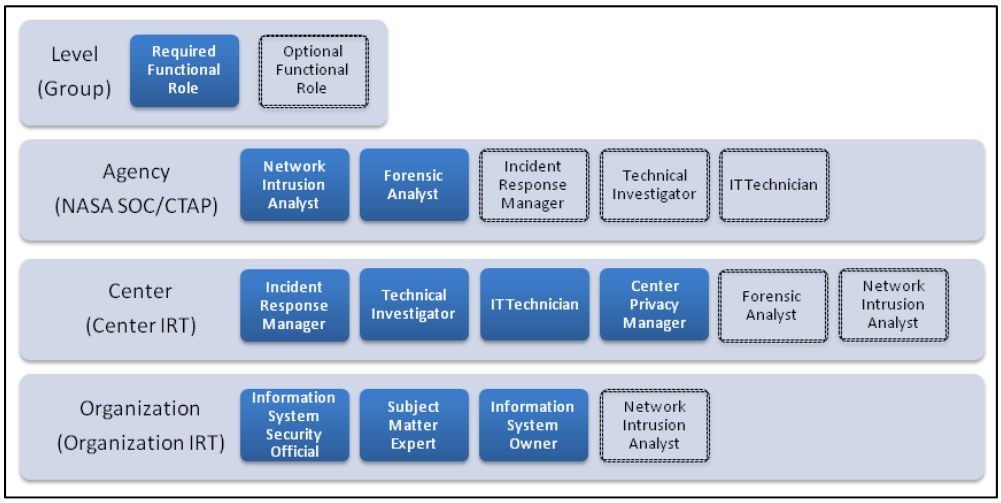


Figure 4 –Mapping Incident Management Roles to Organizations

5.0 Incident Management Lifecycle

5.1 Overview

This section describes each serial phase of the Incident Management Lifecycle, as illustrated in Figure 1 (located in Section 2), and outlines the requirements for each phase. It also describes the three parallel processes that occur throughout the Incident Management Lifecycle.

5.2 Incident Preparation

When the Information Security incident management process has not been activated, NASA is in a state of preparation. Incident Preparation is characterized by several activities:

- Establishing, organizing, and maintaining Incident Response Teams.
- Acquiring and maintaining the necessary tools and resources for incident response activities.
- Keeping the Incident Response Team familiar with their environment through exercises like frequent log reviews to better identify unexplained entries.
- Keeping all clients, servers, and other device clocks synchronized to strengthen event correlation.
- Training users in recognizing and reporting IT security incidents.

5.3 Incident Identification

a. Reporting a Suspected Incident

A report of an Information Security incident is the signal that Incident Preparation activities must be suspended and that the traditional Incident Management process must begin. When an Information Security incident is suspected or confirmed, the preferred methods for reporting it are either by calling the NASA SOC at 877-NASA-SEC, or by opening a ticket in NASA SOC IMS. An Information Security Incident Report shall contain all of the following information, if it is available at the time of the report, remaining information shall be reported as it becomes available:

- Submitter Name
- Submitter Phone Number
- Submitter Email Address
- Victim IP Address
- Victim Hostname / Domain Name
- Victim OS / Service Pack
- Victim Building and Room Number
- Victim System Security Plan Number
- Sensitivity and Description of Information Residing on Victim System (PII/SBU)
- Attacker IP Address
- Attacker Country, City
- Attacker Hostname / Domain Name
- Incident Summary
- Date / Time Incident Occurred
- Date / Time Incident Discovered (when the user detected the problem)
- Exploit Used or IDS/Anti-Virus Alert
- Incident Category
- Labor Hours / Cost of Downtime
- User's Role with NASA
- Systems or Networks the User Connected to Lately
- Symptoms (if user noticed anything strange about the computer)
- User Activity When Problem First Noticed
- User Location When Incident Occurred
- Detailed Description of Incident

b. Initial Response

Once an Information Security incident has been reported, traditional Incident Management processes begin immediately with Incident Identification. Identification is the process of determining whether or not an incident has occurred, and if so, determining the nature of the incident, categorizing the incident, and prioritizing incident response. The IRM or designee shall assign a person to be responsible for handling the incident. The preferred method for assigning an incident is via the IMS. The IRM or designee shall perform analysis to determine if there has actually been an incident and if so to understand its scope.

c. Categorizing and Prioritizing Incidents

Once it has been confirmed that an Information Security incident has occurred, the incident shall be categorized according to Section 3.2 Categorizations. The incident shall then be prioritized per Section 3.4, and shall be responded to in order of priority.

d. Additional Requirements for Specific Classes of Compromised Data

Once it has been confirmed that an Information Security incident has occurred, and if it is determined that sensitive information may be involved, the IRM shall ensure the appropriate functional Subject Matter Expert is involved in the response processes. Table 3 below, couples the information type with the SME that should be involved.

Information Type	Functional Subject Matter Expert to Involve
CLASSIFIED	Office of Protective Services
EAR	Export Control Officer
ITAR	Export Control Officer
PII	Center Privacy Manager
SBU	Center Chief Information Security Officer

Table 3 – Information Types and Subject Matter Experts

In addition to involving the CPM, the Breach Response process detailed in Appendix I shall be followed in the event of PII data compromise.

5.4 Incident Containment

a. Overview of Incident Containment

The overall purpose of Incident Containment is to limit the damage that an incident may cause while at the same time causing the least possible impact to mission-critical processes. The Containment phase of the Incident Management Lifecycle requires critical decision-making (e.g., determining whether to shutdown a system, disconnect it from the network, monitor its activity, or disable functions such as remote file transfer) and consists of short-term, planned actions that may remove access to compromised systems, limit the extent of current damage to a system, and prevent additional damage from occurring. The specific steps that should be followed depend on the type of incident (intrusion, virus, theft, etc.), and whether the incident is in progress (e.g., an intrusion, disruption of service) or is discovered after the action (e.g., a theft of equipment or a discovery within a log audit). Limiting the scope and magnitude of the incident as quickly as possible is a higher priority than allowing the incident to continue in order to gain evidence for identifying or prosecuting the perpetrator.

b. Selection of a Containment Strategy

When an Information Security incident affects mission-critical information or computing services, especially those with FIPS 199 “High” System Security Classifications, the IRM in consultation with the ISO and/or the ISSO, and other key affected parties shall decide how to address the incident while at the same time minimizing impact to mission-critical processes. In the case of a low-risk incident, the IRM may decide to move quickly to eradicate the incident without shutting down the affected system. In the case of a high-risk incident affecting a system with sensitive information or applications, the IRM may direct that the system be shut down or at least be temporarily isolated from the network. If there is a reasonable chance that letting a system continue to run as normal without risking serious damage, disruption, or compromise of data, or to identify a perpetrator, the IRM may determine that operations can continue under close monitoring.

5.5 Incident Eradication

a. Overview of Incident Eradication

Eradication is the application of sufficient technical measures on an affected system to eliminate the causes and effects of an intrusion or attack to a point where the risk of re-emergence of the cause is reduced to zero, or mitigated to a minimal or acceptable level. Once all containment procedures and actions have been completed, and all data which may be useful to performing an ongoing analysis of the compromise is collected, eradication may proceed.

b. Guidelines for Incident Eradication

- **Review Incident Analysis**: Data collected and analyzed shall be used to understand the exploited vulnerability and may inform the minimum requirements for eradication.
- **Perform a Vulnerability Analysis:** A vulnerability analysis tool (such as an automated vulnerability assessment tool) shall be used to scan exposed systems, services, and applications that are connected to the affected systems. Special attention may be paid to web servers/services, databases, or other complex architectures such as Service Oriented Architectures (SOA), mainframes, and e-commerce systems.
- **Improve Security Controls on the affected System and other Systems**: Appropriate protection techniques shall be implemented in the environment where appropriate. These techniques may consist of activities such as: applying security patches, changing the system name or IP address, securing and protecting boundary defense hardware and software, implementing Network Admission Control (NAC), implementing two-factor authentication, or in extreme cases, porting the machine's functions to a more secure operating system.
- **Focus on Removing Malignant Artifacts**: The IRT shall concentrate on the eradication of malignant artifacts (e.g., Trojan horses), and may concentrate on the eradication of benign artifacts if they present serious risk.
- **Thoroughly Remove Artifacts From all Media**: The ISO, or designee, shall ensure that all malicious artifacts are removed from all systems and media (including CD-ROMs and backup media) by using one or more proven commercial eradication applications or by manual surgical removal following an in-depth malware analysis which has identified the entirety of the malware package or by re-baseling the affected host.

5.6 Incident Recovery

a. Overview of Incident Recovery

Recovery is defined as restoration of affected systems to normal operational status. The recovery phase procedures for resumption of normal operations contained in this section provide a framework for use when recovering from an incident. The recovery process begins when the cause of the incident has been eradicated, or mitigated to a degree of risk determined to be acceptable by the ISO and the IRM.

b. Selection Requirements for System Recovery

For systems categorized with a FIPS 199 Low or Moderate Security classification, if the analyses conducted through the lifecycle has provided a high degree of confidence that the incident did not affect the software or the information stored on the system, then there may only be a minimal amount of effort required to provide assurance that the system is properly recovered. In this case, only simple countermeasures shall be needed to protect the system against future occurrences.

If the system has a FIPS 199 High Security classification systems, or in a case where the analyses conducted through the lifecycle has not provided a high degree of confidence that the incident did not affect the system software or data, then there may be a more complex recovery solution requiring a complete restoration of the system to a normal operating condition.

c. Framework for Incident Recovery

The required guidelines for conducting Recovery are:

- **Document the Recovery Phase**: Documentation of the recovery steps can assist in maintaining focus as the recovery process proceeds. All documentation associated with the incident shall be noted in the incident report for later review and reporting.
- **Decide the System Restoration Procedure**: Several restoration options may be available depending on the severity of the incident, the sensitivity of the system affected, and the backup systems available. The selection of the best option may require the involvement and authorization of the application/data owner, the CISO, and/or senior management.

- **Validate Data Restored from Untrustworthy Sources**: In restoring files other than the operating system and applications files, only the most trusted backup files shall be used. Restored system data and user files shall be investigated for altered data or other signs of compromise.
- **Validate the Restored System before Returning to Service**: Validation of the restored system shall be performed by executing a known series of development tests when prior test results are available for comparison. Prior to restoration of network connectivity, the ISSO shall verify that all known vulnerabilities have been mitigated.
- **Get Authorization and Communicate with Users before Restoring Service**: Before reconnecting the recovered system to the network to resume normal operations, the ISSO shall obtain authorization from the IRM and notify any organizations that would be affected.
- **Conduct a review of the security controls:** The IRM shall verify that the system is configured in accordance with the current configuration management guidelines; that logging, auditing, and accounting programs are functional; and any security tools are functioning. The ISSO is responsible for ensuring discrepancies are corrected.
- **Monitor the Restored System**: So as to maintain a high level confidence in the security of the restored system it shall be monitored to prevent additional intrusion, or a recurrence of the incident. Any knowledge gained through analysis should be used to provide insight into an attacker's techniques and/or methods to develop better monitoring techniques. Some items to be monitored may include: failed login attempts, attempts to access back doors, attempts to re-exploit the original vulnerability, and attempts to exploit any new vulnerabilities of the system. Monitoring may be performed at the Agency-level by the NASA SOC, at the Center level by the Center IT Security Team, at the system-level at the direction of the ISSO, etc.

Additional guidelines for conducting Recovery whenever operations allow:

- **Only Perform "Rapid Restoration" When Mission-Critical**: If it is decided to return to operation or maintain the affected system in operational use without completion of the recovery process due to mission-critical requirements, the recovery process may continue in parallel with operational use. Incident analysis and the elimination of vulnerabilities should continue in parallel with rapid restoration to mitigate the risk further incidents. Should system vulnerabilities exist, the system shall be updated as quickly as possible to preclude a recurrence of the same type of incident, the level of monitoring shall be increased and, and if applicable, intrusion detection shall be employed to ensure that a new incident is detected rapidly. It is preferred that mission-critical operations continue on unaffected, fail-over components when possible.
- **Replace the Affected System with a Backup System When Possible**: Employment of a backup system for operational use while the affected system is under examination may be permissible. Because data stored to backup may already be contaminated before the incident is actually reported and addressed, backup tapes shall be carefully examined to ensure the integrity of the data. The compromised system should first be isolated from the network and from all backup systems. The backup system data may then be restored from trusted system backup files rather than using possibly contaminated data files from the affected system. If system mirroring is employed, backup tapes shall be examined to determine at what point the restore should occur in order to ensure the integrity of the data restoration process.
- **Restore the System Offline Whenever Operations Allow**: Restoration of the operational system while it is kept off-line may provide the greatest opportunity for recovery of incident data and for determining the cause and extent of the incident. Operating the system in a stand-alone, single user status may prevent other users, intruders, and malicious processes from accessing or changing the compromised system.
- **Restore the Operating System from Trusted Media Whenever Operations Allow**: Installation of a new operating system may be performed on the affected system only if the activity is conducted with the original software media because compromise of the system may have occurred in many areas including binary and running process files.

Figure 5 below, incorporates the required and additional guidelines as outlined in the Incident Recovery Framework above and maps out the potential paths to be followed during the Recovery phase.

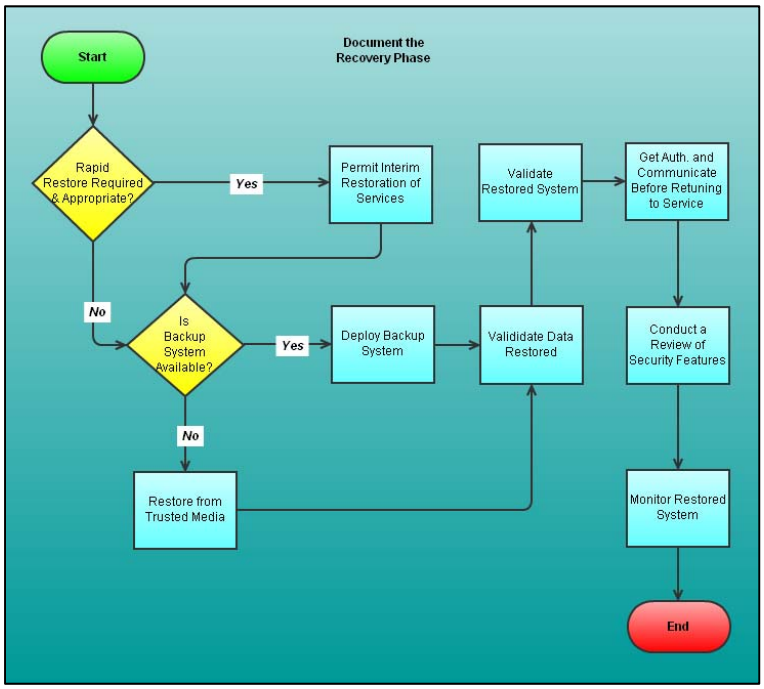


Figure 5 – Incident Recovery Framework

5.7 Incident Follow-Up

a. Overview of Incident Follow-Up

Performing post-incident activity is a critical step in responding to an incident. Post-incident activities enable the IRT and other staff members to learn from the successful and unsuccessful actions taken in response to an incident. Capturing, documenting, and disseminating what worked, and what did not, will help to reduce the likelihood of similar incidents re-occurring. The level of effort required for Follow-Up activities should reflect the scope and impact of the incident.

b. Post-Incident Analysis

So that critical details can accurately be recalled and recorded, a post-incident analysis shall begin as soon as possible. An after-action meeting with all involved parties shall be convened to disseminate details of the incident, address incident response procedures, and to obtain an estimate of costs resulting from the incident. Vulnerabilities uncovered during the incident response and analysis shall be remedied and a decision shall be reached as to whether or not to conduct a new system risk analysis.

c. Post-Incident Report

Information gathered during the incident post-analysis, as well as any other pertinent information, shall be included in an incident response report generated for the incident. The IRT shall prepare a report, including any "lessons learned" and cost analyses, which may be used to further staff awareness (without endangering security mechanisms) and/or can be used in training. This report should be disseminated to relevant personnel, such as the CSO for an organization affected by an incident, a supervisor in the event of a misuse incident, or a CO/COTR in the event of an incident involving contractor performance.

d. Revising Policies, Procedures, and Security Plans

The lessons learned report, derived from incident handling activities, may be incorporated into computer security policies, procedures, and security plans, training, and testing/exercises and the resulting changes implemented. Furthermore, "lessons learned" from each incident may be used to review Agency, Center, and Program-level computer security measures. Based on incident analysis and reporting, corrective actions may be developed and implemented to help prevent any recurrence of the incident, or to more effectively handle a recurrence.

5.8 Incident Documentation

Documentation is a parallel process that runs throughout the Incident Management Lifecycle. All phases of incident management require detailed documentation of actions taken and the conclusions drawn from analysis. Detailed documentation assists in determining the correct response and in supplying vital data for conducting follow-up investigation and producing the post-incident report. Documentation associated with incidents shall be protected in accordance with Agency requirements for Sensitive But Unclassified (SBU) data at a minimum. Documentation shall be stored in the NASA SOC Incident Management System whenever feasible. Documentation shall include any information that is associated with a specific incident, including the following:

- All computer or relative non-IT data, including host and network logs, forensics images, IDS logs, backup logs, and any other data or documentation that provides information about the compromised system(s) or file(s);
- All actions the incident response team initiates;
- Records of conversations with all personnel; and
- Any other auditing information produced by software tools, log files, and similar data.

5.9 Incident Analysis

a. Overview of Incident Analysis

Incident Analysis is an ongoing activity which may occur in sequence or in parallel to other activities throughout the Incident Management Lifecycle. The substantive findings of an Incident Analysis process results in a customized, efficient, and thorough Eradication procedure. Therefore, it is important that all information and facts gathered in the Reporting phase be properly documented and communicated to all parties involved with the Incident.

b. Identifying Artifacts

The primary reason to collect artifacts before, during, and after an incident is to help successfully resolve the incident and prevent its occurrence in the future. Artifacts may also be used for legal proceedings, therefore it is important to document how the artifacts were collected and preserved should they be used as evidence. For this reason, all artifacts transferred to the IRM, designee, or IRT shall be identified and protected. Hardcopy and physical artifacts shall be labeled, dated, signed, and stored in tamper-evident collection materials in a secure location with controlled access. Logical artifacts shall be stored in two locations and secured appropriately.

c. Protecting Artifacts

The validity of artifacts may be called into question within a legal proceeding if it can be shown that the artifact has not been accurately preserved. Physical artifacts shall be kept under lock and key, and logical artifacts shall have access controls; in either case only authorized persons shall have access to the artifact. To preserve their validity, artifacts shall first be stored securely. Second, to demonstrate the integrity of electronic artifacts a cryptographic hash shall be generated. At any point in the future a new matching cryptographic hash may be calculated, to offer mathematical proof that the artifact has not been changed. Third, when possible, logical artifacts shall be stored on tamper-resistant media such as CD-R or DVD-R.

5.10 Incident Communication

a. Overview of Incident Communication

Incident Communication is an ongoing activity that occurs throughout the Incident Management Lifecycle. The purpose is to keep appropriate internal and external parties informed and to maintain situational awareness.

b. Communication Channels

All incident-related information should be treated as Sensitive But Unclassified (SBU) and protected accordingly, including the encryption of email messages containing incident-related information. Transmissions which are derivative of incident response activities but which do not include incident information (e.g., a service request to wipe and reload a computer or change a password) are not considered SBU and do not require such protections. Avoid using compromised hosts or systems for incident handling discussions. If email, chat, or instant messaging systems are believed to be compromised, alternate systems or other out-of-band channels such as telephone, fax, or mail may be used to prevent the information from being intercepted by the attacker.

c. Communication Logs

All Communication should be logged or documented per Section 5.8.

6.0 Incident Management Framework

6.1 Overview

The Incident Management Framework is the collection of practices used to ensure that incident management activities are organized by maintaining situational awareness, rapidly and systematically detecting incidents, and appropriately responding to them. Since the phases of the Incident Management Lifecycle do not directly support Agency objectives to manage the handling of many incidents among different Incident Response Team members, the Incident Management Framework shall be employed to meet those objectives.

6.2 Incident Tracking

The NASA SOC Incident Management System is the mechanism for reporting an incident, tracking an incident as it progresses through the phases of incident management, documenting the confirmation-related research, documenting the response actions performed, securely archiving and sharing artifacts, and managing communications between members of the Incident Response Team.

6.3 The Incident Management Process Flow

Once an incident has been reported the incident management process begins. As an incident proceeds through the process, its status changes as it travels through discrete states of response. When an incident is reported, it begins with a “New” status. The IRM prioritizes and assigns the incident to a Technical Investigator (Assigned) who begins response as prioritized by the IRM (Response Initiated). Artifacts may need to be collected to support the analysis of the suspected incident. Based upon the results of the initial analysis, the Technical Investigator will disposition the suspected incident. If the disposition is a non-incident, deferred, or there is insufficient data to investigate, then it can be immediately resolved. If it is found to be a duplicate, it should be merged with the existing incident. Otherwise, the analysis should indicate that a suspected incident should enter the confirmed state. The analysis should also identify the criticality of the affected resources and determine the severity of the incident. The results of the analysis are recorded in the IMS.

Once an incident is confirmed, the IRM shall notify the appropriate parties, and proceed to perform and conclude the functions of containment, eradication, and recovery as outlined in Section 5, at which point an incident is considered to be Resolved. During the Resolution phase the Technical Investigator shall ensure that all documentation is complete, through, and accurate. As appropriate, the IRM shall review the effectiveness of the incident response process, review all documentation, confirm the disposition of the incident, and if needed identify and recommend improvements. The IRM may conduct a Lessons Learned meeting with all of the appropriate parties as a vehicle to discuss the resolution of the incident.

Once the IRM has determined that all necessary actions are completed, the incident is considered closed.

Figure 6, below, depicts the Incident Management Process Flow.

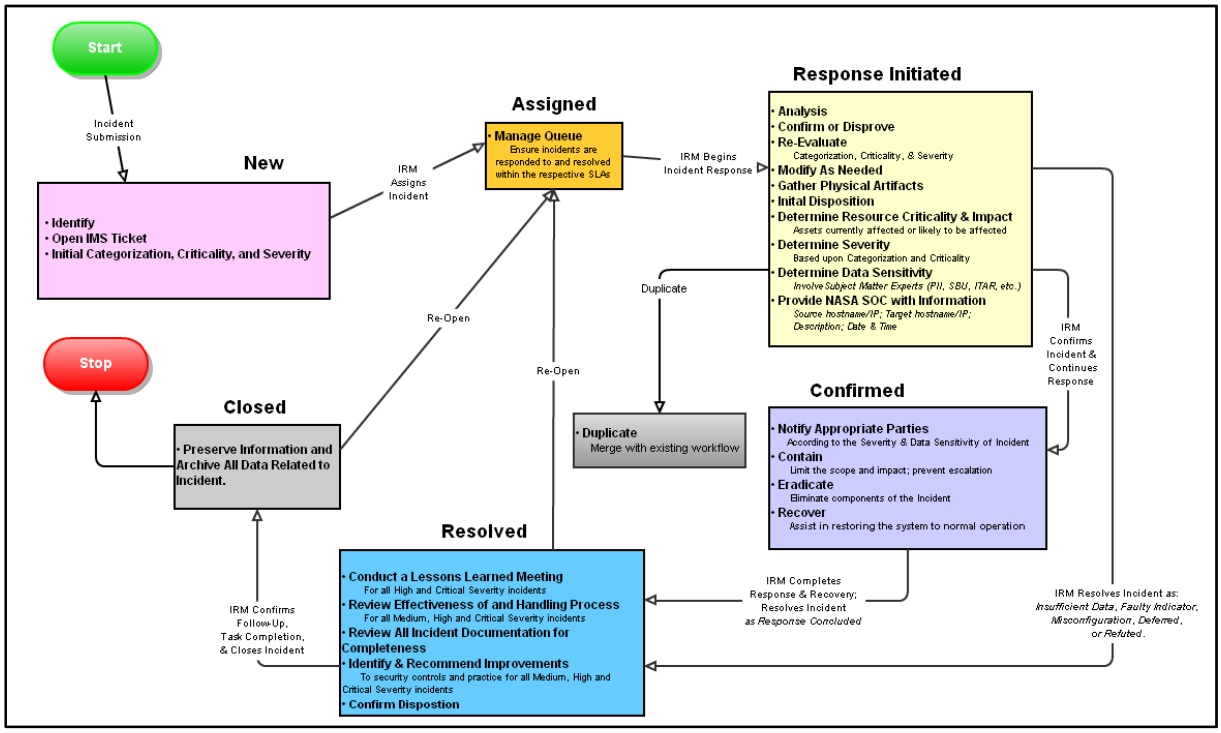


Figure 6 – Incident Management Process Flow

Figure 7 below depicts the relationship between the phases of the Incident Management Lifecycle and the incident statuses within the Incident Management Process Flow from Figure 6 above.

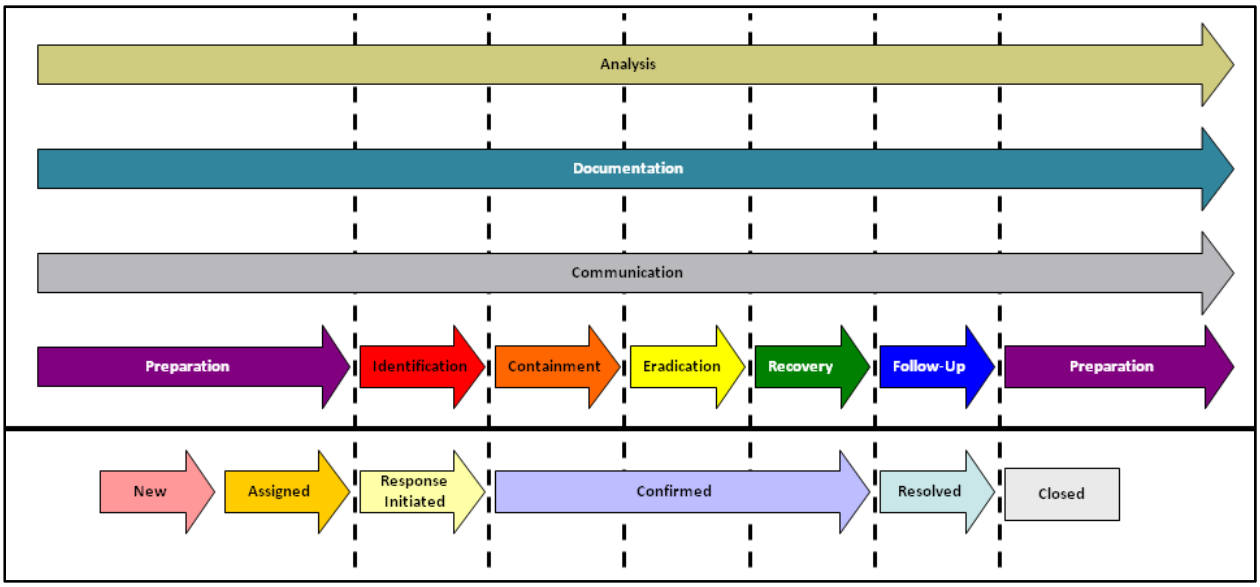


Figure 7 – Mapping the Incident Management Lifecycle to the Incident Management Process Flow

6.4 Mapping the IM Process Flow to the IM Roles

Figure 8 below, is a RACI (Responsible, Accountable, Consulted, and Informed) diagram that maps the Incident Management Roles and Responsibilities from above and outlines how each of the roles, as outlined in Section 4, interact with the states of the Incident Management Process Flow from Figure 6.

A RACI diagram describes the participation by various roles in completing a tasks, project or deliverable. **RACI** is an acronym derived from the four key responsibilities most typically used:

Responsible
: Those who are answerable for the correct, thorough, and successful completion of all work actions needed to achieve a task, project, or deliverable. Typically there is only one role with a participation type of "Responsible."

Accountable
: Those who are not responsible for the completion of a task, project, or deliverable, but are none the less accountable for the work performed.

Consulted
: Those whose opinions are sought concerning activity related to a task, project or deliverable.

Informed
: Those who are kept up-to-date on the progress of a task, project, or deliverable by those who are listed as "Responsible" or "Accountable." Often this is only done at completion of a task, project, or deliverable.

Legend:
R - Responsible
A - Accountable
C - Consulted
I - Informed

		Center CISO/SAISO	Incident Response Manager	Technical Investigator	Network Incident Analyst	IT Technician	Forensic Analyst	Sensitive Data Expert (CPM or other SME)	Information System Owner	IS Security Officer	Incident Reporter
1.0	**New Incident**										
1.1	Identify/Notify SOC	A	I								R
1.2	Involve CPM, or other SME, if required	A	R	C				I	I	I	
2.0	**Assigned**										
2.1	Manage Queue	A	R	C					I	I	
3.0	**Response Initiation**										
3.1	Analysis	I	A	R	C		C		I	I	
3.2	Gather Physical Artifacts		I	A		R	C		I	I	
3.3	Categorize		A	R	C				I		
3.4	Determine Resource Criticality and Impact		A	R					C		
3.5	Identify Compromised Data		A	R				I	C		
3.6	Determine Data Sensitivity	A	C					R			
3.7	Determine Priority	A	R	C					I		
3.8	Provide NASA SOC with Information	I	A	R	C			I	I	I	
4.0	**Confirmed**										
4.1	Notify Appropriate Parties	A	R	I					I	I	
4.2	Contain	A	R	C					I	C	
4.3	Eradicate	I	A	C					R	C	
4.4	Recover	I	A	C					R	C	
5.0	**Resolved**										
5.1	Document Incident		A	R							
5.2	Conduct a Lessons Learned Meeting	A	R	I					I	I	
5.3	Review the Effectiveness of the Handling Process	A	R	I					I	I	
5.4	Identify & Recommend Improvements	A	R	I					I	I	
6.0	**Closed**										
6.1	Preserve Handling Information	A	R								

Figure 8 – RACI Diagram Mapping Incident Management Process Flow to Incident Management Roles

7.0 References

The following references are useful for background information:

- E-Government Act 2002 (Title III: Federal Information Security Management Act - FISMA) – directs NIST to develop Information Security guidelines. <http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=107_cong_public_laws&docid=f:publ347.107.pdf>
- SP 800-53rev3: Recommended Security Controls for Federal Information Systems: Incident Response (IR) Family – The organization implements an incident response capability for security incidents including policies and procedures, training, testing and exercises, handling, monitoring, reporting, assistance, and a response plan. <http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final.pdf>
- NIST SP800-61rev1 "Computer Security Incident Handling Guide" – covers a high level incident handling process. <http://csrc.nist.gov/publications/nistpubs/800-61-rev1/SP800-61rev1.pdf>
- OMB M-06-19 – Reporting Incidents Involving PII. <http://www.whitehouse.gov/omb/memoranda/fy2006/m06-19.pdf>
- OMB Memo, Sept. 20, 2006 – Recommendations for Identity Theft Related Data Breach Notification Guidance. <http://www.whitehouse.gov/omb/memoranda/fy2006/task_force_theft_memo.pdf>
- OMB M-07-16 – Safeguarding Against and Responding to Breach of PII; incident reporting and handling. <http://www.whitehouse.gov/omb/memoranda/fy2007/m07-16.pdf>
- President's Identity Theft Task Force – Ensure effective, risk-based responses to data breaches suffered by federal agencies. <http://www.idtheft.gov/reports/StrategicPlan.pdf>
- NPR 2810.1A - Chapter 17 – Agency guidance for security incident handling. <http://nodis3.gsfc.nasa.gov/npg_img/N_PR_2810_001A_/N_PR_2810_001A_.pdf> <http://nodis3.gsfc.nasa.gov/npg_img/N_PR_2810_001A_/N_PR_2810_001A__Chapter17.pdf >

Appendix A – Acronyms

Acronym	Meaning
ARP	Address Resolution Protocol
AV	Anti-Virus
BPA	Blanket Purchase Agreement
BRT	Breach Response Team
CIO	Chief Information Officer
CIPP/G	Certified Information Privacy Professional/Government
CISM	Certified Information System Manager
CISO	Center Chief Information Security Officer
CISSP	Certified Information System Security Professional
CO	Contracting Officer
Comp TIA	Computing Technology Industry Association
COTR	Contracting Officer's Technical Representative
CPM	Center Privacy Manager
CPU	Central Processing Unit
CSIRT	Computer Security Incident Response Team
CUI	Controlled Unclassified Information
DDoS	Distributed Denial of Service
DNS	Domain Name System
DOD	Department of Defense
DoS	Denial of Service
EAR	Export Administration Regulations
EAR	Enterprise Archive
FIPS	Federal Information Processing Standards
FOUO	For Official Use Only
FTC	Federal Trade Commission
FTP	File Transport Protocol
GCFA	GIAC Certified Forensics Analyst
GCIA	GIAC Certified Intrusion Analysts
GCIH	GIAC Certified Incident Handler
GIAC	Global Information Assurance Certification
GSA	General Services Administration
HTTP	Hyper-Text Transport Protocol
IAPP	International Association of Privacy Professionals
ICMP	Internet Control Message Protocol
IDPS	Intrusion Detection and Prevention System
IDS	Intrusion Detection System
IMS	Incident Management System
IP	Internet Protocol
IR	Incident Response
IRM	Incident Response Manager
IRT	Incident Response Team
ISACA	Information Systems Audit and Control Association
ISC2	International Information Systems Security Certification Consortium (pronounced "ISC-squared")
ISO	Information System Owner
ISP	Internet Service Provider
ISSO	Information System Security Officer
IT	Information Technology
ITAR	International Traffic in Arms Regulations
ITS	Information Technology Security

Acronym	Meaning
MD5	Message-Digest Algorithm 5 is a widely used cryptographic hash function
NAC	Network Admission Control
NASA	National Aeronautics and Space Administration
NetBIOS	Network Basic Input / Output System
NISN	NASA Integrated Services Network
NIST	National Institute of Science and Technology
NPR	NASA Procedural Requirements
OCIO	Office of the Chief Information Officer
ODIN	Outsourcing Desktop Initiative for *NASA*
OIG	Office of the Inspector General
OMB	Office of Management and Budget
OPS	Office of Protective Services
OS	Operating System
OSSP	Office of Security and Program Protection
PII	Personally Identifiable Information
RAM	Random Access Memory
SAISO	Senior Agency Information Security Official
SAOP	Senior Agency Official for Privacy
SANS	Sys Admin, Audit, Network Security: a security standards setting organization
SBU	Sensitive But Unclassified
SLA	Service Level Agreement
SME	Subject Matter Expert
SOA	Service Oriented Architecture
SOC	Security Operations Center
SOP	Standard Operating Procedure
SP	Special Publication
SSN	Social Security Numbers
SYN	A *Syn*chronize request from a client to a server
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
US-CERT	United States-Computer Emergency Readiness Team

Appendix B – Unauthorized Access Use Case

Handling Unauthorized Access Incidents

Unauthorized Access occurs when an individual gains logical or physical access without permission to a federal agency network, system, application, data, files or other resource. Unauthorized Access falls under the US-CERT and NIST Incident definition of category 1.

This checklist is presented as a guide as opposed to a strict sequence of actions to be followed.

Initial Action

- Evaluate information obtained from any external sources to the potential victim computer. This information may include any records or notifications received from external sources outside of NASA. These may include the following; email notifications, intrusion detection system (IDS) logs, Network Flow records, System logs from centralized log database and Firewall logs.
- Evaluate the information gathered and determine if an incident response process is to be activated.
- Open a SOC Incident Management System (IMS) ticket, notify the CISO, IRM and IRT and begin the incident response process. This process issues an initial incident notification by encrypted email and enters the following information into the IMS database:
  - [1] Unique SOC IMS Number
  - [2] Date and time of discovery
  - [3] Center affected
  - [4] Privacy information determination
  - [5] USCERT one hour reporting requirement status
  - [6] System name or IP address
  - [7] Method of discovery
  - [8] Description of symptoms
  - [9] Attached external logs
  - [10] Actions to be taken.
- Assign an IT Technician and/or Forensic Analyst to the incident.
- Notify the local System Administrator of the infected system(s) and instruct them to not to use or modify the system(s) until directed by appropriate security personnel.

Identification

- Evaluate the system or files source for criticality and sensitivity of information (SBU/CUI, PII, ITAR, etc.) using the Severity Index table and determine a priority level for the incident.
- If the compromised system or file source is determined to be of high or critical value or pose substantial exposure to the agency consider disconnecting or blocking the compromised system from the network or Internet.
- Run Live Response tools (Mandiant IR, etc.) to gather all current running process status and system state information. Gather all system log files, Application logs and any other relevant log files.
- Examine all external and local response logs obtained to determine the level of compromise (user, root or data). Look for altered system files, added programs, root kits, Bot Nets, back-doors, hidden special files and directories.
- If identification of the compromise system is determined to be at a system or root level consider blocking the system from external access if not already blocked earlier.
- Determine the scope of compromise by examining network records for potential access to other systems within the agency from the hostile host. If more systems are found to have been accessed run the above identification steps for each suspect system.
- If the file source is non-electronic, refer to the policies and guidance of the NASA Office of Protective Services (OPS) for investigative or forensic techniques.
- Keep the SOC Incident Management System (IMS) database updated with current incident details.

Containment

- If it is determined that the attacker is originating from an external host/network and the attack is escalating, disconnect or block the attacker at the perimeter (NASA/Center) firewall.
- If the compromise is spreading rapidly and/or is considered to be of high risk, consider sending an 'All Personnel' email to warn and instruct employees of the current threat.
- Ensure that all system processes related to the compromise have been stopped and removed from the system.
- Run a full vulnerability scan (preferably credentialed) of the compromised system(s) and submit the scan report to the System Administrator for remediation.

Eradication/Recovery

- Ensure that all files modified or added to the system by the attackers have been removed.
- If the compromise was determined to be at a system or root level it is recommended to reinstall the operating system from an original source.
- Restore any affected data modified or deleted from backups and make changes if needed to the original configuration with modifications necessary to preclude reoccurrence of the incident.
- Review system configurations to ensure the following are current:
    - Versions and patches of all system software
    - Auditing and monitoring of systems
    - System and data access control lists
    - User/System accounts
- Rerun a vulnerability scan on the system(s) to ensure all known issues have been remediated.
- Update, certify, and preserve original copies of the incident logs and other incident-related information to the IMS database.

Post-Incident Activities

- Update monitoring signatures and/or escalate alert responses to prevent a reoccurrence of the incident.
- Document the details of the incident and the steps taken to neutralize the incident and determine the root cause of the infection.
- Perform an analysis of the following areas to determine where performance could have been improved:
    - Whether preparation was adequate;
    - Whether detection was prompt and response procedures were adequate;
    - Whether the incident was sufficiently contained;
    - Whether recovery was adequate; and
    - Whether personnel and organization communications were adequate throughout the response to the incident.
- Submit any recommendations for enhanced computer security processes.
- Update the SOC Incident Management System (IMS) database with all incident details.

For further detail, please see NIST Special Publication 800-61 rev 1 at <http://csrc.nist.gov/publications/PubsSPs.html>.

Appendix C – Malicious Code Use Case

Handling Malicious Code Outbreaks

Malicious code incidents include viruses, worms, Trojan horses, keystroke loggers, backdoors and root-kits. Today malicious code (or Malware) incidents are by far the most prolific and the use of such programs for profit is increasing. Malicious code falls under the US-CERT and NIST Incident definition of category 3.

The terms virus and worms are used to define the method in which malicious code spreads rather than the behavior of the malicious code itself. Worms are self propagating (autonomous) malicious code that uses the network as its transport mechanism and infects other computers on the network by exploiting weaknesses in programs. Viruses depend on the end user to run or execute the malicious code to infect the computer.

Trojan horses, root-kits and backdoors are used to define the nature of concealment. A trojan horse conceals the harmful effects of the malicious code by disguising its true destructive nature. Root-kits on the other hand modify operating system programs to prevent detection. Backdoor malicious code installs programs that allow an intruder access to the computer by bypassing any authentication mechanisms. Backdoor malicious code is sometimes used by BotNets for remote control.

This checklist is presented as a guide as opposed to a strict sequence of actions to be followed.

Initial Action

- Evaluate information obtained from any external sources to the potential victim computer. This information may include any records or notifications received from external sources outside of NASA. These may include the following; email notifications, intrusion detection system (IDS) logs, Network Flow records, System logs from centralized log database and Firewall logs.
- Evaluate the information gathered and determine if an incident response process is to be activated.
- Open a SOC Incident Management System (IMS) ticket, notify the CISO, IRM and IRT and begin the incident response process. This process issues an initial incident notification by encrypted email and enters the following information into the IMS database:
  - [1] Unique SOC IMS Number
  - [2] Date and time of discovery
  - [3] Center affected
  - [4] System name or IP address
  - [5] Method of discovery
  - [6] Description of symptoms
  - [7] Attached external logs
  - [8] Actions to be taken
- Assign an IT Technician and/or Forensic Analyst to the incident.
- Notify the local System Administrator of the infected system(s) and instruct them to not to use or modify the system(s) until directed by appropriate security personnel.

Identification

- If the malicious code is known to be one of the following high risk infection categories, *worm, email SPAMMER, keystroke logger or BotNet*, then the Technical Investigator recommends the removal of the infected system from the network or Internet since these tend to cause high risk behavior to the Agency.
- Evaluate the system for criticality and sensitivity of information (SBU/CUI, PII, ITAR, etc.) using the Severity Index table and determine a priority level for the incident.
- Run Live Response tools (MANDIANT IR, etc.) to gather all current running process status and system state information. Gather all system log files, Anti-virus logs and any other relevant application log files.
- Determine the state of Anti-Virus software: Application name, last update of virus patterns, version, etc.
- If identification of infection has not been determined obtain an Image of the system to run detail forensic analysis.

- Run forensic analysis tools on system or system image to determine the details of the type and nature of the malicious code. These may include root-kit scanners and malicious code detection scanners.
- Keep the SOC Incident Management System (IMS) database updated with current incident details.

Containment

- If it is determined that the originator of the malicious code is an external host/network and the attack is escalating, consider disconnecting or blocking the attacker at the perimeter (NASA/Center) firewall.
- If the infection is propagating and spreading rapidly and/or is considered to be of high risk malicious code, consider sending an 'All Personnel' email to warn and instruct employees of the current threat.
- Ensure that all system processes related to the malicious code have been stopped and removed from the system.
- Run a full vulnerability scan (preferably credentialed) of the infected system and submit the scan report to the System Administrator for remediation.

Eradication/Recovery

- Ensure that all files related to the malicious code have been removed from the system.
- If it is not certain that all files infected by the malicious code were discovered, a reformatting/reimage of the system should be accomplished.
- Restore the affected system(s) and/or network (using original software media to restore software) to the original configuration with any modifications to preclude reoccurrence of the incident.
- Review system configurations to ensure the following are current:
    - Versions and patches of all system software;
    - Auditing and monitoring of systems;
    - System and data access control lists; and
    - User/System accounts.
- Rerun a vulnerability scan on the system to ensure all known issues have been remediated.
- Update, certify, and preserve original copies of the incident logs and other incident-related information.

Post-Incident Activities

- Update monitoring signatures and/or escalate alert responses to prevent a reoccurrence of the incident.
- Document the details of the incident and the steps taken to neutralize the incident and determine the root cause of the infection.
- Perform an analysis of the following areas to determine where performance could have been improved:
    - Whether preparation was adequate;
    - Whether detection was prompt and response procedures were adequate;
    - Whether the incident was sufficiently contained;
    - Whether recovery was adequate; and
    - Whether personnel and organization communications were adequate throughout the response to the incident
- Submit any recommendations for enhanced computer security processes.
- Update the SOC Incident Management System (IMS) database with all incident details.

For further detail, please see NIST Special Publication 800-61 rev 1 at <http://csrc.nist.gov/publications/PubsSPs.html>.

Appendix D – Use Case for Inappropriate Use

Handling Inappropriate Usage Incidents

An *inappropriate usage* incident occurs when a user performs actions that violate acceptable computing use policies. Although such incidents are often not security related, handling them is very similar to handling security-related incidents. Therefore, it has become commonplace for incident response teams to handle many inappropriate usage incidents. Inappropriate Usage falls under the US-CERT and NIST Incident definition of category 4.

Examples of incidents a team might handle are users who:

- Download password cracking tools or pornography;
- Send spam promoting a personal business;
- Email harassing messages to coworkers;
- Set up an unauthorized Web site on one of the organization's computers;
- Use file or music sharing services to acquire or distribute pirated materials; and/or
- Transfer sensitive materials from the organization to external locations.

This checklist is presented as a guide as opposed to a strict sequence of actions to be followed.

Initial Action

- Evaluate information obtained from any external sources to the potential victim computer. This information may include any records or notifications received from external sources outside of NASA. These may include the following; email notifications, intrusion detection system (IDS) logs, Network Flow records, System logs from centralized log database and Firewall logs.
- Evaluate the information gathered and determine if an incident response process is to be activated.
- Open a SOC Incident Management System (IMS) ticket, notify the CISO, IRM and IRT and begin the incident response process. This process issues an initial incident notification by encrypted email and enters the following information into the IMS database:
  - [1] Unique SOC IMS Number
  - [2] Date and time of discovery
  - [3] Center affected
  - [4] System name or IP address
  - [5] Method of discovery
  - [6] Description of symptoms
  - [7] Attached external logs
  - [8] Actions to be taken
- Assign an IT Technician and/or Forensic Analyst to the incident.
- Notify the local System Administrator of the affected system(s) and instruct them to not to use or modify the system(s) until directed by appropriate security personnel.

Identification

Inappropriate usage incidents are most often detected through user reports, such as seeing inappropriate material on a user's screen or receiving a threatening email. There are usually no precursors of inappropriate usage. Table Appendix D-1 lists actions such as unauthorized service usage and access to inappropriate materials. For each such action, the table lists possible indications of the action. The table can be customized easily by the organization to include environment-specific precursors and indications, which should facilitate a more efficient and effective incident handling process.

Inappropriate Action	Possible Indications
Unauthorized service usage (e.g., Web server, file sharing, music sharing)	• Network intrusion detection and network behavior analysis software alerts • Unusual traffic to and from the host • New process/software installed and running on a host • New files or directories with unusual names (e.g., "warez" server style names) • Increased resource utilization (e.g., CPU, file storage, network activity) • User reports • Application log entries (e.g., Web proxies, FTP servers, email servers)
Access to inappropriate materials (e.g., downloading pornography, sending spam)	• Network intrusion detection alerts • User reports • Application log entries (e.g., Web proxies, FTP servers, email servers) • Inappropriate files on workstations, servers, or removable media
Attack against external party	• Network intrusion detection alerts • Outside party reports • Network, host, and application log entries

Table Appendix D-1. Inappropriate Usage Indications

The Incident Response Team should be cautious about assisting with reports of inappropriate usage that are not clearly incidents. For example, a manager might report that an employee seems to be wasting significant time with computers, but the manager has no idea what the employee is doing. The manager might ask the team to monitor the employee's Internet usage and analyze files on the user's hard drive. The team should verify that the request has been approved by appropriate management and human resources personnel via written approval.

Containment, Eradication, Recovery

Inappropriate usage incidents typically require no containment, eradication, or recovery actions, other than possibly deleting objectionable materials or uninstalling unauthorized software. For most inappropriate usage incidents, evidence acquisition is important. Evidence may be needed for prosecuting or disciplining an individual and for limiting liability by demonstrating that the organization did its best to prevent, detect, and halt the activity. Evidence storage is particularly important because internal users have physical access to many facilities. Addressing the threat of having evidence altered or destroyed may require coordination with the organization's physical security staff.

Post-Incident Activities

- Update monitoring signatures and/or escalate alert responses to prevent a reoccurrence of the incident.
- Document the details of the incident and the steps taken to neutralize the incident and determine the root cause of the infection.
- Perform an analysis of the following areas to determine where performance could have been improved:
    - Whether preparation was adequate;
    - Whether detection was prompt and response procedures were adequate;
    - Whether the incident was sufficiently contained;
    - Whether recovery was adequate; and
    - Whether personnel and organization communications were adequate throughout the response to the incident.
- Submit any recommendations for enhanced computer security processes.
- Update the SOC Incident Management System (IMS) database with all incident details.

For further detail, please see NIST Special Publication 800-61 rev 1 at <http://csrc.nist.gov/publications/PubsSPs.html>.

Appendix E – Denial of Service Use Case

Handling Denial of Service Attacks

A Denial of Service (DoS) is an action that prevents or impairs the authorized use of networks, systems, or applications by exhausting resources such as central processing units (CPU), memory, bandwidth, and disk space. Denial of Service falls under the US-CERT and NIST Incident definition of category 2.

Examples of DoS attacks are:

- Using all available network bandwidth by generating unusually large volumes of traffic;
- Sending malformed TCP/IP packets to a server so that its operating system will crash;
- Sending illegal requests to an application to crash it;
- Making many processor-intensive requests so that the server's processing resources are fully consumed (e.g., requests that require the server to encrypt each reply);
- Establishing many simultaneous login sessions to a server so that other users cannot start login sessions;
- Broadcasting on the same frequencies used by a wireless network to make the network unusable; and/or
- Consuming all available disk space by creating many large files.

This checklist is presented as a guide as opposed to a strict sequence of actions to be followed.

Initial Action

- Evaluate information obtained from any external sources to the potential victim computer. This information may include any records or notifications received from external sources outside of NASA. These may include the following; email notifications, intrusion detection system (IDS) logs, Network Flow records, System logs from centralized log database and Firewall logs.
- Evaluate the information gathered and determine if an incident response process is to be activated.
- Open a SOC Incident Management System (IMS) ticket, notify the CISO, IRM and IRT and begin the incident response process. This process issues an initial incident notification by encrypted email and enters the following information into the IMS database:
  - [1] Unique SOC IMS Number
  - [2] Date and time of discovery
  - [3] Center affected
  - [4] System name or IP address
  - [5] Method of discovery
  - [6] Description of symptoms
  - [7] Attached external logs
  - [8] Actions to be taken
- Assign an IT Technician and/or Forensic Analyst to the incident.
- Notify the local System Administrator of the infected system(s) and instruct them to not to use or modify the system(s) until directed by appropriate security personnel.

Identification

DoS attacks can be detected through particular precursors and indications, primarily those listed in the following tables. Table Appendix E-1 lists possible precursors of a DoS attack, explains the reason why each action might be performed, and provides a recommended response to potentially prevent a related incident from occurring. Table Appendix E-2 lists malicious actions such as a network-based DoS, a DoS against an operating system, and a DoS against an application, and possible indications of each action. These tables can easily be customized by the organization to include environment-specific precursors and indications, which should facilitate a more efficient and effective incident handling process.

Precursor	Response
DoS attacks are often preceded by reconnaissance activity—generally, a low volume of the traffic that will be used in the actual attack—to determine which attacks may be effective	If handlers detect unusual activity that appears to be preparation for a DoS attack, the organization may be able to block the attack by quickly altering its security posture—for example, altering firewall rulesets to block a particular protocol from being used or protect a vulnerable host
A newly released DoS tool could pose a significant threat to the organization	Investigate the new tool and, if possible, alter security controls so that the tool should not be effective against the organization

Table Appendix E-1 Possible Precursors of a DoS Attack

Malicious Action	Possible Indications
Network-based DoS against a particular host	User reports of system unavailability: • Unexplained connection losses • Network intrusion detection alerts • Host intrusion detection alerts (until the host is overwhelmed) • Increased network bandwidth utilization • Large number of connections to a single host • Asymmetric network traffic pattern (large amount of traffic going to the host, little traffic coming from the host) • Firewall and router log entries • Packets with unusual source addresses
Network-based DoS against a network	User reports of system and network unavailability: • Unexplained connection losses • Network intrusion detection alerts • Increased network bandwidth utilization • Asymmetric network traffic pattern (large amount of traffic entering the network, little traffic leaving the network) • Firewall and router log entries • Packets with unusual source addresses • Packets with nonexistent destination addresses
DoS against the operating system of a particular host	User reports of system and application unavailability: • Network and host intrusion detection alerts • Operating system log entries • Packets with unusual source addresses
DoS against an application on a particular host	User reports of application unavailability: • Network and host intrusion detection alerts • Application log entries • Packets with unusual source addresses

Table Appendix E-2 Malicious Actions and Possible Indications

Although these tables may be helpful in analyzing incidents, they are missing an important component—the indications that are associated with benign activities. Benign and malicious events may present similar symptoms, which can make it difficult for analysts to promptly determine if an incident has occurred. Extending the indications table to include benign activities should assist in distinguishing benign from malicious activity. For example, if the organization loses Internet connectivity, many—but not all—of the symptoms may be similar to a network-based DDoS. This information should be added to the table, with information as to how the benign activity may be distinguished from its malicious counterpart.

DoS attacks pose some additional challenges in terms of incident analysis:

- DoS attacks often use connectionless protocols (UDP and ICMP) or use a connection-oriented protocol in such a way that full connections are not established (e.g., sending TCP SYN packets to create a synflood attack). Therefore, it is relatively easy for attackers to use spoofed source IP addresses, making it difficult to trace the source of attacks. ISPs may be able to assist in tracing the activity, but it is often more effective to review logs for previous reconnaissance activity that appears to be related. Because the attacker would want to receive the results of the reconnaissance, such activity is unlikely to use a spoofed address, so it may indicate the location of the attacker.
- DDoS attacks often use thousands of workstations that are controlled by a single handler (or no handler at all). These workstations usually have bots installed that are considered “zombies” and are activated by the controller to attack other systems. The victim site will not see the IP of the handler, and even if it could, it is likely that it is just another host that the attacker has compromised.
- Network-based DoS attacks are difficult for IDPS sensors to detect with a high degree of accuracy. For example, synflood alerts are one of the most common false positives in network IDPS products. If an attacker performs a rapid SYN scan, many IDPS products will report it as a synflood, even though the activity is sending only one request to each port. If a server crashes, hosts trying to reconnect to it may keep sending SYN packets. Sometimes many legitimate connections in a short time (e.g., retrieving many elements of a Web page) will also cause a synflood alert to be triggered.
- When an outage occurs, no one may realize that a DoS attack caused it. For example, a Web server may crash occasionally as a result of operating system instability, requiring a reboot for its functionality to be restored. If an attacker sends some specially crafted packets to the Web server that cause it to crash, system administrators may assume the crash resulted from the operating system’s instability and not realize that an attack took place.

Containment

Containment for a DoS incident usually consists of stopping the DoS. Sometimes this is easy; usually it is not. Often the first thought is to block all traffic from the source of the activity. However, as previously mentioned, such attacks often have spoofed source addresses or use thousands of compromised hosts—in either case, making it difficult or impossible to implement effective filtering based on source IP addresses. Even if the organization can block the source addresses that are being used, the attacker can simply move to other IP addresses. Other possible solutions for containing a DoS are as follows:

- **Correct the Vulnerability or Weakness That Is Being Exploited.** For example, if the attack can occur because packet filters do not block packets using UDP port 7 (echo) and a publicly accessible host is accidentally running echo, the filters should be altered to block packets destined for the echo port; and the host’s configuration should be changed so that it no longer offers the echo service. If an unpatched operating system is susceptible to a DoS from specially crafted packets, patch the operating system. The host may need to be temporarily disconnected from the network to halt the DoS while the host is strengthened.
- **Implement Filtering Based on the Characteristics of the Attack.** For example, if the attack is using ICMP echo requests, one could alter the perimeter security to temporarily block such requests from entering the network. Unfortunately, this is not always practical—if an attacker is sending a SYN flood to a Web server’s HyperText Transfer Protocol (HTTP) port, blocking SYN packets destined for that port will itself cause a DoS for users. In addition, most DoS attack tools are versatile, so if one attack method is blocked, attackers can easily switch to another method. Another strategy is rate limiting—permitting only a certain number of packets per second to use a specific protocol or contact a certain host. Although filtering techniques can be valuable in containing incidents, they can introduce additional problems. For example, adding new rules to a router or firewall may have a substantial negative impact on the device’s performance, causing network slowdowns or even a DoS. Organizations should carefully consider where filtering should be implemented (e.g., border router, firewall) and should be prepared to upgrade networking devices if necessary to facilitate filtering of long-term attacks.
- **Have the ISP Implement Filtering.** A network-based DoS from external hosts may overwhelm the organization’s Internet routers. The organization must rely on its ISPs to implement filtering that blocks the activity.
- **Relocate the Target.** If a particular host is being targeted and other containment strategies are not working, the host could

be moved to a different IP address. This is deemed "security through obscurity" because the attacker may locate the moved target and attack it again. The targeted service could be transferred to a different host—one without the same vulnerability.

The decision-making process for containing a DoS incident should be easier if recommended actions are predetermined. This can be done with a matrix or other written guidelines for when each potential solution should be implemented, if ever. The containment strategy may include several solutions in sequence, for example—

[1] Implement filtering based on the characteristics of the attack
[2] Correct the vulnerability or weakness that is being exploited
[3] Have the ISP implement filtering
[4] Relocate the target

Eradication/Recovery

[1] Implement filtering based on the characteristics of the attack
[2] Correct the vulnerability or weakness that is being exploited
[3] Have the ISP implement filtering
[4] Relocate the target

Post-Incident Activities

- Update monitoring signatures and/or escalate alert responses to prevent a reoccurrence of the incident.
- Document the details of the incident and the steps taken to neutralize the incident and determine the root cause of the infection.
- Perform an analysis of the following areas to determine where performance could have been improved:
    - Whether preparation was adequate;
    - Whether detection was prompt and response procedures were adequate;
    - Whether the incident was sufficiently contained;
    - Whether recovery was adequate; and
    - Whether personnel and organization communications were adequate throughout the response to the incident
- Submit any recommendations for enhanced computer security processes
- Update the SOC Incident Management System (IMS) database with all incident details.

For further detail, please see NIST Special Publication 800-61 rev 1 at <http://csrc.nist.gov/publications/PubsSPs.html>.

Appendix F – Extra Discussion

Selection of a Containment Strategy

The containment effort consists of short-term, planned actions that will remove access to compromised systems, limit the extent of current damage to a system, and prevent additional damage from occurring. The specific steps that should be followed depend upon the type of incident (intrusion, virus, theft, etc.), and whether the incident is in progress (e.g., an intrusion, disruption of service) or is discovered after the action (e.g., a theft of equipment or a discovery within a log audit).

Factors to consider when selecting an Incident Containment Strategy include:

- Define the acceptable level of risk to each of the NASA mission processes and the systems and networks that support them;
- Determine to what extent these processes, systems, and networks must maintain confidentiality, integrity, and availability, even during a major incident, and what the relative priority is of each aspect of security;
- Determine whether to inform users that an incident has occurred or is occurring;
- Identify the extent to which containment actions might destroy or mask information required to later assess the cause of the incident;
- If the incident is ongoing, identify the extent to which containment actions might alert the perpetrator (e.g., malicious user, thief, or other individual with malicious intent);
- Identify when to involve senior management in containment decisions, especially when containment includes shutting systems down or disconnecting them from a network; and
- Identify who has the authority to make decisions in situations not covered by existing containment policy.

Cryptographic Hashes

Various aspects of the incident response process require the generation of cryptographic hashes in order to verify the integrity of acquired artifacts. Per guidance from NIST, the reliability of certain older families of hash algorithms (including MD5 and SHA-1) has been reduced due to various cryptographic attacks, and those algorithms are not to be used by Federal agencies. In keeping with that guidance, the authoritative hash used for NASA incident response activities should come from the SHA-2 family, preferably SHA-512. But, for the purpose of interoperability with partners and external data sources not yet using SHA-2 algorithms, an MD5 hash should *also* be generated where possible. This guidance will be revisited when the SHA-3 standard has been finalized by NIST.

Overview of Live Host Analysis

A critical part of Incident Analysis is the collection of volatile data from the victim computer. Volatile data consists of any data which would not be available after the computer is turned off, primarily data stored in RAM. In recent years, more advanced attackers have begun using malware which leaves no traces on the victim hard drive and cannot be identified using dead host analysis. Since a dead host analysis requires a forensic image made after the machine has been powered off, it is important to perform live host analysis to capture as much volatile information as possible before the machine is powered down. The NASA Handbook for Collection in Incident Response should be consulted for detailed procedures for performing Live Host Analysis. Only well-trained and careful IT Technicians should perform volatile data collection.

- ***Do No Harm***: Do no further damage to the system and do not further affect performance in any way. Use a standardized, automated set of simple tools whenever possible to minimize any potential impact. While it is not preferred to log into a compromised system with root or administrative privilege credentials, it is often necessary for forensic tools to operate properly, so do so with an account whose password can be quickly changed and which has those privileges on as few machines as possible.
- ***Operate at a Low Level***: Unlike dead host forensics which function via external control over the media, live host forensics takes place within a live, compromised system which cannot be trusted. To adapt to this condition when performing collection of volatile data, use read-only media containing trusted statically-compiled binaries (which do not rely on system libraries) that use kernel modules or hardware interrupts to collect information (rather than user-level tools). This point seems duplicative; guidance is not necessarily consistent with current best practice.
- ***Do it Quickly***: Because it is imperative to contain the incident as quickly as possible and because the attacker may still have access to the system, it important to only perform actions within the scope of Live Host Analysis and to move on. Attackers

who still have access may detect the activities of the Incident Responder and react by changing tactics to hide themselves better or by destroying data.

- ***Minimize the Footprint***: While it is important to collect volatile data before it is lost, it is also important to preserve non-volatile data on the hard drive and to avoid looking for the attacker using obvious methods which may tip them off. Responders should use simple, discrete tools which do not require being copied to the victim system, do not require use of libraries on the victim system, and which avoid changing access times to files on the victim system.

a. Information Collected During Live Host Analysis

Once the System Administrators and the Incident Reporter have been interviewed, the Incident Responder should visit the location of the victim computer and collect volatile data such as the following (for Windows systems):

- System Date, Time, Time zone
- System Information Summary
- Audit Policy
- ARP Cache
- DNS Cache
- NetBIOS Name Table
- Routing Table
- Current Network Connections
- Running Processes
- Running Services or Daemons
- System, Application, and Security Logs
- The System Registry
- Scheduled Jobs
- Program Started at Boot or User Login
- Users Currently Logged In
- Files Open over the Network
- Open TCP/UDP Ports
- IP Configuration
- Hidden Files/Alternate Data Streams
- Protected System Files
- Various Root Kit Detection Profiling
- Full Memory Dump
- Swap File Dump
- Hibernation File Dump
- Dump of Suspicious Processes Running in Memory

The volatile data should be triaged at the site of the victim computer using a Forensics Laptop to perform the basic analysis required to identify additional volatile data that may need to be collected. Most often this is a memory dump of a suspicious process.

b. Dead Host Analysis

After volatile data has been collected for Live Host Analysis, the IRT may obtain a full volume forensic image of the victim system. The goal of acquiring a forensics image is to preserve a bit-for-bit copy of a data storage device. Attackers are becoming increasingly proficient in quickly destroying evidence of their illegal intrusion, so capturing a forensics image early in incident response may help preserve evidence that might later be destroyed. Assuming the victim hard drive can be preserved as evidence, the forensics image is a working copy that can be used for analysis. If the original hard drive will be modified in any way (e.g., so that it may be put back into service), then two copies of the forensics image should be created and stored in separate locations so that one can serve as evidence and as a backup while the other can be a working copy for analysis. Only well-trained and careful Incident Responders should perform forensic imaging, preferably using tools approved by the NASA SOC. A hard drive is considered an electronic artifact and will require the generation of a cryptographic hash to demonstrate its integrity.

The guidelines for acquiring a forensic image are:

- Employ hardware write blockers to prevent accidental tainting of suspect data whenever possible;

- Ensure that imaging tools account for issues such as Host Protected Areas (HPAs), and have been tested and validated to generate reliable images;
- Never boot the suspect storage device; and
- Generate a cryptographic hash to demonstrate the image's integrity.

c. Malware Analysis

Malware analysis allows the Incident Responder to open the "black box" of an unknown binary to determine the capabilities of the tool which can be used to generate additional investigative leads, providing low-level knowledge of the tool which may allow for identification of additional victims and the creation of signatures for intrusion detection systems and anti-virus software. Often malware analysis may even identify the origin and skill level of the programmer and user of the tool, and sometimes even clues to their identity.

The guidelines for conducting Malware Analysis are:

- Only run malware in a VERY secure analytical environment, including virtualized environments;
- Use simple static analysis tools and perform manual static analysis using a dis-assembler when a safer analysis technique is needed, when you want to perform a dissection of the tool's attributes to determine how it operates, and when you have more time;
- Use simple dynamic analysis tools and perform manual dynamic analysis using a debugger when a more secure analytical environment is available for more in-depth analysis, when you want to observe and manipulate the tool in action to determine what it does, and when you need results quickly; and
- Employ un-packers to expose armored malware, but be careful where you acquire these tools because they cannot always be trusted.

Selection Requirements for System Recovery

The guidelines for conducting Recovery are:

- **Documentation of the Recovery Phase**: Documentation would assist in recovering from future incidents especially if the recovery from the incident involves steps that are used for the first time and are not described in any other documentation.
- **Only Perform "Rapid Restoration" When Mission-Critical**. Rapid restoration offers the least assurance of system integrity and preservation of information that may provide information needed for a complete investigation of the cause of the incident. Specifically, incident analysis and the elimination of vulnerabilities should continue in parallel.
- **Replace the Affected System with a Backup System When Possible**: Employing a backup system for operational use while the affected system is under examination has the advantage of "freezing" the affected system to provide the most complete data for an investigation. However, there would be some operational time lost while the backup system is prepared for operational use. In addition, there may be some incident related-data lost, especially malicious user access data, when the affected system is isolated from the network.
- **Restore the System Offline Whenever Operations Allow**: This option also provides the opportunity to regain control of the system. If the system is not disconnected from the network, there is a risk that the intruder may continue to be connected, undoing recovery steps accomplished on the system. The drawback to this restoration method is loss of operational productivity.
- **Validate Data Restored from Untrustworthy Sources**: System data should be investigated for altered data or other signs of compromise. In an Unauthorized Access incident, malware such as sniffers or backdoors may be left behind. While user productivity benefits from using the most recent, but possibly untrusted, backup files, using the latest trusted backup to restore data files that are known to have not been compromised is preferred.
- **Validate the Restored System before Returning to Service Whenever Possible**: Validating the system is a significant factor in determining when and if a system should be restored to a network or returned to operational status. At a minimum, rudimentary functionality tests should be conducted.
- **Get Authorization and Communicate with Users before Restoring Service:** System users may also be notified that the system is returning to normal operations. Depending on the type of incident, consider requiring all users to change their passwords. Once the affected system has been restored, all users should review restored data files that resided on the compromised system and ensure the files were not affected by the incident. All executables or binary files residing in user areas should also be handled in the same manner as system executables. Conduct a review of the system to ensure security features are functioning properly. Specifically, ensure the system is configured according to the current configuration

management guidelines that any security tools are functioning, and that logging, auditing, and accounting programs are functional.

- **Monitor the Restored System**: Monitoring the previously compromised system will detect additional intrusion attempts and prevent damage quickly. Intruder information may sometimes be gained by monitoring any intruder actions immediately after a system has been restored to operational use. Useful threat information may be obtained from failed login attempts, attempts to access back doors, attempts to re-exploit the original vulnerability, and attempts to exploit new vulnerabilities.

Benefits of Incident Follow-Up

Devoting further resources to an incident after the Recovery Phase is not always cost-effective. However, following up on an incident after the Recovery Phase improves incident handling procedures and will result in an environment with better safeguards and more efficient processes and procedures. Feedback from incident analysis and reporting is essential in the evolution of effective incident response security policies and procedures. If applicable, recommendations contained in the incident report may be adopted by revising security policies, procedures, plans, and user and administrator training in order to prevent recurrence of similar incidents. The recommendations may also be used as the basis for modifying this Incident Response Plan or other incident response procedures. Vulnerabilities uncovered during the incident response and analysis should be remedied and a decision should be reached as to whether or not to conduct a new system risk analysis.

Incident Response Procedure Analysis

Analysis of incident response procedures is key to determining how to protect against and minimize the impact of future occurrences and to assess how well the organization responded to the incident. Questions for consideration in gathering information for analysis and reporting of the incident are as follows:

- What are the details of the incident and what was done to neutralize the effects of the incident? Answers to this question may be used to capture important details in addition to those recorded in the incident log.
- Was there sufficient preparation for the incident by users, computer specialists, and managers?
- Did detection and response processes and procedures work as intended? If not, where did they not work? Why did they not work?
- Was the incident detected in real-time or near real-time?
- Are there incident detection tools, methods of discovery, monitoring procedures, or improvements in these areas that would have improved the capability to detect the incident?
- Was the incident sufficiently contained, and are there response improvements that would have enhanced containment of the incident?
- Were methods to collect evidence sufficient to support a successful investigation and future litigation by law enforcement?
- Could correction procedures have been improved for a more effective recovery?
- What practical difficulties were encountered in responding to the incident?
- Are there updates to policies and procedures that would have enabled a more effective response and recovery?
- Were communications procedures, internal and external, adequate throughout the detection and response processes?
- Was there sufficient preparation for the incident?
- Did detection occur promptly or, if not, why not?
- Could additional tools have helped the detection and eradication process?
- Was the incident sufficiently contained?
- Was communication adequate, or could it have been better?
- What practical difficulties were encountered?
- If privacy related, was the one hour reporting requirement to USCERT met, based upon time of discovery vice time of SOC Report? If not, why?

Incident Response Cost Analysis

An important consideration in post-incident analysis is the determination of financial costs associated with the incident response capability. Deriving a dollar figure associated with an incident would not only assist in assessing damage for prosecution, but would also demonstrate the importance of expenditures associated with computer security. Examples of costs that are typically included in incident response cost analysis are:

- Costs of damaged computer system assets. (Recommend conducting an inventory of the affected computer system assets, not only to discover and determine the cost of damaged assets, but also to provide assurance of the integrity of undamaged assets.);
- Monetary cost associated with personnel time required to deal with the incident;
- Cost due to lost operations; and
- Estimated value of any compromised sensitive information assets. (If applicable, one might show the value of any data accessed but not compromised by a malicious user to show the risk of loss associated with the incident.)

Incident cost is expressed in terms of dollars and reputation; costs should be considered for all phases of the incident response lifecycle with the exception of follow-up activities. Calculate incident dollars cost by quantifying the hourly labor costs for relevant personnel (dollars per hour), then multiplying by the hours expended on work related to the incident, then sum. Calculate the incident reputation cost (high, medium, or low) by considering public knowledge of any of the following (where an incident fits more than one description, use the greater of the impacts):

- System downtime (low);
- Virus outbreak (low);
- Non-critical system compromise, including Web defacement (medium);
- Any system compromise which leads to attacks on third parties (high);
- Exposure of privacy information (high); or
- Mission system compromise (high).

Appendix G - Incident Indicators by Category

Incident Identification can be very difficult because there are many different means of detecting incidents with varying levels of reliability, there is a constant high volume of indicators which are received, and deep technical knowledge and experience are required to analyze incident-related data. Although no single indicator conclusively shows that a computer security incident is taking place, observing one or more prompts the observer to investigate events more closely. System Administrators who encounter one or more indicators should report a suspected IT Security Incident to the NASA SOC and work with the designated Agency, Center, and Organization incident responders to determine exactly what has occurred.

Malicious Action	Possible Indicators\Symptoms
Unauthorized Access	
Root compromise of host	• Existence of unauthorized security-related tools or exploits • Unusual traffic to and from the host • System configuration changes, including: process/service modifications or additions, unexpected open ports, system status changes (restarts, shutdowns), changes to log and audit policies and data, network interface card set to promiscuous mode (packet sniffing), new administrative-level user account or groups • Modifications of critical files, timestamps and privileges, including executable programs, OS kernels, system libraries, and configuration and data files • Unexplained account usage (e.g., idle account in use, account in use from multiple locations at once, unexpected commands from a particular user, large number of locked-out accounts) • Significant changes in expected resource usage • User reports of system unavailability • Network and host intrusion detection alerts • New files or directories with unusual names (e.g., binary characters, leading spaces, leading dots) • Highly unusual operating system and application log messages • Attacker contacts the organization to say that he or she has compromised a host
Unauthorized data modification	• Network and host intrusion detection alerts • Increased resource utilization • User reports of the data modification • Modifications to critical files • New files or directories with unusual names (e.g., binary characters, leading spaces, leading dots) • Significant changes in expected resource usage
Unauthorized usage of standard user account	• Access attempts to critical files (e.g., password files) • Unexplained account usage (e.g., idle account in use, account in use from multiple locations at once, commands that are unexpected from a particular user, large number of locked-out accounts) • Web proxy log entries showing the download of attacker tools
Physical intruder	• User reports of network or system unavailability • System status changes (restarts, shutdowns) • Hardware is completely or partially missing (i.e., a system was opened and a particular component removed) • Unauthorized new hardware (e.g., attacker connects a packet sniffing laptop to a network or a modem to a host)
Unauthorized data access	• Intrusion detection alerts of attempts to gain access to the data through FTP, HTTP, and other protocols • Host-recorded access attempts to critical files
Denial of Service	
Network-based DoS against a particular host	• User reports of system unavailability • Unexplained connection losses • Network intrusion detection alerts • Host intrusion detection alerts

	• Increased network bandwidth utilization • Large number of connections to a single host • Asymmetric network traffic pattern (large amount of traffic going to the host, little traffic coming from the host) • Firewall and router log entries • Packets with unusual source addresses
Network-based DoS against a network	• User reports of system and network unavailability • Unexplained connection losses • Network intrusion detection alerts • Increased network bandwidth utilization • Asymmetric network traffic pattern (large amount of traffic entering the network, little traffic leaving the network) • Firewall and router log entries • Packets with unusual source addresses • Packets with nonexistent destination addresses
DoS against the operating system of a particular host	• User reports of system and application unavailability • Network and host intrusion detection alerts • Operating system log entries • Packets with unusual source addresses
DoS against an application on a particular host	• User reports of application unavailability • Network and host intrusion detection alerts • Application log entries • Packets with unusual source addresses
Malicious Code	
A virus that spreads through email infects a host	• Antivirus software alerts of infected files • Sudden increase in the number of emails being sent and received • Changes to templates for word processing documents, spreadsheets, etc. • Deleted, corrupted, or inaccessible files • Unusual items on the screen, such as odd messages and graphics • Programs start slowly, run slowly, or do not run at all • System instability and crashes
A worm that spreads through a vulnerable service infects a host	• Antivirus software alerts of infected files • Port scans and failed connection attempts targeted at the vulnerable • Increased network usage • Programs start slowly, run slowly, or do not run at all • System instability and crashes
A Trojan horse is installed and running on a host	• Antivirus software alerts of Trojan horse versions of files • Network intrusion detection alerts of Trojan horse client-server communications • Firewall and router log entries for Trojan horse client-server communications • Network connections between the host and unknown remote systems • Unusual and unexpected ports open • Unknown processes running • High amounts of network traffic generated by the host • Programs start slowly, run slowly, or do not run at all • System instability and crashes
Malicious mobile code on a web site is used to infect a host with a virus, worm, or Trojan horse	• Unexpected dialog boxes, requesting permission to do something • Unusual graphics, such as overlapping or overlaid message boxes
Malicious code on a web site exploits vulnerabilities on a host	• Unexpected dialog boxes, requesting permission to do something • Unusual graphics, such as overlapping or overlaid message boxes • Sudden increase in the number of emails being sent and received • Network connections between the host and unknown remote systems
A user receives a virus hoax message	• Original source of the message is not an authoritative computer security group, but a government agency or an important official person

	• No links to outside sources • Tone and terminology attempt to invoke panic or a sense of urgency • Urges recipients to delete certain files and forward the message to others
Inappropriate Usage	
Unauthorized service usage	• Network intrusion detection and network behavior analysis software alerts • Unusual traffic to and from the host • New process/software installed and running on a host • New files or directories with unusual names (e.g., "warez" server style names) • Increased resource utilization (e.g., CPU, file storage, network activity) • User reports • Application log entries (e.g., Web proxies, FTP servers, email servers)
Access to inappropriate materials	• Network intrusion detection alerts • User reports • Application log entries (e.g., Web proxies, FTP servers, email servers) • Inappropriate files on workstations, servers, or removable media
Attack against external party	• Network intrusion detection alerts • Outside party reports • Network, host, and application log entries
Reconnaissance	
Network host and port enumeration scanning	• Network and host intrusion detection alerts • Increased resource utilization

Table Appendix G – 1 Incident Indicators by Category

Appendix H – Quantified Approach for Incident Prioritization

Industry best practice suggest that incidents should be responded to and resolved in a prioritized fashion according to their severity of the incident, the current and potential impact of the incident, and the necessary urgency of a response. The priority will vary with circumstances and can be dictated by the IRM, but generally priority is based on eight factors:

[1] Incident Categorization (Section 3.2)
[2] Information: The classification of any information believed to be compromised
[3] Security Classification: The FIPS 199 System Security Classification of devices compromised
[4] System Impact: The percentage of a system's resources which are affected
[5] Mission Impact: The impact to the Agency Mission
[6] Cost: The projected cost of incident response activities
[7] Urgency: The urgency required for a successful resolution
[8] Publicity: The current publicity

The potential impact of an incident indicates an outcome that is at least somewhat likely to occur given the nature of the threat and the ability of our security controls to mitigate it. For example, if:

- A new network worm begins to spread among moderate security classification devices,
- There are no network firewalls between these devices and a high security classification system,
- There are no anti-virus signatures or host firewalls in the high security system,
- And the devices in the high security system are vulnerable to the exploit the worm uses to spread.

In this case, the malicious code outbreak spreading to the high security classification system is a potential impact of this incident, and the incident should be prioritized as though this outcome were already an actuality.

Table Appendix H-1 and Appendix H-2 may be used to calculate IT Security Incident Priority based on the eight factors identified above. The Incident Priority Value is calculated using Table Appendix H-1 by identifying the Priority Index (values in leftmost column) for each incident attribute (remaining columns) and adding them together. This value is mapped to a Priority Level using the scale found in Table Appendix H-2.

Index Rating	NASA ITS-SOP-015 Incident Categorization	Classification of Compromised Information	FIPS 199 System Security Category	Percent of System Devices \ Accounts Affected	Agency Mission Impact	Projected Cost of Incident Response	Urgency	Current Publicity
0	Inappropriate Use	No \ Public Information	Low	< 0.1%	None	< $1K	Line Staff visibility OR successful resolution does not require response within one month	Unlikely
1	DoS	Company \ Confidential Information		0.1% - 1%	Small affect on productivity \ operations	$1K - $5K	Line Staff visibility OR successful resolution does not require response within one week	Possible
2	Malicious Code	SBU \ FOUO	Moderate	1% - 2%	Major affect on productivity \ operations OR Possible impact on spaceflight schedule	$5K - $10K	Management visibility OR successful resolution does not require response within three days	Probable
3	Unauthorized Access (User Compromise)	ITAR \ EAR		2% - 5%	Possible affect on spaceflight success, Probable impact to spaceflight schedule OR Possible threat to environment	$10K - $50K	Management visibility OR successful resolution does not require response within one day	Active (Small Outlets)
4	Unauthorized Access (System Compromise)	PII	High	> 5%	Any negative effect on funding, reputation, relationships with partners OR Possible threat to human safety	> $50K	Senior Management Visibility OR successful resolution requires immediate response	Active (Large Outlets)

Table Appendix H-1 Priority Factors

Sum of Indices	Priority Level
26 – 30	Critical
16 – 25	High
6 – 15	Moderate
0 – 5	Low

Table Appendix H-2 - Priority Level

NIST guidance dictates that resource criticality and potential technical effect are used to determine the appropriate incident handling actions and their maximum response times. The mechanism at NASA by which response and notification times are generally determined is the Incident Response Service Level Agreement (SLA), which defines the agreed-upon completion time for a type of service under normal conditions. To comply with NIST guidance, SLAs for different incident handling-related tasks are derived from the severity of the incident and, in the case of initiating incident response, the time of day it is reported. What follow is suggested guidance on establishing SLAs, and is not prescriptive.

With respect to incidents there are three types of service: ***response***, ***notification***, and ***resolution***. ***Response*** indicates initiating the process to confirm or refute the reported incident. ***Notification*** indicates fulfilling our obligation to notify NASA and NASA contacts following incident confirmation. ***Resolution*** indicates a variety of activities have occurred to ***handle*** the incident-including containing the incident, eradicating it, and recovering from it. SLAs are defined for each incident handling activity at each severity level.

In the case of initiating incident ***response***, the SLA is also dependent on what time of day the incident report occurs. Daytime (8 AM - 6 PM) response is expected to be quicker than evening (6 PM - 8 AM) response. In the case of notification and resolution, the SLA is the same regardless of the time of day the actions take place.

Table Appendix H-3 may be used to determine the maximum response time for incident response initiation following the report of a suspected incident and for notification and resolution following the confirmation of the incident. Some of these specific SLAs are

derived from the *NIST SP 800-61: Computer Security Incident Handling Guide*, the *NASA CIO Memo: Information Technology Security (ITS) Incident Reporting Requirements*, and the *US-CERT Federal Incident Reporting Guidelines*.

Incident Severity	Daytime Response SLA	Evening Response SLA	Daytime \ Evening Notification SLA	Daytime \ Evening Resolution SLA
Critical	Immediate	2 Hours	30 Minutes	5 Days
High	30 Minutes	4 Hours	1 Hour	10 Days
Moderate	2 Hours	8 Hours	2 Hours	20 Days
Low	8 Hours	12 Hours	1 Week	30 Days

Table Appendix H-3 - Incident Response Service Level Agreements

Appendix I – Procedures for Breach of Personally Identifiable Information (PII)

This Appendix and the procedures contained herein shall be followed by the CPMs in conjunction with the IRM, in the event of a suspected or confirmed breach or incident involving PII. The terms "breach" and "incident" include the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any conditions in which persons that are not authorized to access covered information or PII have access or potential access to it, whether physical or electronic. This appendix executes the requirements related to NPR 1382.1, NASA Privacy Procedural Requirements.

These procedures:

[1] Identify the actions required following a suspected or confirmed incident involving PII;
[2] Identify the first-level review and analysis requirements;
[3] Outlines the process NASA follows which shall be implemented at the Center level via the CPMs, to handle suspected PII incidents and incidents posing a potential risk of identity theft; and
[4] Where appropriate identifies, the roles and responsibilities that may be involved in breach mitigation and notification activities.

Applicable Documents

NASA Policy Directive (NPD) 2540.1, Personal Use of Government Office Equipment Including Information Technology
NASA Procedural Requirement (NPR) 2810.1, Security of Information Technology
NPD 1382.17, NASA Privacy Policy
NPR 1382.1, NASA Privacy Procedural Requirements
OMB Memorandum M-06-19, Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments
OMB Memorandum dated September 20, 2006, Recommendations for Identity Theft Related Data Breach Notification
OMB Memorandum M-07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information
OMB Memorandum M-07-04, Use of Commercial Credit Monitoring Services Blanket Purchase Agreements (BPA)

Personally Identifiable Information Defined

PII refers to information that can be used to distinguish or trace an individual's identity, such as their name, social security number (SSN), biometric records, etc., alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc.[2] Sensitive PII means a combination of PII elements, which if lost, compromised, or disclosed without authorization could be used to inflict substantial harm, embarrassment, inconvenience, or unfairness to an individual. Non-Sensitive PII means information that is available in public sources, the disclosure of which cannot reasonably be expected to result in personal harm.

In the case of a suspected PII breach which occurs through the loss of a government computer, Personal Digital Assistant (PDA), thumb drive, or other electronic or non-electronic files or medium, the PII addressed by this policy is limited to PII that is entrusted to NASA's custody or managed by a contractor on NASA's behalf. PII that is the personal property of the information custodian, or entrusted to that person by friends or family is not covered by this policy, e.g., a personal address book or personal family financial information. Limited personal use of government equipment may be permitted by *NPD 2540.1, Personal Use of Government Office Equipment Including Information Technology*; however, NASA has no responsibility for the loss or compromise of such information when stored by NASA.

Handling Breach of Personally Identifiable Information

As outlined in section 5.3 Incident Identification, NASA views the discovery of a suspected PII data breach as a potential Information Security Incident. All Information Security Incidents, whether suspected or confirmed, involving the breach of PII in any form shall be reported to the NASA SOC immediately upon discovery. The SOC will notify the US-CERT within one hour of discovery as required by *OMB Memorandum M-06-19, Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency*

[2] A more detailed definition of PII is found in NPR 1382, NASA Privacy Policy.

Information Technology Investments.[3] The SOC will notify the IRM of the potential breach of PII. The IRM will work with the CPM to perform a basic assessment of whether or not the incident is a confirmed breach of sensitive PII. Only the CPM, or their designee, may confirm the assessment of sensitive PII.

Breach of Personally Identifiable Information Process

Once a suspected breach is confirmed by the IRM and CPM, the following process shall be followed.

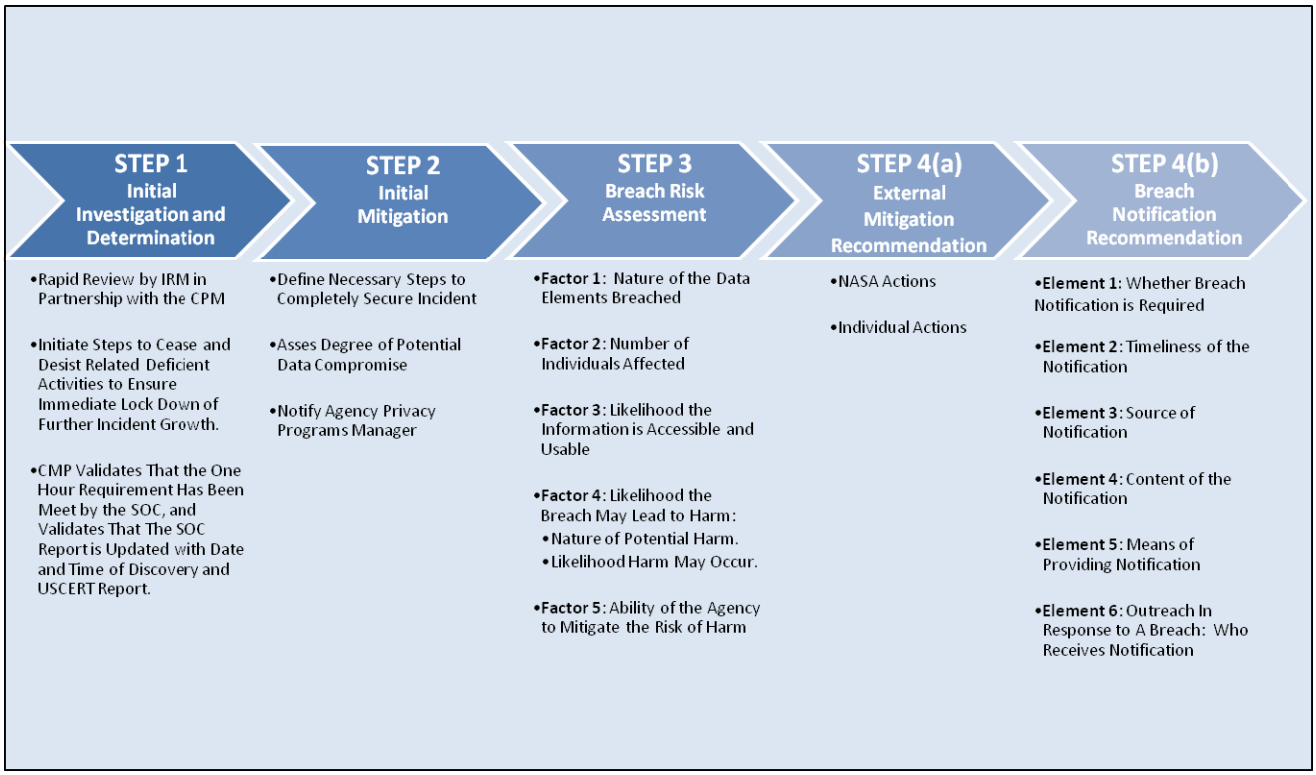


Figure Appendix I-1 - Breach of Personally Identifiable Information Process

Step 1: Initial Investigation and Determination

This step is covered in section 5.3 Incident Identification and is not reiterated in this Appendix. The IRM and CPM shall work this step together. This step includes the CPM making the determination of the sensitivity of the information that the IRM determines is involved in the incident. The CPM will make the determination as to whether the PII is to be considered sensitive, and validate that the SOC has met the one hour reporting requirement per *OMB Memorandum M-06-19*. If sensitive PII is involved, move forward to Step 2 through 4. If sensitive PII is involved, the CPM works with the IRM as a Breach Response Team (BRT) other members may be activated as necessary.

- **BRT Activation and Members**: The BRT is activated by the determination that sensitive PII is involved in an incident. Once this occurs, a BRT lead shall be established, and the NASA Privacy Programs Manager shall be notified by the CPM. Depending on the nature of the breach and the Center's organization, the BRT may be lead by the Center Chief Information Officer, the IRM, the CISO, or the CPM. The BRT may include, as the situation warrants, one or more members of the following offices: OCIO, Inspector General, Center Public Affairs, Center Chief Counsel, Center Human Resources Employee Relations. Additionally, the BRT may include, as the situation warrants, the Center Chief Information Officer, the Contracting Officer/Contracting Officer's Technical Representative, and/or other Subject Matter Experts. Upon completion a copy of the BRT report shall be provided to the NASA Privacy Programs Manager.

[3] In accordance with *OMB Memorandum* M-06-19, the SOC is responsible for reporting all breaches, whether suspected or confirmed. It is the CPM's responsibility to follow up and verify that the one hour requirement for reporting to US-CERT (in accordance with *OMB Memorandum M-06-19*) has been successfully met by the SOC or to record justification or explanation in the event this requirement was not met and report such failure to the Agency Privacy Programs Manager immediately.

Step 2: Initial Mitigation

This step is covered in section 5.4 Incident Containment and is not reiterated in this Appendix. The IRM and CPM may work this Step together. The IRM and the CPM are highly encouraged to work together to define the necessary steps to secure the potential growth of the incident, initially assess the degree of privacy compromise.

Step 3: Breach Risk Assessment

Working with the other members of the IRT, the CPM will establish a plan for any necessary interviews of involved parties as it relates to privacy and begin to assess the five factors that contribute to the risk of harm. The five factors are outlined below.

Factor 1: Nature of the Data Elements Breached: It is difficult to characterize data elements as creating a low, moderate, or high risk simply based on the type of data because the sensitivity of the data element is contextual. A name in one context may be less sensitive than in another context. (For example, breach of a database of names of individuals receiving treatment for contagious disease may pose a higher degree of risk, harm, or embarrassment, whereas a database of names of subscribers to agency media alerts may pose a lower degree of risk, harm, or embarrassment).

Factor 2: Number of Individuals Affected: The magnitude of the number of individuals affected.

Factor 3: Likelihood the Information is Accessible and Usable: The likelihood that the sensitive PII obtained via the breach is accessible and/or usable by unauthorized individuals.

Accessible	The likelihood PII will be accessible by unauthorized individuals. The fact that the information has been lost or stolen does not necessarily mean it has been or can be accessed by unauthorized individuals. If the information is properly protected by a FIPS 140-2 certified encryption solution, for example, the risk of compromise may be low to non-existent. All NASA NOMAD managed Blackberries fall into this category as all stored information on them is properly encrypted with a FIPS 140-2 certified solution.
Usable	The likelihood that any unauthorized individual will know the value of the information and either use or sell the information.

Factor 4: Likelihood the Breach May Lead to Harm: The CPM should assess two aspects of potential harm that may result from the breach: (1) the nature of the potential harm, and (2) the likelihood that harm may occur. The outcome of this risk assessment should be a determination of the risk of harm, and identification of the level of risk.

Nature of Potential Harm	The Privacy Act requires agencies to protect against any anticipated threats or hazards to the security or integrity of records which could result in "substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained" (5 U.S.C. 552a(e)(10)). The CPM should assess the possible harm associated with the loss or compromise of information. Such harm may include the effect of a breach of confidentiality or fiduciary responsibility, the potential for blackmail, the disclosure of private facts, mental pain and emotional distress, the disclosure of address information for victims of abuse, the potential for secondary uses of the information which could result in fear or uncertainty, or the unwarranted exposure leading to humiliation or loss of self esteem.
Likelihood Harm May Occur	The likelihood a breach may result in harm depends on the types of data involved in the incident. SSNs and account information are useful to committing identity theft, as are date of birth, passwords and mother's maiden name. On the other hand, limited personal information such as a name and address or other PII element, if lost, may also pose a significant risk of harm if, for example, it appears on a list of patients at a clinic for treatment of a contagious disease. In considering whether the loss of information could result in identity theft or fraud, additional consultation may be obtained in guidance from the President's Identity Theft Task Force at http://www.idtheft.gov/.

Factor 5: Ability of the Agency to Mitigate the Risk of Harm: The risk of harm will depend on the extent to which NASA can mitigate the further compromise of the system(s) and information affected by the breach. In addition to containing the breach, appropriate countermeasures should be taken, such as monitoring systems for misuse of the personal information and patterns of suspicious behavior. Such mitigation may not prevent the use of the personal information for identity theft, but it can limit the associated harm.

Step 4(a): External Mitigation Recommendation

As part of containment, some corrective actions may need to be executed immediately before Step 4. Beyond the system level actions initially taken, there are external actions that may be taken if warranted, both by NASA as well as by the individuals affected. Actions that individuals can take to protect themselves will depend on the type of information that is compromised. In notifying potentially affected individuals about steps they can take following a data breach, NASA should focus on the steps that are relevant to the particular circumstance. Actions may include:

NASA Actions	**Notify Issuing Bank**: If the breach involves government-authorized credit cards, NASA will do this promptly.
	Notify Bank or Entity that does a transaction on NASA's behalf: If the breach involves individual's bank account numbers (such as those provided to NASA for the purpose of direct deposit of payroll or credit card reimbursements or any benefit payment), NASA will notify the entity that handles that transaction.
	Identity Theft Analysis: At some expense, NASA can engage the service of a company which analyzes whether a particular data loss appears to be resulting in identity theft. This data breach analysis may be a useful intermediate protective action, especially when it is clear whether the identity-theft risk warrants implementing more costly additional steps, or where the risk is such that it is deemed wise to do more than rely on the actions that individuals can take on their own. This kind of analysis is much less costly than providing credit monitoring and, in the event that individuals report themselves as victims of identity theft, can assist in determining if that theft is likely a result of the NASA breach or an unassociated coincidental instance of identity theft.
	Commercial Credit Monitoring: [4] At substantial expense, NASA may elect to procure commercial credit monitoring services to provide affected individuals early detection of the signs of identity theft and potentially minimizing the possible harm. In deciding whether to offer this type of services, NASA should consider the seriousness of the risk of identity theft arising from this data breach, whether related incidents have already been detected and the cost of providing the service. Characteristics of affected individuals should also be considered; there are some populations who, because of their job duties or location, may have difficulty in taking self-protective steps and may warrant special protection from the distraction or effort of self-monitoring.
Individual Actions	**Contact their financial institution:** When financial account information is part of the breach, contact their financial institution to determine whether their accounts should be closed.
	Monitor financial account statements: immediately report suspicious or unusual activity to financial institution.
	Request a free credit report: [5] This can be done at http://www.AnnualCreditReport.com or by calling 1-877-322-8228. It might take a few months for most signs of fraudulent accounts to appear on the credit report; this option is most useful when the breach involves information that can be used to open new accounts.
	Fraud Alert: [6] Place an initial fraud alert on credit reports maintained by the three major credit bureaus. This option is most useful when the breach includes information such as SSNs that can be used to open a new account. After placing an initial fraud alert, an individual is entitled to a free credit report, which they should obtain beginning a few months after the breach, and review for signs of suspicious activity.
	Credit Freeze: Residents of states in which state law authorizes a credit freeze may consider placing a credit freeze on their credit file.[7] This option is most useful when the breach includes information such as SSNs that can be used to open a new account.
	Active Duty Alert: Deployed members of the military may place this on their credit file. This option is most useful when the breach includes information such as SSNs that can be used to open a new account. They serve a similar function as initial fraud alerts, causing creditors to be more cautious in extending new credit. However, active duty alerts last for one year instead of 90 days and do not entitle them to a free credit report. Therefore, this option should be combined with a request for obtaining an annual free credit report.
	Review FTC Information and publications on breaches and identify theft and options: – http://www.ftc.gov/idtheft.

[4] *OMB Memorandum M-07-04* announced that the Government Services Administration (GSA) has established government-wide blanket purchase agreements (PBA) to facilitate procurement of commercial credit monitoring services where necessary. If credit monitoring services are to be acquired other than through the GSA BPAs, NASA must notify GSA and OMB in accordance with M-07-04.

[5] Consumers are entitled by law to obtain one free credit report per year from each of the three major credit bureaus.

[6] A fraud alert is a mechanism that, for 90 days, signals to credit issuers who obtain credit reports on a consumer that they must take reasonable steps to verify the consumer's identity before issuing credit, making it harder for identity thieves to secure new credit lines.

[7] A credit freeze cuts off third party access to a consumer's credit report, thereby effectively preventing the issuance of new credit in the consumer's name.

It should be noted that any public announcement of the breach could itself cause criminals engaged in fraud, under the guise of providing legitimate assistance, to use various techniques, including e-mail or telephone, to deceive individuals affected by the breach into disclosing their credit card numbers, bank account information, SSNs, passwords or other sensitive personal information via a variety of social engineering techniques.[8]

Step 4(b): Breach Notification Recommendation

After determining recommended actions to be taken, the CPM should develop a recommended plan for notification. A recommended notification plan must address if, how, from whom, and when notification must be made to affected individuals. This plan must be developed consistent with the six elements defined in OMB Memorandum *M-07-16*.

Element 1: Whether Breach Notification is Required: The outcome of the risk assessment performed in the Step 3 is considered in this element.[9] The higher the risk of harm, the more likely a breach notification is required. The type of harm should be considered, such as harm to reputation and the potential for harassment or prejudice, particularly when health or financial benefits information is involved in the breach. Under circumstances where notification could increase a risk of harm, the prudent course of action may be to delay notification while appropriate safeguards are put in place. Additionally, an increased risk that the information will be used by unauthorized individuals should influence the decision to provide notification.

Element 2: Timeliness of the Notification: Where notification is required, it should be provided without unreasonable delay following the discovery of a breach, consistent with the needs of law enforcement and national security as well as any remaining measures necessary for the IRT to determine the scope of the breach, and if applicable, to restore the reasonable integrity of the system of records compromised.

Decision to delay notification should be made by the SAOP or a senior-level individual that he/she may designate. In some circumstances, law enforcement or national security considerations may require a delay if it would seriously impede the investigation of the breach or the individual affected.

Element 3: Source of Notification: In general, notification to any individual(s) affected by the breach should be issued from a level appropriate to the magnitude and scope of the breach. Persons making the notification could range from a Center Director, Center CIO, SAOP or the NASA Administrator. The selection of person to provide the notification should be appropriate to the magnitude and nature of information compromised by the breach.

When the breach involves a NASA contractor or a public-private partnership operating a system of records on behalf of NASA, NASA is responsible for ensuring any notification and corrective actions are taken.

Element 4: Content of the Notification: The notification should be provided in writing and should be in concise, plain language.[10] Sample letters are contained at the end of this Appendix. The notice should always be coordinated with the Office of Chief or General Counsel, OCIO, NASA Privacy Programs Manager and should include the following elements:

- A brief description of what happened, including the dates of the breach and of its discovery;
- To the extent possible, a description of the types of personal information involved in the breach (such as full name, SSN, date of birth, home address, account number, disability code, etc.);
- A statement whether the information was encrypted or protected by other means, when determined such information would be beneficial and would not compromise the security of the system;
- What steps, if any, individuals should take to protect themselves from potential harm;
- What NASA has done, or is doing to investigate the breach, to mitigate losses and to protect against any further breaches;

---

[8] One common such technique is "phishing," a scam involving an e-mail that appears to come from a bank or other organization, asking the individual to verify account information, and then directing him to a fake website whose only purpose is to trick the victim into divulging his personal information. See FTC for advice at http://www.ftc.gov/bcp/edu/pubs/consumer/alerts/alt166.htm.

[9] The nature of the data elements compromised is a key factor which should be considered in determining when and how notification should be provided to individuals affected. (For example, theft of a database containing individuals' names in conjunction with SSN or dates of birth may pose a high level of risk of harm, while a theft of a database containing only the names of individuals will likely pose a lower risk, depending on its context).

[10] If it is known that affected individuals are not English speaking, notification should be provided in the appropriate language.

- The name and contact information (including a phone number, e-mail address and postal address) of the NASA official(s) that individuals affected may contact for more information about the incident and actions they should take;
- Credit monitoring information (if appropriate).

Element 5: Means of Providing Notification:[11] The most appropriate means for providing notification will depend on the number of individuals affected and what contact information is available for the affected individuals. Notice provided to individuals affected by a breach should be commensurate with the number of people affected and the urgency with which they need to receive notice. The following are means of notice which may be considered:

Telephone	Telephone notification may be appropriate in those cases where urgency may dictate immediate and personalized notification or when a limited number of individuals are affected. Telephone notification, however, should be contemporaneous with written notification by first-class mail.
First-Class Mail	First-class mail notification to the last known mailing address of the individual in NASA's records should be the primary means notification is provided. Where there is reason to believe the address is no longer current (for example, in the case of former employees), reasonable steps should be taken to update the address by consulting with other agencies such as the US Postal Service. The notice should be sent separately from any other mailing so that it is conspicuous to the recipient. The front of the envelope should be labeled to alert the recipient to the importance of its contents, such as "Data Breach Information Enclosed" and should be marked as originating from NASA to reduce the likelihood the recipient thinks it is advertising mail.
E-mail	E-mail notification can be problematic as individuals may change their private email addresses often. However, where the breach involves NASA employees and contractors, delivering notification to their official NASA-provided e-mail address is acceptable. E-mail notification may be employed in conjunction with postal mail, if the circumstances of the breach warrant this approach.
Existing Government-wide Services	Government-wide services such as USA Services may be used if appropriate. USA Services is a government-sponsored web site with a rich collection of content to benefit the public, government employees and others where breach notification could be posted. This site can be accessed at www.USA.gov.
Newspapers or other Public Media Outlets	In extreme circumstances, it may be appropriate to supplement individual notifications with published notifications in newspapers or other public media outlets. In this case, toll free call centers staffed by trained personnel should be established to handle inquiries from the individuals affected and the public.
Substitute Notice	A substitute notice may be used in the situation where NASA does not have sufficient contact information to provide notification and may consist of a conspicuous posting regarding the breach on the NASA web site and notification to major print and broadcast media. A situation requiring a substitute notice is highly unlikely for NASA.
Accommodations	Special consideration should be given to providing notice to individuals who are visually or hearing impaired consistent with Section 508 of the Rehabilitation Act of 1973 should be given.

Element 6: Outreach In Response to A Breach: Who Receives Notification: For final consideration in the notification process when providing notices is determination of who should receive notification: the individuals affected, the public media or other third parties affected by the breach or the notification. Unless notification to individuals is delayed or barred for law enforcement or national security reasons, once it has been determined to provide notice regarding the breach, individuals affected should receive prompt notification.

In some unique situations involving covered information on members of the public, it may be appropriate to expand the reach of the notification to include the public or the media. Careful planning and execution are required so as not to unnecessarily alarm the public. Especially in the event of broad announcements, NASA should be prepared to respond to inquiries from other government entities such as the Government Accountability Office and Congress.

[11] The magnitude of the number of individuals affected identified in Step 3 may dictate the methods that will be chosen for providing notification, but should not be the determining factor for whether NASA should provide notification.

Ultimately, after evaluating all of these other factors, review and reassess the level of impact already assigned to the information using the impact levels defined by NIST FIPS-199. The impact levels—low, moderate and high -- describe the worst case potential impact on an organization or individual if a breach of security occurs. These impact levels can further help determine when and how notification should be provided.

If the five risk factors are applied appropriately, it is likely that notification will only be given in those instances where there is a reasonable risk of harm and will not lead to the overuse of notification.

Additional Considerations

Contractor Maintained Data: In the situations where the breached PII is maintained by a contractor on NASA's behalf, the Contracting Officer and/or the Contracting Officers Technical Representative should be included on the IRT and are the official liaison to the contractor on this matter. According to the September 20, 2006 OMB memo, NASA retains the responsibility for notification in this situation.

Data Maintained on NASA's behalf by Other Providers: In some cases, PII is maintained on NASA's behalf by other federal agencies or shared service providers. In the case of breach of PII in such a situation, the functional lead or ISO and data owner should be the liaison to the provider. According to the September 20, 2006 OMB memo, NASA retains the responsibility for the notification in this situation.

Communications Plan/ Notification Plan

CPMs should consider working with their Center CISO(s) to outline a basic PII Breach Communications Plan and Notification Plan prior to an incident. As each incident is unique, the basic outline should be flexible enough to adapt to the incident. The implementation of the communications and notification plans during an incident should take into account the 4 step process outlined within this Appendix.

Multi-Center Breach

In a situation where there is a multi-center breach each center IRT is responsible for responding in accordance with their normal procedures as guided by this handbook. In addition, the CPM ensures that the NASA Privacy Program Manager is kept up-to-date on the situation. The NASA Privacy Program Manager works with the SAOP, and any other organizations that are appropriate given the situation, to ensure that NASA handles the multi-center breach properly. The SAOP, or the SAOPs designee, has ultimate responsibility for responding to a multi-center breach at the Agency level.

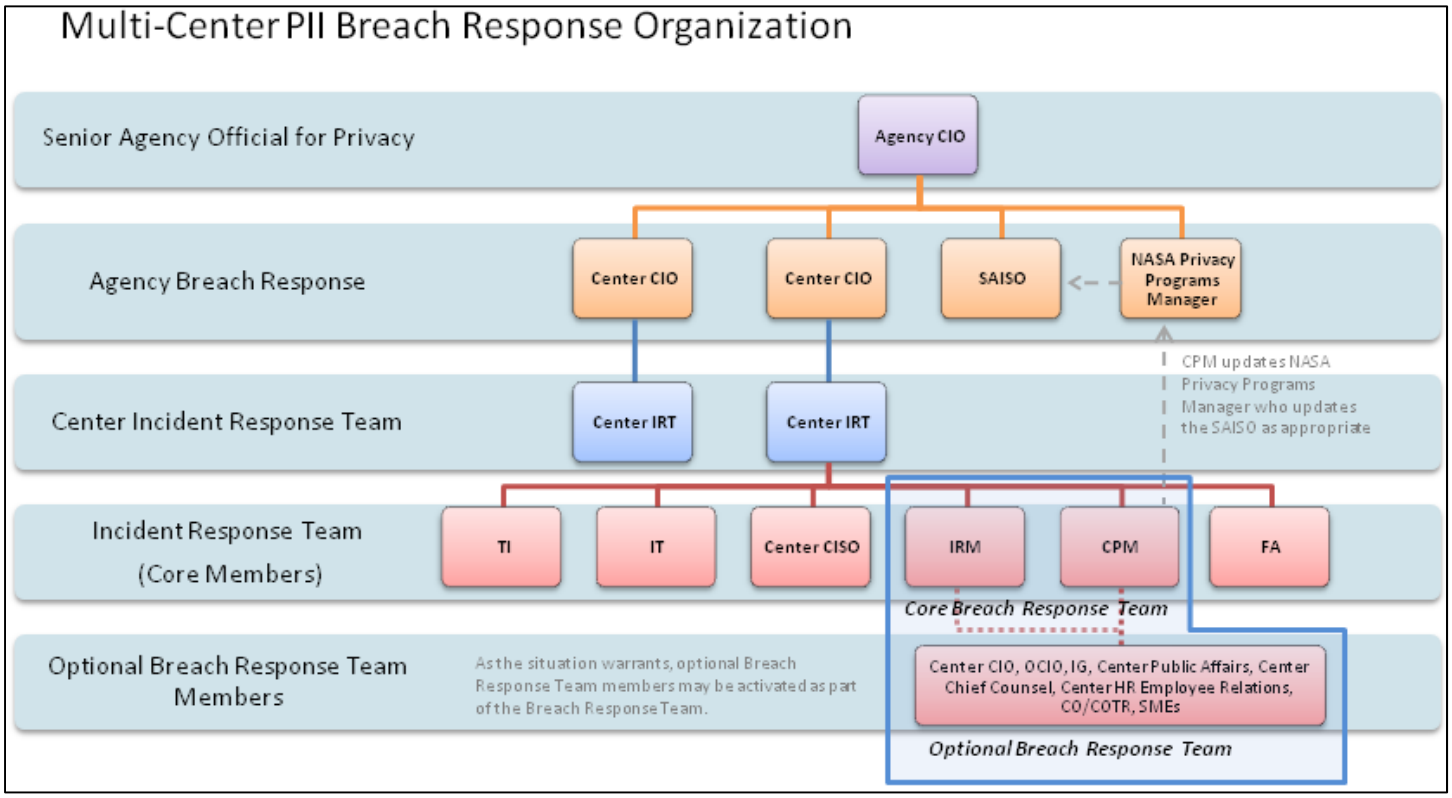


Figure Appendix I-2 – Multi-Center PII Breach Response

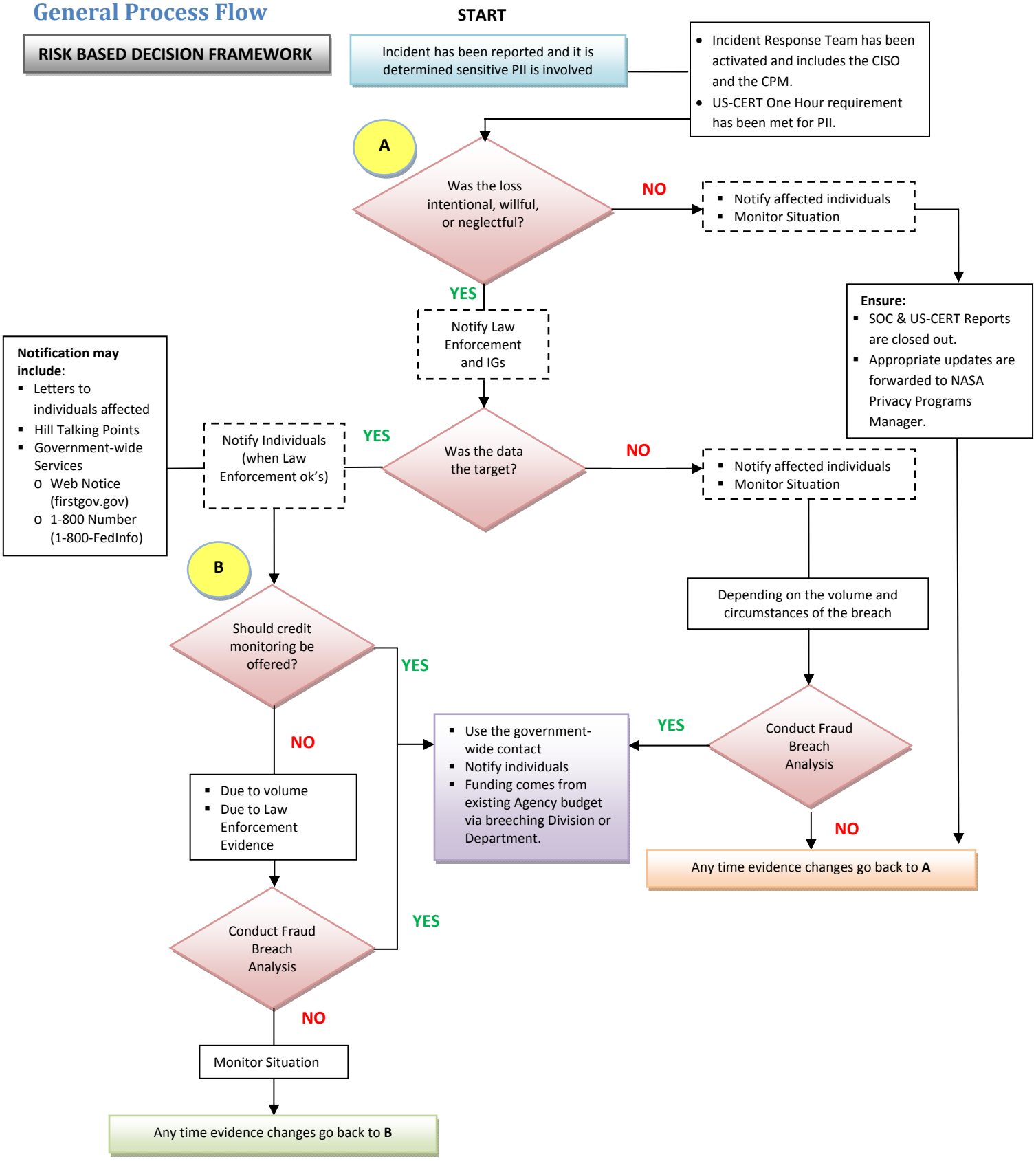
Post Incident Closure

At the conclusion of the steps outlined in this appendix, the IRM reports to the SOC that the incident has been mitigated and warrants closure. The IRM and the CPM jointly make the determination that the PII Breach warrants closure.

Post Incident Follow-Up

The CPM is encouraged to follow the post incident analysis guidelines set forth in the main document.

General Process Flow



Sample Notification Letters

Sample Notification Letter 1: MODEL LETTER FOR THE COMPROMISE OF SOCIAL SECURITY NUMBERS
Dear _____:

We are contacting you about a potential breach of your personal information. [Describe the information compromise and how the Agency is responding to it.]

We recommend that you place a fraud alert on your credit file. A fraud alert tells creditors to contact you before they open any new accounts or change your existing accounts. Call any one of the three major credit bureaus. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts. All three credit reports will be sent to you, free of charge, for your review.

Equifax	Experian	TransUnionCorp
800-525-6285	888-397-3742	800-680-7289

Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission (FTC) recommends that you check your credit reports periodically. Victim information sometimes is held for use or shared among a group of thieves at different times. Checking your credit reports periodically can help you spot problems and address them quickly.

If you find suspicious activity on your credit reports or have reason to believe your information is being misused, call [insert contact information for law enforcement] and file a police report. Get a copy of the report; many creditors want the information it contains to absolve you of the fraudulent debts. You also should file a complaint with the FTC at www.ftc.gov/idtheft or at 1-877-ID-THEFT (877-438-4338). Your complaint will be added to the FTC's Identity Theft Data Clearinghouse, where it will be accessible to law enforcers for their investigations.

We have enclosed a copy of *Take Charge: Fighting Back Against Identity Theft* <*http://www.ftc.gov/bcp/edu/pubs/consumer/idtheft/idt04.htm*>, a comprehensive guide from the FTC to help you guard against and deal with identity theft.

[Insert closing]
Your Name

Sample Notification Letter 2
Dear _____:

On January 1, 2007, a breach of privacy protected personally identifying information occurred at NASA. We believe that your personal information may have been compromised in this incident. The compromised information includes name, social security number, residential address, date of birth, office and home email address, office, and home telephone number.

The theft was immediately reported to local and NASA law enforcement authorities, which are now conducting a joint inquiry into the loss.

We do not believe that the information was specifically the target in this incident. Because the information was password protected and encrypted, we also believe that the probability is low that the information will be acquired and used for an unlawful purpose. However, we cannot say with certainty that this might not occur. We therefore believe that you should consider taking actions to protect against the potential that someone might use the information to steal your identity.

You should be guided by the actions recommended by the Federal Trade Commission (FTC) at its Web site at http://www.consumer.gov/idtheft . The FTC urges that you immediately place an initial fraud alert on your credit file. The Fraud alert initiates a 90-day period during which creditors are required to contact you before a new credit card is issued or an existing card changed. The site also provides other valuable information that can be taken now or in the future if problems should develop.

NASA takes this loss very seriously and is reviewing its current policies and practices with a view of determining what must be changed to preclude a similar occurrence in the future. [Discuss any additional actions the Agency is taking.]

We deeply regret and apologize for any inconvenience and concern this breach may cause you.

Should you have any questions, please call _____.

Sincerely,