Federal Bureau of Prisons

Privacy Impact Assessment
for the
The HRMD Career Connections System

Issued by:
Sonya D. Thompson, SCOP

Approved by: Peter Winn
Chief Privacy and Civil Liberties Officer (Acting)
U.S. Department of Justice

Date approved: May 10, 2023

(May 2019 DOJ PIA Template)

Section 1: Executive Summary

Provide a high-level overview of the information technology (e.g., application, tool, automated process) in non-technical terms that describes the information technology, its purpose, how the information technology operates to achieve that purpose, the general types of information involved, how information may be used and shared, and why a Privacy Impact Assessment was conducted. (Note: this section is an overview; the questions below elicit more detail.)

The Human Resources Management Division (HRMD) Career Connections System is a FedRAMP-certified Salesforce Software-as-a-Service (SaaS) platform that can track and contact prospective candidates for hire at BOP, that have come in from events or advertisements until they are employed with BOP. An integration with BOP's applicant tracking system, Monster Government Solutions (Monster), will allow Monster to send updates to Career Connections so that recruiters can view application progress. BOP has prepared a Privacy Impact Assessment for Career Connections because this system collects, maintains, and disseminates information in identifiable form about prospective candidates, BOP recruiters, and BOP community partners.

The Career Connections system includes a public-facing website which will allow prospective candidates to enter contact information so that a recruiter can reach out to candidates interested in employment with BOP. The recruiters will also be able to view application updates in the Career Connections system from Monster. The website will collect detailed web analytics about the general location of user traffic, the type of browser and operating system used to access the site, the date and time of access, the internet address of the website from which users linked directly to the site, and pages visited. This information is used to improve the performance of the website and leveraged to measure marketing efforts and improve future recruitment strategies. The information of individual website visitors is not identified/stored in the system or available to the system owners. The system uses Google Analytics to capture usage and aggregated metrics on the platform. Prospective candidates may also provide their information through career fairs and a telephone line.

Upon deployment, Career Connections will transform candidate management activities by centralizing the collection of contact information and systematically tracking the status of prospective candidate applications from Monster in real-time.

Section 2: Purpose and Use of the Information Technology

2.1 Explain in more detail than above the purpose of the information technology, why the information is being collected, maintained, or disseminated, and how the information will help achieve the Component's purpose, for example, for criminal or civil law enforcement purposes, intelligence activities, and administrative matters, to conduct analyses to identify previously unknown areas of concern or patterns.

Career Connections will transform candidate recruitment and management activities to alleviate staffing shortages at BOP institutions. Information can be added to Career Connections in a variety of different ways. The public-facing Career Connections website will

allow prospective candidates to supply their information directly to BOP through the website.[1]

Additionally, BOP recruiters conduct in-person career events at a variety of locations. Career Connections has created a digital form for potential applications to fill out at these events, but in some cases, potential applicants may still provide information through a hard copy sign-in sheet which would then be added to Career Connections. Further, the National Recruitment Organization at BOP operates a toll-free phone line that a potential applicant can call to ask questions on BOP Careers. Recruiters operate this phone line and will collect the potential applicant's information if their inquiry relates to BOP Careers. BOP recruiters also partner with organizations that can provide eligible applicants for hire at BOP. Recruiters refer to these as "Community Contacts" and they could include state and local government, military branches, or universities. In these cases, the partner organization would provide the potential applicant's name and email or phone contact information.

Prospective candidates can provide their contact information, desired region(s), and position(s) of interest so that recruiters have enough information to triage and actively engage through communication outreach. After a candidate submits their information, a recruiter can manage the information in Career Connections and track their status. The Monster integration will supply additional information about all applications to BOP, including name, email address, and vacancy specific information (position title, vacancy announcement name, grade(s), selection date, hire date, and certificate name). Career Connections will perform a check against new applications and, when possible, relate applications to existing candidates in the system.

The information regarding candidates can only be retrieved by authorized personnel with access to the system using the name or email of the candidate. Approved DOJ contractors are involved with the design and development of the information system and will continue to provide maintenance and administrative services on the production environment after the information system is deployed.

2.2 Indicate the legal authorities, policies, or agreements that authorize collection of the information. (Check all that apply and include citations/references.)

Authority		Citation/Reference
	Statute	18 U.S.C. §§ 4041, 4042, and 5003 (state inmates), Section 11201 of Pub. L. 105-33; 111 Stat. 740 (DC felons)
	Executive Order	
X	Federal Regulation	28 CFR § 503.1

[1] Career Connections utilizes a recruiting ad platform, Google Ads, that will help find prospective candidates that have the highest likelihood of becoming a BOP employee. The Career Connections public website will include a Google Analytics script that will capture metadata about the aggregated audience, acquisition, and behavior metrics on website visitors for web analytics. This information, along with other audience information captured by Google Ads, allows BOP to define audience segmentations (e.g., age, location) of interest. Google Ads will then attempt to target those requested audience segmentations through various channels (e.g., Google Search Ads, YouTube Ads) in attempts to drive traffic to the website.

Authority		Citation/Reference
	Agreement, memorandum of understanding, or other documented arrangement	
	Other (summarize and provide copy of relevant portion)	

Section 3: Information in the Information Technology

3.1 Indicate below what types of information that may be personally identifiable in Column (1) will foreseeably be collected, handled, disseminated, stored and/or accessed by this information technology, regardless of the source of the information, whether the types of information are specifically requested to be collected, and whether particular fields are provided to organize or facilitate the information collection. Please check all that apply in Column (2), and indicate to whom the information relates in Column (3). Note: This list is provided for convenience; it is not exhaustive. Please add to "other" any other types of information.

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to: A. DOJ/Component Employees, Contractors, and Detailees; B. Other Federal Government Personnel; C. Members of the Public - US Citizens or Lawful Permanent Residents (USPERs); D. Members of the Public - Non-USPERs	(4) Comments
Example: Personal email address	*X*	*B, C and D*	*Email addresses of members of the public (US and non-USPERs)*
Name	X	A, B, C and D	First name, last name of prospective candidates. First name, last name of BOP personnel. Point of contact information for BOP community partner (e.g. Army)
Date of birth or age			
Place of birth			
Gender			
Race, ethnicity, or citizenship			
Religion			
Social Security Number (full, last 4 digits or otherwise truncated)			
Tax Identification Number (TIN)			
Driver's license			
Alien registration number			
Passport number			
Mother's maiden name			

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to: A. DOJ/Component Employees, Contractors, and Detailees; B. Other Federal Government Personnel; C. Members of the Public - US Citizens or Lawful Permanent Residents (USPERs); D. Members of the Public - Non-USPERs	(4) Comments
Vehicle identifiers			
Personal mailing address			
Personal e-mail address	X	A, B, C and D	Email address of prospective candidates.
Personal phone number	X	A, B, C and D	Primary phone number of prospective candidates.
Medical records number			
Medical notes or other medical or health information			
Financial account information			
Applicant information	X	A, B, C, and D	Application-related information and status from prospective candidate submissions, such as: application status, application date, hire date, and preferred locations.
Education records			
Military status or other information	X	A, B, C, and D	Veteran Status, Branch of Service, Service Start Date, Service End Date, Pay Grade, and Pay Level of prospective candidates.
Employment status, history, or similar information			
Employment performance ratings or other performance information, e.g., performance improvement plan			
Certificates			
Legal documents			
Device identifiers, e.g., mobile devices			
Web uniform resource locator(s)			
Foreign activities			
Criminal records information, e.g., criminal history, arrests, criminal charges			
Juvenile criminal records information			
Civil law enforcement information, e.g., allegations of civil law violations			

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to: A. DOJ/Component Employees, Contractors, and Detailees; B. Other Federal Government Personnel; C. Members of the Public - US Citizens or Lawful Permanent Residents (USPERs); D. Members of the Public - Non-USPERs	(4) Comments
Whistleblower, e.g., tip, complaint or referral			
Grand jury information			
Information concerning witnesses to criminal matters, e.g., witness statements, witness contact information			
Procurement/contracting records			
Proprietary or business information			
Location information, including continuous or intermittent location tracking capabilities			
Biometric data:			
- **Photographs or photographic identifiers**			
- **Video containing biometric data**			
- **Fingerprints**			
- **Palm prints**			
- **Iris image**			
- **Dental profile**			
- **Voice recording/signatures**			
- **Scars, marks, tattoos**			
- **Vascular scan, e.g., palm or finger vein biometric data**			
- **DNA profiles**			
- **Other (specify)**			
System admin/audit data:			
- **User ID**	X	A	System admin / audit data and User ID of authorized BOP personnel.
- **User passwords/codes**	X	A	System admin / audit data and User ID of authorized BOP personnel.
- **IP address**	X	A	System admin / audit data and User ID of authorized BOP personnel.
- **Date/time of access**	X	A	System admin / audit data and User ID of authorized BOP personnel.

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to: A. DOJ/Component Employees, Contractors, and Detailees; B. Other Federal Government Personnel; C. Members of the Public - US Citizens or Lawful Permanent Residents (USPERs); D. Members of the Public - Non-USPERs	(4) Comments
- **Queries run**	X	A	System admin / audit data and User ID of authorized BOP personnel.
- **Content of files accessed/reviewed**	X	A	System admin / audit data and User ID of authorized BOP personnel.
- **Contents of files**	X	A	System admin / audit data and User ID of authorized BOP personnel.
Other (please list the type of info and describe as completely as possible):	X	C, D	The website for prospective candidates will capture audience, acquisition, and behavior metrics for web analytics. Status of prospective candidate's application. Event location of initial contact with prospective candidate. Other potential PII may be contained in email messages between prospective candidates and BOP recruiters.

3.2 Indicate below the Department's source(s) of the information. (Check all that apply.)

Directly from the individual to whom the information pertains:					
In person	X	Hard copy: mail/fax	X	Online	X
Phone	X	Email	X		
Other (specify):					

Government sources:					
Within the Component	X	Other DOJ Components		Other Federal Entities	

Government sources:					
State, local, tribal	X	Foreign (identify and provide the international agreement, memorandum of understanding, or other documented arrangement related to the transfer)			
Other (specify):					

Non-government sources:					
Members of the public		Public media, Internet		Private sector	
Commercial data brokers					
Other (specify):					

Section 4: Information Sharing

4.1 Indicate with whom the component intends to share the information and how the information will be shared or accessed, such as on a case-by-case basis by manual secure electronic transmission, external user authorized accounts (i.e., direct log-in access), interconnected systems, or electronic bulk transfer.

Recipient	**How information will be shared**			
	Case-by-case	**Bulk transfer**	**Direct log-in access**	**Explain specifics of the sharing, as well as how these disclosures will support and are compatible with the purposes of the collection.**
Within the Component	X		X	Direct log-in access is granted to approved BOP personnel such as recruiters and HRMD leadership. Ad-hoc requests will be sent to system owners, evaluated to determine need, and the minimum information required to satisfy the request will be exported/sent. Reoccurring requests will be evaluated to determine need and minimum access to the system will be granted to satisfy the request.

Recipient	How information will be shared			
	Case-by-case	**Bulk transfer**	**Direct log-in access**	**Explain specifics of the sharing, as well as how these disclosures will support and are compatible with the purposes of the collection.**
DOJ Components	X			Information may be shared with other DOJ components in support of ad-hoc reporting requests for auditing or aggregated program metrics to measure success. Ad-hoc reporting requests will be sent to system owners, evaluated to determine need, and the minimum information required to satisfy the request will be exported/sent.
Federal entities	X			Information may be shared with other Federal entities in support of ad-hoc reporting requests for auditing or aggregated program metrics to measure success. Ad-hoc reporting request will be sent to system owners, evaluated to determine need, and the minimum information required to satisfy the request will be exported/sent.
State, local, tribal gov't entities				
Public				
Counsel, parties, witnesses, and possibly courts or other judicial tribunals for litigation purposes				
Private sector				
Foreign governments				
Foreign entities				
Other (specify):				

4.2 If the information will be released to the public for "Open Data" purposes, e.g., on data.gov (a clearinghouse for data from the Executive Branch of the Federal Government), and/or for research or statistical analysis purposes, explain whether—and, if so, how—the information will be de-identified, aggregated, or otherwise privacy protected.

N/A

Section 5: Notice, Consent, Access, and Amendment

5.1 What, if any, kind of notice will be provided to individuals informing them about the collection, use, sharing or other processing of their PII, e.g., a Federal Register System of Records Notice (SORN), providing generalized notice to the public, a Privacy Act § 552a(e)(3) notice for individuals, or both? Will any other notices be provided? If no notice is provided, please explain.

The following System of Records Notices published in the Federal Register cover the records in this system:

DOJ-002, DOJ Computer Systems Activity & Access Records, last published in full at 86 Fed. Reg. 37188 (Jul. 14, 2021), https://www.justice.gov/opcl/page/file/1419896/download;

DOJ-003, Correspondence Management Systems (CMS) for the Department of Justice, last published in full at 66 Fed. Reg. 29992 (Jun. 4, 2001), https://www.gpo.gov/fdsys/pkg/FR-2001-06-04/pdf/01-13860.pdf;

OPM/GOVT-1, General Personnel Records, last published in full at 77 Fed. Reg. 79,694 (Dec. 11, 2012), https://www.gpo.gov/fdsys/pkg/FR-2012-12-11/pdf/2012-29777.pdf;

OPM/GOVT-5, Recruiting, Examining, and Placement Records, last published in full at 79 Fed. Reg. 16834 (Mar. 26, 2014), https://www.federalregister.gov/d/2014-06593;

A Privacy Act (e)(3) notice will be provided to prospective candidates on all pages of the application when populating and submitting information required for opportunities. A link to the BOP's privacy notice/policy is available on the footer of all pages for view by candidates.

5.2 What, if any, opportunities will there be for individuals to voluntarily participate in the collection, use or dissemination of information in the system, for example, to consent to collection or specific uses of their information? If no opportunities, please explain why.

The Privacy Act (e)(3) notice provided to prospective candidates on the application will clarify that providing information to BOP through Career Connections is voluntary, but that failure to provide the requested information may prevent BOP from being able to contact the prospective candidate.

5.3 What, if any, procedures exist to allow individuals to gain access to information in the system pertaining to them, request amendment or correction of said information, and receive notification of these procedures (e.g., Freedom of Information Act or Privacy Act procedures)? If no procedures exist, please explain why.

Individuals may follow BOP protocols to receive or amend information collected or stored by BOP through a Privacy Act or FOIA request, which is outlined on the privacy policy page available to all candidates.

Section 6: Maintenance of Privacy and Security Controls

6.1 The Department uses administrative, technical, and physical controls to protect information. Indicate the controls below. (Check all that apply).

X	**The information is secured in accordance with Federal Information Security Modernization Act (FISMA) requirements, including development of written security and privacy risk assessments pursuant to National Institute of Standards and Technology (NIST) guidelines, the development and implementation of privacy controls and an assessment of the efficacy of applicable privacy controls. Provide date of most recent Authorization to Operate (ATO):** ATO issued on 1/30/2024 and expires on 1/29/2027. **If an ATO has not been completed, but is underway, provide status or expected completion date:** **Unless such information is sensitive and release of the information could pose risks to the component, summarize any outstanding plans of actions and milestones (POAMs) for any privacy controls resulting from the ATO process or risk assessment and provide a link to the applicable POAM documentation:**
	This system is not subject to the ATO processes and/or it is unclear whether NIST privacy controls have been implemented and assessed. Please explain:
X	**Monitoring, testing, or evaluation has been undertaken to safeguard the information and prevent its misuse. Specify:** Thorough testing of security controls has been undertaken to ensure the proper monitoring and safeguarding of information.
X	**Auditing procedures are in place to ensure compliance with security and privacy standards. Explain how often system logs are reviewed or auditing procedures conducted:** The system captures an audit of user account modifications and system events that will be reviewed by system administrators on a quarterly basis. Additional auditing of transactional data will be captured and maintained to align with records & information management requirements. A subset of approved internal users (e.g. employees, contractors) have been identified as system administrators to support organization-defined configuration, security, and access control.
X	**Contractors that have access to the system are subject to information security, privacy and other provisions in their contract binding them under the Privacy Act, other applicable laws, and as required by DOJ policy**.
	Each component is required to implement foundational privacy-related training for all component personnel, including employees, interns, and contractors, when personnel on-board and to implement refresher privacy training annually. Indicate whether there is additional training specific to this system, and if so, please describe: No additional system-specific privacy training is required.

6.2 Explain key privacy and security administrative, technical, or physical controls that are designed to minimize privacy risks. For example, how are access controls being utilized to reduce the risk of unauthorized access and disclosure, what types of controls will protect PII in transmission, and how will regular auditing of role-based access be used to detect possible

unauthorized access?

Accounts are created for a subset of identified internal users (e.g., employees, contractors) which leverage single sign-on (SSO) and multi-factor authentication (MFA) using enterprise authentication services. Inbound requests to the internal application are restricted to monitor usage and leverage additional security controls from BOP.

Approved internal users have been identified as system administrators to support organization-defined configuration, security, and access control. The account managers periodically review accounts to identify personnel that no longer need access. Account managers will add new users, remove existing users, or modify existing users. Automatic account management will be applied to inactivate accounts that have not logged into the system for a specified period. The system incorporates security controls to identify and restrict unsuccessful login attempts. Additional password complexity, reset duration, and reset reusage have been implemented to align with BOP standards.

The application utilizes industry best practices for data encryption, including encryption at rest and in transit.

6.3 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.)

The applicable records schedules for the system are detailed below.

GRS 2.1, Item 180

Records documenting agency in-person and on-line recruitment efforts at career fairs, job fairs, visits to colleges, and similar venues. Includes: records documenting planning and logistics of individual recruitment events; record copy of advertisement and materials for distribution; contact information and interest areas collected from potential job candidates; recruitment event reports; correspondence with prospective candidates.

Temporary. Destroy when 1 year old, but longer retention is authorized if required for business use.

Section 7: Privacy Act

7.1 Indicate whether information related to U.S. citizens or aliens lawfully admitted for permanent residence will be retrieved by a personal identifier (i.e., indicate whether information maintained by this information technology will qualify as "records" maintained in a "system of records," as defined in the Privacy Act of 1974, as amended).

_____ No. __X__ Yes.

7.2 Please cite and provide a link (if possible) to existing SORNs that cover the records, and/or explain if a new SORN is being published:

The following System of Records Notices published in the Federal Register cover the records in this system:

DOJ-002, DOJ Computer Systems Activity & Access Records, last published in full at 86 Fed. Reg. 37188 (Jul. 14, 2021), https://www.justice.gov/opcl/page/file/1419896/download;

DOJ-003, Correspondence Management Systems (CMS) for the Department of Justice, last published in full at 66 Fed. Reg. 29992 (Jun. 4, 2001), https://www.gpo.gov/fdsys/pkg/FR-2001-06-04/pdf/01-13860.pdf;

OPM/GOVT-1, General Personnel Records, last published in full at 77 Fed. Reg. 79,694 (Dec. 11, 2012), https://www.gpo.gov/fdsys/pkg/FR-2012-12-11/pdf/2012-29777.pdf;

OPM/GOVT-5, Recruiting, Examining, and Placement Records, last published in full at 79 Fed. Reg. 16834 (Mar. 26, 2014), https://www.federalregister.gov/d/2014-06593.

Section 8: Privacy Risks and Mitigation

When considering the proposed use of the information, its purpose, and the benefit to the Department of the collection and use of this information, what privacy risks are associated with the collection, use, access, dissemination, and maintenance of the information and how are those risks being mitigated?

a. Potential Risks Related to Information Collection

Collecting and maintaining more personal information than necessary to accomplish BOP's official duties is a potential threat to privacy arising from Career Connections. The unnecessary collection of data poses a risk of the loss of personal information to BOP candidates, applicants, and BOP staff, due to the sensitivity of the data involved, such as names and email addresses. BOP mitigates this risk by implementing measures to limit the collection of data to that which is required to complete the authorized and necessary functions of Career Connections. These measures include creating certain defined data fields where required information can be inserted and evaluating each step, form, and field to determine need and minimize the amount of information collected.

There is also a potential privacy risk arising from collecting information of inadequate quality on each individual. To mitigate this, the Career Connections collects information directly from the candidate about whom the information pertains to the greatest extent practicable. The system displays a Privacy Act statement on all pages of the public website when the candidate is populating and submitting required information. A link to the BOP's privacy notice/policy is available on the footer of all pages for candidates which includes information on the following:

1. Information Collected
2. How Personal Information Is Used
3. Child Privacy
4. Cookie Usage
5. External Sites
6. Security

To mitigate the risk of unauthorized access or use, the collected information is safeguarded in accordance with BOP 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.

b. Potential Risks related to the Use of Information

Potential threats to privacy arising from BOP's use of the information in Career Connections include the risk of unauthorized use of information, threats to the integrity of the information arising from unauthorized access or improper disposal of information. BOP mitigates the risk of unauthorized access through the implementation of data access controls, ensuring information is provided only to those individuals who require access to perform their official duties.

Staff are annually trained on how to properly handle sensitive information to mitigate the risks arising from improper use or disposal of the information. The duration of time to retain information is determined when business use ceases in accordance with BOP data storage/retention policy. Additionally, to address the threats to the integrity of the data from unauthorized access, there are no outside users who are permitted access to the internal Career Connections system, including personnel from the larger DOJ community. When a BOP employee departs from the BOP or transitions to a new position, the BOP takes appropriate measures to deactivate the user access and accounts to Career Connections.

c. Potential Risks Related to the Dissemination of Information

There is a privacy risk to individuals arising from the potential disclosure of sensitive information to persons not authorized to receive it and unauthorized data modification and misuse. This risk is mitigated by enforcing access controls and encryption (as described above) and by providing auditing of user and system administration activities. Data transmission, both within and outside the system, is encrypted using the TLS protocol. Data within the system is used and shared only when required by the agency's mission.

Reporting information for auditing or measuring success may be shared on a case-by-case basis with other DOJ components and Federal agencies. Each request is evaluated to determine need, and the minimum information required to satisfy the request will be exported/sent. All data shared with other DOJ components for reporting purposes will be aggregated and will have personal identifiers removed to make individual identification extremely difficult. These restrictions help address the risk of disclosure of information to unauthorized individuals both inside and outside BOP.