Federal Bureau of Prisons

Privacy Impact Assessment
for the
Trust Fund Network (TRUNET)

Issued by:
Sonya D. Thompson
Sr. Deputy Asst. Director/BOP CIO,
BOP's Senior Component Official for Privacy

Approved by: Erika Brown Lee, Chief Privacy and Civil Liberties Officer, Department of Justice

Date approved: [July 15, 2014]

Section 1: Description of the Information System

The Federal Bureau of Prisons (BOP) 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 Trust Fund Network (TRUNET) is an administrative staff network infrastructure which allows BOP to provide oversight and management of inmate funds, maintain commissary inventory[1], and sell products to inmates in the custody of the BOP. Specifically, there are applications of TRUNET that provide various services such as investigative, payroll, telephony services and electronic messaging. This Privacy Impact Assessment (PIA) is intended to cover the network infrastructure. PIAs on the applications residing on TRUNET will be conducted separately. The applications which operate on TRUNET include the following:

- **TRUFACS** - Trust Fund Accounting and Commissary System (TRUFACS). TRUFACS is a real-time information system for processing inmate financial information pursuant to commissary-related transactions. Data collected and stored in the system captures financial transactions (e.g., commissary deposits and withdrawals; purchase and resale of approved commissary products; the payment of court-ordered fines and restitution; medical co-payments, and telephone transactions). Demographic information about inmates is provided by BOP's SENTRY inmate management system. Information about inmate financial records is retrieved from the inmate (via inmate intake interviews) or federal/state courts (regarding outstanding financial obligations such as child support systems). By sending funds to inmates or receiving funds from inmates, members of the public share their name, home address, or financial information. In addition, information on vendors who supply products to institution commissaries to facilitate ordering of commissary products is contained in TRUFACS. TRUFACS includes minor applications such as TRUWEB, a read-only application which displays account

[1] In 1930, the Department of Justice authorized and established a commissary at each Federal institution. Congress first recognized the existence of the Commissary Fund in its fiscal year 1933 Department of Justice appropriation. In response to a request from Attorney General William D. Mitchell, Congress authorized DOJ to retain and use proceeds from the operation of the commissaries to pay commissary employees' salaries. See Act of July 1, 1932, Ch. 361, 47 Stat. 475, 493.

In 1934, as part of the Permanent Appropriation Repeal Act, Congress classified the Commissary Fund and the Prisoners Trust Fund as "trust funds" and provided that "[a]ll moneys accruing to these funds are hereby appropriated, and shall be disbursed in compliance with the terms of the trust." See Ch. 756, § 20(a), 48 Stat. 1224, 1233 (1934) (originally codified at 31 U.S.C. § 725s(a) (1934)). The statutory language pertaining to the Commissary Fund and Prisoners' Trust Fund has remained essentially unchanged since 1934. Today, the funds are listed as "trust funds" at 31 U.S.C. § 1321(a)(21) and (a)(22). Pursuant to 31 U.S.C. § 1321(b)(1), moneys "received by the United States Government as trustee shall be deposited in an appropriate trust fund account in the Treasury. . . [A]mounts accruing to these funds . . . are appropriated to be disbursed in compliance with the terms of the trust."

balance/deposit/withdrawal information to Unit Team staff and TRUPAID, which provides time and attendance information relating to inmate pay. Additional information on TRUFACS can be found in BOP's Privacy Impact Assessment, signed on February 10, 2014.

- **TRUVIEW** - A link analysis application, primarily used by Special Investigative Systems (SIS) staff, to assist with ongoing investigations within the BOP. TRUVIEW analyzes and compares data across multiple Trust Fund applications, which includes, but is not limited to, TRUFONE (Inmate Telephone System), TRULINCS (Inmate Message System), and TRUFACS, which provides users with pertinent investigative information. It also leverages data from the Web Visiting System so that, for example, TRUVIEW can display common phone numbers, email addresses, and/or physical addresses of where funds were sent to or received from across the inmate population of the BOP as compared to visitor information.

- **TRUWEB** – An application used by various non-financial management staff within the BOP in order to view inmate financial information contained in TRUFACS. TRUWEB makes pertinent TRUFACS data available in a read-only format for these individuals. There is no data generated from this application as this application is only a web interface of information contained in TRUFACS.

- **TRUINTEL** – An application for Special Investigative Systems (SIS) staff to manage institution investigations and cases. It includes information relating to inmate gang affiliations, informants, referrals for criminal prosecution, subpoena requests, investigative case files, evidence collection and storage, and reports.

- **TRUPAID** – Trust Fund Accounting for Inmate Details. TRUPAID is a module of TRUFACS that provides the software to process Inmate Performance Payrolls (IPP) and provides budgeting and reporting information. TRUPAID interfaces with TRUFACS, which eliminates the need for manual entry of inmate data to determine pay grades and drug treatment and financial responsibility participation.

- **TRUSEEQ** – An application developed for institution Executive Staff that provides a high-level overview of the following TRUNET applications: TRUFACS, TRUFONE, TRULINCS, TRUINTEL, TRUPAID, and TRUVIEW.

- **TRUTRAC** – An inventory application used by institutions to monitor, order, track, and requisition inmate and general supplies within each BOP institution. Data stored on TRUNET in regards to TRUTRAC includes: vendor name, vendor address, vendor phone number, and inventory information.

Access to TRUNET is controlled via a Lightweight Directory Authentication Protocol (LDAP) service and an access control interface called TRUACCESS[2] which uniquely identifies each user and requires a strong NIST-compliant password. The TRUACCESS and TRUNET LDAP directory contains staff and contractor first and last names, userID, duty location, email address, work address and phone number(s). All TRUNET services (e.g., helpdesk, application access, etc.) require LDAP authentication. Application access, which is web-based, uses secure socket layer (SSL) encryption.

The TRUNET user community includes BOP staff, DOJ staff detailed to BOP locations, and contractor staff who have an appropriate security clearance. TRUNET communications with other BOP and DOJ networks occur via the Justice Unified Telecommunications Network (JUTNet) infrastructure, which is encrypted site-to-site and controlled via JUTNet firewalls. TRUNET is not connected to the internet. TRUNET is an existing system that has been operational since June of 2002. The development and deployment of a number of various applications have been added to TRUNET since that date. In addition, there have been a number of changes to the system including, but not limited to, conversion from paper-based records to an electronic system, a new use of an IT system, and changes in the system that have resulted in information in identifiable form being merged, centralized, or matched with other databases.

This Privacy Impact Assessment (PIA) applies only to the TRUNET infrastructure. Privacy implications for the applications which reside on TRUNET are explained in further detail in individual PIAs (as applicable) for the specific applications.

Section 2: Information in the System

2.1 Indicate below what information is collected, maintained, or disseminated. (Check all that apply.)

Identifying numbers					
Social Security		Alien Registration		Financial account	
Taxpayer ID		Driver's license		Financial transaction	
Employee ID		Passport		Patient ID	
File/case ID		Credit card			
Other identifying numbers (specify):					

[2] TRUACCESS is an application developed to provide a standard secure means of managing and providing access to all current and future Trust Fund applications that exist on TRUNET. This application is used to: request/approve access to specific Trust Fund application groups; provide a portal to access all Trust Fund applications; and perform annual certification of user accounts. The types of data stored on TRUNET for this application include: user names, userIDs, application groups, and user forms.

General personal data					
Name	X	Date of birth		Religion	
Maiden name		Place of birth		Financial info	
Alias		Home address		Medical information	
Gender		Telephone number		Military service	
Age		Email address	X	Physical characteristics	
Race/ethnicity		Education		Mother's maiden name	
Other general personal data (specify):					

Work-related data					
Occupation		Telephone number		Salary	
Job title	X	Email address	X	Work history	
Work address		Business associates			
Other work-related data (specify):	Staff and contractors' duty locations.				

Distinguishing features/Biometrics					
Fingerprints		Photos		DNA profiles	
Palm prints		Scars, marks, tattoos		Retina/iris scans	
Voice recording/signatures		Vascular scan		Dental profile	
Other distinguishing features/biometrics (specify):					

System admin/audit data					
User ID	X	Date/time of access	X	ID files accessed	
IP address	X	Queries run		Contents of files	
Other system/audit data (specify):					

Other information (specify)
The identifiable information on individuals checked in Section 2.1 pertains only to the government employees and/or contractors who manage and use TRUNET. Identification and analysis of the information collected, maintained, or disseminated on the applications residing on TRUNET will be discussed in the applicable PIAs for such applications.

TRUNET contains staff and contractor first and last names, duty location, email address, work address and phone number(s). As part of IT security audits and routine security monitoring, the data is used to uniquely identify users on the network and verify their authorization to access individual systems. Personally identifiable information (PII) is restricted and accessed only by IT systems and application administrators for system security and role management purposes; this PII data is not accessible to ordinary end-users.

2.2 Indicate sources of the information in the system. (Check all that apply.)

Directly from individual about whom the information pertains							
In person		X	Hard copy: mail/fax			Online	
Telephone		X	Email		X		
Other (specify):	Helpdesk Ticket						

Government sources					
Within the Component	X	Other DOJ components		Other federal entities	
State, local, tribal		Foreign			
Other (specify):					

Non-government sources					
Members of the public		Public media, internet		Private sector	
Commercial data brokers					
Other (specify):					

2.3 Analysis: Now that you have identified the information collected and the sources of the information, please identify and evaluate any potential threats to privacy that exist in light of the information collected or the sources from which the information is collected. Please describe the choices that the component made with regard to the type or quantity of information collected and the sources providing the information in order to prevent or mitigate threats to privacy. (For example: If a decision was made to collect less data, include a discussion of this decision; if it is necessary to obtain information from sources other than the individual, explain why.)

There is a privacy risk related to the inadvertent disclosure of sensitive information to persons not authorized to receive it. To mitigate this risk, staff is annually trained on how to properly handle sensitive information and required to undergo information security awareness training prior to gaining access to any BOP system or data. Access to any relevant system or application is limited to those persons who have an appropriate security clearance, which is regularly reviewed, and to persons who have an official need to access such information.

The system includes design choices to ensure that privacy protections are ensured for the sensitive information stored therein. For example, the system uses role-based management to ensure that users can only access and manipulate data in relation to their functional duties and job locations. In other words, users are assigned system permissions equivalent to the level of access necessary for him or her to perform their professional work duties.

Considerations were also made regarding the security and protection of such data to ensure that the system complies with applicable privacy regulations and requirements for the protection of sensitive data. For example, the system is designed to ensure that user accounts are disabled promptly upon staff separation. In general, 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 to access the system. Data transmission in the system is also encrypted.

Section 3: Purpose and Use of the System

3.1 Indicate why the information in the system is being collected, maintained, or disseminated. (Check all that apply.)

Purpose			
	For criminal law enforcement activities		For civil enforcement activities
	For intelligence activities	X	For administrative matters
	To conduct analysis concerning subjects of investigative or other interest		To promote information sharing initiatives
	To conduct analysis to identify previously unknown areas of note, concern, or pattern.		For administering human resources programs
	For litigation		
X	Other (specify): Personal information is collected to create unique user accounts for staff and contractors that need access to applications residing on the TRUNET infrastructure.		

3.2 Analysis: Provide an explanation of how the component specifically will use the information to accomplish the checked purpose(s). Describe why the information that is collected, maintained, or disseminated is necessary to accomplish the checked purpose(s) and to further the component's and/or the Department's mission.

Pursuant to 31 U.S.C. § 1321(b)(1), the BOP is tasked with depositing and dispersing commissary funds on behalf of inmates. The purpose of TRUNET is to provide the infrastructure and support for the Trust Fund Branch applications used to manage commissary operations and services, as described in Section 1.

3.3 Indicate the legal authorities, policies, or agreements that authorize collection of the information in the system. (Check all that apply and include citation/reference.)

	Authority	Citation/Reference
X	Statute	31 U.S.C. § 1321; see also generally, 18 U.S.C. §§ 3621, 4042 (for those inmates sentenced prior to the Sentence Reform Act of 1984), and 5003; and 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. 105-333; 111 Stat. 740).
	Executive Order	
	Federal Regulation	28 C.F.R. Part 506
	Memorandum of Understanding/agreement	
	Other (summarize and provide copy of relevant portion)	

3.4 Indicate how long the information will be retained to accomplish the intended purpose, and how it will be disposed of at the end of the retention period. (Reference the applicable retention schedule approved by the National Archives and Records Administration, if available.)

User account data is maintained in the system so long as the user account remains active. If not subject to a litigation hold, the user account is disabled and eventually deleted in accordance with federal IT security requirements and account management controls (e.g., National Institute of Standards and Technology (NIST) Special Publication 800-53, "Recommended Security Controls for Federal Information Systems and Organizations", Revision 4, April 30, 2013). The applications which reside on TRUNET have separate records schedules which govern data retention which reside therein. For instance, the applicable retention schedule for TRUFACs has been approved by NARA under #N1-129-05-07.

3.5 Analysis: Describe any potential threats to privacy as a result of the component's use of the information, and controls that the component has put into place to ensure that the information is handled, retained, and disposed appropriately. (For example: mandatory training for system users regarding appropriate handling of information, automatic purging of information in accordance with the retention schedule, etc.)

Access to the system is limited to those persons who have an appropriate security clearance, which is

regularly reviewed (user accounts are reviewed on a quarterly basis and recertified on an annual basis). TRUNET is a role-based infrastructure 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.).

In addition, BOP 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. They 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.

Also, all contractors and volunteers who access Bureau information or systems are required to attend initial security awareness and training during orientation. Contractors and volunteers receive an additional 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.

Section 4: Information Sharing

4.1 Indicate with whom the component intends to share the information in the system and how the information will be shared, such as on a case-by-case basis, bulk transfer, or direct access.

Recipient	How information will be shared			
	Case-by-case	Bulk transfer	Direct access	Other (specify)
Within the component	X		X	
DOJ components				
Federal entities				
State, local, tribal gov't entities				
Public				
Private sector				
Foreign governments				
Foreign entities				
Other (specify):				

4.2 Analysis: Disclosure or sharing of information necessarily increases risks to privacy. Describe controls that the component has put into place in order to prevent or mitigate threats to privacy in connection with the disclosure of information. (For example: measures taken to reduce the risk of unauthorized disclosure, data breach, or receipt by an unauthorized recipient; terms in applicable MOUs, contracts, or agreements that address safeguards to be implemented by the recipient to ensure appropriate use of the information – training, access controls, and security measures; etc.)

Information about users and accounts in TRUNET are not shared. Various controls are employed on TRUNET to prevent threats to privacy. Access to the network is limited to those persons who have an appropriate security clearance and are authorized to view the data residing therein. Information is safeguarded in accordance with Bureau rules and policy governing automated information systems security and access (e.g., users must use a unique user ID and password in order to authenticate and use the system, access to the system must be requested and approved by a supervisor, and user accounts are routinely reviewed). All system users are also required to attend Security Awareness Training annually and users with administrative privileges (e.g., network administrators) are required to complete security awareness training for privileged users. Further, users are notified of rules and procedures regarding access to the information contained in TRUNET and its applications, and are required to sign and acknowledge a Rules of Behavior document.

Data contained within TRUNET's applications are shared with various law enforcement components within the Department of Justice (e.g., FBI, U.S. Marshal's Service, EOUSA, Criminal Division, U.S. Parole Commission, and the Office of Inspector General), as well as external parties (e.g., federal, state, local, etc.) for purposes of criminal law enforcement investigations, criminal prosecutions, civil court actions, or regulatory or parole proceedings. Again, the Privacy Impact Assessment for the applicable TRUNET application explains this sharing in more detail, as well as the safeguards in mitigating any potential privacy risks related to intentional, unauthorized access, or inadvertent disclosure of sensitive information to persons not authorized to receive it.

Section 5: Notice, Consent, and Redress

5.1 Indicate whether individuals will be notified if their information is collected, maintained, or disseminated by the system. (Check all that apply.)

X	Yes, notice is provided pursuant to a system of records notice published in the Federal Register and discussed in Section 7.	
	Yes, notice is provided by other means.	Specify how:
	No, notice is not provided.	Specify why not:

5.2 Indicate whether and how individuals have the opportunity to decline to provide information.

	Yes, individuals have the opportunity to decline to provide information.	Specify how:
X	No, individuals do not have the opportunity to decline to provide information.	Specify why not: Individuals must provide identifiable information so that they can be uniquely identified in the system and be provided access to the system. The information is also used for system security and IT-related audits.

5.3 Indicate whether and how individuals have the opportunity to consent to particular uses of the information.

X	Yes, individuals have an opportunity to consent to particular uses of the information.	Specify how: Individuals have the opportunity to consent to non-routine uses specified in the SORN in subsection 7.1 below (e.g., disclosure to a financial organization). If the request for information is non-routine and the individual has not previously provided consent, the individual will be contacted to notify him/her of the request and determine if they consent to the disclosure.
X	No, individuals do not have the opportunity to consent to particular uses of the information.	Specify why not: Individuals do not have the opportunity to provide consent for authorized disclosures made pursuant to 5 U.S.C. 552a(b) (e.g., disclosures made to law enforcement agencies for purposes of a criminal investigation).

5.4 Analysis: Clear and conspicuous notice and the opportunity to consent to the collection and use of individuals' information provides transparency and allows individuals to understand how their information will be handled. Describe how notice for the system was crafted with these principles in mind, or if notice is not provided, explain why not. If individuals are not provided the opportunity to consent to collection or use of the information, explain why not.

Notice to individuals is provided via the System of Records Notice DOJ-002, "DOJ Computer Systems Activity & Access Records," published 64 FR 73585 (12/30/11) and as amended, 66 FR 8425 (1/21/01); 72 FR 3410 (1/25/07), which describes the information collected and purpose for the collection.

Section 6: Information Security

6.1 Indicate all that apply.

X	The information is secured in accordance with FISMA requirements. Provide date of most recent Certification and Accreditation: March 15, 2013 If Certification and Accreditation has not been completed, but is underway, provide status or expected completion date:	
X	A security risk assessment has been conducted and completed as of March 27, 2014	
X	Appropriate security controls have been identified and implemented to protect against risks identified in security risk assessment. Specify: TRUNET is a closed network (no internet access). IT Support staff maintain and follow a patch management plan, deploy and maintain network protection devices such as firewalls, Intrusion Prevention Systems (IPS), and encryption software and enforce IT security controls such as unique user IDs and use of strong passwords.	
X	Monitoring, testing, or evaluation has been undertaken to safeguard the information and prevent its misuse. Specify: A change control process is employed by the Trust Fund Branch ensuring all system changes are approved, tested, and validated prior to implementation in the production environment.	
X	Auditing procedures are in place to ensure compliance with security standards. Specify, including any auditing of role-based access and measures to prevent misuse of information: An annual certification of users is conducted to ensure that appropriate permissions are maintained by users.	
X	Contractors that have access to the system are subject to provisions in their contract binding them under the Privacy Act.	
X	Contractors that have access to the system are subject to information security provisions in their contracts required by DOJ policy.	
X	The following training is required for authorized users to access or receive information in the system:	
	X	General information security training
		Training specific to the system for authorized users within the Department.
		Training specific to the system for authorized users outside of the component.
		Other (specify):

6.2 Describe how access and security controls were utilized to protect privacy and reduce the risk of unauthorized access and disclosure.

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 (e.g., use of passwords, login restrictions, inactivity timeouts, "least-privilege" access, user accounts are routinely reviewed, segregation of duties, and rotation of duties). Each user's access is reviewed and recertified, if appropriate, on an annual basis.

TRUNET contains staff and contractor first and last names, duty location, email address, work address and phone number(s). As part of IT security audits and routine security monitoring, the data is used to uniquely identify users on the network and verify their authorization to access individual systems. Personally identifiable information (PII) is restricted and accessed only by IT systems and application administrators for system security and role-management purposes. PII is not accessible to ordinary end-users of TRUNET.

Section 7: Privacy Act

7.1 Indicate whether a system of records is being created under the Privacy Act, 5 U.S.C. § 552a. (Check the applicable block below and add the supplementary information requested.)

X	Yes, and this system is covered by an existing system of records notice. Provide the system name and number, as well as the Federal Register citation(s) for the most recent complete notice and any subsequent notices reflecting amendment to the system DOJ-002, "DOJ Computer Systems Activity & Access Records," 64 FR 73585 (Dec. 30, 1999), amended, 66 FR 8425 (Jan. 31, 2001); 72 FR 3410 (Jan. 25, 2007).
	Yes, and a system of records notice is in development.
	No, a system of records is not being created.

7.2 Analysis: Describe how information in the system about United States citizens and/or lawfully admitted permanent resident aliens is or will be retrieved.

Information about individuals in TRUNET itself, and not its applications, is retrieved by first name and last name or userID. This information is retrievable only by BOP system administrators (staff and contractors).