Federal Bureau of Prisons

Privacy Impact Assessment
for the
Trust Fund Accounting System (TRUFACS)

Issued by:
Sonya D. Thompson
Sr. Deputy Asst. Director/BOP CIO

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

Date approved: [February 14, 2014]

Section 1: Description of the Information System

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.

TRUFACS is a real-time information system for processing inmate financial information pursuant to commissary-related transactions.[1] 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 inmates (via intake interviews) or federal/state courts (regarding outstanding financial obligations such as child support payments). By sending funds to inmates or receiving funds from inmates, members of the public share their name, home address or financial information (negotiable instruments/checks). 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 balance/deposit/withdrawal information to Unit Team staff and TRUPAID, which provides time and attendance information relating to inmate pay.

TRUFACS is accessed via the Trust Fund Network (TRUNET) and controlled via a Lightweight Directory Authentication Protocol (LDAP) service which uniquely identifies each user and requires a NIST-compliant strong password. All application access, which is web-based, uses secure socket layer (SSL) encryption. TRUFACS is accessed only by BOP employees and contractors, who assist in the management of the system.

---

[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."

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	X
Taxpayer ID		Driver's license		Financial transaction	X
Employee ID		Passport		Patient ID	
File/case ID		Credit card			
Other identifying numbers (specify):					

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

Work-related data					
Occupation	X	Telephone number		Salary	X
Job title	X	Email address		Work history	
Work address		Business associates			
Other work-related data (specify):					

Distinguishing features/Biometrics					
Fingerprints	X	Photos	X	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		Date/time of access		ID files accessed	
IP address		Queries run		Contents of files	
Other system/audit data (specify):					

Other information (specify)
See Attachment A for a complete listing of information maintained in the system.

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		X	Online	
Telephone		Email				
Other (specify):					

Government sources					
Within the Component		X	Other DOJ components		Other federal entities	X: Federal courts
State, local, tribal	X: State courts		Foreign			
Other (specify):	BOP SENTRY Inmate Management System					

Non-government sources					
Members of the public		X	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. There is also the 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. Access to any relevant system 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 in place for sensitive information (financial data) stored therein. For example, the system collects only core inmate demographic data sufficient to identify the inmate involved in the transaction. Other data, such as case management or sentence-related data is not collected or maintained. Additionally, the system uses role-based management to ensure that users can only access and manipulate data in relation to their functional duties. 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. For instance, accounting technicians would only have access to all accounting related screens, but not access to inventory or sales screens. Also, Warehouse/Commissary staff members have access only to specific areas related to managing the ordering, receipt, and sales of inventory. Finally, BOP's Unit Team Staff are only provided 'read only' permissions to monitor account balances and transactions.

The security and protection of case management or sentence-related data was also considered 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 inmate financial transactions are maintained in the same record regardless of whether an inmate's period of confinement is interrupted by release.

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			
X	For criminal law enforcement activities	X	For civil enforcement activities
	For intelligence activities		For administrative matters
X	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		
	Other (specify):		

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.

TRUFACS is a real-time information system for processing inmate financial transactions pursuant to commissary-related deposits and withdrawals. Data collected and stored in the system captures financial transactions (e.g., commissary deposits and withdrawals; the payment of court-ordered fines and restitution; court-ordered child support; medical co-payments, vendor information for providing resale products, and telephone transactions). Information contained in TRUFACS is also necessary for investigative purposes to track suspicious communications, events and transactions, in order to detect potential patterns of criminal activity or fraud (e.g., deposits from unauthorized sources). In general, collection of this information by BOP staff is necessary to meet its federal law obligations, as cited below, to provide managerial oversight and maintain record-keeping responsibility for all financial transactions conducted by current and former inmates.

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 USC 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. 105-33; 111 Stat. 740).
	Executive Order	
X	Federal Regulation	28 CFR 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.)

Scanned files, including BP Form-199s (inmate authorization for repeating monthly withdrawals, etc.).
Disposition: Temporary. Destroy 90 days after verification.

Data entered directly into the system, such as inmate payroll and purchases; funds received from outside sources; and voided transactions. **Disposition:** Temporary. Hard-copy files are maintained for seven years. Electronic records are archived annually when six years old from the date of transaction, and purged seven years from the date of archive, totaling 13 years. System-generated reports (e.g., reconciliation reports; inmate payroll reports) are retained for as they as they are needed. The applicable retention schedule has been approved by NARA under #N1-129-05-7.

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.)

There is a privacy risk related to unauthorized data modification and misuse as a result of BOP's use of the information. This risk is mitigated by enforcing access controls and by providing auditing/oversight of user and system administration activities. Access to any relevant system 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. 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.).

Further, frequent operational use of the data makes the process of data entry transparent and therefore creates a deterrent for unauthorized data modification. For example, purchases in the Commissary must be made using the inmate's ID card or fingerprint. These purchases are then matched against the inventory and reconciled against the inmate's individual balance. Any discrepancies are resolved against the overall books for the commissary fund. This reconciliation process ensures data accuracy in the system and deters employees from making any unapproved data modifications 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). Financial records are reconciled and managed in accordance with Federal Information System Controls Audit Manual (FISCAM) and financial audit requirements. Inmates are also free to request record information via a Freedom of Information (FOIA) request to review the accuracy of their information contained in the system, and to ensure that the information is handled and retained appropriately.

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	
DOJ components		X		
Federal entities	X			
State, local, tribal gov't entities	X			
Public				
Private sector				
Foreign governments				
Foreign entities				
Other (specify):				

Data is shared within BOP and 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. These entities may receive batch downloads of data for integration with other automated systems or the information may be printed and provided to such offices in hard copy. Other federal agencies receive batch downloads of data for integration with other automated systems in accordance with a Memorandum of Agreement. These agencies typically receive information on the source and destination addresses for funds received as well as transactional information for purposes of criminal law investigations. The system is managed with the assistance of private contractors, who also have access to records in the system. Private contracts are subject to the same security requirements as BOP employees.

Additionally, information may be shared with state, local, tribal law enforcement agencies and court officials. The data is shared with these entities for law enforcement and court-related purposes such as criminal and civil investigations, possible criminal prosecutions, civil court actions, regulatory or parole proceedings, or in accordance with the routine uses identified in applicable Systems of Records Notices. Typical information shared with these entities includes names, financial transactions, and addresses. State agencies may access the data via an approved regional information sharing program

with the Department of Justice Law Enforcement Information Sharing initiative (aka "OneDOJ"). Information may also be printed and provided to such entities in hard copy. Hard copy information is handled in accordance with information security policy and directives relating to the handling of sensitive information.

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.)

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. Further, 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 certain uses of the information (e.g., inmate correspondents have an opportunity and/or right to decline to provide information, however inmates may not receive funds from those individuals.); the establishment of an MOA, where applicable, concerning the security and privacy of data once it is shared; and the logging of transactions in the system and investigation of suspicious activity.

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.	
X	Yes, notice is provided by other means.	Specify how: Admission and Orientation sessions conducted when the inmate first arrives at an institution. Vendors are provided notice when providing their Tax Id number prior to purchase of vendor's products.
	No, notice is not provided.	Specify why not:

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

X	Yes, individuals have the opportunity to decline to provide information.	Specify how: The public does have an opportunity and/or right to decline to provide information; however, inmates may not receive funds from those individuals. In addition, vendors are not required to provide information, but by declining to do so will forfeit their ability to do business with BOP.
X	No, individuals do not have the opportunity to decline to provide information.	Specify why not: 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 the Commissary program.

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: Vendors have the opportunity to consent, prior to placing an order, to BOP's use of their financial information in order to do business with them. Individuals do have the opportunity to consent to other uses of the information, (e.g., litigation inquiries for which the United States isn't a party in the proceeding; inquiries from another inmate pursuant to a FOIA request, etc.).
X	No, individuals do not have the opportunity to consent to particular uses of the information.	Specify why not: Information on inmates (e.g. any funds the inmate may have in their possession at the time of entry) is required to be provided for administration purposes (e.g., as part of 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).

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 BOP's System of Records Notice (SORN) BOP-006, "Inmate Trust Fund Accounts and Commissary Record System," (67 FR 11711, March 15, 2002, amended by 72 FR 3410, January 25, 2007), which describes the information collected and purpose for the collection. Additionally, inmates are informed about the process to use the Commissary and how to receive and dispense funds from their Commissary account during Admission and Orientation when they arrive at a BOP facility. Also, when individuals send negotiable instruments to BOP inmates via Western Union or MoneyGram, they sign a consent form indicating that the information they provide must be complete and accurate; and that per U.S. federal law, they obtain, verify, and record information that identifies each person who initiates a transfer through its services. Further, vendors are provided notice, prior to purchase, that their financial information is needed in order to do business with BOP and the federal government,

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: June 11, 2012 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 May 1, 2013.
X	Appropriate security controls have been identified and implemented to protect against risks identified in security risk assessment. Specify: TRUFACS resides on the Trust Fund Branch network known as TRUNET. TRUNET is a closed network without internet access available to its users. IT support staff maintain and follow a patch management plan, and the security controls for the network include firewalls, Intrusion Prevention Systems (IPS), and encryption software and procedures.
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, which is regularly reviewed. TRUFACS 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. For example, purchases in the Commissary must be made using the inmate's ID card or fingerprint. These purchases are then matched against the inventory and reconciled against the inmate's individual balance. Any discrepancies are resolved against the overall books for the commissary fund.

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: BOP-006, "Inmate Trust Fund Accounts and Commissary Record System", 67 FR 11711, March 15, 2002, amended 72 FR 3410, January 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 inmates is retrieved via federal register number and by name. Vendor information is retrieved by name.

ATTACHMENT A

I. Inmate information from Sentry:

- Register Number
- First Name
- Last Name
- Date of Birth
- Sex
- Financial Responsibility Program Participation Status
    - Amount
    - Type
    - Frequency
    - Percentage
- Alias Names
- Nicknames
- Race
- Ethnicity
- Citizenship
- Photograph
- Fingerprints (to uniquely identify inmates)

II. Inmate information from TRUFACS:

- Financial Information (commissary balance, deposits, withdrawals, etc.)

III. Information from persons sending funds to inmates or receiving funds:

- An image of the envelope is captured which may contain First Name, Last Name, and Home Address)
- An image of the negotiable instrument is captured (e.g., check)