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

Information Resource Management Directive 5000.01
The USAP Information Security Program

Organizational Function	Information Resource Management	**Policy Number**	5000.01
		Issue Date	1 August 2004
Policy Category	Information Security Policies and Procedures	**Effective Date**	1 August 2004
		Updated	3 May 2012
Subject	Information Security Program	**Authorized By**	Director, OPP
Office of Primary Responsibility	National Science Foundation Office of Polar Programs Polar Research Support Section	**Responsible Officials**	Primary Responsibility: Mr. Patrick D. Smith Technology Development Manager
			Security Responsibility: Ms. Desari Mattox Information Security Manager
Address	Suite 755 4201 Wilson Blvd Arlington, VA 22230	**Phone** **Fax** **Web**	703.292.8588 703.292.9080 www.nsf.gov/od/opp
Distribution	USAP-Wide	**Status**	Final Policy
Online Publication	http://www.usap.gov/technology/contentHandler.cfm?id=1563		

1. PURPOSE

This directive establishes the security policy for information systems supporting the National Science Foundation (NSF) Office of Polar Programs (OPP), United States Antarctic Program (USAP). It establishes the roles and relationships for information security policy managed by OPP for the USAP in relation to agency-wide policy administered by the NSF Chief Information Officer (CIO), and the NSF Office of Information and Resource Management (OIRM). It establishes the foundation for protecting NSF USAP information systems and provides mandatory, minimum requirements for adequate security of information resources.

2. BACKGROUND

The NSF provides executive management of the U.S. national program in Antarctica. The USAP is the expression of U.S. Antarctic policy and provides for the active and influential presence of the U.S. in Antarctica via an active science research program with cooperative international participation. NSF science research grant recipients perform scientific research in a number of scientific disciplines under USAP sponsorship.

The NSF provides logistics, facilities construction, facilities maintenance and operational infrastructure via a combination of third party federal government (both Department of Defense (DoD) and civil agencies) and private sector sources. The NSF contracts most program operations and logistics, including information technology, to a prime contractor who supports the science grantees and supporting agencies. Additional support for operations activities comes from other government agencies, such as the U.S. Air Force, U.S. Navy, U.S. Coast Guard, U.S. Geological Survey, and National Aeronautics and Space Administration (NASA).

Federal government regulations require the NSF to establish an information security program to assure the integrity of USAP information systems. USAP information system integrity ensures the success of the science research mission by providing global communications to facilitate field experiments and exchange of data within the Antarctic region; protects government and private resources used to execute and administer mission activities; and allows effective access to program information by the general public.

3. GUIDING PRINCIPLES

The USAP operates under several basic guiding principles that form the framework for providing information technology and services support to science and program operation activities.

3.1 General

- USAP conduct within the Antarctic region complies with specific U.S. public laws and federal guidance regarding the Antarctic Treaty System.
- The primary expression of U.S. interests in Antarctica is the USAP scientific research program. Mission operational concepts require the USAP science community to have access to USAP resources for the open flow of information necessary for the successful conduct of research activities.
- The safety of participants in the program is a primary concern.
- The national program status of the USAP includes the responsibility to assist the efforts of other U.S. government agencies within the Antarctic operations environment.
- Constraints in USAP resources require an allocation of resources between conflicting priorities. This requires a balance between the needs of science research, protection of life & property, and mission operations.
- The intrinsic nature of USAP program activities, geographic dispersion of program sites, and the Antarctic Treaty System strongly encourage the active and direct participation of foreign nationals in program operations and science research activities.

3.2 Information Resource Management

- The USAP must protect critical resources in the arena of information management. Examples include: satellite communications bandwidth connecting Antarctic research activities to the outside world; sensitive program-related data (e.g., medical, personnel); and the science data collected as a result of grantee research activities.
- The quality of life of program participants contributes to the success of the USAP mission. The USAP actively promotes the quality of life of remotely stationed participants with special provisions for access to communications resources resulting from its role as the sole U.S. infrastructure provider in the Antarctic regions.
- Consistent with international treaties, federal laws and regulations and NSF agency objectives, the USAP utilizes program-related information to educate the general public about the activities and accomplishments of the program, as appropriate.
- Consistent with federal laws and regulations, the USAP must protect an individual's right to privacy with respect to personal information collected or maintained as part of official program activities (e.g., medical data).
- NSF sponsored USAP information systems do not include national security systems. All NSF USAP information systems are unclassified and are not designed to protect national security or classified information.

4. POLICY

The policy of the USAP is to implement information security in a manner that minimizes the impact on science activities while protecting the underlying infrastructure and assuring the continuation of mission operations.

4.1 Infrastructure Protection

The USAP Information Security Program will implement the information security principles, practices and technical measures needed to ensure the USAP information infrastructure remains accessible to all authorized program participants.

4.2 Major Information Systems

In compliance with federal guidelines, the USAP will prepare and maintain an inventory of its major information systems, indicating the system's priority over other USAP systems. All major information systems will be certified and accredited for operation.

4.3 Information Characterization

The USAP will characterize its information using appropriate federal guidelines to define levels of sensitivity and risk exposure within the program. This characterization will guide the program's implementation of information security policies and procedures to protect information of a sensitive or proprietary nature.

4.4 Public Interface

The USAP Information Security Program will implement the information security principles, practices and technical measures needed to facilitate the USAP's public

outreach activities while protecting the infrastructure and ensuring compliance with federal guidelines.

4.5 Foreign National Participation

The USAP mission requires the active involvement of foreign nationals both in the program operations, and in the science activities that form the basis for the program's existence. The USAP Information Security Program will implement the information security principles, practices and technical measures needed to accommodate the participation of authorized foreign nationals. Foreign nationals who use USAP information resources agree to abide by USAP and NSF policies and procedures for the use of information resources.

4.6 No Classified Information Processing

The USAP information systems are not accredited for processing classified information, as defined by E.O 12968.

4.7 Dual-Use Status

A significant portion of USAP program activities take place at remote or isolated locations managed by the U.S. government, where private sector support infrastructure is not available for the personal use of program participants. Consistent with federal guidelines for agency management of agency resources (5 USC 1103(a)(3)), USAP information systems may be used for morale and welfare purposes as deemed appropriate by program management.

4.8 Non-USAP Systems

Program activities may include systems not provided by the USAP. Owners of such third party systems will ensure these systems comply with USAP minimum standards and procedures for infrastructure access prior to connecting the system to the USAP information infrastructure. Once connected, system owners will ensure the systems operate in a manner that complies with USAP rules of behavior. Failure to comply may result in the denial of infrastructure privileges, up to and including removal from the infrastructure.

4.9 Least Privilege

The USAP will apply the principles of least privilege as appropriate to manage access to sensitive information while maintaining support for the free flow of information to support science activities. USAP information systems users will be granted only those privileges and accesses necessary to accomplish their assigned tasks and authorized activities. Each person having access to NSF USAP information systems will be held accountable for their actions on the system.

5. APPLICABILITY AND COMPLIANCE

This policy shall apply 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.

5.1 USAP Operating Environment

For the purposes of this policy, the USAP operating environment consists of the information resources, systems, technology and users that conduct activities at USAP research stations and their associated field locations, aboard USAP research vessels, and at USAP support stations. Activities that involve the exchange of information between resources connected to the USAP infrastructure and resources at locations outside the boundaries of the program, such as at the home facilities of science grantees, may be considered within the scope of this policy.

5.2 USAP Information Users

For the purposes of this policy, a USAP information user is any person or resource that operates, maintains, or uses the information resources or infrastructure of the USAP. This includes, but shall not be limited to all USAP program participants who fall into any of the following categories: U.S. Government employees including military personnel, research grantees, private citizens, contractor and sub-contractor personnel, and foreign nationals.

5.3 USAP Information Infrastructure

For the purposes of this policy, the USAP information infrastructure includes, but may not be limited to, all USAP computing systems, information systems, data repositories, data communications networks, radio communications systems, telecommunications systems, and interfaces between USAP systems and external systems, such as third party data communications networks.

5.4 USAP Information Resources

For the purposes of this policy, a USAP information resource is a resource that supports the operations and assets of the USAP, including those provided or managed by another agency, contractor, or other source Federal Information Security Management Act of 2002 (FISMA). A USAP information resource is typically procured using NSF USAP budget appropriations. This includes all information resources funded or otherwise acquired by NSF budget appropriations for USAP program operations and operational support for scientific research, to include resources provided by contractors. This includes all information resources funded by NSF USAP budget appropriations, but used by other government agencies for support they provide to the USAP. This includes all information resources funded by NSF USAP budget appropriations for use by science grant activities when these resources are connected to the USAP infrastructure.

5.5 Non-USAP Information Resources

This policy shall apply to all information resources categorized as non-USAP systems when these non-USAP systems are connected to the USAP information infrastructure. A non-USAP information resource is a resource obtained using funds outside of NSF USAP budget appropriations.

5.6 Compliance

All NSF USAP information systems managers, operators and users will comply with this directive. Instances where an information system cannot meet the standards or procedures

established under this policy will be managed within the system certification and accreditation process. The provisions of this policy will be made binding as follows:

- **NSF Employees:** employment conduct guidelines as defined and administered by the NSF Office of Information Resource Management.
- **Contractors to the NSF:** terms and conditions for special contract provisions as defined and approved by the NSF Office of Budget, Finance, and Award Management.
- **NSF Grant Recipients:** terms for general and special grant conditions for inclusion in general grant awards as defined and approved by the NSF Office of Budget, Finance, and Award Management.
- **NSF Interagency Agreements:** terms for explicit reference for inclusion in interagency agreements and amendments for existing agreements as defined and approved by the NSF Office of Budget, Finance, and Award Management.
- **USAP Program Participants, not otherwise covered:** formal notification and consent declaration as a component of official USAP deployment processing, as defined and approved by the Director, OPP, NSF.

6. RESPONSIBILITIES

Within the NSF and the USAP, several organizations have responsibilities that directly affect the security of information resources and information systems.

6.1 NSF Director of Polar Programs

The NSF Director of Polar Programs ensures a comprehensive cost-effective security program is in place to protect NSF USAP information systems. As the USAP Certifying Official, the NSF Director of Polar Programs determines the level of acceptable risk associated with system operation and recommends approval for operation of the site or system to the NSF Chief Information Officer (CIO).

6.2 NSF Head of Polar Research Support Section

The Head of the Polar Research Support Section allocates resources for the USAP Information Security program and to remedy security deficiencies to achieve an acceptable level of risk.

6.3 NSF Polar Research Support Section Technology Manager

The NSF Polar Research Support Section Technology Manager directs the development and implementation of the USAP information security program.

6.4 USAP Information Security Manager

This policy establishes the position of USAP Information Security Manager (ISM) to develop and implement the USAP information security program consistent with this policy, and coordinate information security activities with other USAP program office elements, USAP participants, other NSF offices, and other external organizations. The ISM ensures information security activities are included in project plans and budgets as required by federal regulations (Appendix 1). The ISM ensures all proposed security requirements, and designed solutions comport with the USAP Enterprise Architecture. Per NIST Special Publication (SP) 800-37, at the discretion of the Director, OPP, the

ISM position may be held by a staff member from any USAP participant organization, including contractor personnel.

6.5 USAP Information Technology Users

Information technology users within the USAP will use USAP information resources according to this policy and its subsidiary policies, standards and procedures. Users will be held accountable for their actions in employing NSF USAP information systems. Users will protect their data using available safeguards. Users will report any potential security problems to their manager and to the USAP Information Security Manager. Use of any USAP information resource implies consent to this and all other NSF and USAP policies and procedures.

6.6 USAP Information Technology Users (Foreign Nationals)

Within the USAP, some information resource users may be foreign nationals, who are authorized participants of the program, either in its operations, or its science activities. These individuals, while using USAP information resources, will be subject to all applicable USAP policies, processes, standards and procedures governing use of USAP information resources. Their use of any USAP information resource implies consent to this and all other NSF and USAP policies and procedures.

6.7 NSF Chief Information Officer (CIO)

The NSF CIO serves as the NSF Designated Accreditation Authority (DAA) for all NSF information systems, including USAP information systems.

6.8 NSF Information Security Officer (ISO)

The NSF ISO provides oversight of all USAP information security activities, and acts as liaison between NSF OPP, and other NSF elements, and other government agencies.

7. INFORMATION SECURITY PROGRAM IMPLEMENTATION

The USAP ISM will develop appropriate policies, processes, standards, and procedures to implement its information security program. USAP organizational elements will publish procedures as appropriate to implement specific tasks needed to comply with this policy.

7.1 Guiding Standards

The USAP Information Security Program will follow NSF and NIST standards and guidelines as directed by OMB A-130 where practicable. Where appropriate, best security practices from the DoD and other national security elements may be adapted to meet USAP mission needs. In consultation with the NSF CIO, NSF OPP may adapt or modify NSF policies and procedures to meet USAP mission needs.

7.2 Information Security Organization and Administration

The USAP program office will establish an Information Security staff team to coordinate the program's activities in the areas of information security. This team will administer the program elements and maintain appropriate documentation of information security activities.

7.3 Program Information Categorization

The USAP ISM will examine the information processed and categorize that information to determine the types of sensitive data processed, and to identify other categories of information that may require protection.

7.4 Security Risk Management

The USAP ISM will establish a policy defining a process for managing risk.

7.5 Information Security Architecture

The USAP ISM will ensure that information security is embedded within the development of the USAP Enterprise Architecture, in consultation with other members of the USAP organization and the NSF CIO.

7.6 Acceptable Use

The USAP ISM will publish a policy identifying the acceptable uses of USAP information systems, including those uses that fall within the area of morale and general welfare.

7.7 User Access

The USAP ISM will develop procedures and guidelines to provide information resource users with the access they need to accomplish their work, while applying the principle of least privilege.

7.8 Security Auditing

The USAP ISM will coordinate a program to audit infrastructure activities as appropriate, to identify unauthorized users or unauthorized activities and to ensure the infrastructure remains secure.

7.9 Security Training and Awareness

The USAP ISM will establish a security training and awareness program to comply with public law and federal regulations mandating periodic security awareness training for all users of federal information systems. The USAP training program will include provisions to train grantees on USAP information security policies and procedures. The USAP training program will include provisions for pre-deployment training, and for refresher training to be held at the research stations. Individuals who have access to sensitive information will receive additional training that addresses the proper handling of the sensitive information.

7.10 Personnel Security

The USAP ISM will establish codes of behavior commensurate with the level of access accorded each individual. Personnel whose duties include access to sensitive information will be expected to meet higher standards for information access than users whose duties do not include access to sensitive information.

7.11 Physical Security

The USAP ISM will coordinate the implementation of appropriate physical security measures to protect USAP information resources, commensurate with the risk of harm to those resources.

7.12 Security Incident Management

The USAP ISM will establish a program to identify and manage incidents that could interfere with the ability of the infrastructure to support mission operations. The program will include measures to participate in NSF and other federal government Computer Incident Response Team (CIRT) programs for managing security incidents. The program will ensure the proper and rapid response to internal incidents, or to alerts of external incidents as appropriate.

7.13 Contingency and Disaster Planning

Contingency and disaster plans will be developed and tested to ensure that security controls function reliably and that adequate backup and recovery capabilities are in place.

7.14 Software Management and Protection

The USAP ISM will establish a program to properly manage USAP software resources, and to protect against malicious applications, such as viruses.

7.15 Security Configuration Management

The USAP ISM will coordinate with the USAP Prime Contractor IT organization to ensure that configuration controls for USAP information resources exist, so as to preclude inadvertent or malicious modification or destruction of information, and to detect and prevent malicious destruction or modification of information.

7.16 Certification and Accreditation Program

The USAP ISM will establish a program to identify the security risks associated with operation of all USAP major applications and general support systems, certify those systems for operation, and obtain accreditation from NSF CIO for those systems to operate.

7.17 Non-USAP Systems

The USAP ISM will establish a program to evaluate the risks associated with connecting third-party systems to the USAP infrastructure. The USAP ISM will publish guidelines for participants to help them ensure their third party systems meet USAP standards for infrastructure connection.

7.18 Policy Changes, and New Policies

The USAP ISM will modify existing policies and will develop additional policies as needed to address changes to USAP information security requirements, the overall threat environment or the assumptions under which USAP information security policies were developed.

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*.

                              Dr. Kelly Falkner
                                  Director

REVISION/CHANGE RECORD

Pages	Date	Version	Author/Reviewer	Reason for Change
All	6/9/2011	1.0	Matthew Rogers	Verified alignment with NIST Special Publication 800-53 Revision 2. Changed ISM name.
All	5/3/2012	2.0	Alex Jerasa	Updated key contacts and conducted FY12 review

Appendix 1
Authority References

This appendix provides a list and summary description of the major laws and federal regulations that authorize the NSF to establish this policy and the Information Security Program as a whole.

Reference and Title	Description
5 U.S.C. 552a The Privacy Act of 1974	Identifies the need for protecting a system of records that may contain any item, collection, or grouping of information about an individual.
5 U.S.C. § 301	The head of an Executive department may prescribe regulations for the government of his department, the conduct of its employees, the distribution and performance of its business, and the custody, use, and preservation of its records, papers, and property.
40 U.S.C. § 1401 et seq., PL 100-235 The Computer Security Act of 1987	Provides for a computer standards program within the National Bureau of Standards, provides for Government-wide computer security, and provides for the training in security matters of persons who are involved in the management, operation, and use of Federal computer systems.
40 U.S.C. § 1401 et seq., P.L. 104-106, Division E The Clinger-Cohen Act of 1996	Establishes Federal Government responsibilities, planning, and training policy. Defines sensitive data. Requires Federal computer systems to have security and privacy plans for systems containing sensitive information. Also requires periodic mandatory training for personnel involved in the management, operations, and use of systems containing sensitive information.
42 U.S.C. § 1861et seq. National Science Foundation Act of 1950, as amended and extended.	Establishes the National Science Foundation as an independent agency of the Executive Branch of the United States Government [The Director of NSF is authorized to delegate the performance of functions to officers, agencies, or employees of the Agency. General authority allows the Agency to prescribe such rules and regulations as it deems necessary governing the manner of its operations and its organization and personnel.]
44 U.S.C. § 3501 et seq PL 104-013 Paperwork Reduction Act of 1995	Head of Federal Agency is responsible for administrating information resource management and must appoint a CIO as a direct report and who is responsible for Agency; CIO directed to lead an office responsible for implementation of information policies and information resources management; Agency program officials are responsible for information resources assigned and supporting the official's programs
44 U.S.C. § 3501 et seq., P.L. 106-398 Subchapter II – Government Information Security Act	More commonly known as the Government Information Security Reform Act of 2000 (GISRA). Established guidelines for Information Security Management [applies Government-wide]
44 U.S.C. § 3501 et seq.,	Extends and makes permanent the requirements identified

Reference and Title	Description
P.L. 107-347, Title III The Federal Information Security Management Act of 2002 (FISMA)	in the Government Information Security Reform Act of 2000 (GISRA).
P.L. 104-191 The Health Insurance Portability & Accountability Act (HIPAA) of 1996	Identifies the need for protecting the confidentiality and security of individually identifiable health data.
44 U.S.C. § 3504 (g)	Federal Agencies responsibilities relative to Information Technology privacy and security are defined - implement and enforce applicable policies, procedures, standards, and guidelines on privacy, confidentiality, security, disclosure and sharing of information collected or maintained by or for the agency
44 U.S.C. § 3504 (a)(4)	Each Agency program official shall be responsible and accountable for information resources assigned to and supporting the programs under the official and shall define program information needs and develop strategies, systems, and capabilities to meet those needs, in consultation with the CIO and CFO of the Agency
OMB Circular A-123 Management Accountability and Control	Requires management controls to reasonably ensure that resources are used consistent with agency mission; programs and resources are protected from waste, fraud, and mismanagement (including unauthorized use or misappropriation); and reliable and timely information is obtained, maintained, reported and used for decision-making.
OMB Circular A-130, Appendix III Security of Federal Automated Information Resources	Establishes the minimum security program goals.
OMB Circular A-130, Appendix IV, § 8b(3)	Agency program officials must understand the risk to systems under their control, be responsible for determining the acceptable level of risk, ensuring adequate security is maintained to support and assist the programs under their control, ensuring that security controls comport with program needs and appropriately accommodate operational necessities.
OMB Memorandum M-00-07 Incorporating and Funding Security in Information Systems Investments February 28, 2000	Agency program officials must understand the risk to systems under their control and determine the acceptable level of risk, ensure that adequate security is maintained to support and assist the programs under their control, and ensure that security controls comport with program needs and appropriately accommodate operational necessities
Memorandum 6646, Executive Office of the President, February 5, 1982	Reaffirms and continues the responsibility of NSF to budget for and manage the entire United States national program in Antarctica, including logistics support activities
NSF Manual 7, The NSF Information Security Handbook	Establishes policies and procedures for implementation of the NSF Information Security Program
OMB Memorandum M-03-18 Implementation Guidance for the E-Government Act of 2002	Provides agencies with guidance following the enactment of the E-Government Act of 2002 (Public Law 107-347, 44 U.S.C. Ch 36). The E-Government Act includes the

Reference and Title	Description
	Federal Information Security Management Act of 2002 (FISMA)
OMB Memorandum 03-22 26 September 2003 OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002	Provides guidance to agencies on implementing the privacy provisions of the E-Government Act of 2002

Appendix 2
Definitions

This appendix provides operational definitions of common terms, as they apply to the USAP.

Accreditation

A formal declaration by the Designated Approving Authority (DAA) that an information system is approved for operation employing the safeguards documented in the system Certification. The accreditation statement affixes security responsibility with the DAA and shows that due care has been taken for security.

Adequate security

Security commensurate with the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of information.

Assurance

A measure of confidence that the security features and architecture of an information system mediate and enforce the security policy.

Certification

The technical evaluation of an information system's security features and other safeguards which establishes the extent to which the information system meets the security requirements.

Classified information

See E.O. 12958 for the official definition of classified information.

Data Integrity

The state that exists when data is unchanged from its original source.

Designated Approving Authority (DAA)

The official who has the authority to decide whether the security safeguards prescribed for an information system are adequate to mitigate the risk of system operation.

Information

Any knowledge that may be communicated or documentary material, regardless of its physical form or characteristics. Information is any communication or reception of facts, data, or opinions, in any form, including numerical, graphic, or narrative forms, whether oral or maintained in any other medium, including computerized databases, paper, microfilm, or magnetic tape.

Information Custodian

The person or organization assigned the responsibility of protecting information by its owner. The information custodian implements policies and procedures to protect sensitive information. For the USAP, the information custodian is typically the USAP

Prime Contractor, except when USAP participant organizations retain custody of their information and information resources.

Information Owner

The information owner is the executive, manager, or the individual responsible for the information that must be protected. The owner has the final responsibility for protecting their information, and may be liable for negligence because of the failure to protect their information. The information owner identifies the specific information users and their access levels (read, write, and create). The information owner decides which category to apply to their information, and reviews the categorization periodically as business needs change. The term "information owner" does not alter the condition that the National Science Foundation is the final owner of all information found on USAP information resources, even if the information owner is not a government employee.

Information End User

An end user is considered to be anyone that routinely uses USAP information as part of their job. End users have the responsibility to protect information from unauthorized access and disclosure, commensurate with the requirements of the information's category.

Information Security Architecture

A component of the Enterprise Information Architecture that 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.

Information System

The organized collection, processing, transmission, and dissemination of information in accordance with defined procedures, whether automated or manual Is any interconnected system or subsystem of equipment used to automatically acquire, store, manipulate, manage, move, control, display, switch, interchange, transmit, or receives information

Major Information System

As presented in OMB A-130, the term "major information system" means an information system that requires special management attention because of its importance to an agency mission; its high development, operating, or maintenance costs; or its significant role in the administration of agency programs, finances, property, or other resources.

National Security System

As presented in 40 U.S.C. Sec 1452, a national security system is:

  any telecommunications or information system operated by the United States Government, the function, operation, or use of which – 1. involves intelligence activities; 2. involves cryptologic activities related to national security; 3. involves command and control of military forces; involves equipment that is an integral part of a weapon or weapons system; or subject to subsection (b) of this section, is critical to the direct fulfillment of military or intelligence missions. … [This definition] does not include a system that is to be used for routine administrative

and business applications (including payroll, finance, logistics, and personnel management applications). (40 U.S.C. Sec 1452)

Network

A communications medium and all components attached to that medium whose purpose is the transmission of information.

Non-USAP

Term used to refer to resources not procured with USAP funds. Normally includes resources managed by a science team, or personal resources.

Program Organizational Element

An organization of the US government or a private entity that conducts business with, performs a service to, or otherwise is engaged in an activity with the USAP. Includes but is not limited to the NSF program office, other government agencies, the elements of contractor organizations directly engaged in program activities, and universities engaged in long-term research activities within the program's sphere of influence.

Program Participant

An individual of US or foreign nationality who conducts business with, performs a service to, or otherwise is engaged in an activity with the USAP. Includes but is not limited to science grantees working under NSF funding, employees of the prime contractor and its program subcontractors, government employees assigned to tasks supporting USAP mission needs.

Risk

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 (Source: NIST Special Publication 800-12, and 800-30).

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.

Science Grant Information System

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.

Sensitive Information

Information that is not classified, but whose misuse, loss, unauthorized access to, or modification could adversely impact the NSF USAP. This includes data requiring

protection under the Privacy Act, and data not releasable under the Freedom of Information Act.

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.

USAP Information Infrastructure

Includes any information resource, either provided by the government, or provided by the contractor in response to government tasking, used to accomplish USAP mission activities. Information resources procured using NSF grant money, and managed by a science team, are not considered part of the USAP information infrastructure.

Users

People or processes accessing an information system. NSF USAP Users include Government, Grantee, and supporting contractor personnel that use NSF USAP information system resources.

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.