Federal Bureau of Prisons

Privacy Impact Assessment
for
TRUFONE Inmate Telephone System

Issued by:
Sonya D. Thompson

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: November 29, 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.

TRUFONE is a major application maintained for processing sensitive but unclassified (SBU) inmate communication data. The data collected and stored in this system includes information about inmate telephone calls and contact information.

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?

Inmate Demographic information from Sentry
Inmate first and last name
Inmate Register Number (also known as Federal Register Number)
Housing unit
Public Safety Factor for phone abuse

Other information is also collected including:
Telephone numbers associated with inmate calling list

Biometric information – Voice Verification
Inmate call recordings
Inmate TRUFONE account balance

Volunteer Contractor Information from VCI System
Name
Home telephone
Institution/department

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. Specifically, the information is used to monitor and control communications between federal inmates and the public to gather pertinent law enforcement intelligence.

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) 31 U.S.C. 1321(a)(22). 18 U.S.C. 2510(5)(a)(ii) and 18 U.S.C. 2511(2)(c) authorize BOP to monitor and record inmate telephone calls per the "law enforcement" and "consent" provisions of Title III. See also 28 C.F.R § 540.100 et seq.

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 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. There is also a risk of unauthorized data modification

and misuse. This risk is mitigated by enforcing access controls and by providing auditing /oversight 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.

TRUFONE is a centralized inmate calling system that provides inmates with a secure, efficient and cost effective means of maintaining contact with family, friends, and the community while at the same time prevents crime, fraud and abuse by inmates. System information consists of approved inmate telephone lists and inmate's funds balance. Security features are also built-in to the system such as the capability to conduct live and remote monitoring of approved inmate phone calls.

See Systems of Records Notices for a more detailed list of uses:

- BOP-011, Telephone Activity Record System 67 FR 16762 (04-08-02).

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.)

TRUFONE does not analyze data to provide trends or patterns of unknown areas.

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

Data from this system is used operationally each day and is cleansed due to frequent use, monitoring and review. System accuracy is assured using program edit checks to prevent data/system errors. Data is stored and managed in accordance with Federal Information Security Management Act (FISMA) requirements. Inmates are also free to request record information via a Freedom of Information (FOIA).

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)?

Call recordings are stored temporarily on the system. This data is deleted in the system after 180 days or when no longer required for legal or administrative purposes.

Inmate telephone call data records and TRUFONE transactions and balances are archived annually. Records are deleted 10 years after archiving or when no longer needed for legal or administrative purposes.

The applicable retention schedule has been approved by NARA under #N1-129-05-16.

3.5 Privacy Impact Analysis: 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. TRUFONE is a role-based application that provides a means to restrict users to minimum data and processes necessary to perform their duties. Information is safeguarded in accordance with Bureau rules and policy governing automated information systems security and access (e.g. use of passwords, login restrictions, inactivity timeouts, "least-privilege" access, segregation of duties, and rotation of duties, etc.). Frequent operational use of the data makes the process of data entry transparent and therefore creates a deterrent for unauthorized data modification.

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. The system is managed with the assistance of private contractors on behalf of the BOP, who also have access to certain records.

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. 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?

Certain law enforcement agencies, as noted in 4.1 above, 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. Contractor-supported sites are annually reviewed and audited and are incorporated in the system Certification and Accreditation Plan. 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, labeling and securing sensitive output from the system, and the required use of proper passwords and user identification codes to access the system. 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 BOP personnel; individuals have the opportunity to consent to non-routine uses of the information (section 6.3); and transactions are logged (section 8.6) and suspicious activity is investigated.

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 in accordance with the earlier identified Systems of Records Notices (See Section 3.1 above).

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. Typical information shared with these entities includes names, phone numbers, call records, and recorded phone calls. Information is also shared for other purposes in accordance with the Privacy Act and the applicable system of records notice, mentioned in Section 3.1 above.

5.3 How is the information transmitted or disclosed?

External to BOP users, TRUFONE information is available electronically for viewing in the system by authorized users within the DOJ Office of Inspector General. Other DOJ agencies, as noted in Section 4.1 above, 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 persons, for 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 an electronic Rules of Behavior screen. Users must acknowledge the Rules of Behavior annually or access to the system will be denied.

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

Memoranda of Agreement include requirements for the recipient agency to maintain an audit trail of user activities.

5.7 <u>Privacy Impact Analysis</u>: 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, labeling and securing hardcopy output, and the required use of proper passwords and user identification codes to access the system.

External 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 BOP personnel and cleared contractors; individuals have the opportunity to consent to non-routine uses of the information (section 6.3); the establishment of an MOA concerning the security and privacy of data once it is shared; and the logging of transactions (section 8.6) and investigation of suspicious activity.

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 to the public is provided through the aforementioned System of Records Notice mentioned in Section 3.1 above and BOP policy. Notice is also provided to inmates during Admission & Orientation ("A&O"). Notice

of monitoring is provided to the inmates during A&O and via posted notice on the applicable telephones. Notice of monitoring to the inmate's caller is provided via pre-recording at the outset of every telephone call and is provided periodically during the phone call.

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

Inmates are required to provide information as part of the initial intake and screening process into custody or the re-admittance back into custody. Inmates are also required to provide such information in order to participate in programs, e.g. Commissary, TRUFONE, etc.

The public does have an opportunity and/or right to decline to provide information.

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?

In general, individuals do not have the opportunity to consent to routine uses of the information that are set forth in the system of records notice (e.g. disclosure to law enforcement for a criminal investigation). However, individuals do have the opportunity to consent to other uses of the information, in accordance with the Privacy Act, 5 U.S.C. Section § 552a.

6.4 <u>Privacy Impact Analysis</u>: 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) for BOP's inmate records. The information in this notice includes entities with which and situations when BOP may share investigative records. Notice is also posted in telephone locations. 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?

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 or other persons may seek access to information about themselves by filing a Privacy Act or Freedom of Information Request, subject to any applicable exemptions that may apply

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 FOIA are also available in each institution law library. Information about how to file requests for records is contained in the applicable System of Records Notices and departmental regulations.

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. Contractors who support the system are provided access after receiving an appropriate security clearance. External agency users who are approved and have an appropriate security clearance may access data in 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.

Yes, the system is supported by both BOP and contract staff who manage both the primary and secondary network operations centers. This access is documented in the system's C&A and contingency plans.

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

Role access is controlled by user groups, in conjunction with user IDs and passwords. Only certain groups may be authorized to conduct certain transactions (i.e. process certain sensitive security information) or view certain data.

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

User access and group access for an employee must be requested by a designated staff member indicating that access is required for the performance of their duties. The request and subsequent access is documented.

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, if appropriate, on an annual basis.

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

Transactions are logged and exception reports are routinely reviewed by information security staff, who conduct follow-up investigations if appropriate regarding suspicious or unusual activity. Access to certain sensitive information requires specific authorization and is limited to certain individuals.

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 45-minute 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 system users. 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 Agreements 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 updated on April 11, 2007.

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

TRUFONE is a role-based application that provides a mechanism to restrict the level of access to various screens, reports, and data based on the users position, duties, and responsibilities. However, 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.

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 technologies were evaluated and compared. The BOP had inmate information systems to enable inmate telephone calls but it did not provide the additional security features required to manage and monitor those programs. The migration of this system to a common platform enables the BOP to leverage the data and create operational efficiencies. The centralized database also provides 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. Prior to full implementation of each module and/or system, a pilot was performed first at one and then another institution to ensure that the programs functioned as designed, including maintaining security, privacy and data integrity.

9.3 What design choices were made to enhance privacy?

Data access is restricted to a “least-privilege”, need-to-know basis. Hard copy printouts of data do not contain sensitive information and screen layouts are designed to maintain individual privacy while promoting system efficiency.

Conclusion

The TRUFONE System was developed with the primary goal of providing the inmate population of the Federal Bureau of Prisons with the ability to communicate with the public in a controlled manner and environment that would alleviate any cause or concern in regards to the safety, security, and well being of any other person(s) and their privacy. Any subsequent modifications to this system will maintain this same design goal.