Federal Bureau of Prisons

Privacy Impact Assessment
for the
ACES/Web Visiting System

Issued by:
Sonya D. Thompson
Deputy Assistant Director/CIO

Reviewed by: Vance E. Hitch, Chief Information Officer,
Department of Justice

Approved by: Nancy C. Libin, Chief Privacy and Civil Liberties Officer,
Department of Justice

Date approved: August 30, 2011

Introduction

The Access Control Entry Exit System (ACES)/Web Visiting system is designed to log and track all persons entering and exiting BOP facilities, including staff, contractors, approved volunteers and approved visitors. Information in the system is collected and maintained to better ensure the safety, security and good order of Bureau facilities; to improve staff ability to quickly account for all persons (inmates, visitors, and staff within an institution in the event of an emergency, such as an institution disturbance or a natural disaster); to identify and, where appropriate, determine the suitability of visitors with respect to entering prison facilities.

Section 1.0 The System and the Information Collected and Stored within the System.

The following questions are intended to define the scope of the information in the system, specifically the nature of the information and the sources from which it is obtained.

1.1 What information is to be collected?

Information retrieved and stored by the system may include any information relative to providing safe and secure prison facilities, to protecting the prison population and/or the general public, and/or, where appropriate, to otherwise promoting the interests of effective law enforcement. Examples include identification data such as:

- the person's name
- current residence
- social security number
- digital image
- fingerprint
- alien registration number
- driver's license number
- passport number

Other data collected includes:

- employer
- place and date of birth
- age, height, weight
- telephone number

- hair color, eye color
- sex
- race

1.2 From whom is the information collected?

Information is collected from current and former staff, inmates now or formerly under the custody of the Attorney General or the Bureau, and all visitors to Bureau facilities, including law enforcement personnel, contractors, volunteers, and inmate visitors.

Section 2.0 The Purpose of the System and the Information Collected and Stored within the System.

The following questions are intended to delineate clearly the purpose for which information is collected in the system.

2.1 Why is the information being collected?

The records in this system are maintained to better ensure the safety, security and good order of Bureau facilities; to improve staff ability to quickly account for all persons (inmates, visitors, and staff) within an institution in the event of an emergency, such as an institution disturbance or a natural disaster; to identify and, where appropriate, determine the suitability of visitors with respect to entering prison facilities; and, to more effectively prevent violations of institution policy and/or criminal activity, such as inmate escapes and the introduction of contraband.

2.2 What specific legal authorities, arrangements, and/or agreements authorize the collection of information?

18 U.S.C. 4003, 4042 and 4082 authorize the BOP to manage inmates committed to the custody of the Attorney General. The Bureau is also responsible for individuals who are directly committed to its custody pursuant to the 18 U.S.C. 3621 and 5003 (state inmates), and inmates from the District of Columbia pursuant to section 11201 of Chapter 1 of Subtitle C of Title XI of the National Capital Revitalization and Self-Government Improvement Act of 1997 (Pub. L. 105-33; 111 Stat. 740).

2.3 Privacy Impact Analysis: Given the amount and type of information collected, as well as the purpose, discuss what privacy risks were identified and how they were mitigated.

There is a privacy risk related to the inadvertent disclosure of sensitive information to the persons not authorized to receive it. There is also a risk of unauthorized data use. To mitigate these risks, staff is annually trained on how to properly handle sensitive information. Access to the system is limited to those persons who have an appropriate security clearance which is regularly reviewed. Information is safeguarded in accordance with Bureau rules and policy governing automated information systems security and access. These safeguards include the maintenance of records and technical equipment in restricted areas, and the required use of proper passwords and user identification codes to access the system. Only those Bureau personnel who require access to perform their official duties may access the system equipment and the information in the system. Data transmission is also encrypted.

Section 3.0 Uses of the System and the Information.

The following questions are intended to clearly delineate the intended uses of the information in the system.

3.1 Describe all uses of the information.

The records in this system are maintained to better ensure the safety, security and good order of Bureau facilities; to improve staff ability to quickly account for all persons (inmates, visitors, and staff) within an institution in the event of ah emergency, such as an institution disturbance or a natural disaster; to identify and, where appropriate, determine the suitability of visitors with respect to entering prison facilities; and, to more effectively prevent violations of institution policy and/or criminal activity, such as inmate escapes and the introduction of contraband. Where these efforts fail to prevent such violations, and/or where appropriate, records may be collected and used by the Bureau for investigative purposes. See Systems of Records Notice BOP-010, 60 FR 52013 (10/4/95) later modified by 67 FR 16760 (4/8/02).

3.2 Does the system analyze data to assist users in identifying previously unknown areas of note, concern, or pattern? (Sometimes referred to as data mining.)

No, the system does not data mine.

3.3 How will the information collected from individuals or derived from the system, including the system itself be checked for accuracy?

A background check is performed for individuals who are recorded into this system. At a minimum, an NCIC check is performed to validate data provided by visitors. Each time a visitor visits an institution a legal id is required in order to gain access to the institution. This data is compared to data available in the system. Discrepancies are corrected, if appropriate, at the time of the visit.

Data from the system is used operationally each day and is vetted due to frequent use, monitoring and review. System accuracy is assured using program edit checks to prevent data entry errors. Data entry is also limited by facility location (i.e. users at one facility cannot enter or edit data related to an inmate located at another facility).

3.4 What is the retention period for the data in the system? Has the applicable retention schedule been approved by the National Archives and Records Administration (NARA)?

The system is a centralized mainframe-based application whose use and purpose is consistent with NARA-issued GRS 18, which involves the storage of information used "to protect Government facilities from unauthorized entry, sabotage, or loss" (GRS 18 general description). Under the media-neutral principles where GRS authorities operate (recognized by 36 CFR Part 1228, FDMS Docket NARA-07-0004, RIN 3095-AB43), the information stored in the system is covered under GRS 18, Item 17 Visitor Control Files, Item 21 Security Clearance Administrative Subject Files, and Item 23 Personnel Security Clearance Status Files.

3.5 <u>Privacy Impact Analysis</u>: Describe any types of controls that may be in place to ensure that information is handled in accordance with the above described uses.

Access is controlled via the role-based security of the application. Access is granted only to those persons who are required to use the system to perform required automated functions. Frequent operational use of the data ensures that data accuracy is continuously reviewed by staff and provides a deterrence for unauthorized data modifications. Visitors are also periodically asked to verify the information in the system by front lobby staff. Inmate visiting records are also periodically reviewed by Unit Management and investigative staff.

Section 4.0 Internal Sharing and Disclosure of Information within the System.

The following questions are intended to define the scope of sharing both within the Department of Justice and with other recipients.

4.1 With which internal components of the Department is the information shared?

Data is shared with various law enforcement components within the Department of Justice including the FBI, USMS, EOUSA, Criminal Division, and Drug Enforcement Agency.

4.2 For each recipient component or office, what information is shared and for what purpose?

The offices listed in Section 4.1 have access to routine information in the system, e.g. name, SSN, home address, birth date, race, sex, and other demographic information as well as information such as dates of visits. The data is shared for law enforcement and court-related purposes such as investigations, possible criminal prosecutions, civil court actions, or regulatory or parole proceedings.

4.3 How is the information transmitted or disclosed?

The Department of Justice receives a batch download of data for integration with other automated systems. Data transmission is encrypted. Information may also be printed and provided to DOJ offices in hard copy. Hard copy information is handled in accordance with information security policy and directives relating to the handling of sensitive information.

4.4 Privacy Impact Analysis: Given the internal sharing, discuss what privacy risks were identified and how they were mitigated.

There is a privacy risk related to the inadvertent disclosure of sensitive information to the persons not authorized to receive it. To mitigate this risk, access to the system is limited to those persons who have an appropriate security clearance which is regularly reviewed. Users are trained as to the use of the system and information is safeguarded in accordance with BOP and DOJ rules and policy governing automated information systems security and access. These safeguards include the maintenance of records and technical equipment in restricted areas, and the required use of proper passwords and user identification codes to access the system. Data transmission is also encrypted. Sharing of data also creates a risk that persons might inappropriately modify or misuse data. This risk is mitigated by the access controls listed above and the fact that individuals have the ability to consent and review uses of the information contained in the system.

Section 5.0 External Sharing and Disclosure

The following questions are intended to define the content, scope, and authority for information sharing external to DOJ which includes foreign, Federal, state and local government, and the private sector.

5.1 With which external (non-DOJ) recipient(s) is the information shared?

Information may be shared with federal, state, local, tribal, foreign and international law enforcement agencies and court officials. Information may also be shared with other non-DOJ entities in accordance with Systems of Records Notice BOP-010, 60 FR 52013 (10/4/95), later modified by 67 FR 16760 (4/8/02).

5.2 What information is shared and for what purpose?

Information is shared with federal, state, local, foreign and international law enforcement agencies who have a need for the information to perform their duties, e.g. in the course of apprehensions, investigations, possible criminal prosecutions, civil court actions, regulatory proceedings and other law enforcement activities. Such information includes, e.g., name, SSN, home address, birth date, race, sex, and other demographic information as well as information such as dates of visits.

5.3 How is the information transmitted or disclosed?

Certain federal agencies receive batch downloads of data for integration with other automated systems in accordance with a Memorandum of Agreement. Data transmission is encrypted. State agencies may access the data via an approved regional information sharing program with the Department of Justice Law Enforcement Information Sharing initiative (OneDOJ). Information may also be printed and provided to such offices in hard copy. Hard copy information is handled in accordance with information security policy and directives relating to the handling of sensitive information.

5.4 Are there any agreements concerning the security and privacy of the data once it is shared?

Yes. Memoranda of Agreement restrict use of the data to only authorized purposes and do not permit further redistribution of the data.

5.5 What type of training is required for users from agencies outside DOJ prior to receiving access to the information?

Users are notified of rules and procedures regarding access to the information and in cases where automated access is provided, they are given a Rules of

Behavior document which they must sign and acknowledge.

5.6 Are there any provisions in place for auditing the recipients' use of the information?

Memorandums of Agreements include requirements for the recipient agency to maintain an audit trail of user activities.

5.7 Privacy Impact Analysis: Given the external sharing, what privacy risks were identified and describe how they were mitigated.

There is a privacy risk related to the inadvertent disclosure of sensitive information to the persons not authorized to receive it. To mitigate this risk, access to the system is limited to those persons who have an appropriate security clearance which is regularly reviewed. Users are trained as to the use of the system and information is safeguarded in accordance with BOP and DOJ rules and policy governing automated information systems security and access. These safeguards include the maintenance of records and technical equipment in restricted areas, and the required use of proper passwords and user identification codes to access the system. Data transmission is also encrypted. External sharing of data also increases the privacy risks of unauthorized access and modification and misuse. Additional mitigating controls include the fact that data entry is only performed by BOP personnel; that individuals have the opportunity to consent to non-routine uses of the information (section 6.3); and that an MOA exists concerning the security and privacy of data once it is shared.

Section 6.0 Notice

The following questions are directed at notice to the individual of the scope of information collected, the opportunity to consent to uses of said information, and the opportunity to decline to provide information.

6.1 Was any form of notice provided to the individual prior to collection of information? If yes, please provide a copy of the notice as an appendix. (A notice may include a posted privacy policy, a Privacy Act notice on forms, or a system of records notice published in the Federal Register Notice.) If notice was not provided, why not?

Yes. Notice was provided through a System of Records Notice, BOP-010, first published on October 4, 1995 (60 FR 52013), later modified on April 8, 2002 (67 FR 16760).

6.2 Do individuals have an opportunity and/or right to decline to provide information?

No. Information is required to be provided as part of the visiting process. Failure to provide requested information could jeopardize the safe and orderly running of the institution and the BOP's ability to approve access.

6.3 Do individuals have an opportunity to consent to particular uses of the information, and if so, what is the procedure by which an individual would provide such consent?

Individuals do not have the opportunity to consent to routine uses of the information. Individuals have the opportunity to consent to non-routine uses of the information pursuant to the Privacy Act, 5 USC Section 552a.

6.4 Privacy Impact Analysis: Given the notice provided to individuals above, describe what privacy risks were identified and how you mitigated them.

The privacy risk identified would be the failure of persons to know their information may be collected and what it will be used for. BOP has published a Privacy Act System of Records Notice (SORN) described above for BOP's visitor records. The information in this notice includes entities with which and situations when BOP may share investigative records. This notice, therefore, mitigates the risk that the individual will not know why the information is being collected or how the information will be used.

Section 7.0 Individual Access and Redress

The following questions concern an individual's ability to ensure the accuracy of the information collected about him/her.

7.1 What are the procedures which allow individuals the opportunity to seek access to or redress of their own information?

Requests for information about an individual's own records in the system may be made in writing to the Director, Federal Bureau of Prisons, 320 First Street NW, Washington DC 20534 and should be clearly marked "Privacy Act Request".

7.2 How are individuals notified of the procedures for seeking access to or amendment of their information?

Upon each visit, visitors receive a "Notification To Visitor" Form. Visitors are required to fill out the form. This form provides the rules for visitation and request that each visitor provide their name, address, and vehicle information. Information about contesting record information is also included in the aforementioned System of Records Notice.

7.3 If no opportunity to seek amendment is provided, are any other redress alternatives available to the individual?

N/A.

7.4 Privacy Impact Analysis: Discuss any opportunities or procedures by which an individual can contest information contained in this system or actions taken as a result of agency reliance on information in the system.

Requests to contest the information about an individual's own records in the system may be made in writing to the Director, Federal Bureau of Prisons, 320 First Street NW, Washington DC 20534 and should be clearly marked "Privacy Act Request".

Section 8.0 Technical Access and Security

The following questions are intended to describe technical safeguards and security measures.

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

BOP and DOJ staff with a need to access the system to carry out their duties may be approved for access to the system. External agency users who are approved and have an appropriate security clearance may access data from the system.

8.2 Will contractors to the Department have access to the system? If so, please submit a copy of the contract describing their role with this PIA.

Contractors do not have access to the system.

8.3 Does the system use "roles" to assign privileges to users of the system?

Yes. Role access is controlled with group assignments, user IDs and passwords. Only certain groups are authorized to conduct certain transactions and see certain data and/or reports.

8.4 What procedures are in place to determine which users may access the system and are they documented?

User access for an employee must be requested by a supervisor indicating that access is required for the performance of their duties. The request and subsequent access is documented in the BOP HelpDesk system. When appropriate staff receive a user id for access to the network, user roles are also assigned based upon their job position. Each administrator has access to documentation which indicates the roles that should be assigned to a job position.

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

User access is reviewed and recertified on an annual basis. Role assignments are defined by job positions within the institution.

8.6 What auditing measures and technical safeguards are in place to prevent misuse of data?

The system restricts data entry by institution. In the case of persons who visit multiple institutions, their data is validated upon arrival at each new institution. Only authorized staff are permitted access to the application via role management. Visiting lists are periodically reviewed by institution Unit Management staff and investigative staff.

8.7 Describe what privacy training is provided to users either generally or specifically relevant to the functionality of the program or system?

Users are trained as to the sensitive nature of the data within the system and continuously reminded as to the need to strictly control the viewing and/or output of data from the system. BOP users are trained annually regarding the handling of sensitive information and information security requirements. All employees who are involved in the management, operation, programming, maintenance, or use of a DOJ information system are made aware of the threats to and vulnerabilities of those systems and their responsibilities with regard to privacy and information security.

8.8 Is the data secured in accordance with FISMA requirements? If yes, when was Certification & Accreditation last completed?

Yes. The Certification and Accreditation for the parent system BOPNet was last updated on October 21, 2008.

8.9 Privacy Impact Analysis: Given access and security controls, what privacy risks were identified and describe how they were mitigated.

There is a privacy risk related to the inadvertent disclosure of sensitive information to the persons not authorized to receive it. To mitigate this risk, access to the system is limited to those persons who have an appropriate security clearance which is regularly reviewed. Users are trained as to the use of the system and their roles/responsibilities (e.g Front Lobby Officer, Visiting Room Officer, Unit Management staff, etc.) and information is safeguarded in accordance with BOP and DOJ rules and policy governing automated information systems security and access. These safeguards include the maintenance of records and technical equipment in restricted areas, the required use of proper passwords and user identification codes to access the system, and the use of screensavers and screen filters to protect data display. Data transmission is also encrypted.

Section 9.0 Technology

The following questions are directed at critically analyzing the selection process for any technologies utilized by the system, including system hardware, RFID, biometrics and other technology.

9.1 Were competing technologies evaluated to assess and compare their ability to effectively achieve system goals?

Yes, competing database and application technologies were analyzed and compared during system design. Earlier systems included standalone, local database systems as well as a client-server model. The centralized web-based system provides ease of use, increased data sharing capabilities, reduced data entry and enhanced security controls using role-based management.

9.2 Describe how data integrity, privacy, and security were analyzed as part of the decisions made for your system.

During the requirements analysis and design phase, these issues were addressed

with business stakeholders. BOP policy was also reviewed to ensure adherence. Decisions that were reached by consensus were implemented into the design of the application.

9.3 What design choices were made to enhance privacy?

Role-based security by job function was implemented. This protection ensures that staff only have access to the portions of the application that are relevant to their duties.

Conclusion

The records in this system are maintained to better ensure the safety, security and good order of Bureau facilities; deter and prevent criminal activity; to improve staff ability to quickly account for all persons within an institution in the event of an emergency, and to assist staff in determining the suitability of visitors with respect to entering prison facilities. The system is designed to achieve these goals while maintaining the privacy of the information contained therein.