The National Science Foundation
Polar Programs
United States Antarctic Program

Information Resource Management Directive 5000.08
USAP Security Auditing Policy

Organizational Function	Information Resource Management	**Policy Number**	5000.08
		Issue Date	1 August 2004
Policy Category	Information Security Policies and Instructions	**Effective Date**	1 August 2004
		Updated	15 May 2013
Subject	Security Auditing	**Authorized By**	Section Head, NSF/GEO/PLR/AIL
Office of Primary Responsibility	National Science Foundation Geosciences Directorate Division of Polar Programs Antarctic Infrastructure & Logistics	**Responsible Official**	Primary Responsibility: Mr. Patrick D. Smith Technology Development Manager
			Security Responsibility: Ms. Desari Mattox USAP Information Security Manager
Address	Suite 755 4201 Wilson Blvd Arlington, VA 22230	**Phone**	703.292.8032
		Fax	703.292.9080
		Web	http://www.nsf.gov/div/index.jsp?div=PLR
Distribution	USAP-Wide	**Status**	Final Policy
Online Publication	http://www.usap.gov/technology/contentHandler.cfm?id=1563		

1. PURPOSE

This directive establishes the Security Auditing program for information systems supporting the National Science Foundation (NSF), Geosciences Directorate (GEO), Polar Programs (PLR), United States Antarctic Program (USAP). It describes the tasks of the auditors, and the methods used to ensure integrity, confidentiality, and availability of USAP information resources. Security auditing is used to detect or investigate actual or attempted security violations in any USAP system by recording security relevant events as they occur. Auditors can monitor user or system activity when appropriate, and ensure conformance to USAP information security policies based on their findings.

2. BACKGROUND

Federal information technology regulations require PLR to audit the use of USAP information resources on a regular basis. As resource owner, PLR or it's designated system managers can audit any USAP information resource as part of scheduled activities, or in response to actual security violations. Audit findings indicate the improvements needed to better protect the integrity of USAP information resources.

3. GUIDING PRINCIPLES

- An information system audit will identify both strengths and vulnerabilities of a system with an emphasis on improving the overall USAP information security posture.
- A structured approach to auditing ensures a balanced approach to security and mission execution.
- Audits will remain objective, and not be implemented as a disciplinary tool. However, audit results may be used to support administrative or disciplinary measures if warranted.

4. POLICY

The USAP Information Security Manager will establish a program to periodically audit the use of all USAP information resources. All users, administrators, and owners of USAP information and information resources will support the USAP Information Security Manager in the implementation of this policy and the execution of the audits.

4.1 Operational Definitions

4.1.1 Audit

For purposes of this policy, an audit is the process of comparing actual use of an information resource against the identified policies, processes, instructions and procedures governing the use of the resource. Audit types include, but are not limited to:

- **Compliance Audits.** These audits are based on the USAP's information security framework including the review of supporting procedures, instructions, and guidelines to ensure they comply with approved policies; assessing the efficiency and effectiveness of security policies and procedures; and ensuring that policies have been amended to reflect organizational, process and technology infrastructure changes.
- **Specific Platform Audits.** The auditing of a specific system software, networks, application software, and databases, to ensure that policies, procedures, and instructions are being applied in practice.
- **Technical Audits.** These are audits of specific high-risk areas such as Internet security and data encryption, which involve the assessment of the technical infrastructure in place to determine how adequately it supports the USAP information security objectives.

4.1.2 Audit Report

A report of activities conducted as part of an audit, and the results and recommendations of those activities. An audit report typically follows the structure identified in appropriate National Institute of Standards & Technology (NIST) guidelines.

4.1.3 Audit Trail

An audit trail provides a record of activity which permits information security practitioners to trace a transaction's history or a user's activity, including information about additions, deletions, or changes to information, or to an information resource. Audit trails enable the enforcement of individual accountability by enabling the reconstruction of events.

4.2 Annual Assessments

The USAP Information Security Manager will conduct annual assessments of the security of USAP information resources, in accordance with NIST guidelines. These assessments will include a review of the resource's audit functions and activities.

4.3 Review of Audit Logs

The USAP information system manager will review the audit logs of USAP information resources and summarize the review results in a Monthly status report to the PLR Technology Manager and the USAP ISM. Established reporting mechanisms may be used to convey the results of the monthly audit. The level of detail reported will be determined by the ISM in coordination with NSF.

4.4 Incident Reporting

If a security issue is identified during the audit review, or through other means, the USAP system owner will immediately notify the PLR Technology Manager and the USAP Information Security Manager, who will implement appropriate Incident Response procedures.

4.5 Impromptu Audit

Consistent with their responsibilities for oversight of proper use of USAP information resources, the PLR Technology Manager, USAP Information Security Manager, or the USAP system owner may audit any USAP information resource at any time.

4.6 Archive & Disposal of Audit Logs

The USAP system manager will archive audit logs on a weekly basis, and retain these logs until after they are reviewed as part of the annual assessment, or until authorized to dispose of the logs by the USAP Information Security Manager. Logs not reviewed may be disposed of as appropriate.

4.7 Auditor Access

The USAP Information Security Manager will review and approve access to resources required to complete an audit. Audit-related access may include user or system level access to any information resource within the scope of the audit; electronic or paper copies of information created, processed, stored, or disseminated by the resource; access to physical work areas such as offices, labs, cubicles, and storage areas; and access to network resources to support network monitoring and penetration analysis.

4.8 Temporary Access to Resources

The USAP system manager, subject to approval by the USAP Information Security Manager, will provide audit team members with temporary access to appropriate resources for the duration of the auditing task.

4.9 Functions Audited

At minimum, the USAP Information Security program shall audit the following functions as necessary: access controls, backup controls; system and transaction controls; data library procedures; systems development standards; physical security of information resources; contingency plans; database management. Other functions may be included in an audit to satisfy federal regulations, or NSF direction.

4.10 Logged Information

To support the requirements of this policy and higher level federal guidelines, USAP information resources will incorporate capabilities to log resource use, with all logged activities identified by date and time of occurrence. At a minimum, the following activities will be logged:

- User activities, including logon and logoff, failed logon attempts, and attempts to access unauthorized resources, including web pages and external Internet resources
- Failed attempts to access resources by an unauthorized user
- Creation, reading, updating, or deleting of files and folders
- Program initiation by a user
- Activities of system operator, system administrator, and other users with administrative privileges for the system

4.11 Protection of Resource Logs

Logs of activities related to the use of information resources shall be protected at the same level of the information processed by the resource and released only to authorized individuals. The PLR Technology Manager, the USAP Information Security Manager, or the USAP system owner may authorize release of resource logs at a lower level of protection if needed to facilitate an audit, an investigation, or related administrative activity.

4.12 Audit Report Information

Audit reports shall contain sufficient information to enable the review staff, with no previous connection with the audit, to ascertain the evidence that supports the auditors' significant conclusions and judgments.

5. APPLICABILITY AND COMPLIANCE

This policy 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 policy is as indicated in USAP Information Resource Management Directive 5000.01, *The USAP Information Security Program*.

6. RESPONSIBILITIES

Within the NSF and the USAP, several elements have specific responsibilities that directly affect the security of information resources and information systems.

6.1 USAP Information Security Manager (ISM)

The ISM ensures proper security measures are in place to protect USAP information resources. The ISM ensures personnel performing audits have the necessary skills. During audit activities, the ISM ensures auditors have the necessary access to resources. When an audit indicates deficiencies in the implementation of security controls, the ISM evaluates such deficiencies, identifies the potential risks, and takes appropriate action to correct the deficiencies or mitigate the risks.

6.1 USAP Information System Managers

USAP Information system managers establish and implement auditing procedures and processes to comply with this policy.

7. PROGRAM IMPLEMENTATION

7.1 Implementation

The USAP Information Security Manager and each USAP participant organization will develop appropriate processes, instructions, and procedures to implement this policy.

8. AUTHORITY

This directive is published in conformance with the authority of the National Science Foundation Act of 1950, as amended and extended, the Federal Information Security Management Act of 2002, and NSF guidance.

<div align="center">

Brian Stone

Section Head, NSF/GEO/PLR/AIL

</div>

REVISION/CHANGE RECORD

Pages	Date	Version	Author/Reviewer	Reason for Change
All	6/9/2011	1.0	Matthew Rogers	Verified alignment with NIST Special Publication 800-53 Revision 2. Changed ISM name.
All	5/3/2012	2.0	Alex Jerasa	Updated key contacts and conducted FY12 review
All	5/15/2013	3.0	Desari Mattox	Updated OPP and AIL titles to align with NSF re-organization & Verify alignment with NIST SP 800-53 rev 3.