The National Science Foundation
Polar Programs
United States Antarctic Program

System and Services Acquisition Policy 5000.23

Organizational Function	Information Resource Management	**Document Number**	5000.23
		Issue Date	06/27/2014
Document Category	Information Security Policies	**Effective Date**	06/27/2014
		Review On	06/27/2016
Subject	System and Services Acquisition	**Authorized By**	Mr. Brian Stone Section Head, NSF/PLR/AIL
Office of Primary Responsibility	National Science Foundation Geosciences Directorate Division of Polar Programs Antarctic Infrastructure and 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
Online Publication	http://www.usap.gov/technology/contentHandler.cfm?id=1563		

Document Release History

Release Number	Release Date	Description of Changes	Changes Made By
0.1		Initial creation	Matthew Rogers
1.0	06/19/2014	Updates throughout	USAP ISM

Table of Contents

THIS PAGE INTENTIONALLY LEFT BLANK

1 PURPOSE

This directive establishes the system and services acquisition policy for information systems supporting the National Science Foundation (NSF) United States Antarctic Program (USAP).

2 BACKGROUND

Federal law and Office of Management and Budget (OMB) directives require the establishment of a System and Services Acquisition policy to protect USAP information and information systems.

3 GUIDING PRINCIPLES

- The USAP System and Services Aquisition Program shall be developed in compliance with National Institute of Standards & Technology (NIST) guidelines and NSF/PLR directives.
- System and services acquisition controls must balance operating environments with implementation of effective security controls

4 POLICY

It is USAP policy to protect the confidentiality, integrity and availability of information and information systems by assuring systems, system components and services acquired are secure and do not negatively impact security of pre-existing systems.

System operators, managers, maintainers and providers of USAP information & communication systems shall:

- Determine and incorporate information security requirements for the information system or information system service in mission/business process planning.
- Develop and implement a system development life cycle (SDLC) to manage information systems.
- Integrate information security processes into the SDLC
- Include security requirements in acquisition contracts for information system(s), system component(s), or information system service(s). These requirements shall be in accordance with applicable federal laws, standards, guidelines, NSF contracts, and NSF/PLR directives.
- Require the developer of the information system, system component, or information system service to provide design and implementation information for the security controls to be employed, and to identify the functions, ports, protocols, and services intended for organizational use early in the system development life cycle.
- The USAP shall employ only FIPS 201-approved products list for Personal Identity Verification (PIV) capabilities implemented.

- Require providers of external information system services to comply with applicable federal requirements through an oversight process.
- Assure roles and responsibilities, methods, and techniques of the oversight process are defined.
- Implement a configuration management program for the information system, system component, or information system service. The configuration will control the integrity of changes to include flaw remediation processes.
- Fully document and complete assessment and remediation process to be conducted by the developer of the information system, system component, or information system service.

5 ROLES AND RESPONSIBILITIES

The following roles have specific responsibilities pertaining to system and services acquisition management. The sections below describe only the responsibilities for these roles as they relate to system and services acquisition management. Refer to USAP Information Security Policy 5000.01, *The USAP Information Security Program*, for the full description of the responsibilities for these roles.

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

The AILTechnology Development Manager is the responsible official of the USAP System and Services Acquisition Management Program.

5.2 USAP Information Security Manager (ISM)

The USAP Information Security Manager (ISM) oversees the System and Services Acquisition Management Program. The ISM coordinates the development and implementation of the system and services acquisition management program with Supporting Organizations, System managers, and administrators of USAP information systems to ensure system and services acquisition.

5.3 Supporting Organizations

Supporting organizations are responsible for management of system and services acquisition management processes and implementation of security controls. Also ensure that system and services acquisition is in alignment with guidance from NSF/PLR. Personnel shall provide USAP participants with support and guidance in system and services acquisition.

5.4 Tenant Organizations

Tenant organizations with systems interconnected to the USAP enterprise network are responsible for system and services acquisition in accordance with this policy.

6 SCOPE AND COMPLIANCE

This policy applies to all information resources, systems, technology and users within the USAP operating environment or connected to the USAP network. Compliance with this policy implementation is indicated in National Institute of Standards and Technology (NIST) Special Publication 800-53 Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, and USAP Information Security Policy 5000.01, *The USAP Information Security Program*.

7 POLICY IMPLEMENTATION

7.1 Implementation

Each USAP participant organization will develop appropriate processes, and procedures to implement the USAP System and Services Aquisition program. USAP participant organizations will publish procedures as appropriate to implement this program to comply with this policy. All users of the USAP infrastructure will ensure their systems comply with this policy.

7.2 Policy Review

This policy is reviewed in conjunction with major changes to the USAP information infrastructure or every two years.

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: 2014.06.27 14:22:25 -04'00'