Federal Bureau of Prisons

Privacy Impact Assessment
for the
JIRA Service Desk Application (JSD)

Issued by:
Sonya D. Thompson
Assistant Director / SCOP

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

Date approved: July 30, 2021

(May 2019 DOJ PIA Template)

Section 1: Executive Summary

The JIRA Service Desk application (JSD) is used to enable BOP staff and authorized contractors to create and track requests and incident tickets for information technology (IT) and Human Resources (HR)-related support. The application is accessed via administrative staff workstations from 212 geographical BOP locations. Users submit requests/tickets within the system for assistance. The tickets are then routed to an appropriate support group for action. JSD routes incident tickets to the appropriate support group according to a client's physical location and, in the case of human resource support, according to the intended functional purpose and action (e.g. new hire, retirement, promotion, payroll action, etc.).

BOP has prepared a Privacy Impact Assessment for JSD because this system collects, maintains, and disseminates information in identifiable form about individuals. Information required to identify the user submitting the incident/request is collected, as well as sufficient information to assist the support group to resolve the incident. Typically, this information includes: user IDs, work phone numbers, date and time of incident; work email addresses, facility location, Social Security numbers (SSNs) (for HR tickets, and restricted for viewing only by HR staff and IT system administrators), and other related information.

JSD authenticates user logins via a unique internal e-mail address and password. All transmission of data to/from the system uses the Transport Layer Security (TLS) protocol and is fully encrypted. All actions taken for a ticket are logged in a transaction log attached to each ticket as an audit trail. JSD is only interconnected with the Lightweight Directory Access Protocol (LDAP) system. There are no other interconnections.

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.

Most tickets in JSD are opened for IT support (e.g. password reset, printer repair, workstation software issues). Those tickets are routed by the JSD application to the appropriate location for handling by IT support staff (e.g. a ticket initiated by a staff member in FMC Lexington will be routed to the FMC Lexington IT).

All HR helpdesk ticket requests are routed by the system to the Human Resource Services Center in Grand Prairie, TX and processed by HR staff at that site. The only staff who can view HR tickets are HR staff and Central Office IT helpdesk system administrators (only when IT support with the helpdesk system is required). For HR requests, helpdesk tickets may contain personally identifiable information, such as user's (client) name, SSN, and location information to process payroll, leave and retirement requests.

The JSD application also handles the Bureau's IT Change Management function for IT

staff in the Central Office. Change management is a separate module within JSD which handles requests for changes to Bureau enterprise IT systems and applications. These requests are processed, tracked, and audited in compliance with applicable IT security standards and policies. In addition to the foregoing, change requests in JIRA Service Desk contain additional information such as: references regarding a roll-out plan for the change, a back-out plan, and a date field to indicate when a change is scheduled for subsequent review, including an associated comment field. Also, change requests are classified according to change type (routine, emergency, etc.) and security impact (high, medium, low). Change requests contain a name and email address to identify the requester.

The JSD application will also support reporting of IT security incidents, including breaches of PII. These tickets are opened by IT staff or system owners at the relevant location. The tickets are then routed to the Information Security Programs Office where they are processed in accordance with BOP IT Security policy and DOJ Data Breach policy. Information security incidents are only accessible by the reporting IT department, the Information Security Programs Office, and the Senior Component Official for Privacy (SCOP) and designees. Security incident investigations may require a variety of information, including PII, to be included in the system, depending on the nature of the incident.

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
X	Statute	Federal Information Security Modernization Act of 2014, Public Law No. 113-283; 5 USC 3301-3302: Authority for employment
X	Executive Order	Executive Orders 9397, as amended by 13478, 9830, and 12107; the BOP determined that the use of the SSN is necessary to ensure proper tracking/association between the individual's clearance record and the individual's OPM case file, which is associated with the SSN.
	Federal Regulation	
	Agreement, memorandum of understanding, or other documented arrangement	
X	Other (summarize and provide copy of relevant portion)	OMB Memorandum 17-12, *"Preparing for and Responding to a Breach of Personally Identifiable Information,"*

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	Names of BOP staff or contractors. The system does not routinely collect non-BOP staff or contractor names, however, it may be included if a security incident is being investigated and involves such data.
Date of birth or age	X	A, B, C and D	The system does not routinely collect date of birth or age, however, it may be included if a security incident is being investigated and involves such data.
Place of birth	X	A, B, C and D	The system does not routinely collect place of birth information, however, it may be included if a security incident is being investigated and involves such data.
Gender	X	A, B, C and D	The system does not routinely collect gender information, however, it may be included if a security incident is being investigated and involves such data.

(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
Race, ethnicity or citizenship	X	A, B, C and D	The system does not routinely collect race, ethnicity, or citizenship information, however, it may be included if a security incident is being investigated and involves such data.
Religion	X	A, B, C and D	The system does not routinely collect religion information, however, it may be included if a security incident is being investigated and involves such data.
Social Security Number (full, last 4 digits or otherwise truncated)	X	A, B, C and D	SSNs of BOP staff or contractors. The system does not routinely collect non-BOP SSNs, however, it may be included if a security incident is being investigated and involves such data.
Tax Identification Number (TIN)	X	A, B, C and D	SSNs of BOP staff or contractors are collected as noted above. SSNs are considered TINs. The system does not routinely collect non-BOP TINs, however, they may be included if a security incident is being investigated and involves such data.
Driver's license	X	A, B, C and D	The system does not routinely collect Driver's license information, however, it may be included if a security incident is being investigated and involves such data.
Alien registration number	X	A, B, C and D	The system does not routinely collect Alien registration numbers, however, it may be included if a security incident is being investigated and involves such data.

(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
Passport number	X	A, B, C and D	The system does not routinely collect passport numbers, however, it may be included if a security incident is being investigated and involves such data.
Mother's maiden name	X	A, B, C and D	The system does not routinely collect mother's maiden names, however, it may be included if a security incident is being investigated and involves such data.
Vehicle identifiers	X	A, B, C and D	The system does not routinely collect vehicle identifiers, however, it may be included if a security incident is being investigated and involves such data..
Personal mailing address	X	A, B, C and D	The system does not routinely collect personal contact PII, however, it may be included if a security incident is being investigated and involves such data.
Personal e-mail address	X	A, B, C and D	The system does not routinely collect personal contact PII, however, it may be included if a security incident is being investigated and involves such data.
Personal phone number	X	A, B, C and D	The system does not routinely collect personal contact PII, however, it may be included if a security incident is being investigated and involves such data.
Medical records number	X	A, B, C, and D	The system does not routinely collect medical records numbers, however, it may be included if a security incident is being investigated and involves such data.

(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
Medical notes or other medical or health information	X	A, B, C and D	The system does not routinely collect medical information, however, it may be included if a security incident is being investigated and involves such data.
Financial account information	X	A, B, C and D	The system does not routinely collect financial account information, however, it may be included if a security incident is being investigated and involves such data.
Applicant information	X	A, B, C and D	The system does not routinely collect applicant information, however, it may be included if a security incident is being investigated and involves such data.
Education records	X	A, B, C and D	The system does not routinely collect education records, however, it may be included if a security incident is being investigated and involves such data.
Military status or other information	X	A, B, C and D	The system does not routinely collect military status information, however, it may be included if a security incident is being investigated and involves such data.
Employment status, history, or similar information	X	A, B, C and D	Title and employment information of BOP staff or contractors. The system does not routinely collect non-BOP employment information, however, it may be included if a security incident is being investigated and involves such data.

(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
Employment performance ratings or other performance information, e.g., performance improvement plan	X	A, B, C and D	The system does not routinely collect employment performance information, however, it may be included if a security incident is being investigated and involves such data.
Certificates			
Legal documents	X	A, B, C and D	The system does not routinely collect legal documents, however, it may be included if a security incident is being investigated and involves such data.
Device identifiers, e.g., mobile devices	X	A, B, C and D	BOP issued mobile device phone numbers. The system does not routinely collect this PII on non-BOP individuals, however, it may be included if a security incident is being investigated and involves such data.
Web uniform resource locator(s)			
Foreign activities			
Criminal records information, e.g., criminal history, arrests, criminal charges	X	A, B, C and D	The system does not routinely collect criminal records information, however, it may be included if a security incident is being investigated and involves such data.
Juvenile criminal records information	X	A, B, C and D	The system does not routinely collect juvenile criminal records information, however, it may be included if a security incident is being investigated and involves such data.

(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
Civil law enforcement information, e.g., allegations of civil law violations	X	A, B, C and D	The system does not routinely collect civil law enforcement information, however, it may be included if a security incident is being investigated and involves such data.
Whistleblower, e.g., tip, complaint or referral	X	A, B, C and D	The system does not routinely collect whistleblower information, however, it may be included if a security incident is being investigated and involves such data.
Grand jury information			
Information concerning witnesses to criminal matters, e.g., witness statements, witness contact information	X	A, B, C and D	The system does not routinely collect witness information, however, it may be included if a security incident is being investigated and involves such data.
Procurement/contracting records	X	A, B, C and D	The system does not routinely collect procurement information, however, it may be included if a security incident is being investigated and involves such data.
Proprietary or business information	X	A, B, C, and D	Business email addresses, phone number, and facility of BOP staff or contractor. The system does not routinely collect non-BOP staff or contractor business contact information, however, it may be included if a security incident is being investigated and involves such data.
Location information, including continuous or intermittent location tracking capabilities			
Biometric data:			

(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
- **Photographs or photographic identifiers**	X	A, B, C and D	The system does not routinely collect photographs or photographic identifiers, however, it may be included if a security incident is being investigated and involves such data.
- **Video containing biometric data**			
- **Fingerprints**			
- **Palm prints**			
- **Iris image**			
- **Dental profile**	X	A, B, C and D	The system does not routinely collect dental profile information, however, it may be included if a security incident is being investigated and involves such data.
- **Voice recording/signatures**	X	A, B, C and D	The system does not routinely collect voice recordings or signatures, however, it may be included if a security incident is being investigated and involves such data.
- **Scars, marks, tattoos**	X	C and D	The system does not routinely collect information on scars, marks, or tattoos, however, it may be included if a security incident is being investigated and involves such data.
- **Vascular scan, e.g., palm or finger vein biometric data**			
- **DNA profiles**			
- **Other (specify)**			
System admin/audit data:			
- **User ID**	X	A	BOP staff UserID
- **User passwords/codes**			
- **IP address**			

(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
- **Date/time of access**	X	A	Date and time of access of BOP users.
- **Queries run**			
- **Content of files accessed/reviewed**			
- **Contents of files**			
Other (please list the type of info and describe as completely as possible):			

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	X
State, local, tribal		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	X	Public media, Internet	X	Private sector	X
Commercial data brokers					
Other (specify): Security incident information may derive from contractors, third parties, and other non-government sources.					

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	Information is shared within BOP to authorized staff with direct need to know.
DOJ Components	X			Security incident information is shared with the Justice Security Operations Center (JSOC) and the Office of Privacy and Civil Liberties (OPCL) for investigation, mitigation, and documentation.
Federal entities	X			Security incident information is shared with the Department of Homeland Security's (DHS) Cybersecurity and Infrastructure Security Agency (CISA) if necessary on a case-by-case basis for incident reporting.
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.

Notice is given in the below published SORNs:

JUSTICE/DOJ-002, "Department of Justice Computer Systems Activity and Access Records." Most recent complete notice: 64 Fed. Reg. 73585 (1999). Subsequent notices reflecting adjustments to the system: 66 FR 8425 (2001) (modification of routine uses); 72 FR 3410 (2007) (modification of routine uses). Available at: https://www.gpo.gov/fdsys/pkg/FR-1999-12-30/pdf/99-33838.pdf.

OPM/GOVT-001, "General Personnel Records." Most recent complete notice: 77 Fed. Reg. 79694 (Dec. 11, 2012). Subsequent notice reflecting adjustments to the system: 80 Fed. Reg. 74815 (Nov. 30, 2015) (modification of routine uses). Available at: https://www.govinfo.gov/content/pkg/FR-2012-12-11/pdf/2012-29777.pdf.

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.

None. BOP staff are not provided the opportunity to opt out of participating in the collection, use, or dissemination of their information in the system. BOP staff who do not utilize the system may be unable to perform their job functions or access services requested through the system. Information on members of the public is not normally collected within the system, unless it is added as part of an internal investigation, therefore, they do not have an opportunity to decline to provide information.

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 gain access to information pertaining to them by filing a Freedom of Information Act (FOIA) and/or Privacy Act request. Procedures on how to complete a FOIA/Privacy Act request are published on the BOP's website at www.bop.gov.

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-ed under BOPNet on 9/22/2020. **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:** No outstanding POAMs.
	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:** Documentation is audited during program reviews and internal audits. Access to certain sensitive information requires specific authorization and is limited to select personnel.
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:** User access is audited frequently as part of internal reviews.
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**.
X	**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:** Specific training documents on system use will provided for all authorized users within the BOP.

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?

JSD system roles are assigned and privileges to view data within the system are based on such roles. While general access to the JSD customer portal is available to any user with BOPNet access, user access to specific roles must be initiated by an applicable supervisor. User access

for contractors is requested by the applicable program/project manager. Access to certain sensitive information, such as HR information and security incident information, requires specific authorization and is limited to select personnel. Additionally, access to the system is limited to those persons who have an appropriate security clearance, which is regularly reviewed, and a need to know based on job function. User access is audited frequently as part of internal reviews. There are no outside users who are permitted access to the JSD 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 JSD.

Users are trained as to the sensitive nature of the data within the JSD system and continuously reminded as to the need to strictly control the viewing and/or output of data from the systems. 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. All contractors who access Bureau information or systems are required to attend initial security awareness training during orientation. In order to protect PII and other sensitive information, data transmission is encrypted using the TLS protocol both within and outside the system.

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 approved retention schedules are:

GRS 3.1, Item 030: Configuration and Change Management Records; temporary; Destroy 5 years after system is superseded by new iteration or is terminated, defunded, or no longer needed for agency/IT administrative purposes, but longer retention is authorized if required for business use.

GRS 5.8, Item 10: Technical and administrative help desk operational records; temporary; Destroy 1 year after resolved, or when no longer needed for business use, whichever is appropriate.

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:

JUSTICE/DOJ-002, "Department of Justice Computer Systems Activity and Access Records." Most recent complete notice: 64 Fed. Reg. 73585 (1999). Subsequent notices reflecting adjustments to the system: 66 FR 8425 (2001) (modification of routine uses); 72 FR 3410 (2007) (modification of routine uses). Available at: https://www.gpo.gov/fdsys/pkg/FR-1999-12-30/pdf/99-33838.pdf.

OPM/GOVT-001, "General Personnel Records." Most recent complete notice: 77 Fed. Reg. 79694 (Dec. 11, 2012). Subsequent notice reflecting adjustments to the system: 80 Fed. Reg. 74815 (Nov. 30, 2015) (modification of routine uses). Available at: https://www.govinfo.gov/content/pkg/FR-2012-12-11/pdf/2012-29777.pdf.

Section 8: Privacy Risks and Mitigation

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 JSD. The unnecessary collection of data poses a risk of the loss of personal information to BOP staff, inmates and members of the public due to the sensitivity of the data involved, such as HR-related information and security incident information. 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 JSD. These measures include creating certain defined data fields where required information can be inserted and creating separate modules to handle different kinds of data such as HR information and security incident tickets.

There is also a potential privacy risk arising from collecting information of inadequate quality on each individual. To mitigate this, the JDS collects information directly from the individual about whom the information pertains to the greatest extent practicable. This includes collecting HR-related information from the relevant employees and security incident information from the IT staff or system owners at the relevant location.

In order 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 JSD 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. For

example, SSNs and other HR-related information are restricted for viewing only by HR staff and IT system administrators while information security incidents are only accessible by the reporting IT department, the Information Security Programs Office, and the SCOP and designees. Additionally, access to the system is limited to those persons who have an appropriate security clearance, which is regularly reviewed, and a need to know based on job function.

Staff are annually trained on how to properly handle sensitive information to mitigate the risks arising from improper use or disposal of the information. Additionally, in order to address the threats to the integrity of the data from unauthorized access, there are no outside users who are permitted access to the JSD 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 JSD.

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.

The system does not share HR information outside of authorized individuals within BOP. Security incident information may be shared on a case-by-case basis with CISA, JSOC and OPCL as necessary in order to appropriately investigate, report, and document incidents in accordance with the appropriate authorities. These restrictions help address the risk of disclosure of information to unauthorized individuals both inside and outside BOP.