



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

Information Resource Management Directive 5000.4
USAP Information Security Risk Management

Organizational Function	Information Resource Management	Policy Number	5000.4
		Issue Date	1 August 2004
Policy Category	Information Security Policies and Procedures	Effective Date	1 August 2004
		Updated	24 April 2007
Subject	Risk Management	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
Distribution	USAP-Wide	Web	www.nsf.gov
Online Publication	www.usap.gov	Status	Final Policy

1. PURPOSE

This policy establishes the Information Security Risk Management program for information resources supporting the National Science Foundation (NSF) Office of Polar Programs (OPP), United States Antarctic Program (USAP). Risk is the possibility of something adverse happening. Risk Management is the process of reducing risk by identifying, analyzing, controlling, and minimizing losses associated with events to a point acceptable to an organization. From a security perspective, risk is a function of the likelihood of a given threat source exercising a particular potential vulnerability, and the resulting impact of that adverse event on the organization.

2. BACKGROUND

Federal information technology regulations require USAP information resources to undergo an Information Security Risk Management process to identify the risks associated with their operation and to take steps to reduce, and maintain that risk to an acceptable level.

3. GUIDING PRINCIPLES

- Risk Management is integral to the development and operation of information resources.

4. POLICY

The USAP Risk Management process applies to all USAP information resources.

4.1 Operational Definitions

4.1.1 Risk

Risk is the possibility of something adverse happening. From a security perspective, risk is a function of the likelihood of a given threat source exercising a particular potential vulnerability, and the resulting impact of that adverse event on the organization.

4.1.2 Risk Assessment

The technical evaluation of an information system's security features, safeguards, and vulnerabilities that establish the extent to which the system meets requirements to withstand identified threats at specified levels of risk and probability. The process includes quantifying the impact of potential threats, by putting a price or value on the cost of a lost functionality.

4.1.3 Threat

Any circumstance or event with the potential to cause harm to the NSF USAP through the disclosure, modification or destruction of information, or by the denial of critical services.

4.1.4 Vulnerability

The absence or weakness of a safeguard in an information system's security procedures, design, implementation, or internal controls that could be exploited in an unauthorized manner, resulting in a security breach or a violation of security policies.

4.2 Information Security Risk Management

The USAP Information Security Manager (ISM) will establish an Information Security Risk Management process to identify, analyze, control, and minimize the losses associated with identified threats and vulnerabilities. The program will include procedures for performing information security risk assessments to quantify the impact of potential threats and assign values on the cost of a lost functionality.

4.3 Affected Information Systems

All USAP information resources are covered under this policy. The Information Security Manager, in conjunction with all USAP operational locations, will establish and maintain a list of identified threats and potential losses associated with those threats, and implement appropriate risk reduction measures. Using the guidelines in NSF Manual 7, The NSF Information Security Handbook, the list will be updated periodically, or when

major events occur. A copy of this list will be maintained in the contingency plan for each site.

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 InfoSec RM program in an appropriate manner.

4.5 Site Information Security Assessments

To comply with NSF guidance, the ISM will perform annual risk assessments for each USAP operating location.

4.6 New Information Systems

To comply with OMB Circular A-130, all new information systems acquired or developed for NSF OPP to support USAP science or operations requirements will incorporate the NIST Risk Management process in their project and system life cycle planning.

4.7 Commercial Off The-Shelf Applications

Commercial off-the-shelf (COTS) applications will be evaluated to assess the risks associated with their use. The evaluation will use the Common Criteria where applicable.

4.8 Legacy information systems

Older information systems that play critical roles in the accomplishment of USAP science or operations tasks, but that have exceeded their design lives will be assessed to determine the risks associated with their continued operation.

4.9 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. Per direction of OPP, these systems will be assessed to determine the risks associated with their connection to the USAP information infrastructure.

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

Within the NSF and the USAP, several elements have specific responsibilities with respect to the Information Security Risk Management program.

6.1 USAP Information Security Manager

The USAP Information Security Manager (ISM) develops and implements the Information Security Risk Management process, in alignment with guidance from the NSF CIO and NSF Information Security Officer.

6.2 USAP information systems owners

Owners of USAP information systems ensure their systems comply with appropriate federal guidelines for risk assessment and risk management.

7. POLICY IMPLEMENTATION

7.1 Implementation

The USAP ISM will develop appropriate processes, standards, and procedures to implement the USAP Information Security Risk Management Program. USAP organizational elements will document and publish procedures as appropriate to implement specific tasks needed to comply with this policy.

7.2 Policy Review

The USAP Information Security Manager will review this policy in conjunction with major changes to the information infrastructure, as part of the USAP's participation in agency security audits, after each breach in system security, or every two years. The ISM will submit policy changes and new policies for review and approval by NSF OPP

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 Manual 7, The NSF Information Security Handbook.

KARL A. ERB
Director