FEDERAL BUREAU OF PRISONS
PRIVACY IMPACT ASSESSMENT (PIA)

System Name:	**HR Automation (BOPHires/BOP-Careers)**		
OMB Control # For Information Collections (If Available):			
OMB Unique Identifier For IT Systems (If Available):	011-20-01-05-02-3184-00-403-251		
Program Area SME:	Sandra Parks	**Telephone:**	202-307-3177
Job Title:	Deputy Chief - Staffing, Examining and Employee Relations		
IT Project SME:	Johanny Handel	**Telephone:**	972-352-4292
Job Title:	Deputy Chief – Consolidated Staffing Unit		
Date:	4/26/06		

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?

   Yes

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? No.

b. Are you making a change in business processes:

i. that merges, centralizes, matches or otherwise significantly manipulates existing databases? No

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 B? If yes, submit the existing PIA with this document for review under the PIA process. If no, continue to Question 6.

Yes. PIA is being revised in light of updated guidance.

6. Is this a national security system as defined at 40 U.S.C. 11103? 2 If yes, please attach verification and submit this document for review under the PIA process.

No

[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 BOP's Human Resources Automation system (including BOP-Hires/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.

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):	
Birth date	X
Home address	X
Home telephone	X
Personal e-mail address	X
Fingerprint/other "biometric"	
Other (specify):	
None	
Comment:	

Other Sensitive Information:

Race/ ethnicity	X
Gender/ sex	X
Marital status	X
Spouse name	X
# of children	
Employment history	X
Education level	X
Medical history/information	
Disability	X
Criminal record	X
Financial Data (salary, accounts, etc.)	X (bankruptcy or lien status)
Other (specify):	
Comment:	

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. The system was implemented in 2001.

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 (system replaced paper-based process)
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 concern for the ability to combine multiple identifying elements)	
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 <u>new</u> Request that will collect data that will be in an <u>automated</u> 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 <u>new</u> request and the collected data will be in an <u>automated</u> 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 <u>new</u> or <u>automated</u>)	N/A
Comment:	

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	
Employment Application	X
FOIA/PA Request	
Litigation/Administrative Claim	
Other (specify):	

Internal operations:

Employee payroll or personnel records	X
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):	N/A
State, local, or tribal governments?	N/A
Contractors?	X (Approved, cleared contractors supporting the system)
Others? (specify):	N/A
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 (information is used for limited purposes)
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	
System users must log-in with a password	X
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):	X User accounts are reviewed 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 #)?	Yes. Approx. 60 HR staff Approx. 400 HR staff (Individual users may view and edit their own application)
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:	N/A

Other methods of protecting privacy (specify):	Session data is SSL-encrypted; public access to the system is controlled via two firewalls. Auditing is done at the database level. Audit information is collected for the following events: successful and unsuccessful login attempts, Logoffs, Admin Tasks, etc.
Comment:	

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

Name:	X
Social Security Number (SSN)	X
Identification number (specify type)	
Birth date	X
Race/ ethnicity	X
Home address	X
Home telephone	X
Personal e-mail address	X
Other (specify):	
None	
Comment:	

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