National Science Foundation

MyNSF

Privacy Impact Assessment

January 2024

1. CONTACT INFORMATION

System Owner
David Saunders
External Systems Portfolio Manager OIRM/DIS
(703) 292-4261
dmsaunde@nsf.gov

Project Leader
Peggy Duong
Computer Specialist OIRM/DIS
703-292-4326
pduong@nsf.gov

2. GENERAL SYSTEM INFORMATION

1. **Name of system:** MyNSF

2. **Description of system or electronic collection of information and its purpose.**

   The MyNSF application allows staff to create and manage Panels, Advisory Committees, Committees of Visitors, Site Visits, Sub-committee meetings, and Ad Hoc proposal reviews, create and edit Reviewer Records, check meeting participant availability, manage message subscriptions, view Principal Investigator records, merge duplicate Reviewer and Principal Investigator records, view summary information for pending and approved awards, view institution information, and view and manage Program Officers assigned to a program element.

   MyNSF also integrates with eJacket and iTRAK to allow Grants Specialists to process and approve No Cost Extensions, Other Admin Actions, Post Award Funded actions, New Award actions, and Principal Investigator (PI) Transfers. The approval of award actions within MyNSF triggers the obligation/de-obligation of Federal funds in NSF's financial management system and the creation and modification of award report requirements per NSF's policies and business rules.

   Additionally, MyNSF provides administrative tools for maintaining award information including, but not limited to, close-out of awards, updating clauses, special attention codes, project reports, and PI/co-PI(s).

   MyNSF provides access to most frequently and recently used reports, as well as any custom reports in Enterprise Reporting, which provides NSF staff with access to accurate, well-defined, and reliable data for oversight and reporting on awards and contracts, including commitments, obligations, expenditure information, operating plan information, panels, and post-award actions.

3. **What is the purpose of the system or electronic collection of information?**

   MyNSF provides NSF staff, Program Officers, Administrative Officers, Grants Specialists and Support Staff with a web-based capability to perform many essential business functions related to proposal and award processing. MyNSF captures email address and Institution address for Reviewer Records.

4. **Requested Operational Date?**

   MyNSF became operational in May 2022 in the Amazon Web Services environment.

5. **Does the collection create a new Privacy Act System of Records Notice (SORN), or is the PII collection covered by one or more existing SORNs? If so, name the SORN.**

   Two Privacy Act Systems of Records (SORNs) cover the PII database and the Reviewer database:

   - NSF-50 Principal Investigator/Proposal File and Associated Records
   - NSF-51 Reviewer/Proposal File and Associated Records.
   - NSF-12 Fellowship and Other Awards

6. **What specific legal authorities, arrangements and/or agreements require collection?**

   The legal authorities, arrangements and/or agreements requiring collections are:

   - NSF 17-1: Proposals and Award Policies and Procedures Guide
   - National Science Foundation Act of 1950, as amended (42 USC 1861-75)
   - The Privacy Act of 1974, as Amended, 5 U.S.C.§552 a
   - 20 U.S.C. § 3915; 44 U.S.C § 3101; and 42 U.S.C. § 1869, 1870, 1880, 1881a.
   - Title 5, Chapter III, Part 1320, Controlling Paperwork Burdens on the Public
   - OMB Control Number 3145-0058
   - OMB Control Number 3145-0023

3. PII IN THE SYSTEM

1. **What PII is to be collected, used, disseminated, or maintained in the system or collection?**

   MyNSF provides the capability to create Reviewer Records which include email address and address. The application also displays demographic information entered by the Reviewer in Fastlane or Research.gov. MyNSF also provides the capability to view PI Records.

2. **What are the sources of the PII?**

   NSF Staff create Reviewer Records. Reviewers provide demographic information in Fastlane or Research.gov. External PI Records are created and maintained by PI's in Research.gov. Internal PI Records are created by a limited set of role restricted users in MyNSF to create records for Internally Generated Proposals.

3. **What technologies will be used to collect the PII?**

   MyNSF writes to and displays information from NSF's internal databases.

4. ATTRIBUTES OF THE DATA (USE AND ACCURACY)

1. **Describe the uses of the PII.**

   PII data is used to process NSF proposals. The investigators submit reviews for proposals. NSF keeps a database of reviewers, who can be contacted when NSF program officers want to use a reviewer to review a proposal. The investigators are potential recipients of NSF grants and NSF also keeps contact information on the investigators.

2. **Does the system perform any strictly analytical functions on the PII?**

   The system does not derive new data.

3. **How will the accuracy of the PII collected from individuals or derived by the system be ensured?**

   NSF staff can edit/update reviewer information in MyNSF. As of March 2023, reviewers added to meetings in MyNSF are required to complete a one-time registration process to provide their reviewer profile information in Research.gov. Once a reviewer has a self-managed profile in Research.gov, NSF staff can only update the following reviewer information in MyNSF: email address, reviewer status, and advisory appointment information.

   Data is reviewed by NSF staff. NSF staff can update Reviewer Record information in MyNSF. Reviewer and Principal Investigators records are displayed in MyNSF and can be updated in Research.gov Account Management.

5. SHARING PRACTICES

1. **Describe any sharing of the PII with internal or external organizations.**

   The reviewer information is initially created by NSF staff and may be modified by the reviewer in Research.gov if the reviewer has a self-managed profile. Reviewers who do not have a self-managed account may modify their information under certain circumstances through FastLane. Investigators may register through FastLane and the investigator data is then available in MyNSF. Investigator data may also be data entered in the MyNSF application. This data is also shared with NSF's internal applications including eJacket, Guest, Fastlane and Research.gov. Data is not shared with other agencies.

2. **How is the PII transmitted or disclosed to the internal or external organization?**

   MyNSF resides on the NSF Network – General Support System (GSS), which provides boundary protection and user access, manages application data, and retains audit log files. MyNSF migrated to the NSF Amazon Web Services (AWS) environment, an extension of the NSF Network, in May 2022. The NSF Network (including the NSF AWS environment) is managed by the Division of Information Systems (DIS) Infrastructure Services Branch (ISB).

3. **How is the shared PII secured by external recipients?**

   Data is not shared with other agencies.

6. NOTICE TO INDIVIDUALS TO DECLINE/CONSENT USE

1. **How does the program or collection provide individuals notice prior to the collection of information? If notice is not provided, explain why not.**

   Users receive a system use notification in Research.gov prior to the collection of any information. The information input in Research.gov is displayed in MyNSF.

2. **Do individuals have the opportunity and/or right to decline to provide any or all PII?**

   Yes, individuals can decline PII data in Research.gov.

3. **Do individuals have the right to consent to uses of their PII?**

   Yes, individuals have the right to consent to use of the data.

7. ACCESS TO DATA (ADMINISTRATIVE AND TECHNICAL CONTROLS)

1. **What categories of individuals will have lawful access to the system?**

   NSF administrative and management staff have access to the data with their LAN ID and Password. eJacket and the MyNSF system have access to investigator and reviewer data.

2. **How is permissible access by a user determined? Are procedures documented?**

   - MyNSF uses roles identified and made available via Account and Role Manager (ARM) to implement role restricted functionality.
   - Assigned individuals have access to the data through logon and passwords.
   - Data access is not documented. Systems do document the last person that has updated a given record.

3. **What auditing measures/controls and technical safeguards are in place to prevent exposure or misuse of PII by authorized users, e.g., record browsing, extraction?**

   Merit Review Applications audit records, which includes MyNSF, are reviewed monthly. Any suspicious findings are investigated, reported to appropriate personnel, and action is taken as needed.

4. **Describe privacy training provided users, general or specific, relevant to the program or system?**

   All Intergovernmental Personnel Act (IPA) employees, federal employees, visiting scientists, and contractors must complete annual IT Security and Privacy Awareness Training. IT Security and Privacy Awareness Training discusses such topics as recognizing types for sensitive information that must be protected at NSF (e.g., proprietary , Privacy Act, and confidential financial records); the various Federal laws and guidance that relate to the protection of privacy in individuals and business; and an introduction to NSF's privacy policies (e.g., Information Technology Security and

Privacy Awareness Training Policy, Policy Regarding the Privacy of Sensitive Information, and Policy on Reporting the Breach of Personally Identifiable Information).

5. **Describe the extent to which contractors will have access to the system.**

   NSF contractors who are also System Administrators have access and are required to receive NSF annual IT Security and Privacy Awareness Training and to sign the Rules of Behavior.

6. **Describe the retention period for personal records in the system.**

   Reviewer and investigator data are retained permanently. This data is not archived.

7. **What is the disposition of the personal records at the end of the retention period?**

   N/A

8. SECURITY

Is the PII secured in accordance with FISMA requirements?

NSF Information Security and Privacy Continuous Monitoring (ISCM) activities incorporate compliance with FISMA and ongoing operational security throughout the system's lifecycle. NSF established a continuous monitoring approach that assesses the security state of information systems based on FISMA and NIST security requirements and guidance. Continuous monitoring activities consist of program activities and operational and technical controls (automated and manual) to provide adequate security for NSF systems.

9. PRIVACY ANALYSIS

- The system limits access to only those who have the need.
- Data is reviewed by program officers, their staff and institutions that sponsor investigators that submit proposals.
- Data may be retrieved by querying a variety of data elements. Records for investigators and reviewers have a unique system-generated ID. The data may be retrieved using the unique system identifier or by name.