National Science Foundation

iTRAK
Privacy Impact Assessment

TABLE OF CONTENTS

REVISIONS

Revision Number	Author	Date	Description
Version 1.0	B. Bartel	September 24, 2013	Original Document
Version 1.1	A. McCarthy	April 29, 2016	Review and update
Version 1.2	A. McCarthy	March 20, 2017	Review and update
Version 1.3	G. Pritchard	February 4, 2020	Review and Update

1. Contact Information

a. Project Manager/Information Owner

The information owner is the official with statutory or operational authority for specified information (including personally identifiable information, or “PII”) and the responsibility for establishing the controls for its generation, collection, processing, dissemination, and disposal.[1] The Chief Financial Officer, Office Head, Office of Budget, Finance, and Award Management (BFA) is the owner for PII acquired and maintained about individuals in iTRAK. The Office Head, BFA, is the information owner for iTRAK.

b. System Owner

The system owner is the individual accountable to the information owner for the development, procurement, integration, modification, operation, maintenance, and final disposition of an information technology (IT) system. The system owner for iTRAK is the Branch Chief, BFA, Division of Financial Management, Financial System Branch and the business owner is the Branch Chief, BFA, Division of Financial Management, Accounting Operations Branch.

2. General System Information

a. Name of System or Electronic Collection of Information:

iTRAK

b. Description of System or Electronic Collection of Information:

This PIA encompasses the privacy implications of a cloud-based, core financial management system to be utilized by NSF. iTRAK is an integrated financial management solution with robust reporting capabilities to support the management of financial transactions.

This PIA is prepared because iTRAK collects, maintains, and disseminates PII about employees, contractors/vendors, research proposal reviewers, and recipients of NSF

[1] Definitions of “information owner” and “system owner” are from the “National Information Assurance Glossary” published by the Committee on National Security Systems (CNSS) as Instruction No. 4009 (April 26, 2010) and adopted by the National Institute of Standards and Technology.

federal assistance programs[2]. This PIA ensures compliance with the statute requiring that the agency publish a PIA on the agency's website when it describes an information collection of PII from or about ten or more members of the public.

c. What is the purpose of the System or Electronic Collection of Information?

iTRAK is a core financial management system used to record and process all NSF financial transactions. The system's primary functions include processing:

- payroll and payroll-related transactions for NSF employees;
- travel reimbursements and other personnel payments for NSF employees, research proposal reviewers, and recipients of NSF federal assistance programs;
- payments for contractors and vendors providing goods and services to the Foundation; and
- collections of debts owed to the Foundation. iTRAK is also used to generate statistical and financial transaction reports required for reporting to the Department of the Treasury and Office of Management and Budget (OMB) as well as *ad hoc* reports for internal and management functions. Figure 1 below provides brief descriptions of critical iTRAK functions.

Function	Description
General Ledger	• Performs the financial closing process and financial statement generation in the core financial system to improve financial integrity and audit compliance
Funds Management	• Provides funds control caps across multiple budget/spending levels beyond just appropriation and obligation • Supports continuing resolution capabilities within iTRAK • Allows funds control structure and amounts to be maintained by financial users without intervention from the IT staff
Payment Management	• Enables multiple disbursement files to be sent daily to Treasury • Includes Treasury edits that will eliminate rejections of the disbursement file and the associated re-processing
Receivable Management	• Provides receivable management and collection monitoring capabilities inside the core financial system • Provides automated follow-up capabilities, either event-driven or date-driven, such as dunning letters and follow-up letters
Cost Management	• Allocates costs in the General Ledger based on a variety of allocation methods

[2] NSF federal assistance programs include research grants, graduate research fellowships, and honorary awards.

Function	Description
	• Enables the performance of project cost allocations and overhead recovery through labor burdening or application of cost rates on other direct costs
Reimbursable Management	• Supports establishment of Inter-Agency Agreements (IAA) for incoming IAAs, including automated process in establishment of funding authority • Provides automatic IPAC[3] interface and IPAC processing inside the core financial system, eliminating current manual processes
Funds Balance with Treasury	• Provides expanded payment confirmation capabilities as well as support for automated disbursement-in-transit accounting
Federally Mandated Reporting	• Generates federal reporting directly from the core financial system • Changes to Treasury and OMB requirements are incorporated into the commercial off-the-shelf product and included in new software releases
Operational Reporting	• Provides capability for user-directed report execution and distribution • Provides ad hoc operational reporting, including reporting based on user-driven parameters
Technical Capability	• Enables open/close periods by sub ledger • Provides automated validations at each closing, which leads to a faster and smoother year-end closing
System Management	• Eliminates user's reliance on knowing "transaction codes" • Adheres to Federal CGAC and Standard General Ledger

Figure 1. Critical iTRAK Functionality

d. Requested Operational Date?

iTRAK went into operation on October 14, 2014.

e. Does this collection create a new Privacy Act system of records or is this PII collection covered by one or more existing systems of records? If so, what is the name of the current system of records?

PII collected and maintained by iTRAK is compiled under the following existing Privacy Act systems of records:

- NSF-10, "Employee's Payroll Jacket"
- NSF-13, "Fellowship Payroll"

[3] IPAC is the acronym for Treasury's Intra-Governmental Payment and Collection system.

- NSF-22, “NSF Payroll System”
- NSF-53, “Public Transportation Subsidy Program”
- NSF-57, “Delinquent Debtors File”
- NSF-65, “NSF Electronic Payment File”
- GSA/GOVT-3, “Travel Charge Card Program”
- GSA/GOVT-4, “Contracted Travel Services Program”

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

- 20 U.S.C. 3911-3922 are the charter statutes for the NSF mission to promote science and engineering education in the United States.
- 31 U.S.C. 3511, 3512, and 3523 are statutes requiring federal agencies to establish and maintain systems of accounting and internal controls to provide complete financial disclosure, adequate financial information the agency needs for management purposes, and effective control over and accountability for assets for which the agency is responsible, including audits.
- 31 U.S.C. 3332 is the statute requiring that all federal wage, salary, and retirement payments, vendor and expense reimbursement payments (including grants), and benefits payments shall be paid to recipients by electronic fund transfer to a financial institution.
- 26 CFR 301.6109-1 regulates the use of taxpayer identifying numbers, i.e., Social Security Number (SSN) or Employer Identification Number (EIN), to identify individuals to the Internal Revenue Service (IRS) in all records related to taxable events.
- 5 U.S.C. Chapter 57 contains the statutes governing travel, transportation, subsistence expenses, and allowances.

3. PII in the System

a. What PII is to be collected?

The following categories of PII are collected by iTRAK:

Employee payroll data. Employee's names, addresses, SSNs, salary data, health benefit data, and retirement data are collected for performance of employee payroll services.

Business registration data. The IRS EIN and Data Universal Numbering System (DUNS) number are collected to identify it for payment and tax purposes. iTRAK collects business data for recipients of NSF federal assistance programs as well as vendors offering goods or services to the Foundation.

Personal financial data. An individual's SSN is collected only when required to complete a financial reimbursement to the individual, e.g., payment of a fellowship stipend, a travel expense payment to a proposal reviewer, or a payment to a sole proprietor in exchange for a service offered to the Foundation. An individual's bank account type (e.g., checking or savings), bank routing number, and bank account number are collected to accomplish direct deposits of financial reimbursements.

b. What are the sources of the PII?

iTRAK processes information originating in electronic records collected directly by NSF's federal assistance, human resources, and financial management systems.

iTRAK also processes information transmitted to it from the following external systems:

- Concur. A government-wide travel management system owned by the Government Services Administration (GSA) that is used by federal employees to manage travel authorizations, vouchers and expenditures.
- Department of the Treasury, Financial Management Service, IPAC. A bureau providing a suite of government-wide accounting and reporting services. IPAC provides iTRAK with payment information for payments received from other government agencies.
- Department of the Interior, Interior Business Center (DOI/IBC), Federal Personnel Payroll System (FPPS). DOI/IBC FPPS transmits payroll cost and personnel information to iTRAK and WebTA.
- System for Award Management (SAM) Database. Business-related information about contractors/vendors may be gathered from SAM. SAM is a GSA-owned

system that tracks data on all contractors who do business with the federal government. In the future state, SAM is expected to provide information for both vendors and grantees.

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

This question does not apply to iTRAK because it does not collect PII directly from individuals. PII is received from other systems via direct, automated system connections. No human intervention or manual or offline processes are involved in the movement of electronic records from the source systems to iTRAK that might contribute to an elevated risk of exposure of the PII to those not authorized to have it.

d. What personal identifier or identifiers are used to retrieve an individual's record?

- Employees. NSF-assigned employee numbers are used to retrieve records.
- Grantees and Vendors. DUNS Numbers are used to retrieve records.
- Individuals/Sole Proprietors. SSNs are used to retrieve records.

4. Attributes of the Data (Use and Accuracy)

a. Describe the uses of the PII.

iTRAK uses PII for the processing of financial transactions in support of the purposes stated in section 2.c. iTRAK reporting functions will focus on aggregate data and will not include PII.

b. Does iTRAK perform any strictly analytical functions on the PII?

No analytical functions are performed on PII by iTRAK.

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

iTRAK reads, processes, and reports information originating in electronic records collected directly by NSF's federal assistance, human resource, and financial management systems. Because of its reliance on these systems for its source data, iTRAK depends on the data quality and accuracy controls of the authoritative source systems.

5. Sharing Practices

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

Internal Sharing. Internal disclosure (i.e., within NSF) of PII collected by iTRAK is limited to authorized representatives of the information owner who have a need to access the PII to perform their official duties.

External Sharing. Some iTRAK information may be shared outside NSF to fulfill the purposes described in paragraph 2.c.

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

All PII transmitted to internal or external organizations is transmitted using secure automated system connections. iTRAK employs all safeguards in compliance with the requirements of the Federal Risk and Authorization Management Program (FedRAMP) initiation process.

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

Information may be shared with other federal agencies to fulfill the purposes described in paragraph 2.c. These agencies are 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 their PII?

Notice prior to collection of PII is provided by the several means required by federal statute. These means of notice are as follow:

- For NSF assistance programs, notice is provided in the *Federal Register* in the form of new or amended Paperwork Reduction Act information collection requests.

- Notice of the Privacy Act systems of records listed in paragraph 2.e. of this PIA is published in the *Federal Register*. These constitute notice required by the Privacy Act at 5 U.S.C. 552a (e) (4) of the character and existence of records.
- Website privacy policies are located at the points of collection at NSF websites used by employees or the public. These policies constitute 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, when published on the NSF public website, satisfies the notice requirement of Section 208 (b) of the E-Government Act.

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

This question does not apply directly to iTRAK because the system does not collect PII directly from individuals. At the time of collection, individuals may decline to provide information. However, failure to provide the information may result in the denial or refusal of a benefit and ultimately the failed processing of a financial transaction (e.g., payment, reimbursement, etc.).

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

This question does not apply directly to iTRAK because the system does not collect PII directly from individuals. Due to the nature of the Foundation’s business, PII may be required to process financial transactions. For this reason, individuals that wish to conduct business with the Foundation do not have the ability or right to consent to particular uses of their PII.

7. Access to Data (Administrative and Technical Controls)

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

Access is limited to those who are authorized and have a need to access the system based on their roles in support of the purposes described in paragraph 2.c.

NSF organizational personnel (employees and contractors) who support the technology infrastructure underlying iTRAK and who are authorized representatives of the information owner may have incidental access to PII in the course of carrying out their official duties. Cloud service provider (CSP) personnel may also have access to perform tasks relative to the cloud platform. Some IT support staff may gain access using separate accounts that carry with them administrative (elevated) privileges greater than what is held by most internal users.

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

Authentication is the mechanism whereby a system establishes confidence in an electronic identity presented to it. Authentication answers the questions, who is the user and is the user really who he or she represents himself or herself to be. Authorization is the mechanism whereby the system determines what actions an authenticated identity is entitled to perform in the system.

The IT Help Central function issues network authentication credentials for regular users. Access to the system by a regular NSF user is subsequently controlled by his or her NSF network authentication credential.

Some gain access using administrative accounts that carry elevated privileges above what is held by regular NSF network users. Administrative accounts are subject to a separate approval process requiring the approval of the information owner and Director, Division of Information Systems. The process requires the staff member to acknowledge and sign a "Sensitive PII Rules of Behavior" governing the use of their administrative account. In addition, the CSP issues credentials to perform tasks necessary to iTRAK such as maintenance of the overall cloud platform. Adequacy of the CSP's policy for authentication credentials is reviewed as part of the FedRAMP process.

Authentication of NSF Users inside NSF Premises. Authentication to iTRAK is a byproduct of authentication to the NSF network when the user is on NSF premises. NSF users are issued an NSF network user account as part of their onboarding as an employee or contractor. Local authentication to the network is accomplished with the assigned network user ID and a twelve-character strong password established by the user. Employees (and most contractors) are also issued a Homeland Security Presidential Directive 12 (HSPD-12) Personal Identity Verification (PIV) card.

Contractors who do not require frequent entry to NSF offices may or may not be issued a PIV card at the discretion of the government.

NSF is using PIV cards for logical access to satisfy the requirement of OMB Memo M-11-11[4] for agencies to use the PIV credential as the common means of authentication for access to agency facilities, networks, and information systems. A USB-connected PIV card reader attached to the workstation is used to read the card and match a stored value with the PIN input by the user through the keyboard. The advantage of PIV card authentication is that it represents two-factor authentication, that is, the card is something the user has, and the PIN is something the user knows.

Remote Authentication of NSF Users. Remote authentication means authentication to iTRAK from outside NSF offices (e.g., telecommuting arrangements, on travel). A one-time password-generating hard crypto-token, issued to the individual by NSF, is required for authentication. The NSF network user ID, user password, and the one-time password value from the hard token are combined to remotely authenticate the user to the NSF network. iTRAK may then be accessed using the user's NSF username and password.

Authorization. Upon establishment of a user's account in iTRAK, organizational personnel authorized and having a need to access the system to perform their official duties are assigned to roles in iTRAK based on the principles of separation of duties and least privilege. Thereafter the assigned roles regulate which functions a user may perform and which records, or parts thereof, they may view or modify. A representative of the system owner maintains role assignments, including establishing new users and removing the authorizations of those who depart.

c. What auditing measures/controls and technical safeguards are in place to prevent misuse of PII (e.g., unauthorized browsing or records extraction)?

The iTRAK User Provisioning team performs access level audits annually during recertification. The events are recorded in system logs to permit the detection and/or

[4] OMB Memo M-11-11, "Continued Implementation of Homeland Security Presidential Directive 12 Policy for a Common Identification Standard for Federal Employees and Contractors" (February 3, 2011).

prevention of unauthorized access or inappropriate usage. Access level audits may include:

- Log in/log off and anomalies
- Users with administrative access at database, application, or server levels
- Database access and manipulation activity
- Queries made around PII data
- Elevated permission levels

d. Describe privacy training provided to users relevant to the system.

As a precondition for receiving an NSF network user account, each 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 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 iTRAK while working under an approved telecommuting agreement are required to acknowledge and agree to additional conditions for protection of NSF records that may arise from the work arrangement.

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

Contractors do not have a direct role in the use of iTRAK for the purposes described in paragraph 2.c. Contractors have background roles in supporting the technology infrastructures underlying iTRAK. These roles include computer security tasks and software, database, and communications design, development, and maintenance.

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

Electronic records compiled by the authoritative source systems that feed iTRAK are retained in accordance with published NSF record disposition instructions. Retention of the information may be necessary in order to apply any additional expenditure, make corrections to payments and account balances as appropriate, and for reporting and auditing purposes. Retention periods may vary greatly from system to system.

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

Electronic records compiled by the authoritative source systems that feed iTRAK are disposed of in accordance with published NSF record disposition instructions. The disposition may vary greatly from system to system.

8. Security

Is the PII secured in accordance with FISMA requirements?

NSF has established a comprehensive IT Security Program utilizing a risk-based, layered approach with continuous monitoring. Risk is assessed, understood, and mitigated based on government-wide guidance and industry best practices. Additionally, iTRAK will comply with FedRAMP requirements.

9. Privacy Analysis

This part of the PIA provides a summary recommendation about conformance to the eight Fair Information Practice Principles adopted by the federal government[5].

Transparency. Organizations should be transparent and provide notice to the individual regarding collection, use, dissemination, and maintenance of PII.

[5] Principles described in this PIA are incorporated in “Best Practices: Elements of a Federal Privacy Program” (Version 1.0), sponsored by the Federal CIO Council (June 2010), in NIST Special Publication 800-122, “Guide to Protecting the Confidentiality of PII” (April 2010), and in other government-wide references.

iTRAK achieves this FIPP through the applicable Privacy Act notices published by NSF in the *Federal Register* (and referenced in this PIA) and through publishing this PIA on the NSF website.

Individual Participation. Organizations should involve the individual in the process of using PII and, to the extent practicable, seek individual consent for the collection, use, dissemination, and maintenance of PII. Organizations should also provide mechanisms for appropriate access, correction, and redress regarding use of PII.

iTRAK achieves this FIPP through a combination of means:

- All PII processed by iTRAK is transmitted through automated system links with several source systems. The data is entered in these source systems directly by the individuals.
- Individuals may amend their personal information in the source systems if they believe it is incorrect or outdated. The information will subsequently be amended in iTRAK.
- Record notification, access, and contesting procedures are published in each of the Privacy Act systems of records referenced in this PIA. In addition, regulations published at 45 CFR 613 provide guidance on requests for disclosure of records under the provisions of the Privacy Act and FOIA.

Purpose Specification. Organizations should specifically articulate the authority that permits the collection of PII and specifically articulate the purpose or purposes for which the PII is intended.

iTRAK achieves this FIPP by providing public notice of the authority for, and purposes of, the PII in a publicly posted PIA and in the Privacy Act systems of records referenced in this PIA.

Data Minimization. Organizations should only collect PII that is necessary to accomplish the specified purposes and only retain PII as long as is necessary to fulfill the specified purposes.

iTRAK achieves this FIPP by limiting collection of PII to that which is necessary to process financial transactions in support of the NSF mission. Nevertheless, the PII is subject to the Privacy Act, which creates a specific legal duty to minimize collection; and any PII breach has the potential to create a threat to agency reputation and to extract costs from response efforts.

The following additional circumstances factor into threat of harm from exposure:

- Paper forms are not used, which eliminates widespread handling or viewing of those facts by internal NSF staff. A quarter of data breaches disclosed publicly are from loss of paper records.[6] Paperless modes reduce breach risk.
- Manual processes are replaced with automated processes that will reduce the handling and/or viewing of records by NSF staff.
- Neither full date of birth, nor any part thereof, is collected. The statute defining means of identification for commission of true-name identity theft or financial account takeover indicates presence of the full birth date greatly magnifies potential risk from exposure of a record that includes a person's full name and their SSN.[7]

<u>Use Limitation</u>. Organizations should use PII solely for the purpose(s) specified in the notice. Sharing PII should be for a purpose compatible with the purpose for which the PII was collected.

iTRAK achieves this FIPP through a combination of means:

- The principle of least privilege. Access is assigned to individuals based on his or her authentication credential and by the roles assigned them by the system owner.
- The requirement for organizational persons to sign the NSF Rules of Behavior and complete (and retake annually) a computer security and privacy awareness course.

<u>Data Quality and Integrity</u>. Organizations should ensure, to the extent practicable, that PII is accurate and timely.

iTRAK achieves this FIPP through a combination of means:

[6] Finding from a 2009 report of the Identity Theft Resource Center (*www.idtheftcenter.org*).

[7] The Strategic Plan of the President's Identity Theft Task Force (April 23, 2007), available at *www.idtheft.gov*, discusses the risk from exposure of a combination of personal identifiers.

- Nearly all PII is submitted by the applicant through source systems and is then transmitted to iTRAK via automated system links.
- Individuals are able to access and update their information through source systems and it will subsequently be updated in iTRAK.

Security. Organizations should protect PII (in all media) through appropriate security safeguards against risks such as loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure.

NSF has established a program of continuous monitoring of the effectiveness of system security plans and security control implementations, in accordance with FISMA statutory requirements and National Institute of Standards and Technology (NIST) standards and guidelines. In addition, iTRAK will be compliant with all requirements for FedRAMP initiation.

Accountability and Auditing. Organizations should train all employees and contractors who access and/or use PII, and audit the actual use of PII to demonstrate compliance with these principles and all applicable privacy protection requirements.

iTRAK achieves this FIPP through the following means:

- Periodic awareness training for each NSF employee and contractor about the required methods and practices for protection of PII.
- Acknowledgment of a Rules of Behavior as a condition for establishing a user account for each NSF employee and contractor.
- System Use Notification displayed on the splash page.
- Regular user account management and role-based assignment of privileges.
- Logging of application events necessary for the detection or prevention of unauthorized access to or inappropriate usage of PII.