



**National Science Foundation**

Research.gov  
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) ..... 4

5. SHARING PRACTICES..... 4

6. NOTICE TO INDIVIDUALS TO DECLINE/CONSENT USE..... 5

7. ACCESS TO DATA (ADMINISTRATIVE AND TECHNICAL CONTROLS)..... 5

8. PRIVACY ANALYSIS..... 8

## Revisions

<b>Revision Number</b>	<b>Author</b>	<b>Date</b>	<b>Description</b>
Version 1.0	DIS Security Team	September 2012	Draft deliverable
Version 1.1	DIS Security Team	September 2012	Final deliverable
Version 1.2	DIS Security Team	May 2015	Review and update for format consistency
Version 1.3	DIS Security Team	March 2016	Reviewed and updated

## Privacy Impact Assessment Form

### 1. CONTACT INFORMATION

- a. Project Manager/System Owner(s):
- Information Owner: **Martha Rubenstein**, Chief Financial Officer and Director, Office of Budget, Finance, and Award Management (BFA). (703) 292-8200
  - System Owner, **David Saunders**, Research.gov Project Leader, Office of Information and Resource Management, Division of Information Systems, (703) 292-4261.

### 2. GENERAL SYSTEM INFORMATION

- a. Name of System or Electronic Collection of Information:
- Research.gov (<http://www.research.gov>)
- b. Description of System or Electronic Collection of Information:
- Research.gov provides the general public, policymakers, the research community, and internal staff with information about federally funded research and education as well as the policies, guidelines, and procedures that guide it.
- c. What is the purpose of the System or Electronic Collection of Information?
- Research.gov offers a number of services to the public that include:
    - Research Spending & Results. Gives the research community, policy makers, and the general public insight into federally-funded research by providing information about how federal research dollars are being spent, what research is being performed, and how the outcomes are benefiting society. Information is available for NSF and National Aeronautics and Space Administration (NASA) awards with data being updated daily for NSF and monthly for NASA.
    - Media Upload Form: Gives the research community an opportunity to upload media content for NSF use.
  - In addition to the above services available to the general public, Research.gov also offers certain services to existing grantees under NSF assistance programs.
    - Project Reports – Principal Investigators (PIs) can create, edit, and submit projects reports and Sponsored Project Office (SPOs) can view project reports. The four types of reports are annual, interim, final and project outcomes report. Annual project reports are required for all standard and continuing grants and cooperative agreements. Final reports are required for all standard and continuing grants, cooperative agreements and fellowships. Interim project reports are not required and are used to update the progress of a project any time during or before the award period expires. The Project Outcomes Report is a report written for new and

- existing awards, specifically for the public, that provides insight into the outcomes of NSF-funded research.
  - Institution and User Management. Institution administrators with Research.gov accounts may add users and manage their profiles.
  - Proposal Status: Principal Investigators (PIs) check on the status of proposals.
  - Notification and Requests: PIs and SPOS can create and submit notification and requests to communicate changes in scope, time, staff, or budget of an NSF funded project.
  - Award Cash Management Service (ACM\$) – Organizations can submit cash requests and adjustments, access award level information on payments and balances, and expenditure reports.
- d. Requested Operational Date?
  - Research.gov has been in operation since December 17, 2007.
- 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?
  - PII collected and maintained by Research.gov is covered by the Privacy Act system of records titled NSF-72, “Research.gov.”
- f. What specific legal authorities, arrangements, and/or agreements require the collection of this information?
  - The following statutes provide the statutory authority for collection of PII by Research.gov for the services listed in paragraph 2.c. of this PIA:
    - 20 U.S.C. § 3911-3915 are charter statutes for the NSF mission to promote science and engineering education in the United States.
    - 42 U.S.C. § 1861, 1869, 1870, 1880, and 1881 are additional charter statutes for the NSF mission and for certain additional provisions related to scholarships, graduate fellowships, and honorary awards.
    - 44 U.S.C. § 3101 requires each federal agency to make and preserve records containing adequate and proper documentation of the organization, functions, policies, decisions, procedures, and essential transactions of the agency.
    - 7 U.S.C. § 3318 permits NSF to enter into contracts, grants, and cooperative agreements to further the research, extension, or teaching programs in the food and agricultural sciences of the Department of Agriculture

### 3. DATA IN THE SYSTEM

- a. What data is to be collected?
  - Members of the Public: Research.gov only requires the disclosure of an individual’s email address when registering as a member of the public. In addition, the following information may be voluntarily provided by a member of the public when an individual registers a “NSF Visitor” account:
    - Full name

- Job title
  - Company/organization affiliation
  - Street-city-state-ZIP address
  - Congressional district
  - Telephone and fax numbers
  - Email address
- Grantees: The following information about a grantee is stored under his or her “NSF User” Account at Research.gov.
    - Business contact information. The name, title, and business contact information of the grantee and recipient organization.
    - Grant identification information. The federal grant number or other identifying number assigned by a federal agency and recipient account number.
- b. What are the sources of the data?
- All PII described in this PIA is provided by the individual about whom it relates.
- c. What technologies will be used to collect the data?
- Privacy-enhancing technologies employed by Research.gov when the individual is providing or updating, online, his or her PII are as follow:
    - Secure Socket Layer (SSL) protocol protects the security of the information passing between the individual’s web browser and the NSF system. SSL verifies the identity of the individual’s computer and allows a unique and secure connection via randomly generated encryption keys for each online session.
    - Extended Validation (EV) SSL is available to high-security web browsers and next-generation browser versions to confirm for the individual that they are at the legitimate NSF website and not at a "spoofed" site created by fraudsters for purposes of illegally obtaining another’s personal and financial information.
    - 128-bit encryption authenticates that the individual is accessing the NSF website, enables the secure exchange of encryption keys between the individual’s browser and NSF website in order to encrypt the session, and provides integrity control that terminates a session if information changes between the browser and NSF.
- d. Does a personal identifier retrieve the data?
- Yes: Identifiers used to retrieve records of individuals depend upon the kind of individual seeking access.
    - A member of the general public retrieves his or her own record using a username and password.
    - A grantee retrieves his or her own record using the following identifiers: last name, NSFID, and password.

#### 4. ATTRIBUTES OF THE DATA (USE AND ACCURACY)

- a. Describe the uses of the data:
  - Contact information from a member of the public is used to respond to requests for information or services from NSF.
  - A PI's business contact information is used in the event that NSF must contact the PI.
  - 42 U.S.C. § 1862 requires that outcomes of research funded in whole or in part by NSF be reported to the general public.
- b. Does the system analyze data to assist users in identifying previously unknown areas of note, concern or pattern?
  - No analytical functions, related to the uses in paragraph 4.a. or otherwise, are performed on records containing PII without first anonymizing the identifiable information such that a record cannot be linked back to an individual.
- c. How will the data collected from individuals or derived by the system be checked for accuracy?
  - All PII is provided directly by the individual to whom it relates. Once an individual has established an account in Research.gov, he or she may update or correct the information as they desire.

#### 5. SHARING PRACTICES

- a. Will the data be shared with any internal or external organizations?
  - Internal Sharing: Internal disclosure (i.e., within NSF) of PII collected by Research.gov is limited to NSF Office of the Director, Office of General Counsel, Division Directors, Program Officers, Administrative Officers, and their support staff who are authorized and have a need to view the PII in order to perform their official duties.
  - External Sharing: 42 U.S.C. § 1862 requires that outcomes of research funded in whole or in part by NSF be made public. Reports published on the Research.gov website may include the PI's name and business contact information.
    - Privacy Act Disclosures. External sharing under provisions of the Act is done on a case by case basis pursuant to a condition of disclosure at 5 U.S.C. § 552a(b) or a routine use published in a Privacy Act system of records listed in paragraph 2.e. of this PIA, and in accordance with NSF Privacy Act regulations published by NSF at 45 C.F.R. § 612.
    - Freedom of Information Act (FOIA) Disclosures. External sharing under the provisions of the Freedom of Information Act (FOIA) is done on a case by case basis as required by law and NSF Privacy Act regulations in 45 § C.F.R. § 612.

- Computer Matches. No active computer matching agreements (as defined by the Computer Matching and Privacy Protection Act of 1988 wherein NSF is the source agency and the external entity is the recipient) exist for the PII described in this PIA.
- b. How is the data transmitted or disclosed to the internal or external organization?
  - The means of disclosure to other external organizations or persons permitted under the authority of the Privacy Act or FOIA will depend on the circumstances of the records request presented to NSF.
- c. How is the shared data secured by external recipients?
  - Disclosures under the authority of the Privacy Act are considered on a case-by-case basis, and most relate to a records request from another Executive Branch agency. In such cases, the requesting agency is obligated to protect the information under information security requirements established by the Federal Information Security Modernization Act (FISMA).

## **6. NOTICE TO INDIVIDUALS TO DECLINE/CONSENT USE**

- a. Was notice provided to the different individuals prior to collection of data?
  - Notice prior to collection of PII is accomplished by several means as required by federal statute:
    - For information collected by NSF, notice is provided in the Federal Register in the form of a new or amended Paperwork Reduction Act information collection request.
    - Privacy Act system of records notices are published in the Federal Register, as required by the Privacy Act at 5 U.S.C. § 552a(e)(4).
    - Website privacy policies are located at the points of PII collection at Research.gov. These policies comply with the notice required by the Privacy Act at 5 U.S.C. § 552a(e)(3) and by Section 208(c) of the E-Government Act.
    - This PIA, published on the NSF public website, satisfies the notice requirement of Section 208(b) of the E-Government Act of 2002.
- b. Do individuals have the opportunity and/or right to decline to provide data?
  - Members of the public have the right to decline to provide any PII when registering a “NSF Visitor” account in Research.gov.
  - Grantee PII is necessary and essential to Research.gov functions.
- c. Do individuals have the right to consent to particular uses of the data?
  - Research.gov does not provide options to individuals to limit uses of their PII.

## **7. ACCESS TO DATA (ADMINISTRATIVE AND TECHNICAL CONTROLS)**

- a. Is the data secured in accordance with FISMA requirements?
  - Research.gov 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 user groups only have access to the data that they are authorized to use:
    - External publicly facing Research.gov users
      - Principal Investigator/Co-Principal Investigator (PI/Co-PI)
      - Reviewers
      - Panelists
      - Sponsored Program Office (SPO)
    - Internal NSF administrators of the grants management process in Research.gov
      - Financial Function authorized user
      - Other DIS/IT Help Central authorized users
      - NSF internal Program Officers (POs)
  - In addition to members of the public and grantees registered at Research.gov, certain organizational persons have authorized access to the PII. The scope of this access is as follows:
    - Members of the public and grantees may gain access to functions available under their “NSF Visitor” or “NSF User” account, respectively.
    - Internal NSF staff members have access to applicant or participant PII for management of proposals, grants, fellowships, or honorary awards as part of their official duties.
    - NSF employees and contractors, who support the information technology underlying Research.gov and who are authorized representatives of the information owner, may have incidental access to PII in the course of carrying out their official duties.
    - Some NSF staff may gain access using special user accounts that carry with them elevated privileges greater than what is held by regular internal NSF staff for the purpose of carrying out their official duties.
- c. How is the access to the data by a user determined? Are procedures documented?
- Access to Research.gov services by a member of the public or a grantee is controlled by their registration credential, e.g., password. Policies and procedures for the assignment of organizational persons to non-privileged roles are promulgated by the information owner. Authorized representatives of the information owner, who may have elevated privileges, oversee role assignment using established procedures.

- d. How are the actual assignments of roles and rules verified according to the established security and auditing procedures?
- For requesting administrative privilege access to Research.gov, a NSF user fills out the Administrative Privilege access form. Users must sign Rules of Behavior after completing the annual security and privacy awareness training that addresses appropriate use and protection of sensitive information.
- e. What auditing measures/controls and technical safeguards are in place to prevent misuse (e.g., unauthorized browsing) of data?
- Specific software events are audited that document the access and use of Research.gov. The events are recorded in system logs to permit the detection and/or prevention of unauthorized access or inappropriate usage. The logging of a specific event may be turned on or off, or otherwise adjusted, depending on revised threat assessments or system performance and cost considerations.
- 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-protected information are required to sign a Rules of Behavior agreement. This agreement explicitly details the permissible and appropriate access and actions required when working with NSF resources.
  - Privacy training does not apply to members of the public or grantees who may use Research.gov. The public and grantees can only access private information about their own records.
  - NSF employees and contractors with access to PII: As a precondition for receiving an NSF network user account, each NSF employee and contractor must:
    - Complete (and retake annually) a computer security and privacy awareness course. The course satisfies the requirements of Federal statutes and government-wide policies, in particular the provision at 5 U.S.C. 552(e)(9) to establish rules of conduct for persons involved in the design, development, operation, or maintenance of information covered by a Privacy Act system of records.
    - Sign the NSF standard Rules of Behavior governing the terms of use of protected information and government-provided information technology.

- NSF employees with remote access to PII while working under an approved telecommuting agreement are required to acknowledge and agree to additional conditions for protection of the PII that may arise from the work arrangement.
- g. Will NSF contractors have access to the system? If so, will they be trained on privacy principles?
  - Contractors are required to complete NSF Security and Privacy Awareness training and must sign the NSF rules of behavior to access Research.gov
- 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 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.

- NSF operates Research.gov in accordance with security procedures required by federal law and policy to ensure that information is appropriately secured. NSF has conducted a risk assessment, identified appropriate security controls to protect against identified risk, and implemented those controls. NSF performs monitoring, testing, and evaluation of controls on a regular basis to ensure controls continue to work properly.