The National Science Foundation
Polar Programs
United States Antarctic Program

Information Resource Management Directive 5000.02
USAP Information Security Organization and Administration

Organizational Function	Information Resource Management	**Policy Number**	5000.02
		Issue Date	1 August 2004
Policy Category	Information Security Policies and Instructions	**Effective Date**	1 August 2004
		Updated	11 May 2013
Subject	Information Security Organization & Administration	**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** **Fax** **Web**	703.292.8032 703.292.9080 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 policy establishes the guidelines for organizing and administering Information Security within the National Science Foundation (NSF), Geosciences Directorate (GEO), Polar Programs (PLR), United States Antarctic Program (USAP).

2. BACKGROUND

An Information Security organization is required to implement federal information technology regulations regarding security of information and information resources.

3. GUIDING PRINCIPLES

- The Information Security organization will respond to USAP science and operations needs, striking the balance between security and operational necessity.
- Administration of information security policies, processes, and procedures will consider the effects of security requirements on the entire USAP enterprise.
- Every security requirement will be tied to an operational need, a federal regulation, or an industry standard practice.

4. POLICY

Polar Programs will organize an Information Security function to establish policies, processes, standards, and procedures for information security within the USAP. This function will interpret federal regulations and apply their requirements to USAP information resources; administer programs and execute projects to meet information security objectives; and perform liaison functions between USAP participants and the NSF for matters regarding information security.

4.1 Information Security Policies

Information security policies are statements made by NSF PLR to establish overall policy on information access and safeguards. These statements include directives to create an information security program, establish its goals, and assign responsibilities. The term policy is also used to refer to the specific security rules for particular systems. Additionally, policy is defined as the documentation of information security decisions. The USAP uses three basic types of policies:

- Program policy is used to create an organization's information security program.
- Issue-specific policies address specific issues of concern to the organization.
- System-specific policies focus on decisions taken by management to protect a particular system.

4.2 Information Security Procedures, Instructions and Guidelines

Procedures, Instructions, and guidelines are used to describe how policies will be implemented within the USAP. They offer users, managers, and others a clearer approach to implementing policy and meeting organizational goals. Instructions and guidelines specify technologies and methodologies to be used to secure systems. Procedures are yet more detailed steps to be followed to accomplish particular security related tasks. Instructions, guidelines, and procedures may be promulgated throughout an organization via handbooks, regulations, or manuals. NIST Special Publication (SP) 800-12, *An Introduction to Computer Security: The NIST Handbook*, provides more detailed information on the development of procedures, instructions and guidelines.

4.3 Information Security Organization

Polar Programs will establish a functional organization to manage and administer all information security activities within the USAP. The USAP Information Security Manager (ISM) leads this organization. The organization will be staffed with appropriate management

and technical personnel to address information security issues related to USAP science and operations activities.

4.4 Information Security Manager (ISM)

The ISM creates, updates, administers, and implements policies and procedures governing the information security practices of all USAP participants and USAP information resources. The ISM serves as liaison with the NSF Information Security Officer (ISO), and the ISOs of other government agencies participating in the USAP. The ISM establishes projects and programs within the USAP to achieve the information security objectives identified by the federal government, the NSF Chief Information Officer (CIO) and the PLR Technology Manager. The ISM helps USAP participants comply with USAP information security policies, processes, instructions and procedures. Under the guidelines presented in National Institute Standards & Technology (NIST) Special Publication (SP) 800-37, *Guide for applying the Risk Management Framework to Federal Information Systems*. NSF PLR reserves the right to staff the ISM position from one of the USAP participant organizations.

4.4 Information Security Staff

The ISM will organize, train and equip an information security staff to address management and technical issues related to the security of USAP information resources, and to remain cognizant of current threats and vulnerabilities identified within the information technology industry. The staff may include government and contractor personnel.

4.5 Information Security Advisory Group

The USAP ISM will convene Information Security Advisory Groups as needed to address specific information security issues that have enterprise-wide consequences. The advisors shall include representatives from NSF PLR, the USAP Prime Contractor, other USAP participant organizations, and members of the user groups affected by the issue of interest. The Advisory Group will be chartered to review policies and procedures and make recommendations for their improvement and implementation to the USAP Executive Management Board and to the USAP ISM. Final management authority for the USAP Information Security program resides with the Section Head, AIL.

4.6 Information Security Administration

The USAP Information Security organization will administer all programs and projects designed to implement or maintain information security requirements. Administrative activities include, but are not limited to, the following:

- Develop security polices, processes, instructions and procedures.
- Determine roles and responsibilities for information security within the USAP.
- Develop and implement information security plans for applications, systems, and operating locations as required by federal regulations and NSF directives.
- Evaluate USAP infrastructure compliance with information security policies, processes, instructions and procedures.
- Establish processes and procedures for access to sensitive systems and information.

- Establish processes and procedures to minimize the likelihood of disruptions, to recover from disasters, and to respond to security incidents.
- Develop programs to increase awareness among USAP participants of information security issues and responsibilities.
- Develop the information security architecture and apply appropriate standards to secure USAP information resources.

4.7 Information Security Violations

Violation of any provision of USAP information security policies may result in one or more of the following actions:

- Limitation of an individual's access to some or all USAP systems.
- Disciplinary actions, in accordance with NSF policy and the policies of the sponsoring organization.
- Requirement of the violator to provide restitution for any improper use of information/service.
- Initiation of legal action by the NSF including, but not limited to, criminal or civil prosecution under appropriate federal laws.

4.8 Information Security Policy Process

The USAP ISM will establish a process for the development of information security policies. This process will include provisions for the review of existing and proposed policies by USAP participants, and will allow sufficient time for participants to submit comments for consideration about the policies under review.

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

In addition to the responsibilities identified in USAP Information Resource Management Directive 5000.01, *The USAP Information Security Program*, the following officials have specific responsibilities related to Information Security and Organization.

6.1 Section Head, Antarctic Infrastructure & Logistics (AIL)

The Section Head, AIL, designates the USAP ISM and directs all USAP participants to support the Information Security program.

6.2 USAP Information Security Manager (ISM)

The ISM leads the Information Security organization and administers the Information Security program. The ISM ensures that the capabilities of the organization are

appropriate for operational needs, and ensures all organizational activities are included in project plans and budgets as appropriate.

6.3 USAP Participant Organizations

Each USAP participant organization will designate an Information Security representative who will coordinate the organization's information security activities with the USAP ISM to minimize duplication of effort, properly manage the balance between operations and security, and to serve in the USAP Information Security Advisory Group.

7. IMPLEMENTING INFORMATION SECURITY ORGANIZATION AND ADMINISTRATION

7.1 Implementation

The ISM directs the implementation of this policy, and coordinates all USAP information security activities with appropriate NSF elements, including the NSF CIO, NSF ISO and the NSF Inspector General.

7.2 Support from USAP Prime Contractor AKA Antarctic Support Contractor

The Antarctic Support Contractor (ASC) provides primary contracted information technology and communications (IT&C) operations, maintenance and services delivery management of the NSF-owned/managed IT&C infrastructure supporting the USAP. A contracted requirement of the ASC includes the full compliance of FISMA, NIST, and related NSF information security guidance as promulgated by NSF. The ASC is required to maintain an active and effective information security/assurance capability in response. The ASC is responsible for assigning a lead information Security/assurance capability, to include designated personnel.

7.3 USAP Participant Organizations

Each USAP participant organization implements information security policies, processes, instructions and procedures in coordination with the ISM.

7.4 USAP Information Security Advisory Group

The ISM establishes the Information Security Advisory Group, which meets periodically to consider information security issues and make recommendations to PLR and the USAP Executive Management Board.

8. AUTHORITY

Publication of this policy is 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.

Brian Stone
Section Head, NSF/GEO/PLR/AIL
bstone@nsf.gov

Digitally signed by bstone@nsf.gov
DN: cn=bstone@nsf.gov
Date: 2014.05.22 19:45:12 -04'00'

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	5/11/2013	3.0	Desari Mattox	Updated OPP and AIL titles to align with NSF re-organization & Verify alignment with NIST SP 800-53 rev 3.