The National Science Foundation
Office of Polar Programs
United States Antarctic Program

Information Security Instruction 5000.12-1
USAP Incident Response and Management

Instruction Number	5000.12-1	**Authorized by**	Information Security Manager, U.S. Antarctic Program
Distribution	USAP-wide	**Issue Date**	18 September 2007
		Effective Date	18 September 2007
		Updated	27 May 2009
Office of Primary Responsibility	National Science Foundation Office of Polar Programs Polar Research Support Section	**Responsible Officials**	Primary Responsibility: Mr. Patrick D. Smith Technology Development Manager Security Responsibility: Mr. Benjamin Bergersen Information Security Manager
Address	Suite 755 4201 Wilson Blvd Arlington, VA 22230	**Phone** **Fax**	703.292.8051 703.292.9080
Distribution	USAP-Wide	**Web**	www.nsf.gov/od/opp
Online Publication	http://www.usap.gov/technology	**Status**	Final

Table of Contents

Appendices

1. PURPOSE

This United States Antarctic Program (USAP) Information Security Instruction implements requirements of USAP Information Resource Management Directive 5000.12, *USAP Incident Response and Management*; *NSF Policy and Procedures for Responding to Computer Security Events*, August 2005; Office of Management and Budget (OMB) Circular A-130, *Management of Federal Information Resources*, and additional direction provided by the Federal Information Security Management Act (FISMA) of 2002.

USAP Information Resource Management Directive 5000.12, *USAP Incident Response and Management*, directs that:

- The USAP will establish a Computer Incident Response Capability (CIRC) program to respond to and manage adverse activities that threaten the successful conduct of science and operations in the USAP.
- The USAP CIRC will include a Computer Incident Response Team (CIRT) to respond to and manage information security incidents.

The actions outlined in this instruction utilize guidance of National Institute of Standards and Technology (NIST) Special Publication (SP) 800-61, *Computer Security Incident Handling Guide.*

2. APPLICATION

This instruction applies to all information resources, systems, and technology and to all users of these resources, systems and technology within the USAP operating environment or connected to the USAP information infrastructure. Compliance with this instruction is as indicated in USAP Information Security Policy 5000.1, *The USAP Information Security Program.*

3. AUTHORITY

Publication of this instruction is in conformance with the authority of NSF Manual 7, *The NSF Information Security Handbook,* and NSF USAP Policy, Information Resource Management Directive 5000.12, *USAP Incident Response and Management*.

The NSF CIO (Chief Information Officer) is the governing authority responsible for reporting incidents that occur on the USAP information infrastructure to US-CERT. The NSF CIO has delegated authority through the Office of Polar Programs (OPP) Director, who delegates through USAP policy 5000.12 to the USAP Information Security Manager (ISM) to implement and manage the USAP CIRC.

Benjamin Bergersen
Information Security Manager
United States Antarctic Program

4. RESPONSIBILITIES

USAP Information Security Manager

The USAP Information Security Manager (ISM):

- Ensures the USAP CIRC program conforms to National Science Foundation (NSF) incident response policies and procedures.
- Manages the USAP CIRC program and the USAP CIRT. The ISM establishes the process and procedures for USAP-wide incident response and management and composition of the incident response team.
- Establishes and coordinates the USAP CIRT comprised of appropriate management and technical representatives from the USAP prime contractor and other supporting organizations (e.g. Coast Guard, NASA, etc.).
- Provides the formal interface between the USAP CIRC and the NSF agency computer incident response protocol.
- Has decision making authority for Incident Response and Investigation.

USAP Prime Contractor

The USAP prime contractor is the lead information technology, systems, and services provider for the USAP. As such, the USAP prime contractor is tasked by NSF to provide information security and assurance for the USAP Information Technology (IT) program. Therefore, the USAP prime contractor is responsible for:

- Establishing a Computer Incident Response Team (CIRT)[1] consisting of technical experts across all IT functional areas required to respond to computer incidents in accordance with instruction provided in this document.
- Establishing incident response and management procedures outlining the necessary steps to rapidly and effectively respond to and manage the wide-spectrum of potential incidents.
- Creating an incident response matrix outlining response times for action for high and medium incidents in accordance with *Appendix B: USAP Incident Notification Matrix*.

The USAP prime contractor is responsible for the operations and management of IT operations and services at all USAP operating locations, which includes:

- Establishing a CIRT at each USAP site that maintains an IT manager or senior IT lead as the CIRT lead.
- Providing incident response training to members of the CIRT.
- Coordinating responses to incidents at their respective locations. At each operating location, the USAP prime contractor provides the primary CIRT members and support structure.
- Working in partnership with other CIRT teams as appropriate when an incident involves a supporting organization.

[1] Members of the CIRT are listed in Table 1: USAP Core Incident Response Team. When necessary additional members identified in Table 2: USAP Extended Incident Response Team may be involved in the incident handling process.

USAP System Owners and Operators

The computing environment within the USAP accommodates a multitude of system owners/operators from various supporting and supported organizations. Examples of supporting organizations are: USAP prime contractor, SPAWAR Systems Center Charleston, PACAF/Support Force Antarctica, US Coast Guard, etc. Examples of supported organizations are: grantees from any number of host universities and Federal agencies, tenant Federal agencies such as NOAA and NASA, etc. System owners/operators must identify key personnel responsible for responding to an incident involving systems under their control and management.

5. INCIDENT RESPONSE

The incident response process has several phases, from initial preparation through post-incident analysis. This section describes how the major phases of the incident response process[2] are addressed in the USAP:

- Detection/Discovery/Prioritization
- Containment/Eradication/Recovery
- Notification
- Analysis
- Remediation
- Documentation/Reporting

Preparation

Incident Team Membership

The USAP prime contractor CIRT is comprised of a core membership detailed in *Table 1: USAP Core Incident Response Team*. The core team is responsible for initial detection, response, analysis and containment of incidents that occur on the usap.gov network. Core team members are involved in incident response activities as the designated authority deems appropriate for responding to an incident.

Other supporting organizations are responsible for establishing and maintaining a CIRT for addressing incidents that occur in their respective environments residing outside of the usap.gov network.

Table 1: USAP Core Incident Response Team (CIRT)

Position	Role
IT Director	Primary Authority (Site Representative)
IT Security Manager	Secondary Authority (Incident Management)
Technical Operations Manager	Third Authority (Mitigation Responsibility)

[2] The order of activities performed is dictated by the type and severity of the event under investigation.

Position	Role
Senior Systems Architect	Fourth Authority (Technical Consultant)
Incident Response Manager	Incident Handling, Security Analysis and Computer Forensics Expertise
Application Specialist	Application Expertise
Systems Manager	Server Expertise Primary
Systems Administrator	Server Expertise Secondary
Networks Manager	Networks Expertise Primary
Network Engineer	Networks Expertise Secondary
Project Manager	Communications Coordinator
Senior Technical Writer	Documentation
Client Services Manager	Desktop Expertise Primary
PC Technician	Desktop Expertise Secondary

In the event of a NSF escalated incident, the CIRT is expanded to include positions listed *Table 2: USAP Extended Incident Response Team*. Extended team members participate in incident eradication, recovery and post-incident activities.

Table 2: USAP Extended Incident Response Team (EIRT)

Position	Role
Office of Polar Programs	NSF/USAP Authority
USAP Information Security Manager	NSF Liaison (USAP CIRC/NSF Reporting)
NSF Technical Advisor	Technical consulting
McMurdo IT Manager	Station Expertise
Palmer IT Manager	Station Expertise
Pole IT Manager	Station Expertise
RPSC Application Specialist	Specific Application Expertise
SSSV Manager	Station Expertise
Other Functional Representatives as required	PACAF/SFA, SPAWAR
Supported Organizations as required	CTBTO, NASA, NOAA, etc and grantees

Training

The USAP prime contractor and other supporting organizations are responsible for providing incident detection and response training to members of their respective CIRT, and for personnel responsible for following incident response standard operating procedures (SOPs). Policy and procedural awareness training is provided to all USAP participants in order to educate the general USAP population on how to avoid, identify, and address an incident.

Incident Management Tools

The CIRT is equipped with the necessary tools and resources of value prior to and during incident handling. Tools include, but are not limited to:

- CIRT team member contact information and on-call information for other teams within the organization
- Pagers or cell phones for off-hour support teams and incident reporting mechanisms
- Encryption software for communications among team members and with external parties
- "War Room" for central communications and coordination
- Secure storage facility
- Hardware and software for computer forensics such as workstations, backup devices, blank media, packet sniffers and protocol analyzers, and other computer forensic software
- Documentation, enterprise architecture schematics, and baseline data of network, system and application activity

Beyond the identified tools, preparation also includes recommended best practices for securing networks, systems and applications such as:

- Patch management
- Host and client security
- Network and network perimeter security
- Malicious code prevention (See USAP Instruction, 5000.14-1, *USAP Computer Screening*)
- User computer security awareness (See USAP Instruction, 5000.9-1, *USAP Information Security Awareness Program*)

Procedure Development

The CIRT develops procedures for addressing the following common incident types (NIST 800-61, *Computer Security Handling Guide*, provides specific advice for these type incidents):

- Denial of Service
- Malicious Code
- Unauthorized Access
- Scans/Probes/Attempted Access
- Inappropriate Use

The CIRT also develops procedures for addressing Personally Identifiable Information (PII) suspected and confirmed spillages/breaches in accordance with *NSF Bulletin No. 07-15: NSF Policy on Reporting the Breach of Personally Identifiable Information*.

The USAP prime contractor ensures the aforementioned prevention tools and procedures are developed and maintained.

Detection and Analysis

Detection

The most challenging part of the incident response process is accurately detecting and assessing possible incidents, determining whether an incident has occurred and, if so, the type, extent, and magnitude of the problem. Signs of an incident fall into one of two categories: *precursor* or *indication.* See Section 6: *Glossary* for definitions.

Since incident detection should not be strictly reactive, the CIRT makes use of prevention tools and analysis, allowing the organization to detect activities (precursors) that are likely to precede an incident. If precursors are detected through automated or manual tools, the CIRT takes actions to prevent the incident by altering the security posture of the USAP. Examples of automated and manual tools include:

- Network and host-based intrusion detection systems (IDS)
- Antivirus software
- File integrity checking software
- Third-party monitoring service
- The use of network device, operating system, service and application logs
- Information on new vulnerabilities and exploits

The USAP prime contractor identifies and advocates for the necessary tools to provide this functionality.

Analysis

Trained and effective incident response teams are an important component of the overall incident response capability. The USAP prime contractor is responsible for establishing and training the USAP CIRT. The USAP ISM ensures the USAP prime contractor provides a suitable team, and as required, that other USAP supporting and supported organizations provide effectively trained personnel as part of the USAP incident response program.

Expectations regarding the detection and analysis techniques for incident analysis supplied by the USAP prime contractor are as follows:

- Profile networks and systems – Measuring the characteristics of expected activity so that changes can be more easily identified. Profiling is one of the most effective technical measures for aiding in incident analysis.
- Understand normal behaviors – Incident response team members study networks, systems, and applications to gain a solid understanding of what normal behavior is so that abnormal behavior can be recognized with ease.
- Use centralized logging and create a log retention policy.
- Perform event correlation among multiple indication sources.

- Keep all host clocks synchronized.
- Maintain and use a knowledge base of information.
- Run packet sniffers to collect additional data.
- Filtering log data.

Documentation

The CIRT maintains records about the status of incidents, along with other information pertinent to the investigation. The CIRT safeguard all data related to incidents, as there is often sensitive information contained. To reduce the risk of sensitive information being released inappropriately, the team ensures that access to incident data is restricted properly. Only authorized personnel has access to incident information on a need-to-know basis.

As soon as the CIRT detects that an incident is occurring or has occurred, all facts regarding the incident are immediately recorded. A logbook is used to record the incident. The log contains:

- System events
- Telephone conversations
- Observed changes in files - changes that may lead to a more efficient, more systematic, and less error-prone handling of the problem
- Every step taken by incident handlers from the time the incident was detected, dated and signed by the incident handler.
- Comments from incident handlers
- Contact information for other involved parties (e.g., system owners, system administrators)
- A list of evidence gathered during the incident investigation
- Next steps (e.g., waiting for a system administrator to patch an application)
- Meeting minutes
- Action items

All applicable incident documentation, including logs, is labeled with *For Official Use Only* within the document.

When possible, CIRT incident handlers work in teams of at least two: one person records and logs events while the other person performs the technical tasks.

Prioritization

The CIRT prioritizes the response to each incident based on the estimated business impact caused by the incident, and coordinates these priorities with the USAP CIRC in the event of conflicting resource requirements. The USAP CIRC and CIRT utilize the prioritization guidelines found in *Appendix A: USAP Incident Prioritization Matrix*. By providing a framework for making incident handling decisions, the matrix saves incident handlers' time. Incidents are not handled on a first-come, first-served basis as a result of resource limitations.

Escalation

The CIRT establishes an escalation process for situations in which team members do not respond to an incident within the designated timeframe. The escalation process

states how long a person will wait for a response and what the person will do if no response occurs.

Notification

When the incident is analyzed and prioritized, the CIRT notifies the appropriate individuals within the immediate organization and other impacted organizations based on the timeframes listed in *Appendix B: USAP Incident Notification Matrix*.

Separate forms are used for formal written reporting of technical and PII breach incidents that occur within the USAP to the NSF for escalation to US-CERT. These forms are provided in *Appendix C: USAP Technical Incident Reporting Form*, and *Appendix D: USAP PII Disclosure Incident Reporting Form*.

All applicable incident documentation including reports, are labeled with *For Official Use Only* within the document.

Containment, Eradication and Recovery

The CIRT creates and documents containment strategies for each major type of incident. The containment strategy is designed to control an incident before the spread of the incident overwhelms resources, and takes into account the level of acceptable risk. Criteria for determining the appropriate strategy addresses:

- Potential damage to and theft of resources
- Need for evidence preservation
- Service availability (e.g., network connectivity, serviced provided to external parties)
- Time and resources needed to implement the strategy
- Effectiveness of the strategy (e.g., partially contains the incident, fully contains the incident)
- Duration of the solution (e.g., emergency workaround to be removed in four hours, temporary workaround to be removed in two weeks, permanent solution)

The CIRT will not consider delay of the containment of an incident so that CIRT members can monitor the attacker's activity, usually to gather additional evidence. Delayed containment is dangerous because an attacker may escalate unauthorized access or compromise other systems in a very short period of time. The USAP may be liable if the attacker uses the compromised system to attack other systems.

Evidence Log

CIRT members clearly document how all evidence, including compromised systems, has been preserved. Evidence is accounted for at all times; whenever evidence is transferred from person to person, chain of custody forms detail the transfer and include each party's signature. An example of a recommended evidence log can be found at *Appendix E: USAP Evidence Chain of Custody Log*.

A detailed log is kept for all evidence, and includes the following information:

- Identifying information (e.g., the location, serial number, model number, hostname, media access control (MAC) address, and IP address of a computer)

- Name, title, and phone number of each individual who collected or handled the evidence during the investigation
- Time and date (including time zone) of each occurrence of evidence handling
- Location(s) where the evidence was stored

All applicable incident documentation including log files, are labeled with *For Official Use Only* within the document.

Evidence Collection

The CIRT develops evidence collection procedures for incident handlers designed to preserve the evidentiary status of the information. Evidence is acquired from a system of interest as soon as it is suspected that an incident may have occurred. From an evidentiary standpoint, it is beneficial to obtain a snapshot of the system as-is immediately before incident handlers, system administrators, and others may inadvertently alter the state of the machine during investigation.

Incident handlers create a *message digest* (generate a cryptographic checksum for the file) for log files, and other pieces of digital evidence using software and a message digest algorithm that are FIPS 140-2 and FIPS 180-2 validated. If the file is modified and the checksum recalculated, this activity demonstrates that the integrity of the file has changed. Conversely, an unchanged message digest serves to prove the information remains unchanged for evidentiary purposes.

Before copying the files from the affected host, the CIRT captures the volatile information that may not be recorded in a file system or image backups, such as:

- Current network connections
- Processes
- Login sessions
- Open files
- Network interface configurations
- Contents of memory
- The local clock time on each logging host and what deviation, if any, there is from the actual time

The CIRT executes care when acquiring this information from a live system, as any action performed on the host itself alters the state of the machine to some extent. Also, the attacker may currently be on the system and notice the handler's activity, potentially resulting in disastrous consequences.

Incident handlers use a write-protected floppy or a CD that contains trusted commands and all dependent files so that all necessary commands can be run without using the affected host's commands. Incident handlers also use write blocker programs that prevent the host from writing to its hard drives.

When it becomes necessary to collect forensics from a grantee system that is an active part of a science instrumentation system, additional coordination is required to avoid potential conflicts for forensics gathering and harm to the on-going research activity. The incident response protocol must provide due diligence in dealing with potential incidents on grantee systems to balance the need for immediate reaction for forensics capture against the harm or potential for harm to an on-going research project.

Disk Images and File System Backups

After acquiring volatile data, the CIRT incident handler immediately makes a full disk image to sanitized write-protected or write-once media so that the original disk is not altered or damaged during analysis. A disk image preserves all data on the disk, including deleted files and file fragments. If it is possible that evidence may be needed for prosecution or internal disciplinary actions, the handlers makes at least two full images, labels them properly, and securely stores one of the images to be used strictly as evidence. All evidence is tagged and stored in a secure location. If the handlers may acquire and secure the original disk as evidence, the second image can then be restored to another disk as part of system recovery.

If the business impact of taking down the system outweighs the risk of keeping the system operational, disk imaging may not be possible. A standard file system backup can capture information on existing files, which may be sufficient for handling many incidents, particularly those that are not expected to lead to prosecution.

Log Files

During evidence collection, the CIRT acquires copies of supporting log files from other resources, such as firewall logs that may show what IP address an attacker used.

- Logs are copied to sanitized, write-protected or write-once media
- One copy of the logs are stored as evidence, whereas a second copy is restored to another system for analysis

Identifying the Attacker

During incident handling, system owners and others typically want to identify the attacker. Although this information can be important in future prosecution, incident handlers remain focused on containment, eradication, and recovery. The primary goal of the CIRT team is to minimize the business impact. *Under no circumstances will the CIRT scan the attacker's system*. However, the CIRT may perform the following activities:

- Validating the attacker's IP address: incident handlers may attempt to validate that an address was not spoofed by using pings, trace routes, or other methods of verifying connectivity. Care must be taken as pings may tip off the attacker that the organization has detected the activity. If this occurs before the incident is fully contained, the attacker can cause additional damage, such as wiping out hard drives with evidence of the attack.
- Researching the attacker through search engines.
- Using incident databases.
- Monitoring possible attacker communications channels such as certain IRC channels to boast of web sites they have defaced.

In the event that the NSF Office of Inspector General (NSF/OIG) or other applicable law enforcement requests the identity of the attacker, the USAP prime contractor responds per the direction of the NSF.

Eradication and Recovery

After an incident has been contained, eradication may be necessary to eliminate components of the incident, such as deleting malicious code and disabling breached

user accounts. For some incidents, eradication is either not necessary or is performed during recovery. Because eradication and recovery actions are typically operating system or application-specific, the Technical Operations department of the primary contractor develops the required procedures.

Post-Incident Activity

Lessons Learned

A CIRT lessons learned meeting is held within five days of the end of the incident in order to learn from potential mistakes and to improve the incident response process. Questions to be answered include:

- Exactly what happened, and at what times?
- How well did the staff and management perform in dealing with the incident? Were the documented procedures followed? Were they adequate?
- What information was needed sooner?
- What steps or actions were taken that might have inhibited the recovery?
- What would the staff and management do differently the next time a similar incident occurs?
- What corrective actions can prevent similar incidents in the future?
- What additional tools or resources are needed to detect, analyze, and mitigate future incidents?

Not only is it important to invite meeting participants who have been involved in the incident that is being analyzed, but it is also wise to consider who should be invited for the purpose of facilitating future cooperation. It is imperative to have a meeting agenda and document the major points of agreement and action items, and to communicate them to parties who could not attend the meeting.

Incident Report

All declared incidents are reported to the USAP ISM in a timely manner, and a written incident report is submitted. Incident reporting by the USAP prime contractor to OPP for incidents other than those involving personally identifiable information (PII), are verbal during the incident, verbal and a written summary by the next weekly status report, and a written report within 30 days, or sooner as required by OPP. For incidents involving the unauthorized release of PII, verbal incident reporting by the USAP prime contractor to OPP occurs immediately but no later than within one (1) hour of discovery/detection. The written report format follows NSF guidelines defined in *Appendix F: NSF Management Review and Summary of Incident*.

The written report is valuable for future use as it provides a reference to assist in handling similar incidents, creates a formal chronology of events that is important for legal reasons, and creates a monetary estimate of the amount of damage the incident caused in terms of loss of software and files, hardware damage, and staffing costs (including restoring services) which may become the basis for subsequent prosecution activity. Incident reports, records, and evidence will be retained by the USAP prime contractor in compliance with NIST SP 800-61, *Computer Security Incident Handling Guide*, and General Records Schedule 24 (GRS 24). The retention period is for three

years following the end of NSF administrative proceedings, legal proceedings, follow-up actions, or the end of the USAP prime contractor's contract, whichever is longer.

All applicable incident documentation including log files, are labeled with *For Official Use Only* within the document.

Using Collected Incident Data

Lessons learned activities should produce a set of objective and subjective data regarding each incident. Over time, this incident data is useful in several capacities:

- The total hours of involvement and the cost may be used to justify additional funding of the incident response team and tools
- A study of incident characteristics may indicate systemic security weaknesses and threats, as well as changes in incident trends
- The data may be included into the risk assessment process, ultimately leading to the selection and implementation of additional control elements
- Reporting under FISMA requirements

The USAP CIRC decides what incident data to collect based on reporting requirements and the expected return on investment from the data (e.g., identifying a new threat and mitigating the related vulnerabilities before they can be exploited). Reportable data is included in monthly USAP and OPP Information Security reports.

Evidence Retention

Evidence is retained by the CIRT in compliance with NIST SP 800-61 and General Records Schedule 24 (GRS 24). The retention period is for three years following the end of NSF administrative proceedings, legal proceedings, follow-up actions, or the end of the USAP prime's contract, whichever is longer.

6. REFERENCES

Document	Name and Location
NIST SP 800-61	*Computer Security Incident Handling Guide* http://www.csrc.nist.gov/publications/nistpubs/index.html
NSF Bulletin 07-15	*NSF Office of Information and Resource Management, NSF Bulletin NO. 07-15: NSF Policy on Reporting the Breach of Personally Identifiable Information*
US-CERT PII Reporting Requirements, August 15 2006	*United States Computer Emergency Readiness Team Personally Identifiable Information Reporting Requirements* http://www.us-cert.gov/federal/reportingRequirements.html
OMB Memorandum 06-16	*Office of Management and Budget Memorandum for Chief Information Officers M-06-16* http://www.whitehouse.gov/omb/memoranda/fy2006/m06-16.pdf

Document	Name and Location
OMB Memorandum 06-19	*Office of Management and Budget Memorandum for Chief Information Officers M-06-19* http://www.whitehouse.gov/omb/memoranda/fy2006/m-06-19.pdf
NSF Policy August 2005	*NSF Policy and Procedures for Responding to Computer Security Events*
USAP Information Resource Directive 5000.12	*USAP Incident Response and Management* http://www.usap.gov/technology
USAP Information Resource Directive 5000.9	*USAP Information Security Awareness Program* http://www.usap.gov/technology

7. GLOSSARY

Event

Any observable occurrence in any system and/or network. Examples of events include the system boot sequence, a system crash, and packet flooding within a network. An event may be an indication that an incident is occurring.

FISMA - Federal Information Security Management Act (2002)

Provides a framework to ensure comprehensive measures are taken to secure federal information and assets.

Incident

An incident is the act of violating an explicit or implied security policy. These include, but are not limited to: attempts (either failed or successful) to gain unauthorized access to a system or its data; unwanted disruption or denial of service; the unauthorized use of a system for the processing or storage of data; changes to system hardware, firmware, or software characteristics without the owner's knowledge, instruction, or consent.

Indication

A sign that an incident may have occurred in the past or may be presently occurring.

NSF - National Science Foundation

An independent federal agency created by Congress in 1950 “to promote the progress of science; to advance the national health, prosperity, and welfare; to secure the national defense…”

OMB - Office of Management and Budget (US Government)

OMB’s predominant mission is to assist the President in overseeing the preparation of the federal budget and to supervise its administration in Executive Branch agencies.

OPP - Office of Polar Programs

The OPP manages and initiates National Science Foundation funding for basic research and its operational support in the Arctic and the Antarctic.

PII – Personally Identifiable Information

Information about an individual maintained by an agency which can be used to distinguish or trace an individual's identity, such as a combination of their name, social security number, date and place of birth, mother's maiden name, biometric record.

PII Breach

An event in which persons other than authorized users, or for an unauthorized purpose, have access or potential access to PII, whether physical or electronic.

Precursor

A sign that an incident may occur in the future.

Profiling

Profiling is measuring the characteristics of expected activity so that changes can be more easily identified. Profiling is one of the most effective technical measures for aiding in incident analysis.

RPSC - Raytheon Polar Services Company

Raytheon Polar Services was formed to specifically meet the needs of the National Science Foundation's Office of Polar Programs. NSF/OPP contractor for the United States Antarctic Program.

SAISO - Senior Agency Information Security Office

Utilized for reporting to the United States-Computer Emergency Readiness Team (US-CERT).

USAP - United States Antarctic Program

Funded by the US Government's National Science Foundation, USAP supports scientific research in Antarctica and the Southern Ocean.

8. INSTRUCTION REVIEW

The USAP ISM reviews this instruction in conjunction with major changes to the information infrastructure, as part of the USAP's participation in agency security audits, after each breach in system security, or every two years. The USAP ISM submits policy and instruction changes for review and approval by the NSF OPP.

APPENDIX A: INCIDENT PRIORITIZATION MATRIX

Priority	Criticality	Definition	Examples
1	Critical/High	An incident that causes possible life-threatening activity that affects critical systems or information. There is a strong need for corrective measures. A system may continue to operate but a corrective action plan must be put into place as soon as possible. An incident is considered critical if a compromised system or entire network (e.g. single host, sub-networks, entire site location) will cause significant damage if the affected system is kept online. An incident which affects a science system such that the conduct of the experiment would be harmed. An incident is also considered critical if the event potentially led to the unauthorized access or release of personally identifiable information (PII).	- Root or Administrative compromise - Denial of Service - Suspected or confirmed unauthorized access or release of PII
2	Medium	Incident could become public, provide unauthorized access to network and/or non-critical systems or information; affects systems resources or shows active targeting of critical systems. Corrective actions are needed and a plan must be developed to incorporate these actions with a reasonable time.	- User compromise - Successful Virus or Worm - Scanning of critical systems - Website Defacement*
3	Low	Incident shows active targeting of non-critical systems or potential threat to network. The system owner must determine whether corrective actions are still required or decide to accept the risk. Only NSF may accept the risk.	- Scanning of non-critical systems or external firewalls - Detection and elimination of malicious logic before infestation

** Some examples may be upgraded in priority level based on situation.*

APPENDIX B: USAP INCIDENT NOTIFICATION MATRIX

Priority Level	Event Type	Response/Activities	Time
Critical	Suspected or Confirmed Unauthorized Access/ Unauthorized PII Release: an individual gains logical or physical access without permission to a federal agency network, system, application, data, or other resource; unauthorized release ("spill") personally identifiable information (PII).	- Immediate notification to USAP ISM that the event has occurred, is being investigated, and/or corrective actions that have/will be taken to mitigate impact/risk - USAP ISM immediately escalates to OPP for escalation to the NSF CIO - NSF CIO report to US-CERT on every incident involving the suspected or confirmed unauthorized access or release of PII	Immediately but no later than within one (1) hour of discovery/detection.
Critical	Compromise: an attempted intrusion is believed to have successfully compromised systems within the USAP domain and is actively attempting to compromise or gain access to additional resources (either within the USAP domain or external)	- CIRT notification to USAP ISM that an event has occurred, is being investigated, and/or corrective actions that have/will be taken to mitigate impact/risk - USAP ISM escalates to NSF CIRT for Incident determination, per NSF CIRT procedures for system owners	Two (2) hours from detection
High	Attack: an attempt to bypass security controls on a system within the USAP domain has been detected	- CIRT notification to USAP ISM that an event has occurred, is being investigated, and/or corrective actions that have/will be taken to mitigate impact/risk - USAP ISM escalates to NSF CIRT for Incident determination, per NSF CIRT procedures for system owners	Four (4) hours from detection
Medium	Denial of Service: excessive latency or slow-down of access to resources that could be a symptom of a DoS attack or unauthorized/inappropriate	- CIRT Core Team investigates event and makes assessment - CIRT notification to	Upon verification

Priority Level	Event Type	Response/Activities	Time
	use of resources	USAP ISM for info and possible dissemination NSF-wide	
Medium	Alarms: suspicious alarms that require further information to assess the damage or threat	- CIRT Core Team investigates event and makes assessment - CIRT notification to USAP ISM for info and possible dissemination NSF-wide	Upon verification
Medium	Vulnerability: alerts to hardware, software, or system vulnerabilities released from vendors, media services, or other reliable sources (SANS, CERT)	- CIRT Core Team investigates event and makes assessment - CIRT notification to USAP ISM for info and possible dissemination NSF-wide	Upon verification
Low	Suspicious Activities: an instance in which activities are detected that do not appear to be normal or authorized. Could be social engineering, E-mail messages, or other communications	- CIRT Core Team investigates event and makes assessment - CIRT notification to USAP ISM for info and possible dissemination NSF-wide	Upon verification
Low	Probe: any effort associated with information gathering effort that could be a precursor to an attempted compromise of USAP domain resources. Includes web queries, scans, and ping/port sweeps.	- CIRT Core Team investigates event and makes assessment - CIRT notification to USAP ISM for info and possible dissemination NSF-wide	Upon verification

APPENDIX C: USAP TECHNICAL INCIDENT REPORTING FORM

The form provided in this appendix is tailored for reporting technical incidents that occur on the USAP network, and is based on US-CERT reporting guidelines. This form is used by the CIRT Lead to report a technical incident to the USAP ISM for escalation to US-CERT. If evaluation of the technical incident indicates that there is suspicion or confirmation of the unauthorized disclosure of PII as a result of the incident, the CIRT Lead also reports the potential PII breach to the USAP ISM for escalation to US-CERT, by submitting the form provided in *Appendix D: USAP PII Disclosure Incident Reporting Form*.

Contact Information	
Does this report involve U.S. Government Federal Civilian Systems?	☐Yes ☐No
Reporting POC Name	
Organization Name	
Job Title	
Email Address	
Telephone number	
From what country are you making this report	
From what time zone are you making this report	
With what sector are you affiliated?	U.S. Federal Civilian Agency
Please provide your complete postal mailing address	
U.S. Federal Civilian Agency	
Please Identify the U.S. Government Federal Civilian agency	Independent Agencies
Support Action Requested	☐Phone call requested ☐Email response requested ☐No action requested
Support Action Timeframe	☐ Immediate ☐ Within 24 hours ☐ Within one week (5 business days) ☐ Within 30 days
Please select the independent agency.	National Science Foundation (NSF)

Technical Information

Remember: It is important to report all known information related to the incident in a timely manner. Therefore, include information available at the time of the incident in the initial report, and update later revisions as the investigation progresses.

Note: If incident related information is provided in an attached document, please reference the document in the appropriate subsection of this form.

Infrastructure Information	
Please identify activities attempted by the intruder and possible motives [Check all that apply]	
☐ Exposure of Information	☐ Theft of information technology resources
☐ Theft of other assets	☐ Alteration/destruction of information
☐ Loss of Reputation of target	☐ Increase notoriety of attacker
Please identify all the activities and motives accomplished by the intruder. [Check all that apply]	
☐ Exposure of Information	☐ Theft of information technology resources
☐ Theft of other assets	☐ Alteration/destruction of information
☐ Loss of Reputation of target	☐ Increase notoriety of attacker
☐ Other Provide explanation:	

General Incident Information

How did you initially become aware of the incident?	☐Automated software notification (e.g. firewall) ☐Automated review of log files ☐Manual review of log files ☐System anomaly (such as crashes, slowness) ☐Third-party notification ☐Don't know ☐Other Provide explanation:
Attack Technique (Vulnerability Exploited / Exploit Used	☐I know the CVE, CERT VU or Bugtraq number ☐Virus, Trojan horse, worm, or other malicious code ☐Denial-of-service attack or distributed denial-of-service attack ☐Unauthorized access to the affected computer privileged compromise (root or administrator access) user account compromise/web compromise (defacement) ☐Scanning or probing (reconnaissance) activity ☐ Other Provide explanation:
☐I know the CVE, CERT VU or Bugtraq number	If Known, the US-CERT Alert number If Known, the CVE number If known, the Bugtraq number
☐Virus, Trojan horse, worm, or other malicious code	What is the name or description of the virus? What type of anti-virus software is installed on the affected computer(s) ☐ None ☐ McAfee ☐ Norton Anti-Virus ☐ Sophos

	☐ VirusMD ☐ Don't know ☐ Other Provide explanation: Did the anti-virus software detect the virus? ☐ Yes ☐ No ☐ Don't know When was the anti-virus software last updated? ☐ Less than a day ago ☐ 1 to 7 days ago ☐ More than a week ago ☐ More than a month ago ☐ More than two months ago ☐ Don't know

☐Denial-of-service attack or distributed denial-of-service attack	How were the affected hosts involved in the denial of service? ☐Victim of a denial-of-service attack ☐Participant in a denial-of-service attack ☐Both a victim and a participant in a denial-of-service attack Can you identify the tool used in the attack? (Potential tools include: carko, Mstream, Ramen, shaft, stecheldrath, satchel, Stick, trinoo, TFN, TFN2K). Provide more information here:
☐Unauthorized access to the affected computer privileged compromise (root or administrator access) user account compromise/web compromise (defacement)	Please identify the type of unauthorized access ☐Web defacement ☐User account compromised ☐Root/privileged account compromised ☐Other Provide explanation:
☐Scanning or probing (reconnaissance) activity	How did you discover the reconnaissance activity? ☐Operating system logs ☐Network monitor data ☐Intrusion detection software ☐Firewall software ☐Don't know ☐Other Provide explanation: Please enter any alerts, error messes, or log extracts that you believe explain or support the problem you are reporting. (If possible, cut and paste the information here: Please identify the software and version used to generate the alerts, messages, or logs:
☐Other	Please enter information that best describes the technique of the attack:

Network Activity Information	
Please identify the protocols involved in the attack. [Check all that apply]	☐ TCP ☐ UDP ☐ ICMP ☐ IPsec ☐ IP Multicast ☐ Ipv6
Please identify source ports involved in the attack. Example: 23,25,60-90,1024-	
Please identify destination ports involved in the attack. Example: 23,25,60-90,1024-	
Impact of Attack Information	
Number of hosts affected	
Number of customers affected	
Time of first attack	
Time attack was detected	
Has the attack ended?	☐Yes ☐No
Duration of attack as of this report (hours)	
Estimated recovery time as of this report (wall clock hours)	
Estimated recovery time as of this report (staff hours)	
Estimated damage amount as of this report (US$ loss)	
Host(s) Involved Information	
Please specify how you would like to provide host information	☐ I have no host information ☐ I can enter each host's information individually ☐ I can provide the host information in bulk format
☐ I can enter each host's information individually	Does this host represent an attacking or victim host? ☐ Victim ☐ Attacker ☐ Both
	Hostname:
	IP Address:
	Do you have administrative responsibilities for this host? ☐ Yes ☐ No

	What is the operating system of the affected computer? ☐ Apple Mac Version: ☐ Cisco Version: ☐ Linux Version: ☐ Sun Solaris Version: ☐ Windows Version: ☐ Other OS and Version: ☐ Don't know
	If known, what is the patch level or software revision of the operating system?
	What is the primary purpose(s) of this host? [check all that apply] ☐ User desktop machine ☐ User laptop machine ☐ Web server ☐ Mail server ☐ FTP server ☐ Domain controller ☐ Domain name server ☐ Time server ☐ NSF/file system server ☐ Database Server ☐ Corporate application server ☐ Other infrastructure services Provide explanation:
	Actual impact on host? ☐ none ☐ failed ☐ degraded ☐ destroyed
	Potential impact on the host? ☐ none ☐ failed ☐ degraded ☐ destroyed
	I have more hosts to report: ☐ Yes ☐ No
☐ I can provide the host information in bulk format	What is the format of the bulk data?
	Please enter bulk host information here:
Additional Information Related to the Incident	
Is there anything else you would like to tell us concerning this report?	

APPENDIX D: USAP PII DISCLOSURE INCIDENT REPORTING FORM

The form provided in this appendix is tailored for reporting PII disclosure incidents that occur in the USAP, and is based on guidance provided in *NSF Bulletin No. 07-15: NSF Policy on Reporting the Breach of Personally Identifiable Information*, and *United States Computer Emergency Readiness Team Personally Identifiable Information Reporting Requirements*. This form is used by the CIRT Lead to provide a written report of a suspected or confirmed unauthorized disclosure of PII to the USAP ISM for escalation to US-CERT. Note that in the case of a PII incident, the CIRT Lead is required to verbally notify the USAP ISM of the incident within one hour of discovery.

Contact Information	
Does this report involve U.S. Government Federal Civilian Systems?	☐Yes ☐No
Reporting POC Name	
Organization Name	
Job Title	
Email Address	
Telephone number	
From what country are you making this report	
From what time zone are you making this report	
With what sector are you affiliated?	U.S. Federal Civilian Agency
Please provide your complete postal mailing address	
U.S. Federal Civilian Agency	
Please Identify the U.S. Government Federal Civilian agency	Independent Agencies
Support Action Requested	☐Phone call requested ☐Email response requested ☐No action requested
Support Action Timeframe	☐ Immediate ☐ Within 24 hours ☐ Within one week (5 business days) ☐ Within 30 days
Please select the independent agency.	National Science Foundation (NSF)

Incident Information IMPORTANT: Do not disclose actual PII content or material in this form, as this information is not required for reporting purposes.	
Provide a detailed description of how the PII was disclosed: unauthorized access, theft, data spillage, etc.	
What type(s) of PII data elements that were exposed: (e.g., full name, Social Security number, date of birth, home address, account number, disability code, etc.)?	
Did the PII breach include:	☐ SSN (PII) ☐ HIPAA (Medical) ☐ A123 (Financial) ☐ Security Breach (e.g., passwords, configurations, external IP addresses)
How many people were impacted by the PII breach?	
Was the disclosed information protected? If so, how was the information was protected; password protected, encrypted, no protection, etc.?	☐Yes ☐No
What is the scope of the disclosure: internal, external, how many unauthorized individuals had access, etc.?	
Provide a summary of the mitigation steps taken and/or strategy to contain the incident; impacted systems (file server, print, mail server, web server, etc.) taken offline and sanitized; cached data deleted; onsite/offsite back-ups, etc.	
Was a Law Enforcement or Inspector General notified? If so, what is the case number, LE/IG contact information, etc.?	☐Yes ☐No
What is the agency doing to investigate the breach, to mitigate losses, and to protect against any further breaches of this nature?	
What is the status of incident: Open, Closed, Pending.	☐Open ☐Closed ☐Pending
What steps should individuals take to protect themselves from potential harm, if any?	
Who should affected individuals contact at the agency for more information? Include a toll-free telephone number, e-mail address, and postal address.	
Additional Information Related to the Incident	
Is there anything else you would like to tell us concerning this report?	

APPENDIX E: CHAIN OF CUSTODY LOG

The following is an example of the chain of custody log utilized by the USAP.

IDENTIFYING INFORMATION FOR HARD DRIVE

Name of Manufacturer:	_____
Serial Number, Bar Code Number, or other Unique Identifier:	_____
Model Number and Size, if known:	_____
Jumper or Switch Configuration, if applicable:	_____

PHOTO: Please attach photo of hard drive to this form

CUSTODY LOG (to be filled in by each person who handles the hard drive, or had the drive in their possession)

Name:	_____
Job Responsibility:	_____
Date/Time Possession Began:	_____
Date/Time Possession Ended:	_____
Purpose for taking possession:	_____
	_____
State of drive while in possession (i.e. Locked up, in transit, under test, etc.);	_____

APPENDIX F: NSF MANAGEMENT REVIEW AND INCIDENT SUMMARY

<Date>

NSF Management Review and Summary of

<Division> Intrusion *<Date>*

Background
<Organization's Background>

Description of Incident
Incident Type: *<Incident Type>*

<Description of Incident>

Remediation

<Remediation Process>

<Restoration Efforts>

Impact
<Effect of the event>

Cause
<Detected Cause>

Estimated Cost of Assessment
<Estimated cost of contractor personnel to remediate the vulnerability>

Estimated Total Labor Hours	*<Hours>*	Estimated total Labor costs	*<$Amount>*
Estimated material Costs	*<$Amount>*	Estimated Service Downtime Cost	*<$Amount>*
		Total Estimated Cost	*<$Amount>*

Conclusion
<Summary of Conclusion>

Recommendations
<Recommendations to help mitigate the risk and impact>