FEDERAL BUREAU OF PRISONS
PRIVACY IMPACT ASSESSMENT (PIA)

System Name:	**TruNet**		
OMB Control # For Information Collections (If Available):			
OMB Unique Identifier For IT Systems (If Available):		011-20-01-01-01-2602-00-102-005 011-20-01-01-01-2709-00-102-005	
Program Area SME:	Mike Atwood	**Telephone:**	(202) 307-3144
Job Title:	Chief, Trust Fund Branch		
IT Project SME:	Rich Esteves	**Telephone:**	(202) 616-7000
Job Title:	Chief, IT Section		
Date:	4/14/06		

Please submit the completed form to the Chief – IT Planning & Development in the Office of Information Systems (OIS). If any question does not apply, state "Not Applicable (N/A)" and briefly explain why it is not applicable.

Part A: Is A PIA Required?

Instructions for this part: If you answer "no" to all of Questions 1-4 below, please briefly describe the IT system being exempted in Part B.1, and submit this document for review and approval. If you answer "yes" to any of Questions 1-4, continue to Question 5.

1. Are you developing or procuring a new IT system or project that collects, maintains, or disseminates information:
   a. about U.S. citizens or aliens lawfully admitted for permanent residence; and
   b. that does NOT pertain only to government employees or contractors?

   No

2. Are you initiating a new electronic collection of information under the Paperwork Reduction Act?

   No

3. Are you making a change to an existing IT system that creates new privacy risks? For example:

a. Are you applying a new technology to an existing system that significantly changes how information is managed in the system?

Yes.

b. Are you making a change in business processes:

i. that merges, centralizes, matches or otherwise significantly manipulates existing databases? Yes

ii. that results in significant new uses or disclosures of information or incorporation into the system of additional information? No

c. If this information has been collected previously:

i. Are new or significantly larger groups of people being impacted?[1] No

ii. Is new data being added resulting in new privacy concerns? No

iii. Is data being added from a commercial or public source? No

4. Is this information individually identifiable? (Does it pertain to specific individuals who can be identified either directly or in conjunction with other data?) If no, do not answer any more questions and submit this document for review under the PIA process. If yes, continue to the next question.

Yes

5. Has a PIA or similar evaluation been conducted? If yes, does the existing PIA address the questions in Part Two? If yes, submit the existing PIA with this document for review under the PIA process. If no, continue to Question 6.

Yes, a PIA already exists for part of this system. (See Attachment A. The PIA is being updated to reflect the updated 2006 BOP PIA Guidance.)

6. Is this a national security system as defined at 40 U.S.C. 11103? If yes, please attach verification and submit this document for review under the PIA process.

[1] This includes new electronic collections of information in identifiable form for 10 or more persons (excluding agencies, instrumentalities, or employees of the federal government). See 44 USC Chapter 35 and implementing regulations, 5 CFR Part 1320.8.

Part B: Provide a brief description of what personal information is collected.

1. Please provide a general description of the system, including its purpose.

The Trust Fund Network is the Bureau's infrastructure for inmate trust fund related systems including the Trust Fund Accounting and Commissary System (TRUFACS) and the Inmate Telephone System (ITS). TRUFACS is the Bureau's inmate trust fund accounting system. The primary purpose of the system is to oversee inmate monies and track commissary inventories. Additional functionality has been added to the system to include inmate payroll, investigative capabilities, and phone account maintenance.

ITS-3 is a 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.

Other Trust Fund-related applications run on the Trust Fund Network and databases may be cross-linked for analysis and security purposes.

2. If this automated system (or Information Collection Request) involves personally identifiable information on members of the public, then *place an 'X' in any of the categories that apply below:*

Personal Identifiers:

Name	X
Social Security Number (SSN) .	X
Other identification number (specify type):	X (inmate register number)
Birth date	X
Home address	X
Home telephone	X
Personal e-mail address	X
Fingerprint/other "biometric"	
Other (specify):	X (Approved phone numbers on the inmate's phone list)
None	
Comment: **See Attachment B for additional data elements**	

Other Sensitive Information:

Race/ ethnicity	X
Gender/ sex	X
Marital status	
Spouse name	X (relationship status only; no

	names)
# of children	
Employment history	
Education level	X
Medical history/information	
Disability	
Criminal record	
Financial Data (salary, accounts, etc.)	X (inmate deposit fund account)
Other (specify):	
Comment: **See Attachment B for additional data elements**	

3. Type of electronic system or information collection. Fill out Section A, B, or C as applicable.

A. If a new electronic system (or one in development): Is this a new electronic system (implemented after April 2003, the effective date of the E-Government Act of 2002)?

No. System infrastructure was originally implemented in 2002.

B. If an existing electronic system: Mark any of the following conditions for your existing system that OMB defines as a "trigger" for requiring a PIA (if not applicable, mark N/A):

Conversion: When paper-based records that contain personal information are converted to an electronic system	X (Note: conversion was from old electronic system to newer system)
From Anonymous (Non-Identifiable) to "Non-Anonymous" (Personally Identifiable): When any systems application transforms an existing database or data collection so that previously anonymous data becomes personally identifiable	
Significant System Management Changes: When new uses of an existing electronic system significantly change how personal information is managed in the system. (Example #1: when new "relational" databases could combine multiple identifying data elements to more easily identify an individual. Example #2: when a web portal extracts data elements from separate databases, and thereby creates a more open environment for exposure of personal data)	
Merging Databases: When government databases are merged, centralized, matched, or otherwise significantly manipulated so that personal information becomes more accessible (with special	X (data from various BOP systems is

concern for the ability to combine multiple identifying elements)	compared for analysis)
New Public Access: When new public access is given to members of the public or to business partners (even if the system is protected by password, digital certificate, or other user-authentication technology)	
Commercial Sources: When agencies systematically incorporate into databases any personal data from commercial or public sources (ad hoc queries of such sources using existing technology does not trigger the need for a PIA)	
New Inter-agency Uses: When agencies work together (such as the federal E-Gov initiatives), the lead agency should prepare the PIA	
Business Process Re-engineering: When altering a business process results in significant new uses, disclosures, or additions of personal data	
Alteration in Character of Data: When adding new personal data raises the risks to personal privacy (for example, adding financial information to an existing database that contains name and address)	

C. If an Information Collection Request (ICR): Is this a new Request that will collect data that will be in an automated system? Agencies must obtain OMB approval for information collections from 10 or more members of the public. The E-Government Act of 2002 requires a PIA for ICRs only if the collection of information is a new request and the collected data will be in an automated system.

Yes, this is a new ICR and the data will be automated	N/A
No, the ICR does not require a PIA because it is not new or automated)	N/A
Comment:	N/A

4. Why is the personally identifiable information being collected? How will it be used? Mark any that apply:

General:

Inmate Visiting	
Inmate Correspondence	
Inmate Telephone Calling List	X
Employment Application	
FOIA/PA Request	
Litigation/Administrative Claim	

Inmate Financial Management	X
Institution Security	X
Other (specify):	

Internal operations:

Employee payroll or personnel records	
Payment for employee travel expenses	
Payment for services or products (to contractors) – if any personal information on the payee is included	
Computer security files – collected in order to grant network/system access	
Other (specify):	
Comment:	

Other lines of business (specify uses):

5. Will you share the information with others (e.g., another agency for a programmatic purpose, or outside the government)? Mark any that apply:

Federal agencies? (specify):	X (FBI, DEA, federal judiciary – upon subpoena, and other federal agencies for legitimate law enforcement purposes)
State, local, or tribal governments?	X (Yes, for legitimate law enforcement purposes)
Contractors?	X (Contractors supporting the system)
Others? (specify):	
Comment:	

6. Can individuals "opt-out" by declining to provide personal information or by consenting only to particular use (e.g., allowing their personal information to be used for basic visiting eligibility determination, but for not for sharing with other government agencies)?

Yes, they can "opt-out" by declining to provide private information or by consenting only to particular use	
No, they can't "opt-out" – all personal information is required	X

Comment:	

If Yes, please explain the issues and circumstances of being able to opt-out (either for specific data elements or specific uses of the data):

7. How will the privacy of the information be protected/secured? What are the administrative and technological controls? Mark any that apply and give details if requested:

System is only accessible to law enforcement personnel	X (and approved, cleared contractors)
System users must log-in with a password	X (passwords changed every 90 days)
When an employee leaves: • How soon is the user ID terminated (1 day, 1 week, 1 month, unknown)? • How do you know that the former employee no longer has access to your system? (explain your procedures or describe mitigating controls):	1 day User accounts are reviewed on a quarterly basis and recertified on an annual basis. Employee HR exit procedures include notification to IT staff regarding departures of employees.
Are access rights selectively granted, depending on duties and need-to-know? If Yes, specify the approximate # of authorized users who have either: • Full access rights to all data in the system (specify #)? • Limited/restricted access rights to only selected data (specify #)?	Approx. 10 (hdqtrs only) Up to 24,000 users who are monitoring phone calls live

Are disks, tapes, and printouts that contain personal information locked in cabinets when not in use? (explain your procedures, or describe mitigating controls):	Yes, sensitive information is secured from inadvertent disclosure. Required handling of sensitive information is described in Program Statement 1237.13 "Information Security Programs"
If data from your system is shared with another system or data warehouse, who is responsible for protecting the privacy of data that came from your system but now resides in another? Explain the existing privacy protections, or mitigating controls:	Authorized disclosure of sensitive information is described in Program Statement 1351.05 "Release of Information"
Other methods of protecting privacy (specify):	
Comment:	

8. If privacy information is involved, by what data elements can it be retrieved?
Mark any that apply:

Name:	X
Social Security Number (SSN)	
Identification number (specify type)	X (inmate register number)
Birth date	
Race/ ethnicity	
Home address	
Home telephone	
Personal e-mail address	
Other (specify):	
None	
Comment: See Attachment B for a list of data elements collected in the system	

Other Comments (or details on any Question above):

PART C: DETERMINATION BY BOP PRIVACY OFFICER

_____ _____

Wanda Hunt Date
BOP Privacy Officer/Advocate
Legal Administration – FOIA/Privacy
Office of General Counsel
Federal Bureau of Prisons

PART D: APPROVAL BY BOP CHIEF INFORMATION OFFICER

_____ _____

Sonya D. Thompson Date
Deputy Asst Director/BOP Chief Information Officer
Information, Policy and Public Affairs Division
Federal Bureau of Prisons

Attachment A

U.S. Department of Justice

Federal Bureau of Prisons

Washington, DC 20534

September 3, 2002

MEMORANDUM FOR MICHAEL A. ATWOOD, CHIEF
TRUST FUND BRANCH, ADMINISTRATION DIVISION

\s\

FROM: Wanda Hunt, Chief
FOIA/PA Section, Office of General Counsel

SUBJECT: Privacy Impact Assessment for TRUFACS

Both the Computer Security Act and the Privacy Act require that all databases/applications running on a federal agency computer system be reviewed to determine if they contain data retrievable by a personal identifier and that any such data be covered by a currently published Privacy Act System of Records notice.

We have reviewed the recently developed TRUFACS system and determined that it does contain records to be protected under the Privacy Act, and that these records are covered by the following Privacy Act System of Records notice (copy attached):

> JUSTICE/BOP-006, entitled “Inmate Commissary Accounts Record System”, published March 15, 2002, at 67 FR 11711.

In addition, we understand that this system will be implemented throughout the Bureau through a financial services contract pursuant to an Inter-Agency Agreement with the Department of Treasury, Financial Management Services. Your staff should review the agreement and underlying contract to ensure that the contractor has been directed to comply with the Privacy Act and JUSTICE/BOP-006. Any request for release of contractor records should be directed to the Bureau’s Freedom of Information Act/Privacy Act (FOIA/PA) office.

If we can be of any further assistance, please give me a call at 514-4807.

Attachment

Attachment B

Data

Inmate Demographic Information (from Sentry system)

Register Number
First Name
Last Name
Date or Birth
Sex
Housing
Education Level
Financial Responsibility Program Participation Status
- Amount
- Type
- Frequency
- Percentage

Public Safety Factor
Alias Names
Nick Names
Race
Ethnicity
Religious Preference
Citizenship
Tentative Release Date
Central Inmate Monitoring Status
FBI Number
ICE Number
Social Security Number

Other Inmate Information from Sentry System

Disciplinary Related Information
- Institution
- Offense Code
- Offense Description
- Date/time
- Report Number
- Notes

Inmate Photos
- Photo
- Photo Description

Current Assignments
Security Threat Group (STG) Information
- STG Name
- Faction
- Level of Participation

Skills
Sentence History

Volunteer/Contractor Information from VCI System

Name

Social Security Number (SSN)_ .
OPM NACI Case No.
Birth date
Race
Birth date
Home address
Home telephone
Personal e-mail address
Race
Gender/Sex
Sponsoring Organization and Address
Employment History
Criminal/Military History

VISITING - Visitor List

Register Number
Institution
First Name
Last Name
Address Line
City
State
Zip
Phone Number
Email Address
Identification Type
Identification Number
Relationship to Inmate
Start Date
End Date
Visitor Photograph
Visitor Status

VISITING - Visit

Register Number
Institution
Date In
Date Out

Staff Information

First Name
Last Name
Office Address
Office Phone
Residence Phone
Office Email
Residence Email

Victim Information

Register Number
Victim Name
Email
Other Email
Phone
Work Phone
Cell Phone