The National Science Foundation
Polar Programs
United States Antarctic Program

System and Communications Protection Policy 5000.21

Organizational Function	Information Resource Management	**Document Number**	5000.21
		Issue Date	06/27/2014
Document Category	Information Security Policies	**Effective Date**	06/27/2014
		Review On	06/27/2016
Subject	System and Communications Protection	**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	09/20/2013	Initial creation	Matthew Rogers -BAH
1.0	06/03/2014	Updates throughout	USAP ISM

Table of Contents

THIS PAGE INTENTIONALLY LEFT BLANK

1 PURPOSE

This directive establishes the system and communications protection 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 system and communications protection policy to protect the confidentiality, integrity and availability of information and information system.

3 GUIDING PRINCIPLES

- Technical, physical and process measures may be used to protect systems and communications
- Implementation of system and communications protections will take into account its operating environment and impact on USAP operational requirements
- Technical capabilities, or limitations, of the information system will be taken into account during implementation of system and communication protections
- Information security and privacy protection implementation will be coordinated to the greatest extent feasible to assure those activities are successful while reducing duplicate or unnecessary efforts

4 POLICY

It is USAP policy to protect the confidentiality, integrity and availability of information systems, data residing within these systems and the communications among these systems and with systems external to the USAP accreditation boundaries.

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

- Separate user functionality (including user interface services) from information system management functionality in its systems. Unauthorized and unintended information transfer via shared system resources shall be prevented.
- Protect systems against or limit the effects of denial of service attacks.
- Implement boundary protection. This protection shall address the external boundary as well as key internal boundaries, which shall be identified in the system security plan.
- Logically separate sub networks for publicly accessible system components from internal networks.
- Manage and document interfaces used and their protection capabilities to connect to external networks.

- Limit the number of the external network connections to assure effective traffic monitoring.
- Terminate USAP network connections at the end of the session or after a period of inactivity for remote sessions
- Protect the integrity and confidentiality of transmitted and at rest Personally Identifiable Information (PII) and Sensitive Information (SI) with federally compliant encryption.
- Establish and manage cryptographic keys for required cryptography employed within the information system.
- Configure collaborative computing to prohibit remote activation unless an exception has been approved by NSF/PLR.
- For systems employing Public Key Infrastructure (PKI), issue, or obtain from an approved service provider, public key certificates under an appropriate certificate policy.
- Define acceptable and unacceptable mobile code and mobile code technologies. Examples of mobile code include scripts (JavaScript, VBScript), Java applets, ActiveX controls, Flash animations.
- Authorize, monitor, and control the use of Voice over Internet Protocol (VoIP) within the information system through established usage restrictions and implementation guidance for VoIP technologies, based on the potential to cause damage to the information system if used maliciously.
- Encrypt all Domain Name System (DNS) services
- Configure internal Domain Name System (DNS) servers to: only process name/address resolution requests from internal clients.
- Configure external DNS servers to: only process name/address resolution information requests from external clients.
- Configure USAP information systems to request and perform data origin authentication and data integrity verification on the name/address resolution responses the system receives from authoritative sources for recursive or caching resolver DNS servers.
- Provide fault-tolerant name/address resolution service for all information systems
- Provide mechanisms to protect the authenticity of communications sessions.

5 ROLES AND RESPONSIBILITIES

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

5.2 USAP Information Security Manager (ISM)

The USAP Information Security Manager (ISM) provides oversight of the system and communications protection program and compliance with this policy. Coordinates assessment of security controls for system and communications protection.

5.3 Supporting Organizations

Supporting organizations assist with the development of system and communications protection procedures and standards. Also ensure system and communications protection is in alignment with guidance from NSF/PLR. Personnel shall provide USAP participants with support and guidance in system and communications protection.

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*.

7 POLICY IMPLEMENTATION

7.1 Implementation

Each USAP supporting organization shall develop appropriate processes, and procedures to implement the USAP System and Communications-Protection 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 14:22:53 -04'00'