Federal Bureau of Prisons

Privacy Impact Assessment for the

MILLENNIUM/SAP System

Issued By:
Sharad Tilak
Chief Information Officer
Federal Prison Industries

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: August 30, 2011

Introduction

Millennium is a system operated by Federal Prison Industries (FPI), which is a self-sustaining, wholly-owned corporation of the Department of Justice (DOJ), managed within the Federal Bureau of Prisons. FPI provides work and educational opportunity for Federal inmates incarcerated in the Bureau of Prisons (BOP), and is a preferred procurement source under part 8.6 of the Federal Acquisition Regulation for federal agencies. FPI finances itself by providing manufactured goods and services to the Federal Government.

Millennium is a Commercial-Off-The-Shelf software system using SAP (English translation of full name is System Analysis and Program Development) for standard Enterprise Resource Planning solutions to support manufacturing from cradle to grave.

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?

Name information and work address is collected from FPI employees. Social Security Numbers, name and home address information is collected for some released inmates who have medical claims against BOP due to work-related injuries which occurred during incarceration. This information is provided by BOP and is used by FPI to pay the inmate claimants. Banking information is collected from customers and vendors in order to do business. Banking information includes account number and routing number. Customers and vendors also provide Tax Identification Number (TINs) or Social Security Numbers (SSNs).

1.2 From whom is the information collected?

Name information and office address is collected from the BOP at the time of employment and is used in the system for corporate contact information. The name information is also collected for payment of travel disbursements and uniform allowances for the BOP/FPI staff at the BOP/FPI field facilities along with the work address for such FPI employees. Payments to employees are by check and not direct deposit, therefore, no further employee information is needed.

SSN and home address information is collected from the BOP at the time of the inmate's incarceration. (SSN information, if available, is obtained from court documents or the individual directly.) This information is used by FPI to pay the inmate claimants.

Customers and vendors provide their names and banking information, as well as their TIN or SSN. Larger customers and vendors typically provide a TIN, but some of the smaller customers and vendors do not have a TIN, so they provide a SSN.

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?

Pursuant to Title 18, U.S.C. Section 4121, et seq. FPI was established to provide meaningful work and educational opportunities to persons incarcerated in the custody of the Attorney General. These work opportunities include manufacturing and providing goods and services to federal agencies. In accordance with 18 USC Section 4126, inmates assigned to FPI are compensated for their work. Additionally, inmates assigned to FPI, as well as other inmates assigned to BOP work assignments within the institution may be compensated following their release from prison for work-related injuries which occur during incarceration.

Millennium transmits inmate compensation payments to the Department of Treasury. All vendor disbursements submitted to the Department of Treasury are required to have either a Tax Identification Number (TIN) or Social Security Number (SSN). Thus, SSNs are utilized in the disbursement of inmate compensation payments.

Pursuant to its corporate operations, FPI establishes customers, markets to them, and maintains corporate contacts. This work includes staff travel, supervision of inmates, and marketing. Name information is collected to maintain customer relations and compensate staff for their ancillary expenses in carrying out their work.

2.2 What specific legal authorities, arrangements, and/or agreements authorize the collection of information?

Pursuant to 18 U.S.C. § 4126 and 28 C.F.R. Part 301, former inmates or their dependents may receive compensation for injuries sustained while on their inmate work assignments with FPI or other BOP work activity in connection with the maintenance, or operation of the institution in which they are confined. The compensation process requires the collection of personal information for each claimant.

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.

Privacy risks are mitigated by the limited amount of PII that is collected. Sensitive information such as inmate SSNs, vendor and customer banking information are restricted to users on a need-to-know basis. The method used to restrict the information is role-based authorizations within the Millennium system.

Potential privacy risks to the information in Millennium are mitigated by the following measures. Millennium data resides in the structured query language (SQL) database at the Justice Data Center-Rockville, which has physical security and logical security. There is a virtual private network (VPN) between the production data at the Justice Data

Center-Rockville and FPI. Network traffic is encrypted between local area network (LAN) sites on the wide area network (WAN) via the Justice Uniform Network (JUTNET). JUTNET also provides encryption for Millennium/SAP data transmitted to the Department of Treasury. Credit Card information is encrypted and identified Personnel Identification Information (PII) is masked in Millennium/SAP in order to control unauthorized use or disclosure.

Paper documents with personal information are maintained in locked file cabinets and/or a file room with limited access, so this is the mitigation strategy for potential compromise of documents containing PII.

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.

Inmates are compensated for their work as well as compensated in the event of any work related injuries which occur during incarceration. The identifying information coupled with the record of the inmate claim helps to ensure that proper claims are paid.

Staff are reimbursed for travel and uniform allowances by check. The checks are mailed to the employee's duty station. Because payment is not made by direct deposit, only name and duty location information are required. Travel allowance is processed by having the BOP/FPI employee submit receipts, which are approved by the supervisor. The next step is to have this information sent to the financial group and there is a travel authorization number issued to assist in filling out the expenses, for approval and processing.

Vendors and customers are compensated through direct deposit with their banking and routing information as well as TIN or if there is no TIN, a SSN. This direct deposit is sent to Treasury. Treasury will then process the direct deposit.

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.)

No. The system does not do data mining.

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

Collected information is used to make some type of payment to individuals. Acknowledgement of receipt or non-receipt verifies the accuracy of the information. Since there is an approval process by the BOP/FPI employee's supervisor and it goes through appropriate checks with authorized individuals in the financial group, this is checked for accuracy and the receipts assist in verifying the appropriate amount. For inmate claims, there is a paper process and procedure, which is checked for accuracy as any claim or payment is appropriately documented.

For vendor payments, the following process and checks for accuracy are in place. There is a vendor master within Millennium, which contains the masked banking information for the vendors who work with FPI. When an invoice is received by FPI, financial management enters this information into Millennium. Then the Millennium system does a payment run, where the system searches for what invoices are due to be paid and a payment is set up and sent to Treasury for processing. This information can be checked for accuracy by comparing the vendor master with the central contractors registry. Also, Millennium can run reports to make sure that payments to vendors and customers have been accurately processed. All vendors are registered with the Central Contractors Registry (CCR) managed by the Business Partner Network (bpn.gov).

The Millennium system checks only generic types of edits such as the length and inclusion of zip codes, tax identification numbers, banking information, type of payment, etc.

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)?

The retention period is eight years which has been approved by the National Archives and Records Administration under records authority N1-129-04-08.

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.

The use of the Millennium system is governed by approved User IT Security General Rules of Behavior which summarizes laws and guidelines from various federal and DOJ documents, such as OMB Circular A-130, DOJ Order 2640.2 (series), and the DOJ IT Security Standards, for the use of DOJ computing resources. They are to be followed by all users (DOJ employees and contractors) who use any computing resources that support the mission and functions of the Department of Justice.

Also, accounting system financial records are governed by Office of Management and Budget, Department of Treasury, and General Accounting Office internal control laws, regulations, policies, and procedures.

Millennium is a financial system, so it has the appropriate separation of duty and audit checks in place to ensure that the information is used only for the intended purposes. FPI has a specific group, the Authorization Audit License Compliance (AALC), which reviews failed transactions, and failed logins. Millennium has an audit trail that includes who created the documents in Millennium. System monitoring is done to review failed updates and user locks. There is separation of duties and a role/activity group to make sure there are no conflicting transactions. If there are conflicting transactions, then there must be a mitigation strategy for the conflicting transactions. This mitigation strategy must be documented and approved by the business process owners.

FI (finance) and MMB (procurement) training is provided to employees that have access to sensitive information. The payment vouchering process is structured so that no

payments to inmates or employees can be processed until they are properly approved.

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?

None. The information is not shared internally with other DOJ components.

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

None. The information is not shared internally.

4.3 How is the information transmitted or disclosed?

None. The information is not shared internally.

4.4 Privacy Impact Analysis: Given the internal sharing, discuss what privacy risks were identified and how they were mitigated.

None. There is no risk since information is not shared internally.

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?

Data is shared with the U.S. Department of Treasury for the payment of inmate compensation claims related to work injuries, staff uniform allowance, and staff travel reimbursement as well as payments and collections from vendors and customers.

5.2 What information is shared and for what purpose?

SSN or Tax Identification number, name, address, and banking information are shared to identify customers and vendors entitled to payment and make disbursement of payment.

5.3 How is the information transmitted or disclosed?

Information is transmitted through the Department of Treasury's Secure Payment System (SPS). SPS uses 2048 bit keys and SHA-2 for encryption of its data.

5.4 Are there any agreements concerning the security and privacy of the data once it is shared?

Yes. There is an Interconnection Security Agreement between the Department of Treasury and DOJ Federal Prison Industry/Bureau of Prisons (FPI/BOP).

5.5 What type of training is required for users from agencies outside DOJ prior to receiving access to the information?

The Department of Treasury is governed by the same federal regulations and guidelines as the Department of Justice mentioned in item 3.5.

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

There is an Interconnection Security Agreement (ISA) between DOJ FPI/BOP and the Department of Treasury and Millennium has annual security assessments conducted on its system. Since Millennium is a financial system, there are many auditing requirements on the recipients' use of the information from the Federal Information System Controls (FISCAM) controls which are used for financial systems as well as DOJ FISMA requirements. The Department of Treasury is subject to regular audit by the Office of Inspector General, General Accounting Office, and Independent Audit firms.

5.7 Privacy Impact Analysis: Given the external sharing, what privacy risks were identified and describe how they were mitigated.

The Department of Treasury is the Federal Government's agency for managing and monitoring the finances of the U.S. government. One privacy risk is the potential compromise of data sent from DOJ to Treasury, which is mitigated by AES encryption and PKI which is used for SPS. DOJ data is protected by a firewall and is monitored by the Justice Security Operations Center (JSOC) with JUTNET. Data sent to Treasury is protected by AES 256-bit encryption and there is an Interconnection Security Agreement between BOP/FPI and the Department of Treasury. Authorized users at the Department of Treasury will decrypt the information once it is received and follow procedures to process the payment in SPS.

Payments sent to Treasury through SPS are protected with AES 256 encryption and protected by JUTNET. On Treasury's end, every SPS user at a federal agency must have a Public Key Infrastructure (PKI) Credential in order to access the system. PKI will also be used to sign certifications electronically. Every SPS user at the agency (DOJ) must have a token which will contain the PKI Credential for user authentication and document signing. Therefore, data is protected at DOJ, in transit from DOJ to Treasury and by the Department of Treasury. The potential compromise of data at rest and in transit is protected by a firewall, JSOC monitoring for any attempts or actual compromise of Millennium data, AES 256 encryption and the use of PKI for SPS users at DOJ who send payments to Treasury.

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?

The following SORNs act as the notice to individuals about the collection of information. Millennium does not collect the information itself from individuals, this information is collected by BOP.

BOP-001 Prison Security and Intelligence Record System
67 FR 41449 (06-18-02)

BOP-008 Inmate Safety and Accident Compensation Record System
67 FR 41452 (06-18-02)

DOJ-006 Personnel Investigation and Security Clearance Records for the Department of Justice
67 FR 59864 (09-24-02)
69 FR 65224 (11-10-04)

DOJ-009 Emergency Contact Systems for the Department of Justice
69 FR 1762 (01-12-04)

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

No. Information from staff is initially collected as part of the employment application process. Information about inmates is collected as part of the sentencing process (by U.S. Probation Officers in preparation of the Pre-sentence Investigation Report) and by BOP in preparation for release to the community. Customers and vendors need to provide the banking, routing and TIN or SSN to be able to do business with FPI.

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?

No. Information is required in order to process travel and uniform allowance dispersals (for staff) and inmate compensation checks (for inmates). Customers and vendors have to provide the information to be able to do business. Any potential misuse of the data is mitigated by the fact that Millennium is a financial system, so there are technical and security practices and audit procedures which protect against the misuse of data. Also, Millennium uses role based access, which ensures that authorized users only have permissions and access to use the information for its intended purpose.

6.4 Privacy Impact Analysis: Given the notice provided to individuals above, describe what privacy risks were identified and how you mitigated them.

Privacy risks have been mitigated through the notice provided in the SORNS, listed above.

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?

Pursuant to 28 C.F.R. Part 301, as part of the individuals right to an appeal of the initial determination, they may be provided with a copy of the documentation collected as part of their claim.

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

All inmates are subject to an Admission and Orientation presentation, upon designation to any Federal Bureau of Prisons correctional institution. During this presentation, the Inmate Accident Compensation Program is explained in detail, including the requirement that the claimant must keep the Federal Bureau of Prisons notified of their current personal information in writing at all times during the pendency of the claim. Additionally, each inmate is provided with a personal copy of the Inmate Accident Compensation Procedures.

7.3 If no opportunity to seek amendment is provided, are any other redress alternatives available to the individual?

Not applicable.

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.

Pursuant to 28 C.F.R. Part 301, the claimant has appeal rights of the initial determination to the Inmate Accident Compensation Committee (Committee), and if not satisfied with the decision of the Committee, the claimant may file a final appeal to the Chief Operation Officer, FPI.

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?

FPI has defined the following user groups: central office users, field locations users, special or super users, expired users, and contracting/external users.

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, DOJ contractors who have access to Millennium have undergone the appropriate DOJ background investigation (National Agency Check with Inquiries or NACI) and have read and signed the Rules of Behavior and take CSAT, which includes privacy training. DOJ contractors to Millennium have access based upon geographic access and role based access, based upon the position description and segregation of duties. For example, DOJ contractors in SAP consulting services will have permissions on the system to assist with SAP security maintenance, troubleshoot production problems and provide expertise to SAP staff.

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

Yes. All users in the Millennium system are granted role base access. Roles are developed and issued with the concept of least privilege access. This allows only authorized access for users which are necessary to accomplish their assigned task.

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

Yes. Network Access (ISM), SAP Security Guide (SEC) and SAP Authorization Policy (AALC or Authorizations, Audit, Licenses and Compliance) document Millennium or SAP access.

8.5 How are the actual assignments of roles and rules verified according to established security and auditing procedures?

When a user requests to have access to the UNICOR system, his/her supervisor must fill out the Network Access Management (NAM) form or show proof they approve the request in Heat Self Service (iHEAT or HSS). The iHEAT ticket is sent to (Management Information Systems Branch) MISB's Helpdesk and then forwarded to the AALC Helpdesk in iHEAT.

Once the AALC Helpdesk receives the ticket, Helpdesk staff will verify the information. Depending on the request, AALC will simulate a SoD report for potential SoD conflicts. The AALC Helpdesk staff will send an email to the role Business Process Owner(s) to obtain the approval(s) for user change(s) and the SoD report, where applicable. Any

unmitigated SoD conflicts are mitigated by the role-BPO and reviewed by the Internal Control and Compliance Group (ICCG).

When the AALC Helpdesk staff receives all the approval(s) from role-BPO(s), they authorize the User Administrator to make the change on the requestors account.

A review of authorization approvals is conducted bi-weekly by the role-BPO(s) to ensure no user was granted access to SAP without proper review.

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

Millennium is a financial system, so it employs the Federal Information System Controls Audit Manual (FISCAM) security controls for auditing and other technical safeguards. All users of Millennium/SAP have role based access based upon least privilege. Regular audit procedures, as required by DOJ and FISCAM, are followed to ensure that information used in Millennium/SAP is only done by authorized users and is not misused by any users. Millennium/SAP security logs are reviewed to ensure that Millennium users are not misusing the data.

In addition, SAP Security monitors a number of transactions, external processes, etc for inappropriate or suspicious behavior.

Every year, all user accounts are re-certified to ensure access granted is appropriate.

Lastly, SAP User accounts which are inactive in excessive of 90 days have the roles or authorizations removed from the account.

8.7 Describe what privacy training is provided to users either generally or specifically relevant to the functionality of the program or system?

Annual BOP Training and the DOJ CSAT, which includes privacy training is provided to Millennium users.

8.8 Is the data secured in accordance with FISMA requirements? If yes, when was Certification & Accreditation last completed?

Yes. Certification & Accreditation was completed on February 14, 2008. Annual security assessments are completed for Millennium and Certification and Accreditation is completed every three years. The current C&A has been granted a 180-day extension beyond the three year period and a new C&A will be completed prior to the expiration of the 180-day extension.

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

The risk of unauthorized access and use of the system is mitigated by the following measures. Access to the Millennium system is restricted to authorized personnel who have received a NACI. The system is configured in accordance with NIST guidelines, e.g., password authentication and verification, user account management and monitoring, physical and environmental controls, etc. The system is certified and accredited and audited each year by the Office of the Inspector General. Roles within

the system are managed so that information is restricted only to those who have a need to know based upon least privilege.

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. We hired the Gartner group to evaluate available software. Companies presented their capabilities/software based on our requirements. We elected the best fit for our requirements.

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

All the competing companies were provided with a list of our data integrity requirements, such as inmate access and control requirements. The selected company had integrated security restraints and has the capability for further enhancement to meet future security needs.

9.3 What design choices were made to enhance privacy?

The security design is based on a "need to know" basis. All users do not have access to all available data and this access is (can be) controlled centrally or on a distributed basis.

Conclusion

The Millennium system assists the Bureau of Prisons in managing its inmate population and providing work and educational opportunities to inmates. The system was constructed to strictly control any information used therein and to mitigate risks to that information. It is used to process any inmate claims for injury sustained while working in the prison, process reimbursement for BOP employees and to process payments to customers and vendors. Millennium is a financial system, so it has the appropriate FISCAM and DOJ security controls and requirements, which also ensure that the information used in Millennium is only used by authorized users and only for the intended purpose.