Federal Bureau of Prisons

Privacy Impact Assessment
for the
SENTRY Inmate Management System

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

Reviewed by: Luke McCormack, Chief Information Officer
Department of Justice

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

Date approved: July 2, 2012

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.

SENTRY is a real-time information system consisting of various applications for processing sensitive but unclassified (SBU) inmate information and for property management. Data collected and stored in the system includes information relating to the care, classification, subsistence, protection, discipline, and programs of federal inmates. SENTRY was developed and implemented in 1981 and continues to be updated to reflect new requirements. SENTRY has also been modernized to take advantage of web-based technologies.

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 information is collected in the system:

- Computation of sentence and supporting information;
- Information concerning pending charges, and wanted status, including warrants;
- Information relating to notification to other federal and non-federal law enforcement agencies prior to the inmate's release;
- Records of the allowance, forfeiture, withholding and restoration of good time;
- Information concerning present offense, prior criminal background, sentence and parole;
- Identification data including, but not limited to, the following:
    - Name,
    - Date of birth,
    - Social Security number,
    - Inmate register number (also known as Federal Register Number),
    - FBI number,
    - District of Columbia Department of Correction (DCDOC) Number,
    - Immigration and Customs Enforcement (formerly Immigration and Naturalization Service) Number,
    - Driver's license (if available),
    - Home address,

    - Physical description,
    - Sex,
    - Race,
    - Religious preference,
    - Photographs,
    - Digital image, and
    - Drug testing and DNA samples, test results, and analysis records;

- Institution designation and housing assignments, including separation orders, and supporting information;
- Work and payroll records;
- Program selections, assignments, skills assessments, and performance or progress reports;
- Prison conduct records, including information concerning disciplinary actions and reviews, and participation in escapes, assaults, and disturbances;
- Economic, social, and religious background, including special religious dietary requirements;
- Educational data, including industrial and vocational training;
- Physical and mental health data;
- United States Parole Commission orders, actions and related information;
- Transfer information, including dates and destinations;
- Mail and visiting records;
- Release processing information;
- Administrative remedy-related records;
- Investigatory information; and
- Referrals of non-federal inmates to Bureau custody and/or referrals of Bureau inmates to state custody.

Records are retrievable by identifying data, including name, inmate register number, FBI number, DCDOC or ICE number and/or Social Security number.

1.2 From whom is the information collected?

The information is collected from persons committed to the custody of the Attorney General, including those sentenced to terms of imprisonment and those in pre-trial custody. Information may also be collected from federal, state, local, foreign and international law enforcement agencies and personnel; federal and state prosecutors, courts and probation services; educational institutions; health care providers; relatives, friends, and other interested individuals or groups in the community; former or future employers; state, local and private corrections staff; and Bureau staff and institution contractors and volunteers.

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 serves as the primary record system on these individuals and includes information critical to the continued safety and security of federal prisons and the public.

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 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 inadvertent disclosure of sensitive information to the persons not authorized to receive it. To mitigate this risk, staff 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 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. The data is also segregated, limiting staff's ability to update inmate data unless the inmate is physically located/assigned to the local site. Data transmission is also encrypted. There is also a risk of unauthorized data modification and misuse. This risk is mitigated by enforcing access controls and encryption (as described above) and by providing auditing of user and system administration 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 information is used to manage the BOP inmate population including housing and work assignments, sentence computation and implementation, discipline, security classification, and program needs. See the System of Records Notice for the Inmate Central Records System (JUSTICE/005), 67 FR 31371 (05-09-02), modified on 72 FR 3410 (01-25-07), and soon to be further modified for a detailed list of uses.

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 used operationally each day and is "cleansed" (updated) 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). Inmates are also free to file a request pursuant to the Privacy Act and/or through the BOP's Administrative Remedy Program to review accuracy of information contained in the system.

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. Records are transferred to NARA 60 years after record creation in SENTRY or when records are no longer needed for agency use and purposes, whichever is later. The applicable retention schedule has been approved by NARA under (# N1-129-04-07).

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. System transactions are logged and exceptions are reviewed on a routine basis. Data edit checks are included in program code to ensure appropriate and accurate entry of data. Staff are routinely trained on the use and handling of information in the system.

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, U.S. Parole Commission and Office of Inspector General.

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

The offices listed in Section 4.1 have read access to routine information in the system, e.g. name, SSN, home address, birth date, race, sex, etc as well as other information such as work and unit assignments, disciplinary record, and sentencing information. 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. Access to sensitive transactions (i.e. update capability) is restricted generally to BOP staff, although some USMS users do have the ability to load inmate data into the system as part of the transit process.

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. Certain agencies receive batch downloads of data for integration with other automated systems. 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 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 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 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 as permitted by the Privacy Act, including the routine uses set forth in the aforementioned SORNs, and as otherwise permitted by law.

5.2 What information is shared and for what purpose?

Information is shared for law enforcement and court-related purposes such as investigations, possible criminal prosecutions, civil court actions, or regulatory or parole proceedings, and, prior to release of an inmate, to the chief law enforcement officer of the state and local jurisdiction in which the released inmate will reside, as required by 18 U.S.C. 4042(b). Information is also shared for other purposes in accordance with published the System of Records Notice mentioned above in Section 3.1.

5.3 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. Certain federal agencies receive batch downloads of data for integration with other automated systems in accordance with a Memorandum of Agreement. 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 via 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, as well as privacy and security requirements to protect the data. System transactions are also logged and exception reports are routinely reviewed.

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 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 allowing only certain BOP personnel to enter data and allowing individuals the opportunity to consent to non-routine uses of the information. External sharing of data also increases the privacy risks of unauthorized access and modification and misuse. Additional mitigating controls include allowing only certain BOP personnel to enter data; allowing individuals the opportunity to consent to non-routine uses of the information; and following Memoranda of Agreement requirements regarding the security and privacy of data after 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?

Notice was provided through the applicable System of Records Notice. (See Section 3.1 above.)

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 sentencing process, the initial intake and screening of the individual into custody, the re-admittance of the individual back into custody, or the release of the individual into the community.

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, e.g. disclosure to law enforcement personnel, the judiciary, etc. Individuals have the opportunity to consent to non-routine uses of the information pursuant to the Privacy Act, 5 USC Section 552a, e.g. disclosure to an academic institution with whom the inmate wishes to share his personal information.

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 Notices for BOP's inmate central records, which covers information maintained in SENTRY. 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?

Inmates may file an administrative grievance in accordance with 28 CFR Section 542.10. This program allows an inmate to seek redress for any aspect of his/her confinement, including the accuracy of information collected about him/her. Inmates may seek access to information about themselves by filing a Privacy Act Request.

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

Inmates receive notification of the procedures for filing grievances as part of the admission into each facility (i.e. the Admission and Orientation program). The relevant BOP policies regarding the Administrative Remedy Program and Privacy Act are also available in each institution law library.

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 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 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.

Staff employed by private prison contractors housing BOP inmates have access to the system.

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

Role access is controlled by terminal IDs, in conjunction with user IDs and passwords. Only certain terminals may be authorized to conduct secure web transactions (i.e. process sensitive security information).

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

User access and terminal 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.

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 and recertified on an annual basis. Each terminal is also reviewed and recertified on an annual basis. Each Memorandum of Agreement authorizing external agency use is reviewed and reauthorized, if required, on an annual basis.

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

Sentry transactions are logged; exception reports are routinely reviewed by Information Security staff, who conduct follow-up investigations regarding suspicious or unusual activity. Access to certain sensitive information or transactions (e.g. Witness Security data, sensitive medical data, etc.) requires specific authorization and is limited to certain terminals/users.

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.

All contractors and volunteers who access Bureau information or systems are required to attend initial security awareness and training during orientation. Contractors and volunteers also receive a refresher security awareness training during annual training sessions. The Information Security Programs Office is responsible for providing the information on security requirements, procedures and configuration management necessary to conduct the initial briefings for all users on SENTRY. External users are trained as to the use of the system and required to sign and acknowledge Rules of Behavior before access is granted. Memoranda of Agreement with external agencies

also require the appointment of an information security coordination to enforce the security and privacy aspects of the sharing program.

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 October 2008; and a recertification will occur in 2012.

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 Sentry 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, e.g. screen filters are used to protect display, update transactions are only available to certain approved users, and timeout/inactivity restrictions are in place. These safeguards also 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.

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?

At the time of its development twenty years ago, no viable alternative existed. Many correctional systems were using paper-based mechanisms to log and monitor their inmate populations; others were using local or decentralized databases. The BOP had an inmate information system but it provided no operational data and contained numerous errors. The decision was made to provide an operational, centralized database which could provide staff with accurate, real-time information concerning the inmate population.

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

Risk management was addressed initially through a feasibility study performed by an outside consultant. Development was also structured to minimize risks; the design phase included extensive input and meetings with subject matter staff and end-users, including the Warden's Advisory Group. Prior to full implementation, a pilot was performed first at one and then another institution. A Management Review was conducted in 1980 to assess the acceptability of SENTRY to field personnel. The study provided objective and timely input to BOP management by addressing the SENTRY IT resource requirements in accordance with SENTRY plans. Full implementation of the SENTRY system occurred in 1981. The system is being updated in 2012 to migrate to a new web-based platform and to replace outdated mainframe technology.

9.3 What design choices were made to enhance privacy?

At the time of development, the BOP considered an online system jointly supportive of BOP, the Parole Commission, the USMS and Federal Prison Industries (FPI). A security task force, which included personnel from DOJ, the National Bureau of Standards, the Association for Computing Machinery, and BOP, determined that FPI support should not be integrated with SENTRY activities due to the potential for cross talk between inmate activities and SENTRY. The Mitre Corporation performed a detailed security analysis and also recommended that FPI support come from its own dedicated computer system.

Conclusion

Since its inception, Sentry was designed to automate resource-intensive, operational functions within each institution. Each module effectively replaced extensive paper flows, therefore reducing staff time, eliminating errors, and providing for more efficient, secure operations. Any modifications or enhancements to Sentry programs continue to follow that same design goal.