Federal Bureau of Prisons

Privacy Impact Assessment
for the
HR Automation System

Issued by:
Sonya D. Thompson
Deputy Assistant Director/CIO

Reviewed by: Eric Olson, Acting Chief Information Officer, Department of Justice

Approved by: Nancy C. Libin, Chief Privacy and Civil Liberties Officer, Department of Justice

Date approved: November 10, 2011

Introduction

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 BOP's Human Resources Automation system (BOP-HIRES and BOP-Careers) is a contractor-managed system used for various tasks, including the following: generating and managing BOP vacancies; collecting and viewing applicant data, including qualification and contact information; corresponding with applicants via electronic mail in regards to a specific application; generating mailing lists for employment notification purposes; and building HR-related reports and applicant rankings.

BOP-Careers is used to manage vacancies for all merit promotion positions throughout the BOP. It is integrated with USAJobs and vacancies are publicized using that site. BOP-HIRES is a system for external applicants to apply for positions that are open continuously: Correctional Officers, Medical Officers, Physician Assistants, Nurse Practitioners, Dental Officers, Registered Nurses, and Clinical Psychologists. The systems are managed under contract with Monster Government Solutions.

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?

The following identifiable information is collected:

- Name
- Social Security Number (SSN)
- Birth date
- Home address
- Home telephone number
- Personal e-mail address
- Race/ethnicity*
- Gender/sex*
- Marital status
- Employment history
- Education level
- Disability and financial data (salary)

** Voluntary demographic information provided by the applicant. It is only used for reporting*

purposes.

1.2 From whom is the information collected?

The information is collected from persons currently employed with the BOP and those seeking employment with the BOP. The information is collected electronically as part of the application process. The personally identifiable information (PII) collected uniquely identifies the applicant or employee throughout the application/hiring process.

Section 2.0 The Purpose of the System and the Information Collected and Stored within the System.

The following questions are intended to delineate clearly the purpose for which information is collected in the system.

2.1 Why is the information being collected?

The information is collected to uniquely identify the applicant or employee during the application process and for purposes of employee payroll processing and personnel recordkeeping.

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

The U.S. Government is authorized to ask for this information under Exec. Order 10,577, 19 Fed. Reg. 7521, 9315 (Nov. 22, 1954); 5 U.S.C. §§ 3301-3302; and 5 C.F.R. pts. 5, 731 and 736. Additionally, Exec. Order 9397, 8 Fed. Reg. 16,095 (Nov. 22, 1943), as amended by Exec. Order 13,478, 73 Fed. Reg. 70,239 (Nov. 18, 2008) permits Federal agencies to use the Social Security Number (SSN) to help identify individuals in agency records. After the BOP applied the principles in OMB Memorandum 07-16, *"Safeguarding Against and Responding to the Breach of Personally Identifiable Information,"* along with other applicable statutes and regulations, the BOP determined that the use of the SSN is necessary to distinguish between individuals with duplicate names and to ensure proper tracking/association between the individual's clearance record and the individual's OPM case file, which is associated with the SSN. The display of SSNs is masked and only the last four digits are displayed.

2.3 <u>Privacy Impact Analysis</u>: Given the amount and type of information collected, as well as the purpose, discuss what privacy risks were identified and how they were mitigated.

There is a minimal privacy risk related to the inadvertent disclosure of sensitive information to persons not authorized to receive it. To mitigate this minimal risk, staff

are annually trained on how to properly handle sensitive information and annually trained on information security practices and procedures. Access to the system is restricted to authorized HR personnel staff, all of whom have an appropriate security clearance that is regularly reviewed. Information is safeguarded in accordance with Bureau rules and policy governing automated information systems security. Access is only available via the internal BOP network. The display of SSNs is masked and only the last four digits are displayed. Established IT security safeguards include the maintenance of records and technical equipment in restricted areas and the required use of strong passwords and unique userIDs to access the system. Only those Bureau personnel who require access to perform their official duties may access the system and record changes are tracked and audited through the use of history transaction tracking logged by userID. The contractor-managed system and facilities are audited, certified, and accredited in accordance with DOJ IT security requirements and standards.

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.

The information is used for generating and managing BOP vacancies; collecting and viewing applicant data, including qualification and contact information; corresponding with applicants via electronic mail in regards to a specific application; generating mailing lists for employment notification purposes, and building HR-related reports and applicant rankings. Additional uses of the information are described in the applicable System of Records Notices:

- DOJ-002, DOJ Computer Systems Activity & Access Records, 64 Fed. Reg. 73,585 (Dec. 30, 1999); 66 Fed. Reg. 8425 (Jan. 31, 2001); 72 Fed. Reg. 3410 (Jan. 25, 2007);
- DOJ-006, Personnel Investigation and Security Clearance Records for the Department of Justice, 67 Fed. Reg. 59,864 (Sept. 24, 2002); 69 Fed. Reg. 65,224 (Nov. 10, 2004); 72 Fed. Reg. 3410 (Jan. 25, 2007);
- OPM/GOVT-1, General Personnel Records, 71 Fed. Reg. 35,342 (June 19, 2006)**;**
- OPM/CENTRAL-9, Personnel Investigations Records, 58 Fed. Reg. 19184 (Apr. 12, 1993).

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.)

The system does not data mine.

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

Data from the system is verified by applicants/employees and other employment records. System accuracy is assured using program edit checks to prevent data entry errors.

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 applicable retention schedule is General Records Schedule 1, "Civilian Personnel Records," issued by NARA. The retention schedule is as follows:

- Records relating to case files are temporary;
- Certificate of Eligibles - 2 years;
- Employment applications – retained until separation (in system); after OPM audit or 2 years whichever is earlier (paper);
- Merit Promotion case files - after OPM audit or 2 years after personnel action whichever is earlier;
- Delegated agreements - 3 years after termination of agreement;
- Correspondence concerning applications, eligibles' certificates and all other examining operations - cut off annually, destroy 1 year after cutoff;
- Register of eligibles - cut off annually, destroy 5 years after cutoff; and
- Canceled/ineligible applications - return to applicant with notice of ineligibility or destroy ineligible applications 90 days after date of action or when register is terminated whichever is sooner.

3.5 Privacy Impact Analysis: Describe any types of controls that may be in place to ensure that information is handled in accordance with the above described uses.

Access to the system is limited to those persons who have an appropriate security clearance, which is regularly reviewed. Staff are trained in the use of the system and in safeguarding the information contained therein. Information is safeguarded in accordance with Bureau rules and policy governing automated information systems security and access. For example, the display of SSNs is masked and only the last four digits are displayed. Access to the system must be requested by the applicable supervisor. In addition, user access and removal is documented and retained for audit purposes. Further, login and password restrictions are in place and user accounts are reviewed on a routine basis. The contractor-managed system and facilities are audited, certified, and accredited in accordance with DOJ IT security requirements and standards.

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?

BOP does not normally share information from the HR Automation System with any other DOJ component; however, should the need arise to share this information, it may only be shared as legally permissible, including in accordance with the Privacy Act.

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

N/A.

4.3 How is the information transmitted or disclosed?

N/A.

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

N/A.

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?

BOP does not normally share information from the HR Automation System with non-DOJ recipients; however, should the need arise to share information from this system, BOP will do so only as legally permissible, including in accordance with the Privacy Act. In particular, the system of records notices listed for HR Automation (see Section 3.1 above) set forth various permissible routine uses that may apply if BOP determines it necessary to share information from the HR Automation Systems.

5.2 What information is shared and for what purpose?

N/A

5.3 How is the information transmitted or disclosed?

N/A

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

N/A

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

N/A

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

N/A

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

N/A

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?

A Privacy Act notice is published on all applicable forms to be completed by the employee or applicant. The following Systems of Records Notices also provide the

individual with notice:

- DOJ-002, DOJ Computer Systems Activity & Access Records, 64 Fed. Reg. 73,585 (Dec. 30, 1999); 66 Fed. Reg. 8425 (Jan. 31, 2001); 72 Fed. Reg. 3410 (Jan. 25, 2007);
- DOJ-006, Personnel Investigation and Security Clearance Records for the Department of Justice, 67 Fed. Reg. 59,864 (Sept. 24, 2002); 69 Fed. Reg. 65,224 (Nov. 10, 2004); 72 Fed. Reg. 3410 (Jan. 25, 2007);
- OPM/GOVT-1, General Personnel Records, 71 Fed. Reg. 35,342 (June 19, 2006)**;**
- OPM/CENTRAL-9, Personnel Investigations Records, 58 Fed. Reg. 19184 (Apr. 12, 1993).

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

The information may be provided voluntarily. BOP, however, may not be able to complete processing of the application or complete it in a timely manner, if the information is not provided. This omission may affect the applicant's employment prospects or an employee's promotion opportunities.

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?

The information collected is used for the purpose of determining an applicant's eligibility for initial employment or an employee's eligibility for reassignment or promotion. The BOP protects such information from unauthorized disclosure.

The collection, maintenance, and disclosure of employment information are governed by the Privacy Act. The information collected during the employment process may be disclosed with consent or as otherwise as permitted by the Privacy Act, 5 U.S.C. § 552a(b), including pursuant to the routine uses set forth in published system of records notices.

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

The privacy risk identified would be the failure of persons to know their information may be collected and for what it will be used. DOJ and OPM have published Privacy Act system of records notices for applicant and employee records. The information in these

notices include entities with which and situations when DOJ may share investigative records. Furthermore, Privacy Act notices appear on forms that collect information that is entered into HR Automation. These notices, therefore, mitigate the risk that the individual will not know why the information is being collected or how the information will be used.

Section 7.0 Individual Access and Redress

The following questions concern an individual's ability to ensure the accuracy of the information collected about him/her.

7.1 What are the procedures which allow individuals the opportunity to seek access to or redress of their own information?

Individuals provide the information collected in the system and attest by signature on the collection form to its accuracy. Individuals are also provided the opportunity during the clearance process to personally explain, refute, or clarify any information entered on the requisite clearance forms before a final decision is made as to their eligibility for hire. Requests to see or contest the information about an individual's own records in the system may be made though the submission of a Privacy Act request as indicated in the applicable system of records notice.

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

Individuals are provided instructions on the collection form(s) (e.g. SF-85) on how to access or amend information. Individuals are also provided the opportunity during the clearance process to personally explain, refute, or clarify any information entered on the requisite clearance forms before a final decision is made as to their eligibility for hire. If their clearance is denied, suspended or revoked, they will be notified in writing and be provided with the specific information regarding their appeal rights and due process. Additionally instructions are provided on related application and security forms regarding changes or updates to data that may be required after submission. Privacy Act systems of records notices and DOJ regulations (28 C.F.R. Part 16) also provide notice of such procedures.

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

N/A.

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.

Individuals provide the information collected in the system and attest by signature on any collection form (SF-85, SF-85P, SF-85PS or SF-86) as to its accuracy. Individuals are also provided the opportunity during the clearance process to personally explain, refute, or clarify any information entered on the requisite clearance forms before a final decision is made as to their eligibility for hire.

If their clearance is denied, suspended or revoked, individuals will be notified in writing and be provided with the specific information regarding their appeal rights and due process. Additionally instructions are provided on related security forms regarding changes or updates to data that may be required after submission. The Privacy Act systems of records notices and DOJ regulations (28 C.F.R. Part 16) also provide notice of such procedures.

Individuals seeking access to records about an individual's own records in the system may submit a Privacy Act request as indicated in the applicable system of records notice.

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?

Full access rights to all data in the system is accessible to approximately 65 Human Resource staff and limited/restricted access rights to approximately 400 Human Resource staff. Individual users may view and edit their own application. Contract system administrators have access to system software and hardware to manage its operation (see Section 8.2 below).

8.2 Will contractors to the Department have access to the system? If so, please describe their role with this system.

Yes. Monster Government Solutions manages the system including software, user interfaces and web systems. Monster Government Solutions is contractually obligated to comply with DOJ privacy and IT security requirements and standards and the system is subject to audit and review as part of annual government IT audits (e.g. FISMA, A-123, etc.). The system is certified and accredited in the same manner as other government-managed systems.

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

Yes, roles are assigned to access data, including roles for regular users (HR staff) and roles for IT administrators. Regular users have "read" privileges. A subset of HR staff have elevated privileges to "modify" or "delete" data. IT administrative staff (contract) have privileges to modify system software in accordance with their functional responsibility.

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

User access must be requested by a supervisor indicating access is required for the performance of their duties. The request and subsequent access is documented.

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

User access must be requested by a supervisor indicating access is required for the performance of their duties.

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

Access to the system is strictly limited to select HR staff with a need-to-know. Access to the system is controlled via userID and password, and data transmission is protected using SSL encryption. Logs are reviewed on a routine basis to identify anomalies or suspicious events.

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

Users are trained as to the sensitive nature of the data within the system and continuously reminded of the need to strictly control the viewing and/or output of data from the system. BOP users are trained annually regarding the handling of sensitive information and information security requirements. All employees who are involved in the management, operation, programming, maintenance, or use of a DOJ information system are made aware of the threats to and vulnerabilities of those systems and their responsibilities with regard to privacy and information security.

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

Yes, the data is secured in accordance with FISMA requirements. The data center in which the system resides utilizes firewalls and intrusion detection systems to monitor unauthorized access. Physical access to facilities is controlled by key card. Policy prohibits the download of PII information without specific authorization to a portable device. Laptops run full disk encryption.

The system was recertified and reaccredited on November 19, 2008.

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

There is a privacy risk related to the inadvertent disclosure of sensitive information to persons not authorized to receive it. To mitigate this risk, access to the system is limited to those persons who have an appropriate security clearance which is regularly reviewed. Users are trained as to the use of the system and information is safeguarded in accordance with BOP and DOJ rules and policy governing automated information systems security and access. These safeguards include the maintenance of records and technical equipment in restricted areas, and the required use of proper passwords and user identification codes to access the system. Data transmission is also encrypted.

Section 9.0 Technology

The following questions are directed at critically analyzing the selection process for any technologies utilized by the system, including system hardware, RFID, biometrics and other technology.

9.1 Were competing technologies evaluated to assess and compare their ability to effectively achieve system goals?

The system is a routine database used to monitor employee and applicant packages. No significant technologies were used to develop the system. BOP analyzed the benefits and drawbacks of developing its own system vs. contracting for a system using a proven contractor. In light of the efforts involved in managing an external system accessible to the public, the BOP chose to contract for the system.

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

Development was structured to minimize risks. The design phase included extensive input and meeting with subject matter staff and end users. Prior to full implementation, a pilot was performed.

9.3 What design choices were made to enhance privacy?

The principle of “least privilege” was employed to ensure that only those persons with a need to view the data can access the system. User accounts are approved by the system owner.

Conclusion

The HR Automation system was implemented in 2001 to replace a paper-based process. The system was constructed to strictly control information used therein and to mitigate risks to the information. Any modifications or enhancements to the system continue to follow that same design goal.