The National Science Foundation
Polar Programs
United States Antarctic Program

Identification and Authentication Policy 5000.19

Organizational Function	Information Resource Management	**Document Number**	5000.19
		Issue Date	6/27/2014
Document Category	Information Security Policies	**Effective Date**	6/27/2014
		Review On	6/27/2016
Subject	Identification and Authentication	**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**	703.292.8032
		Fax	703.292.9080
		Web	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	05/03/2013	Initial Creation	Matthew Rogers - BAH
1.0	05/30/2014	Updates throughout	USAP ISM

Table of Contents

THIS PAGE INTENTIONALLY LEFT BLANK

1 PURPOSE

This directive establishes the policy for managing user identification and authentication in order to access information and 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 Identification and Authentication Policy to implement and protect access to information and information systems.

3 GUIDING PRINCIPLES

In developing methods and processes for identification and authentication, the program shall follow these guiding principals:

- USAP must monitor and control access to its network and infrastructure to protect information and information systems, identification and authentication of its users and devices is vital in accomplishing this
- The technical controls for implementing identification and authentication may be supplemented or augmented with processes and procedures where necessary

4 POLICY

It is USAP policy to protect the confidentiality, integrity and availability of information systems.

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

- Ensure all USAP information systems[1] have a means to enforce user accountability for system activity (both authorized and unauthorized) to be traced to a specific user or to an approved user group.
- Ensure all information systems have a method of user and device identification and authentication. Systems that do not meet this requirement must be explicitly authorized by NSF/PLR.
- Manage identifiers and authenticators for both users and devices to ensure appropriate authorization, assignment, and termination.

[1] **USAP Information System** - Information systems directly supporting the mission of the United States Antarctic Program; including those provided or managed by another federal agency, contractor, or other source. A USAP information system is typically procured using NSF program funds for USAP operations or has property accountability to NSF. Such systems may consist of:

a) **Government Owned Contractor Operated (GOCO) Systems** - U.S. Government owned systems where a contractor provides design, development, deployment, operations, and/or phase-out.

b) **Government Owned Government Operated (GOGO) Systems** - U.S. Government owned systems where a component of the U.S. Government provides design, development, deployment, operations, and/or phase-out.

- Ensure USAP systems use federally approved cryptographic authentication.
- Ensure all authenticator feedback is obscured.
- Ensure non-USAP users are identified and authenticated under the same requirements as USAP users.

5 ROLES AND RESPONSIBILITIES

The following roles have specific responsibilities pertaining to identification and authentication management. The sections below describe only the responsibilities for these roles as they relate to identification and authentication. 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 identification and authentication management program.

5.2 USAP Information Security Manager (ISM)

The USAP Information Security Manager (ISM) oversees the USAP identification and authentication management program. Coordinates the activities of USAP and supporting organizations[2] in the implementation of this policy.

5.3 Supporting Organizations

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

5.4 Tenant Organizations

Tenant organizations with systems interconnected to the USAP enterprise network are responsible for securing their systems in accordance with this policy.

6 SCOPE AND COMPLIANCE

This policy applies to supporting organizations and tenant organizations within the USAP operating environment or connected to the USAP network. Compliance with this policy implementation is indicated in OMB M-06-16 – *Protection of Sensitive Agency Information*, 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*.

[2] Supporting organizations refers to any participant organization that utilizes the IT&C infrastructure as a means to support USAP mission requirements.

7 POLICY IMPLEMENTATION

7.1 Implementation

Each USAP supporting organization shall develop appropriate processes, and procedures to implement the USAP identification and authentication program. Supporting organizations shall publish procedures as appropriate to implement this program to 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 14:21:42 -04'00'