National Science Foundation

NSF AuthentX Identity Management System (IDMS)

Privacy Impact Assessment

Version: 1.1

Date: 12/04/2006

Table of Contents

Revisions

Revision Number	Author	Date	Description

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).

Privacy issues addressed by this assessment include:

1. The use of the information must be controlled.
2. Information may be used only for a necessary and lawful purpose.
3. Individuals must be informed in writing of the principal purpose and routine uses of the information being collected from them.
4. Information collected for a particular purpose should not be used for another purpose without the data subject's consent unless such other uses are specifically authorized or mandated by law.
5. Any information used must be sufficiently accurate, relevant, timely and complete to assure fair treatment of the individual.

Homeland Security Presidential Directive 12 (HSPD-12) requires improved processes to strengthen Personal Identity Verification (PIV) of all Federal employees and contractors. National Institute of Standards and Technology's (NIST) Federal Information Processing Standards Publication 201-1 (FIPS 201-1) provides implementation guidance for HSPD-12.

HSPD-12 emphasizes the need to protect privacy of Government employees and contractors. The HSPD-12 requirements for privacy and security controls include:

1. Naming a Senior Agency Official for Privacy (i.e., the NSF CIO) to oversee the privacy protections related to implementation of the Personal Identity Verification (PIV) process.
2. Publishing a Privacy Act statement available to all employees and contractors.
3. Conducting a Privacy Impact Assessment (PIA) of the systems that support the PIV process. This must be submitted to OMB Privacy Officials for review.
4. Publishing a Privacy Act System of Records Notice (SORN) in the Federal Register, for public comment (current SORN is being amended).

1.1 Organizational Background

At NSF, the Divisions of Human Resources Management (HRM) and Administrative Services (DAS) have the lead with implementing the HSPD-12 requirements. In the PIV process, HRM authorizes the issuance of ID cards by examining identity source documents and completing and adjudicating required background investigations. DAS issues the cards to authorized Applicants and manages the card life cycle. HRM is responsible for NSF's Personnel Security System of Records (SOR) (NSF-26), while DAS is responsible for the NSF Photo Identification Card SOR (NSF-66) and for this new system.

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 be integrated into the system 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

A critical component of completing the C&A process is categorizing the information type(s) that the system processes. An information type is defined as "*a specific category of information (e.g., privacy, medical, proprietary, financial, investigative, contractor sensitive, security management), defined by an organization or in some instances, by a specific law, Executive Order, directive, policy, or regulation*[1]." Some NSF systems process privacy information. Thus, this PIA serves to determine to what extent this privacy information must be adequately protected.

XTec's AuthentX COTS product is an identity and credential management and authentication system. This enterprise system has the ability to issue and manage smart cards in a distributed or centralized card production capacity. At NSF card enrollment and issuance will be centralized. The system, owned and operated by XTec, uses a Web portal to enter and store information about the individual employees/contractors, and about their credential record. This Web site will only be accessible from within the NSF network and to the AuthentX server via secure communications, and only to those users who play a specific role in the PIV process (sponsor, enrollment official, registrar, issuance official, etc.). Potential cardholders present themselves at a badging office containing an AuthentX Enrollment Station. They will show the proper credentials sufficient to establish their identity. The enrollment process will include verifying the identity and privileges information and capturing the data including a photo image and fingerprints. Data captured during the enrollment process are forwarded over the Internet to the central AuthentX database, which is hosted offsite. Fingerprint information is forwarded to the FBI as well as the AuthentX database. The smart card is encoded at that point with the image, fingerprint template, data, and with a secure key. Cards are then delivered to NSF for activation and issuance. **The XTec AuthentX "appliance" (secure XA node)** will push data from the AuthentX system to the C-Cure system to ensure that NSF's legacy system remains the definitive data source of all identity and physical access cards.

The operational environment for the NSF Photo Identification Card System (NSF-66) consists of a personal computer-based COTS security system, C-Cure 800. The system consists of a server, photo and signature capture and input devices, and connections to NSF's card readers located throughout the building. The system is used for card issuance and management. The server is in a highly secure building location in a locked room and is password-protected. The server is connected to the NSF LAN and to the AuthentX system via a secure XA node (see above).

---

[1] FIPS 199, Standards for Security Categorization of Federal Information and Information Systems, February 2004, Section 3, page 1.

Communication among Administrative Officers (AOs), HRM and DAS (as documented in the standard operating procedures) is generally handled through regular email. Social Security Number is not transmitted via email.

The operational environment for the NSF Personnel Security System (NSF-26) consists of a limited access, password protected database. Only the Personnel Security Officer (Chief of the Employee Relations Branch, HRM) and two Personnel Security Specialists have access to the database. The database is populated with names, dates and other personnel management data by the system administrators as investigations are requested and adjudicated. Information from the database is released on a need-to-know basis as identified in the System of Records Notice. In addition, the database is used to confirm and track the procedural steps and dates (e.g., NACI initiated on [date]) for an employee or contractor to receive an ID card.

4. PRIVACY IMPACT ASSESSMENT CRITERIA

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

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 should be 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., person's name, SSN, etc.) to be collected or processed by the GSS or MA or reference *the NSF Information Categorization and Sensitivity Assessment.*	Required fields: first name, middle initial, last name, government agency, photo, user ID, fingerprints, social security number, date of birth, citizenship, affiliation, eye color, hair color, height, ID source documents, card topology template, card type, card unique ID, card pickup location, emergency responder, card issuer ID, card serial number, expiration date, process date, card change date, law enforcement, special designation, card PIN, card issue date, FASC-N, issuance counter, credential status, ready action, user role, building name, sponsor name, sponsor email, room number, COTR name, background investigation type, initiation date, adjudication date, fingerprint adjudication date, contract end date

Privacy Criteria	Descriptive Response
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).	Applicant, Sponsor (AO, COTR), HRM Personnel Security staff, DAS Issuing Personnel. Investigation results from the FBI and OPM are entered by HRM Personnel Security staff following adjudication.
3. What NSF files and databases are used?	Email, paper files, XTec hosted database, appliance database, C-Cure database.
4. What other Federal Agencies, if any, are providing data for use in the system?	FBI and OPM provide investigation results used in suitability adjudications.
5. From what other third party sources will data be collected?	N/A
6. What information will be collected from the employee?	See response to question #1 above (personal information)
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).*	Visual check of IDs. HRM ensures FBI/OPM investigation results are accurate.
8. How will data be checked for completeness?	The AuthentX system enforces completeness by not allowing the user to continue unless required fields are entered
9. Is the data current? How do you know? What mechanisms were used to validate the data's currency?	Information is collected directly from the employee or contractor as he/she enters on duty or as the badge is renewed
10. What data elements are described? What level of detail is used in documenting data elements?	See response to question #1 above
11. If data elements are documented, what is the name of the document?	N/A

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).	Access is restricted to a small group of employees in the Employee Relations Branch (ERB) of the Division of Human Resource Management (HRM), a small group of employees in the Facilities and Operations Branch (FOB) of the Division of Administrative Services (DAS), approved sponsors, and credential printing staff and system administrators at XTec Incorporated.
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?	Authorized users have access to all data in the system in accordance with their position duties. Users are trained to know what is considered to be proper access. AuthentX automatically documents data access by using a role based access system. Each administrator is given a password and is assigned a particular role. Data are accessible based on the privileges assigned to each role. If data changes are made they are stored in audit logs within the system. For user access the AuthentX system records Date/Time of access, Admin name of user, and Remarks of the system (i.e., Access denied, Access ok, etc.).
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?	Access is restricted by roles and the use of user IDs/passwords. Authorized users need access to the set of data contained in the system as described in Section 4.1, question 1.
4. How or what tools are used to determine a user's data access?	Access is restricted by roles and the use of user IDs/passwords.
5. Describe the criteria, the procedures, the controls, and the responsibilities in place regarding the manner in which data access is documented.	The AuthentX solution automatically documents data access by using a role based access system. Each administrator is given a password and is assigned a particular role. Data are accessible based on the privileges assigned to each role. If data changes are made they are stored in audit logs within the system. For user access the AuthentX system records Date/Time of access, Admin name of user, and Remarks of the system (i.e., Access denied, Access ok, etc.).

Privacy Criteria	Descriptive Response
6. Do other systems share data or have access to data in this system? If yes, explain.	The XA Node appliance pushes data to NSF-66.
7. Who has the responsibility for protecting the privacy rights of the individuals affected by any system interface?	Authorized personnel of XTec, Inc.; NSF (HRM, DAS and Sponsors); FBI; and OPM
8. Will other agencies share data or have access to data in this system?	OPM and FBI provide investigative data used in suitability adjudications
9. How will the NSF use this data?	To produce photo identification cards; to identify the bearer of the card as a Federal employee or contractor; and to track stolen or lost cards.
10. Who is responsible for assuring proper use of the data?	Authorized personnel of NSF, the FBI, OPM and XTec share this responsibility.
11. How will the system ensure that agencies only get the information they are entitled to?	Only trained users with a user ID, password and the registrar role (i.e., three employees) can transfer fingerprint data to the FBI via FTS. Only fingerprint data and a few personal identifiers (including required SSN) are shared with the FBI and OPM.

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 PIV card is a requirement for Federal employment, as well as a requirement for all contractors (on-site more than 6 months). The data are used solely in support of the PIV process and NSF's compliance with HSPD-12.
2. Will the system derive new data or create previously unavailable data about an individual through aggregation for the information collected?	No

Privacy Criteria	Descriptive Response
3. Will the new data be placed in the individual's record?	No
4. Can the system make determinations that would not be possible without the new data?	No
5. How will the new data be verified for relevance and accuracy?	No
6. If data is being consolidated, what controls are in place to protect the data from unauthorized access or use?	No
7. If processes are being consolidated, are the proper controls remaining in place to protect the data and prevent unauthorized access? Explain	No
8. How will the data be retrieved? Can the data be retrieved using a personal identifier (i.e., name, address, etc.)? If yes, explain.	Data can be retrieved by user ID, email address, social security number and last name. Retrieval is necessary to make changes to the cardholder's information, to manage (activate/reissue/revoke/disable) a card throughout the card life cycle, and to provide reports to authorized management officials.
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?	 N/A N/A N/A N/A
10. How will these affects be mitigated?	N/A

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.	The information is used only in connection with PIV card management and is only disclosed to individuals with a bona fide need to know
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?	The system is only used for data entry at NSF, and the authoritative database for card management resides at NSF. The AuthentX system is operated offsite on behalf of NSF.
3. Explain any possibilities of disparate treatment of individuals or groups.	None
4. What are the retention periods of data in this system?	Per FIPS 201-1 credentials will be reissued every 5 years and data will be updated accordingly. NSF-26 – Data are maintained during the course of employment (i.e., requirement for physical access to NSF space). Data are retained for 2 years after employee/contractor separation. NSF-66 – Data are maintained during the course of employment (i.e., requirement for physical access to NSF space). Data are retained up to 90 days after employee/contractor separation, NTE date or card revocation; then the data are deleted.
5. What are the procedures for eliminating the data at the end of the retention period? Where are the procedures documented?	Per the standard operating procedures for badge issuance and maintenance: “The PIV credential is non-transferable and must be returned to NSF when there is no longer a bona fide need…. When time-limited ID badges expire, they will be deactivated and must also be returned to DAS. The PIV badges can be deactivated and recalled for any reason at the discretion of DAS, the employee’s sponsor or an Enrollment Official.” Data are deleted from C-Cure within 90 days of badge deactivation in accordance with routine procedures.

Privacy Criteria	Descriptive Response
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?	AuthentX data are captured as employees and contractors enter on duty, and are backed up on a regular basis. NSF-26 – Access database is backed up twice monthly. NSF-66 – Employees can review and update their personal information as needed. Data are reviewed at card renewal by authorized personnel. C-Cure database is backed up twice monthly and data are stored at a secure off-site location. The database back up system is tested twice yearly to ensure data integrity and availability. Facilities Management staff review the DIS list of LAN/email IDs every 60 days to determine that ID cards are still required by contractors, to ensure currency of data. Discrepancies are resolved with AOs. The Contractor confirms the continuing need for ID cards for the Contractor's employees through regular reports.
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?	No. This system uses no new technologies.
8. Will this system provide the capability to identify, locate, and monitor individuals? If yes, explain.	No
9. Will this system provide the capability to identify, locate and monitor groups of people? If yes explain.	No
10. What controls will be used to prevent unauthorized monitoring?	Access data are password-protected and only accessible from two terminals located in locked areas that can be accessed by only a very limited number of authorized users.
11. Under which System of Record notice does the system operate? Provide number and name.	NSF Photo Identification Card System, NSF-66
12. If the system is being modified, will the System of Record require amendment or revision? Explain	Yes. System of Record Notice for NSF-66 has been revised.

Additional Assistance

For additional assistance with completing this assessment, you may contact Division of Information Systems Security Officer at 703-292-4225.

Review Authority

Reviewed by Leslie Jensen, NSF Privacy Act Officer.