



The National Science Foundation Polar Programs United States Antarctic Program

Information Privacy Program Policy

5000.18

<p>Organizational Function Information Resource Management</p> <p>Policy Category Information Privacy Policy</p> <p>Subject Information Privacy</p> <p>Office of Primary Responsibility National Science Foundation Geosciences Directorate Office of Polar Programs Antarctic Infrastructure and Logistics</p> <p>Address Suite 755 4201 Wilson Blvd Arlington, VA 22230</p> <p>Distribution USAP-Wide</p> <p>Online Publication http://www.usap.gov/technology/contentHandler.cfm?id=1563</p>	<p>Policy Number 5000.18</p> <p>Issue Date 3/21/2017</p> <p>Effective Date 3/21/2017</p> <p>Review On 3/31/2022</p> <p>Authorized By Scott Borg USAP Authorizing Official</p> <p>Responsible Official Mr. Timothy Howard USAP Information Security Manager</p> <p>Phone 703.292.2272</p> <p>Fax 703.292.9080</p> <p>Web http://www.nsf.gov/div/index.jsp?div=PLR</p> <p>Status Final</p>
--	---

Document Release History

Release Number	Release Date	Description of Changes	Changes Made By
1.0	8/8/2016	Initial Release for signature	BAH/ Desari Mattox
1.1	3/21/2017	Minor edits; final signature	NSF/T. Howard

Table of Contents

1	PURPOSE	3
2	BACKGROUND.....	3
3	GUIDING PRINCIPLES.....	3
4	DEFINITION	4
5	POLICY	4
6	ROLES AND RESPONSIBILITIES.....	4
6.1	Chief Privacy Officer (CPO).....	5
6.2	Privacy Act Officer (PAO)	5
6.3	Assistant General Counsel for Privacy	5
6.4	USAP Authorizing Official (AO).....	5
6.5	USAP Information Security Manager (ISM)	5
6.6	Antarctic Support Contract (ASC)	5
6.7	Participating Organizations.....	6
7	SCOPE AND COMPLIANCE	6
8	POLICY IMPLEMENTATION	6
8.1	Implementation	6
8.2	Policy Review.....	6
9	AUTHORITY	6

1 PURPOSE

This directive establishes the information privacy policy for information systems supporting the National Science Foundation (NSF) United States Antarctic Program (USAP) managed by the Office of Polar Programs (OPP).

2 BACKGROUND

The Privacy Act of 1974, 5 U.S.C. § 552a, regulates the collection, maintenance, use and dissemination of personal information by federal executive branch agencies. The purpose of the Privacy Act is to balance the government's need to maintain information about individuals with the rights of individuals to be protected against unwarranted invasions of their privacy stemming from federal agencies' collection, maintenance, use and disclosure of personal information about them.

A system of records is defined by the Privacy Act as "a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual." 5 U.S.C. § 552a (a)(5). Rules exempting systems of records from certain Privacy Act requirements can be found in 28 CFR Part 16, Subpart E. NSF/USAP Privacy Act System of Records can be found at https://www.nsf.gov/policies/privacy_act.jsp

Federal law and Office of Management and Budget (OMB) directives require the establishment of a privacy policy to protect the confidentiality, integrity, and availability of Personally Identifiable Information (PII), and to ensure privacy principles are enforced including transparency, notice, and choice.

Most privacy controls implemented by the USAP privacy program are inherited under the umbrella of the NSF Privacy Program and are documented in NSF Office of Information and Resource Management (OIRM), Division of Information Systems (DIS), *Information Security Handbook Manual 7, Version 10.0*. However, due to the USAP's unique operational environment in the Antarctic region, the NSF has granted OPP permission to tailor the federal privacy & security controls to its operating environment to inform risk-based decision making for OPP information technology operations. The control tailoring ensures appropriate security requirements and security controls are applied to all federal information and information systems. The resulting set of security controls establishes a level of privacy & security due diligence for the Office of Polar Programs¹.

3 GUIDING PRINCIPLES

In developing methods and processes for information privacy, the program shall follow these guiding principles:

- Safeguard the privacy and PII of users through the implementation of privacy controls in conjunction with security controls

¹ Permission for OPP to tailor its own controls is documented in NSF Office of Information and Resource Management (IRM), Division of Information Systems (DIS), *Information Security Handbook Manual 7, Version 10*, section 1.2, April 2016, pg. 2 [https://inside.nsf.gov/tools/toolsdocuments/Inside NSF Documents/Handbook_2016.pdf](https://inside.nsf.gov/tools/toolsdocuments/Inside%20NSF%20Documents/Handbook_2016.pdf), retrieved 25May2016

- Limit the risk exposure of PII by ensuring its collection aligns with the overall USAP mission and operational need
- Store collected PII data in accordance with established federal laws and regulations to avoid inappropriate access, use, and disclosure

4 DEFINITION

Personally Identifiable Information. OMB M-07-16 defines “personally identifiable information” as information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother’s maiden name, etc.

PII examples provided by National Institute of Standards & Technology (NIST) Special Publication (SP) 800-122, *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)* include but are not limited to:

- Name, such as full name, maiden name, mother’s maiden name, or alias;
- Personal identification number, such as social security number (SSN), passport number, driver’s license number, taxpayer identification number, or financial account or credit card number
- Address information, such as street address or email address
- Personal characteristics, including photographic image (especially of face or other identifying characteristic), fingerprints, handwriting, or other biometric data (e.g., retina scan, voice signature, facial geometry)
- Information about an individual that is linked or linkable to one of the above (e.g., date of birth, place of birth, race, religion, weight, activities, geographical indicators, employment information, medical information, education information, financial information)

5 POLICY

It is USAP policy under the auspices of the NSF to protect the confidentiality, integrity and availability of its information systems. The Program shall develop, implement, and maintain an organization-wide governance and privacy program to ensure compliance with all applicable laws and regulations regarding the collection, use, maintenance, sharing, and disposal of sensitive and personally identifiable information (PII) by programs and information systems;

System operators, managers, maintainers and providers of USAP information and communication systems shall implement privacy controls in compliance with the current version of NIST SP 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*.

6 ROLES AND RESPONSIBILITIES

The following roles have specific responsibilities pertaining to information privacy. The sections below describe responsibilities for these roles as they relate to information privacy. Refer to USAP Information Security Policy 5000.01 *The USAP Information Security Program* for the full description of the responsibilities for these roles.

6.1 Chief Privacy Officer (CPO)

The NSF Chief Privacy Officer has overall responsibility and accountability for ensuring the agency's implementation of information privacy protections, including the agency's full compliance with federal laws, regulations, and policies relating to information privacy.

6.2 Privacy Act Officer (PAO)

The NSF Privacy Act Officer resides in the Office of the General Counsel (OGC) and is responsible for compliance with the Privacy Act. The duties of the PAO include:

- Handling requests for disclosures under the Privacy Act
- Maintaining the accounts of systems of records
- Handling requests for correction of records
- Consulting with OGC where questions arise as to the interpretation of the Privacy Act
- Providing information to support the annual Privacy Act report
- Reviewing and advising System Owners on Privacy Impact Assessments

6.3 Assistant General Counsel for Privacy

The Assistant General Counsel for Privacy is responsible for the review and interpretation of privacy law.

6.4 USAP Authorizing Official (AO)

The USAP Authorizing Official is the responsible official for the USAP Privacy Program.

6.5 USAP Information Security Manager (ISM)

The USAP ISM provides oversight of information security and privacy controls supporting the USAP Privacy Program, compliance with this policy and coordinates assessments of privacy controls.

6.6 Antarctic Support Contract (ASC)

The ASC² provides implementation and monitoring of privacy controls. The ASC conducts incident response for privacy events and ensures completion of primary privacy documentation including, but not limited to:

- 1) Security Review Forms (SRFs)
- 2) Information Categorization and Security Assessments (ICSAs)
- 3) Privacy Impact Assessment (PIA)
- 4) Privacy procedural documentation
- 5) Privacy and Incident Response training

² Leidos is the USAP's prime contractor referred to in this document as the ASC. The ASC provides primary contracted information technology and communications (IT&C) operations, maintenance and services delivery management of the NSF-owned/managed IT&C infrastructure supporting the USAP. A contracted requirement of the ASC includes the full compliance of FISMA, NIST, and related NSF information security guidance as promulgated by NSF. The ASC is required to maintain an active and effective information security/assurance capability.

6.7 Participating Organizations

Participating organizations that have the need to access sensitive data in the course of their official duties are responsible for avoiding inappropriate access, use, or disclosure, and, assist with the development of privacy program management procedures and standards. Each participating organization ensures that privacy program management of USAP sensitive/PII data is in alignment with guidance from OPP.

Tenant organizations with systems interconnected to the USAP enterprise network are responsible for securing USAP-controlled sensitive/PII their systems interface with is in alignment with guidance from OPP.

7 SCOPE AND COMPLIANCE

This policy apply to all participating organizations involved in the creation, use, maintenance, and disposal of sensitive information, including personally identifiable information 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*, NIST SP 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*, and USAP Information Security Policy 5000.01, *The USAP Information Security Program*.

8 POLICY IMPLEMENTATION

8.1 Implementation

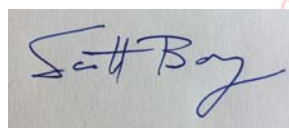
Each USAP participating organization shall develop appropriate processes and procedures as necessary to implement the USAP information privacy program.

8.2 Policy Review

This policy is reviewed in conjunction with major changes to the NSF information privacy program, or every five years.

9 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 Modernization Act of 2014 and NSF Guidance.



Digitally signed by SCOTT G BORG
DN: c=US, o=U.S. Government,
ou=National Science Foundation,
ou=Users, cn=SCOTT G BORG,
serialNumber=NSF0185738055
Date: 2017.03.21 18:57:27 -04'00'

Scott Borg
Authorizing Official
U.S. Antarctic Program