National Science Foundation

Financial Accounting System (FAS)
Privacy Impact Assessment

Date: November 29, 2007
Version: 1.1

Table of Contents

Revisions

Revision Number	Author	Date	Description
Version 1.1	F. Wenger	9-26-07	Update from the original document dated 2005.
Version 1.1	M Tillotson	11-29-07	Edits based on DFM, G. Holden review

1. BACKGROUND

The Privacy Impact Assessment (PIA) is a vehicle to address privacy issues in information systems. The PIA template establishes requirements for addressing privacy during the information systems development process; it defines and documents the privacy issues a project must address and outline; and serves as part of the Certification and Accreditation (C&A) process for a NSF General Support System (GSS) or a Major Application (MA).

1.1 Organizational Background

The NSF Financial Accounting System (FAS) is a major application and is managed by two NSF organizations as follows:

- The financial responsibilities are in the Office of Budget, Finance, and Award Management (BFA), Division of Financial Management (DFM), Financial Systems Branch (FSB).
- The FAS application development and maintenance responsibility resides in the Office of Information & Resource Management (OIRM), Division of Information Systems (DIS), Administrative Systems Branch (ASB).

2. SCOPE

Protecting an individual's right to privacy is predicated on various Federal laws, directives, and standards; the overarching Federal laws being the Privacy Act of 1974 and the more recent E-Government Act of 2002. Federal guidance requires that, where possible, the PIA process is integrated into the GSS/MA life cycle. Therefore, this PIA is base-lined using instruction from NIST SP 800-64, *Security Considerations in the Information System Development Life Cycle* and other Federal guidance.

3. ENVIRONMENT

The FAS business operations are conducted across NSF's Local Area Network (LAN) and Wide Area Network (WAN), referred to as NSF's Network. The NSF Network is a General Support System (GSS); the NSF Network includes servers that utilize the Windows operating systems in a network of interconnected domain controllers and file servers, operating in a distributed client/server environment.

The FAS is NSF's primary system for allocating and managing funds. The FAS provides the full spectrum of financial transaction functionality for a federal agency. FAS presents accounting data, and related forms and functions using the Multiple Document Interface (MDI) interface, which allows all FAS windows to be presented as a sheet within an application frame window. A main window, known as an MDI frame, is where all system activity occurs. If the MDI frame is closed, the application and any open window in the application are also closed.

4. PRIVACY IMPACT ASSESSMENT CRITERIA

The following sections contain the appropriate questions that are used to collect the required GSS/MA information. The NSF Privacy Act Officer and other reviewing officials will analyze the results to ensure that an individual's personal identifiable information is adequately secure. The completed PIA will be forwarded to the appropriate individuals for review.

4.1 Data in the System

The sources of the system information are an important privacy consideration. The information becomes especially important if the data is gathered from other than NSF records. Information collected from non-NSF sources is verified, to the extent practicable, for accuracy, that the information is current, and the information is complete. Accurate information is important if the information will be used to make determinations about individuals.

Privacy Criteria	Descriptive Response
1. Provide a general description of the information type (i.e., persons name, SSN, etc.) to be collected or processed by the GSS or MA.	The FAS contains all information necessary to administratively support the mission of the Foundation. Specifically, it contains data required to monitor funding and produce financial reports and support FISCAM requirements. Within the FAS, only personal data about NSF employees necessary to facilitate payment of funds due them for legitimately reimbursable travel costs, miscellaneous expenses incurred (form 1164) and any taxable moving expenses is kept. The FAS keeps only the information necessary to liquidate legitimate obligations incurred and to where applicable produce the required tax forms at year-end (i.e. Form 1099M). The information consists of the tax id number (either EIN or SSN), name, address, and banking information.
2. What are the sources of the information in the system? (*Note: This is an important privacy consideration if the data is gathered from other than NSF records).*	The majority of the information in FAS comes from internal NSF award processing. The information is either key-stroked directly by a staff member or is passed by another internal NSF mission system to support that systems functionality. DOI through OPM's Employee Express gathers name, address, SSN and banking information. The data is then transmitted to the NSF using secure FTP. Other Federal agencies provide standard pieces of information (none of it personal) such as the funding codes to be used by NSF.
3. What NSF files and databases are used?	Data from the NSF proposal, awards, and training databases contribute to the data that is kept in the system.
4. What other Federal Agencies, if any, are providing data for use in the system?	US Congress, OMB, Dept. of the Treasury's Financial Management System, GSA, Dept. of the Interior, and the IRS. The FAS system has direct data transfer interface connections to external entities; the Federal Reserve Bank (FRB) of

Privacy Criteria	Descriptive Response
	Richmond.
5. From what other third party sources will data be collected?	The PNC Bank and NSF Grantee institutions.
6. What information will be collected from the employee?	The employee's address and banking are collected from Employee Express (OPM) and transferred to DOI, which then transfers the information to NSF.
7. If data is collected from sources other than NSF records, how is it being verified for accuracy? *(Note: This is especially important if the information will be used to make determinations about individuals).*	NSF has a trusted relationship with OMB, DOI, Dept. of the Treasury, and GSA. As Federal agencies, they have a responsibility in assuring that the data provided to NSF is accurate and current. Furthermore, NSF analyzes and reconciles general ledger balances on a monthly basis.
8. How will data be checked for completeness?	When any data is transferred into the system, the system enforces a variety of edits and business rules to assure that all necessary pieces of information are present before it processes the data.
9. Is the data current? How do you know? What mechanisms were used to validate the data's currency?	All data from feeder systems are processed on a real time basis. Furthermore, NSF analyzes and reconciles general ledger balances on a monthly basis.
10. What data elements are described? What level of detail is used in documenting data elements?	The FAS Data Dictionary contains a list of all data columns used by the system.
11. If data elements are documented, what is the name of the document?	The FAS Data Dictionary

4.2 Access to the Data

Who has access to the data in a system must be defined and documented. Users of the data can be individuals, other systems, and other agencies. Individuals who have access to the data can be system users, system administrators, system owners, managers, and developers. When individuals are granted access to a system, their access should be limited, where possible, to only that data needed to perform their assigned duties. If individuals are granted access to all of the data in a system, procedures need to be in place to deter and detect browsing and unauthorized access. Other systems are any programs or projects that interface with the system and have access to the data.

Privacy Criteria	Descriptive Response
1. Who has access to the data in the system? (Note: Users of the data can be individuals, other systems, programs, projects, or other agencies. Individuals who have access to the data can be system users, system administrators, system owners, managers, and developers).	The NSF Division of Financial Management (DFM) determines who will have access to the Financial Accounting System (FAS) with regard to persons that have permissions to read, write, or delete financial data. Only DFM staff can provide the access to the various update processes. Personnel outside of DFM must provide either an email or written request, with approval/knowledge of the office head before DFM will process the access request. There is a segregation of duties edit within the UPM that prohibits the assignment of the disbursing job class and any job class that allows the update or input of banking information. DFM staff regularly produces and reviews reports on user capability. System developers, project leaders, and NSF database administrators have access to some or all of the data in these systems.
2. Where individuals are granted access to all of the data in a system, what procedures are in place to deter and detect browsing and unauthorized access?	Individuals who need to examine FAS data but are not authorized to modify are granted browse access only. Other users, with a need-to-know receive insert, delete, or update capability based on DFM-controlled permissions via the User Profile System (UPM). Whenever a row of data changes in FAS, the system records the last user, program, and date of change to that row. Access is further limited by entries in the UPM system. Persons with access to Personally Identifiable Information (PII) are required to sign a Sensitive Information Rules of Behavior (ROB).
3. When individuals are granted access to a system, how is their access being limited, where possible, to only that data needed to perform their assigned duties?	Individuals are granted access through the User Profile Maintenance (UPM) System. The UPM controls access to each NSF system through giving each individual specific access to only the data they need to access to complete their job. Each systems proponent or system manager assigns access.
4. How or what tools are used to determine a user's data access?	Only DFM staff can provide the access to the various update processes. Personnel outside of DFM must provide either an email or written request, with approval/knowledge of the office head before DFM will process the request. In addition, there is a segregation of duties edit within the UPM that prohibits the assignment of the disbursing job class and any job class that allows

Privacy Criteria	Descriptive Response
	the update or input of banking information. DFM staff regularly produces and reviews reports on user capability.
5. Describe the criteria, the procedures, the controls, and the responsibilities in place regarding the manner in which data access is documented.	Personnel outside of DFM must provide either an email or written request, with approval/knowledge of the office head before DFM will process the request. Access to all the data on the system is limited to the type of user accessing the system. This is documented in the security plan for the system. Individuals who need to examine FAS data but are not authorized to modify are granted browse access only. Other users receive insert, delete, or update capability based on DFM-controlled permissions via the User Profile System. When a row of data changes in FAS, the system records the last user, program, and date of change to that row. Access is further limited by entries in the UPM system.
6. Do other systems share data or have access to data in this system? If yes, explain.	FAS has incorporated interfaces with Guest Travel and Reimbursement System; the Central Contractor Registration (CCR) system; e-Travel; e-Training (Learning Management System); and e-Procurement (Automated Acquisition Management System) systems. The FAS Identification and Authentication (I&A) is done between Integrated Time and Attendance System (ITAS) and FAS. An interface with UPM is required to determine an individual's specific permissions to FAS data.
7. Who has the responsibility for protecting the privacy rights of the individuals affected by any system interface?	The DFM and the program office using the interfacing system are responsible for protecting the rights of the individuals affected by the interface. DFM coordinates very closely with DIS and the Office of General Counsel on all privacy issues related to the system. With the FAS, the on-line interfaces have no bearing on individuals.
8. Will other agencies share data or have access to data in this system?	NSF sends 1099 data to the IRS. All data sent to other Federal agencies from the system are required under various laws, etc. and allow those agencies to accomplish their missions.
9. How will the NSF use this data?	NSF makes Electronic Funds Transfer (EFT) and check payments to vendors, employees, and

Privacy Criteria	Descriptive Response
	grantees through the daily check and EFT file transmissions to the Dept. of the Treasury's Financial Management System. NSF's payroll functions are serviced by the Federal Personnel/Payroll System (FPPS) which is maintained by DOI/NBC.
10. Who is responsible for assuring proper use of the data?	Each Federal agency that receives data from NSF is responsible for insuring the proper security controls are in place to protect the data. Each NSF new employee and contractor reads and signs a copy of the NSF Rules of Behavior; this document outlines those data security rules that have been implemented for protecting NSF data. In addition, those persons that can read SSNs are required to read and sign the Sensitive Information Rules of Behavior.
11. How will the system ensure that agencies only get the information they are entitled to?	NSF's programs identify datasets through a specific filename. The FAS software code identifies those filenames that are transmitted to external business partners. Other NSF systems that interface with FAS also use filenames to identify datasets that are shared internally.

4.3 Attributes of the Data

When requirements for the data to be used in the system are being determined, those requirements must include the privacy attributes of the data. The privacy attributes are derived from the legal requirements imposed by the Privacy Act of 1974. First, the data must be *relevant and necessary* to accomplish the purpose of the system. Second, the data must be *complete, accurate and timely*. It is important to ensure the data has these privacy attributes in order to assure fairness to the individual in making decisions based on the data.

Privacy Criteria	Descriptive Response
1. Explain how the use of the data is both relevant and necessary to the purpose for which the system is being designed?	The FAS is the NSF's primary system for managing funds allocated to the NSF. The FAS provides the full spectrum of financial transaction functionality for a federal agency. FAS presents accounting data, and related forms and functions.
2. Will the system derive new data or create previously unavailable data about an individual through aggregation for the information collected?	The FAS does not aggregate or create new data about individuals. The FAS provides NSF's financial data and interface data for other l functions.

Privacy Criteria	Descriptive Response
3. Will the new data be placed in the individual's record?	The FAS does not create new data.
4. Can the system make determinations that would not be possible without the new data?	No. The systems that provide input into FAS does not create new data that would make it possible to allow determinations to be made.
5. How will the new data be verified for relevance and accuracy?	Since FAS does not create new data. This question is not applicable.
6. If data is being consolidated, what controls are in place to protect the data from unauthorized access or use?	The FAS data is not consolidated. Therefore, this question is not applicable.
7. If processes are being consolidated, are the proper controls remaining in place to protect the data and prevent unauthorized access? Explain	The FAS processes are not consolidated. Therefore, this question is not applicable.
8. How will the data be retrieved? Can the data be retrieved using a personal identifier (i.e., name, address, etc.)? If yes, explain.	The FAS does not allow data retrieval by person or personal identifier. Therefore, this question is not applicable.
9. What are the potential effects on the due process rights of individuals with respect to the following: • Consolidation and linkage of files and systems; • Derivation of data; • Accelerated information processing and decision-making; • Use of new technologies?	These questions are not applicable to the FAS since FAS does not interfere with an individual's due process rights since the application does not consolidate and link files, derive data, accelerate information processing and decision making.
10. How will these affects be mitigated?	This question is not applicable.

4.4 Maintenance of Administrative Controls

Automation of systems can lead to the consolidation of processes, data, and the controls in place to protect the data. When administrative controls are consolidated, they should be evaluated so that all necessary controls remain in place to the degree necessary to continue to control access to and use of the data.

Data retention procedures should be documented. Data retention procedures require review to ensure they meet statutory requirements. Rules must be established for the length of time information is kept and for assuring that it is properly eliminated (i.e., archived, deleted, etc.) at the end of that time.

The intended and potential monitoring capabilities of a system must be defined and safeguards must be installed to ensure privacy and prevent unnecessary intrusion.

Privacy Criteria	Descriptive Response
1. Explain how the system and its use will ensure equitable treatment of individuals.	Personal information (SSN, name, address, and banking information) is required by law for disbursement and taxation purposes.
2. If the system is operated in more than one site, how will consistent use of the system and data be maintained in all sites?	FAS is operated and maintained at one location, the NSF headquarters office in Arlington, VA.
3. Explain any possibilities of disparate treatment of individuals or groups.	FAS processing does not create possibilities for disparate treatment of individuals or groups.
4. What are the retention periods of data in this system?	All FAS data is retained. Data is never removed from the system.
5. What are the procedures for eliminating the data at the end of the retention period? Where are the procedures documented?	At this point, FAS data has never been removed (archived). However, future plans include electronically archiving records at the National Archives.
6. While the data is retained in the system, what are the requirements for determining if the data is still sufficiently accurate, relevant, timely, and complete to ensure fairness in making determinations?	FAS management keeps point in time information for all financial transactions for auditing purposes. Therefore, all data is accurate at the time it is used for the transaction.
7. Is the system using technologies in ways that NSF has not previously employed? How does the use of this technology affect individual's privacy?	The FAS does not use technologies in unusual ways.
8. Will this system provide the capability to identify, locate, and monitor individuals? If yes, explain.	The FAS does not provide a capability to identify, locate and monitor individuals.
9. Will this system provide the capability to identify, locate and monitor groups of people? If yes explain.	The FAS does not provide a capability to identify, locate and monitor groups of people.
10. What controls will be used to prevent unauthorized monitoring?	Access to the FAS data is strictly controlled and reviewed regularly under the FAS Security Plan.
11. Under which System of Record notice does the system operate? Provide number and name.	This listing was documented in the previous FAS PIA which is dated May 13, 2005. NSF-3: Application and Account for Advance of Funds; NSF-10: Employee Payroll Jacket

Privacy Criteria	Descriptive Response
	NSF-22: NSF Payroll System NSF-65: NSF Electronic Payment File GOVT-3: Travel Charge Card Program GOVT-4: Contracted Program Travel Services
12. If the system is being modified, will the System of Record require amendment or revision? Explain	The FAS is not being modified at this date.

Additional Assistance

For additional assistance with completing this assessment, you may contact NSF Privacy Act Officer, Leslie Jensen, at x5065 or the NSF Privacy Advocate, Mary Lou Tillotson, at x4264.

Review

When the PIA is complete, please submit the PIA to the NSF Privacy Act Officer for review at ljensen@nsf.gov and to the NSF Privacy Advocate at mtillots@nsf.gov.