The National Science Foundation
Polar Programs
United States Antarctic Program

Information Resource Management Directive 5000.16
The USAP Security Assessment & Authorization Program

Organizational Function	Information Resource Management	**Policy Number**	5000.16
		Issue Date	1 August 2004
Policy Category	Information Security Policies and Instructions	**Effective Date**	1 August 2004
		Updated	17 May 2013
Subject	Security Assessment & Authorization Program	**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 Assessment and Authorization (SA&A) Program formerly known as the Certification and Accreditation (C&A) program for information systems supporting the National Science Foundation (NSF), Geosciences Directorate (GEO), Polar Programs (PLR), United States Antarctic Program (USAP). This directive establishes quality controls for the security of information resources. Assessment is the process of testing the effectiveness of security controls. Authorization is the management acceptance of the evaluated risk factors and the resulting approval or denial to operate the system. The SA&A program applies to all applications and systems that are determined to be Major Applications or General Support Systems, as defined by the Federal Information Security Management Act of 2002 (FISMA). The USAP SA&A program includes activities to support the implementation of NSF and FISMA directives.

2. BACKGROUND

Federal information technology regulations require USAP information systems to undergo a security SA&A process to identify the risks associated with their operation. USAP information system integrity ensures the success of the science research mission by providing reliable global communications to facilitate field experiments and exchange of data within the Antarctic region. It also protects government and private resources used to execute and administer mission activities while allowing effective access to program information by the general public.

3. GUIDING PRINCIPLES

- The USAP SA&A process will be an integral element of information systems development and operation.
- The USAP SA&A process is based on existing federal and NSF directives, particularly those listed in 5000.01, Appendix 1.
- Science grant systems will be included in the SA&A process as directed by NSF PLR.

4. POLICY

The SA&A process will implement the policies of the NSF and the National Institute of Standards and Technology (NIST) as they apply to the USAP.

4.1 Operational Definitions

4.1.1 Assessment

The testing and/or evaluation of the management, operational, and technical security controls in an information system to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.

4.1.2 Authorization

The official management decision given by a senior organizational official to authorize operation of an information system and to explicitly accept the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation based on the implementation of an agreed-upon set of security controls.

4.1.3 Designated Approving Authority (DAA)

Per NSF Manual 7, The NSF Information Security Handbook, the DAA for USAP systems is the NSF Chief Information Officer (CIO).

4.1.4 General Support System

As defined in Circular A-130, Appendix III, a General Support System is an interconnected set of information resources under the same direct management control that shares common functionality. A system normally includes hardware, software, information, data, applications, communications, and people. Examples of a system are: a local area network (LAN) including smart terminals that support a branch office; an agency-wide backbone; a communications network; a departmental data processing center including its operating system and utilities; a tactical radio network; and shared information processing service organization.

4.1.5 Major Application

Circular A-130 defines a major application as an application requires special attention to security due to the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application. Note: All Federal applications require some level of protection. Certain applications, because of the information in them, however, require special management oversight and should be treated as major. Adequate security for other applications should be provided by security of the systems in which they operate.

4.2 Security Assessment & Authorization Program (SA&A)

The USAP Information Security Manger (ISM) will establish a program to assess and authorize the NSF-funded information systems used within the program. The program will include a process for assessing and authorizing systems, and procedures to guide information system managers through the process. Personal use systems are not normally included in the assessment process, unless identified as part of a science grant system requiring certification review.

4.3 Identification of Included Information Systems

All Information and Information Technology, applications and systems determined to be either Major Applications or General Support Systems (hardware, software, information, data, applications, communications, and people) must complete the SA&A process. Using the guidelines in Manual 7, the ISM will establish and maintain a list of major applications and general support systems. The list will be updated annually, or when major changes occur. The list will be included in the USAP Information Security Plan.

4.4 Participation

All USAP organizational elements, U.S. Government employees, research grantees, private citizens, contractors and sub-contractors personnel, and foreign nationals will support the SA&A program in an appropriate manner.

4.5 New Information Systems

To comply with OMB Circular A-130, all new information systems acquired or developed by any USAP participant organization to support program requirements will incorporate provisions for security assessment & authorization in their project and system life cycle planning. All new systems acquired or developed by any USAP participant organization will be checked against the criteria for major applications or general support systems provided by NSF/CIO. If the new information system is determined to be a major application or a general support system, the project to acquire the system will include funding in the system development plans to accomplish the system assessment and authorization.

4.6 Commercial Off-The-Shelf Applications

Commercial off-the-shelf (COTS) applications are covered by the SA&A activities for the general support system on which they reside, unless the COTS product is identified as a major application.

4.7 Existing & Outdated Information Systems

Some USAP information systems that play an essential role in mission accomplishment entered into operation prior to implementation of this policy and have exceeded their design life. Where replacement systems have been identified and are under development, the SA&A process will focus on the replacement system. Where no replacement has been identified, the SA&A process will evaluate the existing system. NSF PLR will make the final determination as to whether or not a system requires assessment & authorization.

4.8 Periodic Review of Information Systems

Federal guidelines direct that NSF perform an independent review or audit of the security controls in each major application or general support system at least every three years, or with a major change and based on these results, perform an annual review of the overall NSF-wide information security program. These periodic reviews also include the USAP operating locations. At the start of each fiscal year, the USAP Information Security Manager will identify the systems to be reviewed in that fiscal year. This information will be included in the USAP Information Security Plan.

4.9 Federal Information Security Management Act of 2002 (FISMA)

The official management decision given by a senior organizational official to authorize operation of an information system and to explicitly accept the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation based on the implementation of an agreed-upon set of security controls.

4.10 Non-USAP Systems

Any Non-USAP system connected to the USAP information infrastructure must be evaluated to determine if an assessment is required as part of the connection arrangements. NSF PLR makes the final determination as to whether or not a Non-USAP system requires an assessment review as part of the connection arrangement.

4.11 Non-USAP Sites and Facilities

A non-USAP site or facility supports the USAP mission in some form, but is outside the direct management responsibility of the NSF. An example is commercial satellite facility relaying information from a USAP operating location to the Denver Operating location. This policy applies to non-USAP locations only to the extent required by federal law, or the grant, contract or other operating agreement in place between NSF and the party responsible for the non-USAP location.

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

6.1 Section Head, Antarctic Infrastructure & Logistics (AIL)

The Section Head, AIL, is the responsible Official for USAP information systems, and is the USAP System Owner. The System Owner's responsibilities are as the former Certifying Official. The System Owner ensures that any security deficiencies are documented in the SA&A Package. The System Owner determines the level of acceptable risk associated with system operation and recommends for or against authorization to the NSF CIO, who is the DAA.

6.2 Technology Development Manager, Antarctic Infrastructure & Logistics (AIL)

The Technology Development Manager oversees the development and implementation of USAP SA&A activities.

6.3 USAP Information Security Manager (ISM)

The USAP ISM implements the SA&A program and coordinates its activities with other IT programs and organizations. The USAP ISM ensures project plans and budgets include SA&A activities as appropriate. The ISM coordinates SA&A activities with the NSF Information Security Officer, and with other USAP participating agencies. This includes planning the efforts, obtaining evaluation resources, and overseeing production of the SA&A package. The USAP ISM works closely with the designated SA&A lead to make recommendations to the USAP System Owner.

6.4 USAP Information Systems Owners and Developers

System owners and development managers will ensure their systems comply with this policy, with NSF assessment & authorization guidance, and with NIST instructions.

6.5 Non-USAP Information Systems Owners and Developers

System owners and development managers for Non-USAP systems will ensure their systems comply with this policy, with NSF assessment & authorization guidance, and with NIST instructions to the extent applicable for their systems.

7. ASSESSMENT & AUTHORIZATION PROGRAM IMPLEMENTATION

The USAP Information Security Manager will develop appropriate policies, processes, and procedures to implement the USAP SA&A Program. The USAP SA&A program will identify security risks associated with operation of all applicable information systems to assess and authorize those systems for operation. USAP participant organizations will publish procedures as needed to comply with this policy.

7.1 Guiding Standards

The USAP SA&A process will be based on existing federal and NSF directives.

7.2 Security Assessment & Authorization Organization and Administration

The USAP ISM will establish teams as needed to complete SA&A activities. These teams will complete SA&A activities for their assigned systems, and ensure documentation packages are completed. These teams will support the certification activities of all USAP participant organizations and Non-USAP systems owners, as directed by NSF PLR.

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 19:51:35 -04'00'

REVISION/CHANGE RECORD

Pages	Date	Version	Author/Reviewer	Reason for Change
All	06/09/2011	1.0	Matthew Rogers	Verified alignment with NIST Special Publication 800-53 Revision 2. Changed ISM name.
All	05/03/2012	2.0	Alex Jerasa	Updated key contacts and conducted FY12 review
All	05/17/2013	3.0	Desari Mattox	Updated OPP and AIL titles to align with NSF re-organization & Verify alignment with NIST SP 800-53 rev 3