



National Science Foundation (NSF)

FastLane
Privacy Impact Assessment

Table of Contents

1.	CONTACT INFORMATION.....	1
2.	GENERAL SYSTEM INFORMATION.....	1
3.	DATA IN THE SYSTEM.....	2
4.	ATTRIBUTES OF THE DATA (USE AND ACCURACY)	2
5.	SHARING PRACTICES.....	3
6.	NOTICE TO INDIVIDUALS TO DECLINE/CONSENT USE.....	4
7.	ACCESS TO DATA (ADMINISTRATIVE AND TECHNICAL CONTROLS).....	4
8.	PRIVACY ANALYSIS.....	6

Revisions

Revision Number	Author	Date	Description
Template Update	M. Tillotson	July 2008	Updated the PIA template
2.0	Amde Kifle	4/20/2010	Transferred and updated the PIA to the new template
2.0	A. McCarthy	February 2014	Reviewed for updates – no changes
2.1	A. McCarthy	May 2015	Updated throughout
2.2	A. McCarthy	March 2016	Annual update

Privacy Impact Assessment Form

1. CONTACT INFORMATION

- a. Project Manager/System Owner(s):
- System Owner: **David M. Saunders, Jr.**, External Systems Portfolio Manager, Office of Information and Resource Management, Division of Information Systems, 703-292-4261
 - Project Leader, **William Daus**, FastLane Project Manager, Office of Information and Resource Management, Division of Information Systems, 703-292-5191.

2. GENERAL SYSTEM INFORMATION

- a. Name of System or Electronic Collection of Information:
- FastLane (<http://www.FastLane.nsf.gov>)
- b. Description of System or Electronic Collection of Information:
- FastLane is the National Science Foundation's (NSF) web-based grants management system used by over 250,000 scientists, educators, technology experts and administrators, including the country's top researchers.
 - Designed as a web-based interactive real-time system, FastLane is used to conduct NSF business over the Internet. FastLane covers the full range of transactions between a research organization, its researchers, and NSF.
 - The FastLane system operates in Internal, Public Access, Remote Access, and External Security Domains. These Security Domains define a specific group of users with a set of controlled FastLane objects. Objects include FastLane servers, the FastLane application, the backend database, system routines, support programs, and user class data set access levels (with similar security access enforced by security control policies).
 - FastLane Travel and Reimbursement allows panelists to register for the panel, enter/update personal information, provide social security number (SSN) and enter/update financial institution information for reimbursement or payment. A panelist's financial institution data is required to process panel participation payments and reimbursements. NSF will protect and will not display a panelist's SSN on any materials.
- c. What is the purpose of the System or Electronic Collection of Information?
- To prepare and submit NSF proposals for funding, check on the status of proposals, peer-review budget revisions, post-award notifications and requests.
- d. Requested Operational Date?
- The FastLane is a 'Steady State' system in Operations and Maintenance mode that has been in production since 1997.

- e. Does this collection create a new Privacy Act System or is this information collection covered by an existing Privacy Act System? If so, what is the name of the current Privacy Act System?
 - The FastLane system is covered under the following existing Privacy Act System of Record Notices (SORNs):
 - NSF-12: Fellowships and Other Awards
 - NSF-50: Principal Investigator/Proposal File and Associated Records
 - NSF-51: Reviewer/Proposal File and Associated Records
 - NSF-54: Reviewer/Fellowships and Other Awards File and Associated Records
- f. What specific legal authorities, arrangements, and/or agreements require the collection of this information?
 - [NSF 16-1: 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. DATA IN THE SYSTEM

- a. What PII is to be collected?
 - FastLane processes proposals and awards. As part of this processing, the following PII is collected: name, address, e-mail, and SSN (where necessary for business purposes in FastLane Travel and Reimbursement).
- b. What are the sources of the PII?
 - Information is provided directly from authorized external users (i.e., scientists, educators, technology experts, research administrators, graduate students, and panelists) over the public Internet.
- c. What technologies will be used to collect the data?
 - The FastLane system operates in Internal, Public Access, Remote Access, and External Security Domains as defined by a specific group of users with a set of controlled FastLane information objects. Objects include FastLane servers, the FastLane application, the backend database, system routines, support programs, and user class data set access levels (with similar security access enforced by security control policies).
- d. Does a personal identifier retrieve the data?
 - Yes.

4. ATTRIBUTES OF THE DATA (USE AND ACCURACY)

- a. Describe the uses of the PII:

- FastLane data supports the NSF proposal and award lifecycle.
- b. Does the system analyze data to assist users in identifying previously unknown areas of note, concern or pattern?
- FastLane does not create new data that would allow users to identify previously unknown areas of note, concern or pattern. FastLane is designed to facilitate and automate the proposal development and submission, merit review, and award administration processes.
- c. How will the data collected from individuals or derived by the system be checked for accuracy?
- FastLane is an interactive web-based application that enforces edits and business rules which check for data completeness.

5. SHARING PRACTICES

- a. Will the data be shared with any internal or external organizations?
- Other Federal agencies do not have direct access to, or input data to, FastLane.
 - NSF staff and support contractors have controlled access to the data necessary to review proposals, authorize grants, and monitor compliance with the Proposal and Award Policies and Procedures Guide:
<http://www.nsf.gov/pubs/policydocs/pappguide/nsf16001/>
 - Privileged internal data stored in FastLane databases is only shared with authorized internal and external users. These users include but are not limited to the FastLane system administrators, database administrators, and some members of the NSF operational (i.e., Division of Information Systems) support teams.
 - The External System Branch (ESB) manages FastLane. In addition, the NSF Division of Information Systems (DIS) staff works with various organizations to establish the initial ability to access FastLane. When an institution registers with FastLane, the IT Help Central Team Members review the registration application prior to approving access to FastLane.
- b. How is the PII transmitted or disclosed to the internal or external organization?
- Users have access to only those FastLane functions required to complete their job responsibilities. Principle Investigators (PIs), grantees, research administrators, reviewers, program officers and their designees have specialized access to restricted FastLane functions. Only the FastLane database administrators have access to all of the data in the FastLane database. The FastLane DBAs and Staff are knowledgeable in proper access protocols; Rules of Behavior, and the use of query tools is tracked by monitoring software.
 - FastLane users have access to only those functions they need to conduct their job responsibilities. Specific roles (i.e., Principal Investigators, program officers, etc.) have only the permissions required to complete their FastLane responsibilities
 - Users can retrieve their own data through FastLane only if they are a registered FastLane user. Principal Investigators and Sponsored Research Office officials log into FastLane using their last name, NSF ID, and password.

- c. How is the shared PII secured by external recipients?
 - Authorized FastLane users have the capability to review their information online via a secure web application interface. In addition, they can make corrections and updates online.

6. NOTICE TO INDIVIDUALS TO DECLINE/CONSENT USE

- a. Was notice provided to the different individuals prior to collection of data?
 - FastLane displays a System Use Notification in accordance with NIST guidance. Privacy Act information links are posted for all FastLane access points.
- b. Do individuals have the opportunity and/or right to decline to provide data?
 - Yes.
- c. Do individuals have the right to consent to particular uses of the data?
 - Yes.

7. ACCESS TO DATA (ADMINISTRATIVE AND TECHNICAL CONTROLS)

- a. Is the data secured in accordance with FISMA requirements?
 - FastLane major application data is secured in accordance with FISMA requirements and has an Authorization to Operate.
- b. Which user group(s) will have access to the system?
 - The following users group only have access to the data which they are authorized to use:
 - External publicly facing FastLane users
 - Principal Investigator/Co-Principal Investigator (PI/CO-PI), Other Authorized User
 - Reviewers
 - Panelists
 - Sponsored Program Office (SPO), Authorized Organizational Representatives at Institutions
 - Internal NSF administrators of the grants management process in FastLane
 - NSF OIRM/DIS and IT Help Central authorized users
 - NSF internal Program Officers (POs)
 - NSF Office of the Director
 - NSF Office of General Counsel
- c. How is the access to the data by a user determined? Are procedures documented?
 - Special access to FastLane by internal NSF staff/contractors is determined by an individual's manager/supervisor based on role and business need. The request includes completion, review and approval of the FastLane access form(s). A request to gain access must be documented and communicated to the FastLane Operations and Maintenance team.

- d. How are the actual assignments of roles and rules verified according to the established security and auditing procedures?
- The requestor's manager reviews the roles and access being requested, signs an authorization form accordingly and the appropriate signed forms are submitted. The System Manager reviews and verifies the request. Annual verification confirms the role and if there is still a need for access. System accounts are monitored and updated or disabled as appropriate. Only authenticated users have access to the system, per access control procedures.
- e. What auditing measures/controls and technical safeguards are in place to prevent misuse (e.g., unauthorized browsing) of data?
- FastLane tracks users' access and makes that data available to the management for their review to ensure all FastLane activities are authorized and prevent misuse of the access / data. In addition, user accounts are controlled by the permissions set up in the database for each environment.
- f. Describe the privacy training provided to users, either generally or specifically 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 of sensitive information that must be protected at NSF (e.g., Privacy Act and financial records); the various Federal laws and guidance that relate to the protection of privacy for individuals and sensitive business information; and an introduction to NSF's privacy policies.
 - NSF staff and contractors that access Privacy Act information are required to sign a Rules of Behavior agreement. These agreements explicitly detail the permissible and appropriate access and actions required when working with NSF resources.
- g. Will NSF contractors have access to the system? If so, will they be trained on privacy principles?
- NSF contractors have access to only those FastLane functions required to complete their job responsibilities.
 - NSF contractors that access Privacy Act-protected information are required to sign a Rules of Behavior agreement. These agreements explicitly detail the permissible and appropriate access and actions required when working with NSF resources.
 - NSF contractors are knowledgeable in proper access protocols, the Rules of Behavior agreement and the use of querying tools are tracked by monitoring software.
 - NSF contractors are required to annually complete IT Security and Privacy Awareness training. The training includes segments addressing privacy issues. Promulgated as a mandatory NSF wide policy, individuals that fail to complete this training within the prescribed timeframe automatically have their account and

application access restricted to minimal functionality. Upon successful completion of this training appropriate access is restored.

- h. Has the retention schedule been established by records management? If so, what is the retention period for the data in the system?
 - Grants management records are maintained according to NSF Grant and Control Records Schedule N1-307-88-2 at <http://www.nsf.gov/policies/records/sch882.jsp>.
- i. What are the procedures for identification and disposition of the data at the end of the retention period?
 - NSF transfers electronic records to the National Archives and Records Administration (NARA) three years after close of case files using approved file transfer protocols. Records are disposed of according to NARA retention schedules.

8. PRIVACY ANALYSIS

Given the amount and type of data being collected, discuss what privacy risks were identified and how they were mitigated.

- In order to protect personally identifiable information, NSF eliminated the use of Social Security Numbers (SSNs) in business processes and system, including FastLane, wherever possible. As of September 6, 2008 FastLane users are required to use their NSF ID to access FastLane.