National Science Foundation

Privacy Impact Assessment

for the

Research.gov System

April 2024

Updated October 2024

1. CONTACT INFORMATION

<Enter the name of the system owner, title, the name of the directorate or division and the system owner's telephone number.>

System Owner
Name: David Saunders
Title: Research.gov Project Leader, Office of Information Resource Management (OIRM), Division of Information Systems (DIS)
Directorate/Division: OIRM/DIS
Telephone Number: (703) 292-4261
dmsaunde@nsf.gov

Point of Contact
Stephanie Yee
Division of Information Systems (DIS)
703 292-7495
syee@nsf.gov

2. GENERAL SYSTEM INFORMATION

1. Name of collection or system: Research.gov (https://www.research.gov/)

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

<Write a brief paragraph about the system or collection that conforms to the following format. The first sentence describes the system or collection and its function in plain English (leave out details about the underlying technology). The second sentence states whether the system or collection is for internal purposes or serves the public. The third sentence explains the reason the system or collection is being created. Relate the reason to the program or NSF's mission.>

Research.gov provides grants management for the research community. Currently, grantee services include Account Management, Award Cash Management Service (ACM$), Notification and Requests, Password Management, Research.gov Proposal Preparation and Submission, Project Reports, Proposal Status, supplemental funding requests, the Graduate Research Fellowship Program (GRPF), and Public Access. The site is also available to the public for exploring products in the NSF Public Access Repository system.

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

<Provide a concise, general description of the project or system using non-technical language. Clarify whether the system or collection is for internal NSF purposes or whether the system or collection provides a service to the public. Describe the purpose(s) for which the records are collected. Generally, the purpose should be apparent in a statute or an executive order or can be

reasonably inferred from it as a necessity to administer an agency program. If System of Records Notice (SORN) exists, the purpose should parallel what's in the SORN.>

In addition to the above services available to the public, Research.gov also offers certain services to existing grantees under NSF assistance programs. Excluding the Graduate Research Fellowship Program (GRFP) since it is covered under their own PIA.

- Proposal Preparation and Submission - Research.gov supports preparation and submission of all submission types (letters of intent, preliminary proposals, and full proposals) as well as all proposal types referenced in the PAPPG.

- Supplemental Funding Request Preparation and Submission - Research.gov supports preparation and submission of post-award supplemental funding requests.

- 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.

- Account Registration and Management: External users of Research.gov create log-in credentials and basic user information for account recovery. NSF Account Registration and Management system also provides a way to request and assign various system roles that are needed to access various functions within the grants management systems. For example, a user with a PI role has access to the Proposal Submission functions.

- Proposal Status: Principal Investigators (PIs) check 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.

- Public Access – PIs can access the NSF Public repository (NSF-PAR) to submit their peer-reviewed, journal articles, conference papers, conference proceedings, and datasets associated with their NSF Award.

- Graduate Research Fellowship Program (GRFP) - The GRFP module and supporting systems allow for:

- Applicants apply to the GRFP through an online application available in the application module. Applicants can complete, review, and check the status of their application through this module. The annual application period opens in late July each year and closes in mid-October.
- Reference Writers to submit letters of reference for GRFP Applicants through the Reference Letter Submission (RLS) module in Research.gov. All reference letters must be submitted to NSF by the annual deadline in late October.
- Reviewers evaluate assigned applications online based on NSF's merit review criteria of Intellectual Merit and Broader Impacts. Review panels are conducted virtually each year in January.
- GRFP Fellows to manage their Fellowship Status and report the progress of their graduate studies via an annual activity report online in the Fellows module. GRFP Fellowships are awarded annually in early April and new Fellows must accept their award and declare their Fellowship Status by the deadline in late April. Current Fellows must submit their Annual Activity Report and declare their Fellowship Status by the same deadline.
- GRFP Officials to manage the activities of Fellows at their institution. Officials approve change requests in Fellowship Status and field of study as well as organization transfers through the GRFP Officials module. GRFP Officials are required to submit Completion and Program Expense Reports for current Fellows at their institutions each Fall. Officials certify progress and submit Grants Roster Reports for all Fellows at their institutions each Spring.

- Individual Banking - Research.gov also offers services to people who require direct payment from NSF, such as invitational speakers or Intergovernmental Personnels Act Assignments (IPAs) under the module called "Individual Banking".

4. Requested Operational Date?

   <Provide the estimated planned date when the system will begin operation or when the collection of PII begins.>

   Research.gov has been in operation since December 17, 2007.

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.

   <It is unlikely that a new system or collection would trigger writing a new SORN. It is more likely that a new or modified collection or system would require amending and republishing an existing SORN. As a reminder, a SORN is triggered by the collection of information that is retrieved by a personal identifier, e.g. name or Social Security number.>

   PII collected and maintained by Research.gov is covered by the Privacy Act system of record notices (SORNs):

- NSF-72: Research.gov
- NSF-76: Account Registration and Management
- NSF-65: for Individual Banking
- NSF-12: Fellowships and Other Awards
- NSF-50: Principal Investigator/Proposal File and Associated Records
- NSF-54: Reviewer/Fellowships and Other Awards File and Associated Records.

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

<List the full legal authority for operating the system, specifically the authority or executive order that authorizes collection and maintenance of the PII. Provide the authorities in a manner that is understandable to any potential reader. In other words, do not simply provide a legal citation; use statue names or regulations in addition to citations.>

The following statutes provide the statutory authority for collection of PII by Research.gov:

- 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 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. PII IN THE SYSTEM

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

<Identify and list all information in identifiable form that is collected and stored in the system or collection. The information could include, but is not limited to, date of birth, Social Security number, passport number, or other unique identifying number or characteristic. Justification for sensitive identifiers, such as full birth date and Social Security number, is always required.>

Fellowship and Award information PII is covered under SORN NSF-12: Fellowships and Other Awards and SORN 54: Reviewer/Fellowships and Other Awards File and Associated Records.

Principal Investigator/Proposal File and Associated records are covered under SORN NSF-50: Principal Investigator/Proposal file and Associated Records.

Individual banking collects the following information however it is not saved in the research.gov database and is transferred to iTRAK which has its own SORN NSF-65: NSF Electronic Payment File.

2. What are the sources of the PII?

<List the individual, entity or entities providing the PII. For example, is the information collected directly from an individual as part of an application, or is it collected from other sources, such as a data aggregator. Describe why information from sources other than the individual is required.>

All PII described in this PIA is provided by the individual to whom it relates.

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

<Because of the nature of NSF's mission, it is unlikely technologies beyond paper-based inputs, online data entry or web-interfacing methods are used to collect PII. The question is intended to explain the role of other technologies that might raise novel privacy vulnerabilities. For example, technologies involving physical access control, position sensing (e.g., GPS) and biometric capture might be suspected of leading to surreptitious monitoring of individuals. The PIA should give assurances that such vulnerabilities are addressed.>

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.

4. ATTRIBUTES OF THE DATA (USE AND ACCURACY)

Describe the uses of the PII.

<Identify and list each use, both internal and external to NSF, of the information collected or maintained, including each major programmatic activity supported by the system. In the grants area, for example, uses might be "to receive a proposal," "to schedule a panel," or "to generate

a grant funding commitment." "Purpose" and "use" are different, however. Each use must be compatible with the purpose and statutory authority established for the system.

When nonproduction use of PII is justified based on evaluation of cost and/or feasibility, the nature of the use, the justification, and any compensating safeguards, such as methods for obscuring the data, should be documented in the PIA. Examples of nonproduction uses include supporting software development or testing, regular training of new system users, research purposes or assisting visualization in meetings.[1]

1.

- 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 if 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 public.

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

<Some systems sift through large amounts of information in response to a user inquiry or programmed functions, raising concerns about limits on use, drawing inaccurate conclusions about an individual, or reaching unfair adverse determinations about eligibility for a right, benefit, or privilege provided by government. PII captured in tracking cookies for web measurement and customization is a common example.

Describe any analytical functions. If the system or collection stores the new information about an individual, explain what its uses are. Describe whether new information is made part of the individual's existing record or a separate record is created. Describe measures, such as obscuring data, to reduce privacy vulnerabilities from these analyses.>

No, the system does not analyze data to assist users in identifying previously unknown areas of note, concern, or pattern. The system does help users and NSF staff identify cases of duplicate accounts being created for the same individual. These system checks are being enhanced to support NSF's policy that prohibits users from having more than one NSF ID. There are no additional analytics being introduced.

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

<Describe the process used to check the accuracy of information an individual provides, or if there are any online or administrative means to correct the individual's record. Typically, an individual provides information, and NSF relies on the individual to provide accurate information at the time the information was provided.>

[1] Vulnerability when data is applied to nonproduction uses is explained in NIST Special Publications 800-53, Appendix J, and NIST 800-122.

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

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

   <Internal sharing means with any organizational element within NSF. For internal sharing, don't elaborate office by office on usual and ordinary purposes that should already be documented as uses. If PII is shared internally for other reasons, document the nature of the sharing. For example, if a copy of the entire database is provided periodically to a strategic planning office for its enterprise data warehouse, explain that sharing.>

   - 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 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.

2. How is the PII 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.

   <Describe how the information is transmitted to each program office, contractor-supported IT system, and other organization or IT system. For example, is the information transmitted

electronically, by paper, or by some other means? Is the information shared in bulk, on a case-by-case basis, or does the sharing partner have direct access to the information?>

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.

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

<Identify and list the names of any federal, state, or local government agency or private sector organization with which information is shared. List who is responsible for assuring the security and privacy of the data once it is shared; and if possible, include a reference to and quotation from any Memorandum of Understanding, contract or other agreement that defines the parameters of the sharing agreement. Where there is a specific authority to share the information, provide a citation to the authority and statute name. State what specific information is shared with each specific partner.>

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

The following questions address actions taken to provide notice to individuals of their right to consent/ decline to collection and use of information (other than required or authorized uses) and how individuals can grant consent.

<In many cases, agencies provide written or oral notice before they collect information from individuals. That notice may include a posted privacy notice, a Privacy Act statement on forms, a PIA, or a SORN published in the Federal Register. Describe what notice was provided to the individuals whose information is collected by the system or collection.

Provide information on any notice provided on forms or on websites associated with the collection or system. Describe how the notice provided for the collection of information is adequate to inform those impacted.>

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

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.

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

   <Describe whether individuals can decline to provide information, and whether there are any consequences if they decline to provide information. Consequences might include, for example, limiting their access to certain services or disqualifying them from eligibility for a privilege or legal benefit. When individuals are required to grant consent for NSF to use their information, explain how individuals would grant consent, e.g., checking a box to opt-in.>

   Grantee PII is necessary and essential to Research.gov functions.

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

   <The question is directed at whether an individual may provide consent for specific uses or the consent is given to cover all uses of their information. If specific consent is required, how would the individual consent to each use? For example, is the system or collection designed to permit opt-in or opt-out consent?>

   Research.gov does not provide options for individuals to limit uses of their PII.

7. ACCESS TO DATA (ADMINISTRATIVE AND TECHNICAL CONTROLS)

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

   <Describe the categories of individuals who can access the system. More than one category may exist. For example, reviewers of grant proposals may access the system to create or update their NSF account. An employee might access a reviewer's profile to assign the individual to a panel.>

   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
     - Meeting Participants
     - Sponsored Program Office (SPO)
     - Authorized Organizational Representative (AOR)
     - Administrators
     - Graduate Research Fellowship Program (GRFP) Coordinating Official (CO)
     - Graduate Research Fellowship Program (GRFP) Financial Official (CO)

  - Other Authorized users (OAU)
  - Invitational Travelers
  - Intergovernmental Personnel Act (IPAs) Assignments

- Internal NSF administrators of the grants management process in Research.gov
  - Financial Function authorized user
    Other DIS/IT Service Desk authorized users
- In addition to members of the public and grantees registered at Research.gov, certain organizational persons have authorized access to the PII within downstream applications inside NSF. The scope of this access is as follows:
  - Members of the public and grantees may gain access to functions available under their "NSF User" account, respectively.
  - Internal NSF staff members have access to applicant or participant PII for NSF 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 while 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.

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

   <Describe the means to limit the use of application functions or services, or access to electronic records, by authorized users. Common methods involve administrative policies on separation of duties or software-defined user roles that implement least privilege.>

   Access to Research.gov services for members of the public or grantees is managed through a one-time enrollment in an available Multifactor Authentication (MFA) option. After enrolling, users sign in to Research.gov using their selected MFA option.

   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.

   For requesting administrative privilege access to Research.gov, an 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.

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?

<Describe what events bearing on access and usage are logged by the application to permit detection of suspicious or abnormal user activity or to compile evidence of such activity.

Auditable events may relate to any of the following:

- User-initiated actions, such as successful log-on or session termination
- Authorization actions, such as the software permitting access by a user to an application function or a record.
- Actions taken by users with elevated privileges, such as starting, stopping or deleting an audit log.
- Describe the overall process of assessing and reporting activity within the system. Aspects of the process include the frequency of review of audit logs, parties involved in application log analytics and the policy for escalating findings to management.>

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.

NSF logs login activities, including successful and failed attempts. There are controls in place that lock the user account for a period after five unsuccessful login attempts. User sessions are terminated once the user logs off or if the session maximum time is reached. System administrative actions like starting and stopping of servers by the admins are logged.

In addition, reCAPTCHA is implemented to mitigate any BOT processing. Also, as part of the API calls, NSF provides the roles used to access different functionalities within Research.gov. Only users with assigned roles can get different functionality within Research.gov.

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

<Training is a requirement of the Privacy Act, FISMA and numerous OMB policies. Training can be interpreted in a PIA to include all the following safeguards:

- User access agreement
- Rules of behavior (agency-wide rules and/or tailored application rules)
- System warning banner
- Annual privacy awareness training>

- 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, particularly 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.

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

   <Describe contractor access to the PII in terms of their roles and responsibilities. Will contractors have regular user duties equivalent to government users? Will contractors have duties requiring elevated privileges? Describe the necessity of the access provided to contractors to the system and whether clearance is required>.

   NSF contractors have access to only those Research.gov functions required to complete their job responsibilities.

   - NSF contractors are knowledgeable in proper access protocols, Rules of Behavior and the use of querying tools are tracked by monitoring software.

   - NSF contractors are required to annually complete the NSF Rules of Behavior for Access to IT Resources

   - Including Sensitive Information, Non-public and Personally Identifiable Information (PII)

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

<The retention periods of data/records that NSF manages are contained in the control schedules maintained by the NSF records management office. The control schedules are for the most common records NSF creates and maintains. Therefore, "maintained indefinitely" is not an acceptable answer. If the data is subject to the Privacy Act, the answer should agree with the "Retention and Disposal" section of the System of Records Notice (SORN).>

Grants management records must be maintained according to NARA's General Records Schedule (GRS) 1.2, Grant and Cooperative Agreement Records.

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

<Describe the circumstances under which the records are retired to a federal records center and/or destroyed. If the data is subject to the Privacy Act, the answer should also agree with the "Retention and Disposal" section of the SORN.>

The Records Management Staff (RMS) will be working to strike/remove Item 14 (as well as other items) from N1-301-88-2, an outdated schedule that required eJacket data to be permanent. It conflicts with NSF and NARA's agreement to utilize GRS1.2, referenced above, which states that grant and cooperative agreement records are temporary records. Please review the specific Item numbers in GRS 1.2 – column: *Disposition Instructions*.

8. SECURITY

Is the PII secured in accordance with FISMA requirements?

<State whether there is an Authority to Operate (ATO) for the system. NSF systems comply with FISMA requirements for Authority to Operate. Note that all NSF systems and collections containing PII are categorized as "moderate" under the Federal Information Processing Standards Publication 199, Standards for Security Categorization of Federal Information and Information Systems.>

PII in Research.gov is secured in accordance with FISMA requirements. Research.gov was issued an ongoing authority to operate as part of the Merit Review Applications on May 8, 2020. The Merit Review Applications have a FIPS 199 security categorization of Moderate and are continuously monitored as described in the NSF Information Security Continuous Monitoring Program.

9. PRIVACY ANALYSIS

<Describe any potential threats to privacy as a result of NSF's use or extraction of PII. Examine potential threats to privacy using the CIA (confidentially, integrity and availability) triad.

For example,

- The confidentiality of PII can be compromised by individuals with elevated privileges. State that NSF requires individuals with elevated privileges to sign a Rules of Behavior document, or name access controls to prevent the unauthorized download of PII data.

- Other examples include mandatory training about how individuals with elevated privileges handle, retain or dispose of PII data.
- Encrypting PII and/or secure-handling procedures are other options to consider when identifying ways to protect PII from unintentional exposure.
- Regularly review and analyze information system audit records.

- Review whether data loss prevention tools and access controls are in place.>

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.