Federal Bureau of Prisons

Privacy Impact Assessment
for the
Volunteer/Contractor Information 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 Federal Bureau of Prisons protects society by confining offenders in the controlled environments of prisons, and community-based facilities that are safe, humane, and appropriately secure, and which provide work and other self-improvement opportunities to assist offenders in becoming law-abiding citizens.

The Volunteer/Contractor Information (VCI) System collects demographic information for security clearance tracking of all of volunteers, contractors, and non-paid interns entering BOP facilities. System data is matched against the Federal Bureau of Investigation's (FBI's) records via a Name Check for security purposes.

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?

The following identifiable information is collected:

Name
Social Security Number (SSN)
OPM National Agency Check w/ Inquiries (NACI) Number

Other information is also collected including:
Birth date
Citizenship
Home address
Home Telephone Number
Cell Phone Number
Email Address
Race
Sex

Records are retrievable by identifying data, including name and/or SSN.

1.2 From whom is the information collected?

The information is collected from persons entering BOP facilities as contractors, volunteers, and non-paid interns.

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 information is collected to assist the Attorney General and the Bureau of Prisons in meeting statutory responsibilities for the safekeeping, care and custody of incarcerated persons. It includes information critical to the continued safety and security of federal prisons and the public and is used to identify individuals who access BOP facilities. Specific identifiable information, such as SSN, is collected to ensure the unique identification of the individual.

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

18 U.S.C. 4042 authorizes 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 Colombia 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 disclosure of sensitive information to the persons not authorized to receive it. To mitigate this risk, staff members are annually trained on how to properly handle sensitive information. Access to the system is limited to those persons who have an appropriate security clearance. 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. There is also a risk of misuse of data. This is mitigated by providing oversight of user and system administrator activities.

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 data is provided to the Federal Bureau of Investigation for purposes such as investigations, intelligence monitoring, or possible criminal prosecutions. Other routine uses include those listed in the following System of Records Notices:

- DOJ-006, Personnel Investigation and Security Clearance Records for the Department of Justice, 67 FR 59864 (09-24-02); 69 FR 65224 (11-10-04); 72 FR 3410 (01-25-07)

- OPM/GOVT-1, General Personnel Records (see e.g. 71 FR 35342 06-19-06))

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.)

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?

Data from the system is reviewed by the FBI and monitored for law enforcement purposes. 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 persons 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)?

Data is retained permanently.

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 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, e.g. users must authenticate to the system using their userid and password, access to the system must be requested and approved by a supervisor, and user accounts are routinely reviewed. Data in the system is also periodically reviewed.

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 the FBI. System data is matched against the FBI's records via a name check for security purposes.

.

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

The office listed in Section 4.1 is provided with information in the system, e.g. name, SSN, home address, birth date, race, sex, etc The data is shared for law enforcement and court-related purposes such as intelligence, investigations, security clearances, and possible criminal prosecutions.

4.3 How is the information transmitted or disclosed?

Information is available electronically for viewing in the system by authorized users within the respective agency. Data transmission is encrypted. The FBI receives a batch download of data for integration with their automated system. 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.

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 disclosure of sensitive information to 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, the required use of proper passwords and user identification codes to access the system, the use of encryption for data transmissions, appropriately labeling hard copy materials to alert staff as to the sensitive nature of the data, storing hard copy printouts in secure, locked locations, and requiring authorization to remove hardcopy materials from the workplace. Sharing of data also increases the privacy risks of unauthorized access and modification and misuse. Additional mitigating controls include: data entry is only performed by select BOP personnel and individuals have the opportunity to consent to non-routine uses of the information.

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 is not shared by BOP with any non –DOJ entities.

5.2 What information is shared and for what purpose?

N/A

5.3 How is the information transmitted or disclosed?

N/A.

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

N/A.

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

N/A.

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

N/A.

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

N/A.

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?

Notice was provided through a System of Records Notice, OPM/GOVT-I, General Personnel Records; DOJ-006, Personnel Investigation and Security Clearance Records for the Department of Justice. Notice is also provided on applicable collection forms, e.g. Standard Form 85 ("Questionnaire for Non-Sensitive Positions").

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

The information may be provided voluntarily. BOP, however, may be unable to complete the background investigation or complete it in a timely manner, if the information is not provided. This omission may affect the contractor's or volunteer's access to the applicable BOP facility.

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 may 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. DOJ and OPM have published Privacy Act System of Records Notices (SORNs, see 6.1 above) for records in VCI. The information in this notice includes entities with which and situations when BOP may share these records. Also, notice is given on forms where information is collected from individuals. These notices, therefore, mitigate 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?

Individuals provide the information collected in the system and attest by signature on the collection form as to its accuracy. Individuals are provided instructions on the collection form(s) (e.g. SF-85) on how to access or amend information. Individuals are also provided the opportunity during the clearance process to personally explain, refute, or clarify any information entered on the requisite clearance forms before a final decision is made as to their eligibility for hire.

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

Individuals are provided instructions on the collection form(s) on how to access or amend information.

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

N/A. See question 7.2 above.

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.

See question 7.1 above.

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 staff with a need to access the system to carry out their duties may be approved for access to 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.

No. Contractors do not have access to the system.

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

Yes, roles are assigned to access data, including roles for regular users and roles for IT administrators.

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

User access must be requested by a supervisor indicating access is required for the performance of their duties. The request and subsequent access is documented in the BOP HelpDesk system.

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

Each user's access is reviewed by program and IT staff.

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

Access to the system is strictly limited to select staff with a need-to-know. Access to the system is controlled via userID and password. Information in the system is regularly reviewed.

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 data is secured in accordance with FISMA requirements. The Certification and Accreditation was last completed on May 2, 2005.

8.9 <u>Privacy Impact Analysis</u>: 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 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, the maintenance and review of user access documentation, and the periodic review of the data contained in the system. 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?

The system is a routine tracking database used to monitor contractor/volunteer access. No significant technologies were used to develop the system. The specific technologies in the system were selected for ease of use, system efficiencies, and reporting capabilities.

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

Development was structured to minimize risks; the design phase included extensive input and meetings with subject matter staff and end-users. Prior to full implementation, a pilot was performed.

9.3 What design choices were made to enhance privacy?

The principle of “least privilege” was employed to ensure that only those persons with a need to view the data can access the system. User accounts are approved by the system owner.

Conclusion

The VCI database was constructed to strictly control information used therein and to mitigate risks to the information. Any modifications or enhancements to the system continue to follow that same design goal.