National Science Foundation

NSF AuthentX Identity Management System (IDMS)

Privacy Impact Assessment

Version: 2.0

Date: 11/4/2008

Table of Contents

Revisions

Revision Number	Author	Date	Description
Version 2 (template)	M Tillotson	July 2008	Updated the PIA template
Version 2.0	M Crawford	November 2008	Updated AuthentX PIA per new format
Version 2.0	L Jensen	Nov 25, 2008	Reviewed

Privacy Impact Assessment Form

1. CONTACT INFORMATION

Project Manager/System Owner:

Laurie Pena-Ariet, Head, Facilities Management Section, OIRM/DAS, 703-292-7554

2. GENERAL SYSTEM INFORMATION

1. Name of System or Electronic Collection of Information:

NSF AuthentX Identity Management System (IDMS)

2. Description of System or Electronic Collection of Information:

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 centralized card production capacity. At NSF, card enrollment and issuance is centralized. The system, owned and operated by XTec Inc., uses a Web portal to enter and store information about the individual employees/contractors, and about their credential record. This Web site is only 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, approver, issuance official, etc.). Potential cardholders present themselves at a badging office containing an AuthentX Enrollment Station. They show the proper credentials sufficient to establish their identity. The enrollment process includes 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 OPM as well as the AuthentX database. The smart card is encoded at that point with the image, fingerprint template, data, and a secure key. Cards are then printed at NSF and are ready 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. This capability is not scheduled for installation until the end of calendar year 2008.

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

The PIV card is a requirement for Federal employment, as well as a requirement for all contractors (on-site more than 6 months) who need access to NSF facilities. The data are used solely in support of the PIV process (including physical access control) and NSF's compliance with HSPD-12. Data are collected 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.

4. Requested Operational Date?

The system was operational on October 27, 2006.

5. Does this collection create a new Privacy Act System or is this information collection covered by an existing Privacy Act System? If so, what is the name of the current Privacy Act System?

This collection is covered under the NSF Photo Identification Card System, NSF-66

6. What specific legal authorities, arrangements, and/or agreements require the collection of this information?

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. These authorities require the collection and use of personal information including identity documents, photo images and fingerprints for purposes of: 1) conducting personnel security investigations; 2) verifying claimed identities; and 3) granting access to Federal facilities.

7. Is this an Exhibit 300 system/project?

No. Expenditure data are only included as one entry in the Infrastructure, Office Automation, and Telecomm Investment exhibit.

3. DATA IN THE SYSTEM

1. What data are to be collected?

Required fields include: 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, card issuer ID, card serial number, expiration date, process date, card change date, card PIN, card issue date, Federal Agency Smart Credential Number (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, and contract end date.

2. What are the sources of the data?

Applicant (employee, contractor, IPA or guest) provides the vast majority of the data as they enter on duty (or, for current employees and contractors, as cards are issued or renewed). Additional data are provided by the Sponsor (HRM, AO or COTR), HRM Personnel Security staff, and DAS Issuing Personnel. Investigation results from the FBI and OPM are entered by HRM Personnel Security staff following adjudication of personnel investigations.

3. Why are the data being collected?

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 (including physical access control) and NSF's compliance with HSPD-12. Data requirements are described in FIPS 201-1.

4. What technologies will be used to collect the data?

Individual applicant presents himself/herself to HRM Personnel Security staff for enrollment, which includes taking of a photo and fingerprints (via a digital camera and fingerprint scanner), capturing source identity documents by scanning, and entry of additional data via a Web portal into AuthentX. Card issuance requires the use of a fingerprint scanner to verify identity. This system uses no new technologies.

5. Does a personal identifier retrieve the data?

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.

4. ATTRIBUTES OF THE DATA (USE AND ACCURACY)

1. Describe the uses of the 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.

2. Does the system analyze data to assist users in identifying previously unknown areas of note, concern or pattern?

No.

3. How will the data collected from individuals or derived by the system be checked for accuracy?

Data are captured as employees and contractors enter on duty (or as credentials are issued or renewed for current employees and contractors). Applicants who enroll for a PIV credential must present two valid identity documents which are reviewed by enrollment staff. Applicants directly provide the vast majority of data. Applicants can review and update their personal information as needed. HRM ensures FBI/OPM investigation results are accurate. Card issuance staff also inspect two forms of ID and require a fingerprint match when activating and issuing the card for use. The database is periodically reviewed by enrollment and issuance staff for accuracy.

5. SHARING PRACTICES

1. Will the data be shared with any internal or external organizations?

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 system administrators at XTec, Inc. The data will not be shared with any other organization. Other Federal agencies may require the disclosure of certain data (e.g., fingerprints, PIN number, etc.) from the card itself to grant access to their facilities. This use is governed by HSPD-12 and FIPS 201-1.

2. How are the data transmitted or disclosed to the internal or external organization?

The system uses a Web portal to enter and store information about the individual employees/contractors. This Web site will only be accessible from within the NSF network via secure communications, and only to those users who play a specific role in the PIV process (sponsor, enrollment official, issuance official, etc.). Data captured during the enrollment process are forwarded over a secure Web portal to the central AuthentX database, which is hosted offsite. Fingerprint information is forwarded electronically to OPM and the FBI as well as to the AuthentX database. The smart card is encoded at that point with the image, fingerprint template, data, and with a secure key.

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

Only trained users with a user ID, password and the registrar role (i.e., three employees) can transfer fingerprint data electronically to the FBI and OPM. Only fingerprint data and a few personal identifiers (including required SSN) are shared with the FBI and OPM. Security of the data by the FBI and OPM is governed by government-wide regulations.

6. NOTICE TO INDIVIDUALS TO DECLINE/CONSENT USE

1. Was notice provided to the different individuals prior to collection of data?

Yes. Applicants can decline to provide the data, but they will then be unable to access NSF facilities except by using a visitor's badge.

2. Do individuals have the opportunity and/or right to decline to provide data?

Yes.

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

Approved uses are described in System of Records notice NSF-66, NSF Photo Identification Card System.

7. ACCESS TO DATA (ADMINISTRATIVE AND TECHNICAL CONTROLS)

1. Is the data secured in accordance with FISMA requirements?

   If **Yes,** provide the date that the Certification and Accreditation was completed.

   If **No**, answer questions 2-5 below.

C&A was approved by the NSF CIO on October 27, 2006.

2. Which user group(s) will have access to the system?

3. How is the access to the data by a user determined? Are procedures documented?

4. How are the actual assignments of roles and rules verified according to the established security and auditing procedures?

5. What auditing measures/controls and technical safeguards are in place to prevent misuse (e.g., unauthorized browsing) of data?

6. Describe the privacy training provided to users, either generally or specifically relevant to the program or system?

All personnel who use the system are trained on privacy matters before they are granted access. This includes the confidentiality of the data, the disclosure of information only to authorized users with a bona fide need to know, etc. All personnel must also complete NSF's IT security training.

7. Will NSF contractors have access to the system? If so, will they be trained on privacy principles?

A very limited number of contractors have access to the system, and they undergo the same training described above.

8. Has the retention schedule been established by records management? If so, what is the retention period for the data in the system?

Personnel Security, 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 Photo Identification Card System, 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.

9. What are the procedures for identification and disposition of the data at the end of the retention period?

Retention of the data regarding personnel investigations is governed by government-wide regulations.

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 the C-Cure card management system within 90 days of badge deactivation in accordance with routine procedures.

8. PRIVACY ANALYSIS

Given the amount and type of data being collected, discuss what privacy risks were identified and how they were mitigated.

- Data completeness: The AuthentX system enforces completeness by not allowing data entry to continue unless required fields are entered.
- Data accuracy: Most personal information is obtained directly from the applicant (discussed above).
- Data access: Access is restricted to a small group of administrative employees, approved sponsors, and system administrators at XTec Inc. Access is restricted by roles and the use of user IDs/passwords. Data are only accessible from two workstations located in a locked room that can be accessed only by a very limited number of users. 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.

- Data disclosure: Data are only disclosed to authorized users who have an appropriate role in the PIV process, such as enrollers and issuers. OPM and the FBI are only given the data necessary for them to conduct required name checks and investigations.
- Documenting data 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.).
- Division of responsibilities: Users of the system can only perform operations associated with their assigned roles (such as enroller, approver, issuer, etc.), to eliminate the possibility that a credential could be issued by one individual.
- Special requirements: HSPD-12 mandated:
    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.