The National Science Foundation
Office of Polar Programs
United States Antarctic Program

Information Resource Management Directive 5000.5
USAP Information Security Architecture

Organizational Function	Information Resource Management	Policy Number	5000.5
		Issue Date	1 August 2004
Policy Category	Information Security Policies and Procedures	Effective Date	1 August 2004
		Updated	24 April 2007
Subject	Information Security Architecture	Authorized By	Director, OPP
Office of Primary Responsibility	National Science Foundation Office of Polar Programs Antarctic Infrastructure & Logistics	Responsible Official	Mr. Patrick D. Smith Technology Development Manager
Address	Suite 755 4201 Wilson Blvd Arlington, VA 22230	Phone	703.292.8032
		Fax	703.292.9080
		Web	www.nsf.gov
Distribution	USAP-Wide	Status	Final Policy
Online Publication	www.usap.gov		

1. PURPOSE

This directive establishes the requirement for an Information Security Architecture (ISA) for information systems supporting the National Science Foundation (NSF) Office of Polar Programs (OPP), United States Antarctic Program (USAP). The ISA will provide the USAP with the standards to implement Information Security principles and practices. The ISA uses standards to align policies and procedures with technologies and tools in support of USAP business processes. The ISA is an integral element of the larger Enterprise Information Architecture.

2. Background

Federal information technology guidance in OMB Circular A-130 requires NSF to establish an Enterprise Information Architecture (EA). An Information Security Architecture that applies industry standards to meet business requirements is an integral component of the EA. NSF OPP has established the USAP Enterprise Architecture as a strategic component of USAP information systems management, and assigned responsibility for the EA to its prime contractor.

3. Guiding Principles

- The Information Security Architecture will be aligned with USAP enterprise objectives for the use and protection of information and information resources integral to USAP business processes.
- The Information Security Architecture will be integrated within the USAP Enterprise Information Architecture, which will establish the framework for information systems development and operation in support of USAP enterprise business processes.
- The Information Security Architecture will adapt industry standards and best practices for information security to USAP science and operations needs.
- The USAP Information Security Architecture will align with the NSF Information Security Architecture where practicable. Variations from the NSF architecture to support USAP mission needs will be coordinated with the NSF CIO

4. POLICY

The USAP Information Security Manager will create and maintain an Information Security Architecture as part of the larger USAP Enterprise Information Architecture.

4.1 Operational Definitions

4.1.1 Information Security Architecture (ISA)

A component of the Enterprise Information Architecture. The ISA provides the structure for implementing enterprise-wide information security. It defines the information security standards to which the enterprise must adhere as the information architecture evolves.

4.1.2 Information System

An information system is any interconnected system or subsystem of equipment used to automatically acquire, store, manipulate, manage, move, control, display, switch, interchange, transmit, or receives information.

4.2 Information Security Architecture

The Information Security Manager will create and maintain an Information Security Architecture that is aligned with, and a component of, the USAP EA, and is based on guidance contained in the NSF Information Security Architecture. The ISA will examine the information security aspects of USAP business processes and the information required to support those processes. The ISA will also examine issues related to the management of sensitive information as categorized using Information Resource Policy 5000.3, *Information Categorization*.

4.3 USAP Information Resources

All USAP information resources will adhere to the standards identified in the USAP Information Security Architecture.

4.4 New Information Systems

New information systems proposed for development or acquisition will incorporate the standards identified in the USAP Information Security Architecture.

4.5 Commercial Off The-Shelf Applications

Commercial off-the-shelf (COTS) applications will be evaluated to assess their compliance with USAP EA standards.

4.6 Legacy USAP Information Systems

Legacy USAP information systems will be evaluated against the standards of the ISA to determine if a variance exists. Based on the evaluation, NSF OPP will determine a course of action to bring the legacy system into compliance with the architecture, or to approve an exception to the architecture for the legacy system until such time that a replacement system can be developed or acquired.

4.7 Non-USAP Systems

Non-USAP systems, as defined in Information Resource Policy 5000.17, *Non-USAP Systems*, must adhere to the guidance of the ISA while they are connected to the USAP information infrastructure.

4.8 Science grant information systems

Information systems employed within a science grant project that are managed by the grant team. These systems are typically procured using NSF grant funds, or funds from the sponsoring institution. For the purposes of the USAP, these systems are typically considered non-USAP systems. Science grant systems will adhere to the USAP Enterprise Information Architecture, unless granted a waiver by NSF OPP.

4.9 Evaluation of USAP Infrastructure

The ISM will work with the USAP IT Architects to assess the current infrastructure and identify issues related to its support of enterprise business processes. This assessment will be conducted every two years, and will integrate existing NSF requirements for annual security assessments.

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 Security Policy 5000.1, *The USAP Information Security Program*.

6. RESPONSIBILITIES

6.1 NSF Polar Research Support Technology Manager

The NSF Polar Research Support Technology Manager orchestrates the development of the Enterprise Information Architecture and the component Information Security Architecture.

6.2 USAP Information Security Manager (ISM)

The USAP Information Security Manager directs the activities related to the development of the Information Security Architecture, and coordinates those activities with the USAP Information Technology Architects.

6.3 USAP Information Technology Architects

The USAP Information Technology Architects ensure information security principles and policies are included at all levels of the USAP Enterprise Information Architecture, and in all information systems deployed in support of USAP mission needs.

7. IMPLEMENTATION

7.1 Information Security Architecture

The ISM will implement this policy by creating and maintaining an Information Security Architecture document, and updating that document, as the business needs change, or every two years.

7.2 Policy Review

The USAP ISM will initiate reviews to this policy as necessary, to strengthen enterprise-wide adherence to established information security principles and practices. Other reasons to review this policy include major changes to the information infrastructure, vulnerability findings during USAP's participation in enterprise-wide security audits, or every two years. The ISM will submit policy changes and new policies for review and approval by NSF OPP.

8. AUTHORITY

This directive is published 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 Manual 7, The NSF Information Security Handbook.

KARL A. ERB

Director