Federal Bureau of Prisons

Privacy Impact Assessment
for the
Inmate Visiting System

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: [March 27, 2023]

(May 2019 DOJ PIA Template)

Section 1: Executive Summary

The Federal Bureau of Prisons (BOP) is responsible for the custody and care of federal offenders. As part of such custody, the BOP ensures inmates maintain community ties by providing a capability for inmates to visit with family, friends, and members of the public. The Inmate Visiting System, hereinafter called IVIS or system, is used to manage and monitor such activity. BOP has prepared a Privacy Impact Assessment for IVIS because this system collects, maintains, and disseminates information in identifiable form about visitors, as well as affiliated inmates and BOP staff.

The system retrieves and displays inmate data, such as, the inmate's name, register number, housing unit assigned, and work detail from the BOP's inmate management system. The system also contains inmate visitor data, such as, approved inmate visitor name, relationship to the inmate, date of birth, sex, race, ethnicity, driver's license or state id number, passport number, alien registration number, legal residence, phone number, and date of approval.

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.

The BOP is responsible for the management, custody, and care of individuals who are directly committed to its custody. Information in the system is collected and maintained to better ensure the safety, security, and good order of BOP facilities; to improve staff ability to quickly account for inmates and inmate visitors onsite in the event of an emergency, such as an institution disturbance or a natural disaster; to identify and, where appropriate, determine the suitability of inmate visitors with respect to entering BOP facilities; and, to more effectively prevent violations of institution policy and/or criminal activity, such as inmate escapes and the introduction of contraband.

In order to initiate the visiting process, inmates must request the Visitor Information form to send to potential visitors (e.g. friends and family). Potential visitors will fill out the form and submit it to the BOP for approval. The information collected is used by BOP staff to initiate background investigations and determine suitability to visit the inmate. The background check is not conducted within IVIS, however, once the background process is completed, relevant information on approved visitors is entered into the IVIS application by BOP staff. IVIS is then used by BOP front office staff to account for visitors at BOP facilities.

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	18 USC § 3621, 4042, and 5003 (state inmates), Section 11201 of Chapter 1 of Subtitle C of Title XI of the

		National Capital Revitalization and Self-Improvement Act of 1997 (Pub. L. 105-33); and 111 Stat. 740 (DC felons)
	Executive Order	
	Federal Regulation	
	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, C, and D	First and last names of BOP staff, inmates, and visitors.
Date of birth or age	X	C and D	Date of birth of visitors.
Place of birth			
Gender	X	C and D	Gender of visitors.
Race, ethnicity or citizenship	X	C and D	Race and ethnicity of visitors.
Religion			
Social Security Number (full, last 4 digits or otherwise truncated)	X	C	Social Security Numbers of visitors that are U.S. Citizens.
Tax Identification Number (TIN)			

(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
Driver's license	X	C and D	Driver's license number of visitors, if provided.
Alien registration number	X	C and D	Alien registration number of visitors that are not U.S. Citizens.
Passport number	X	C and D	Passport numbers of visitors that are not U.S. Citizens.
Mother's maiden name			
Vehicle identifiers			
Personal mailing address	X	C and D	Personal mailing address of visitors.
Personal e-mail address			
Personal phone number	X	C and D	Personal phone number of visitors.
Medical records number			
Medical notes or other medical or health information			
Financial account information			
Applicant information			
Education records			
Military status or other information			
Employment status, history, or similar information	X	C and D	Work detail of the inmate.
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			
Whistleblower, e.g., tip, complaint or referral			

(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
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	X	C and D	Housing Unit of the inmate.
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	User IDs of BOP staff and contractors.
- **User passwords/codes**			
- **IP address**			
- **Date/time of access**	X	A	Date and time of access of BOP staff.
- **Queries run**			
- **Content of files accessed/reviewed**			
- **Contents of files**			
Other (please list the type of info and describe as completely as possible):	X	A, C, and D	BOP staff User IDs, inmates federal register numbers, State IDs of visitors (if provided). Relationship between the visitor

(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
			and inmate and length of the relationship.

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		Hard copy: mail/fax	X	Online	
Phone		Email			
Other (specify):					

Government sources:					
Within the Component	X	Other DOJ Components		Online	
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		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	Access to the system is limited to only those BOP staff who require access to perform their official duties and such access is further refined via the use of role/group access management to enforce "least privilege" policies.
DOJ Components				
Federal entities				
State, local, tribal gov't entities				
Public				
Counsel, parties, witnesses, and possibly courts or other judicial tribunals for litigation purposes	X			Records will be provided on a case-by-case basis pursuant to valid legal process.
Private sector			X	System contractors will have direct log-in access for maintenance and production access to those aspects of the system managed by them.
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.***

Members of the public wishing to enter a BOP facility for inmate visitation are provided the BOP's Visitor Information form #BP-A0629, which provides notice of the collection, use and possible sharing of their information. BOP is in the process of updating the form to include a full Privacy Act § 552a(e)(3) Statement. Additionally, the SORNs listed below provide additional generalized notice to the public.

DOJ/BOP-005, Inmate Central Records System, last published in full at 84 Fed. Reg. 19808 (May 6, 2019), available at https://www.govinfo.gov/content/pkg/FR-2019-05-06/pdf/2019-09204.pdf.

DOJ/BOP-010, Access Control Entry-Exit System, last published in full at 67 Fed. Reg. 16760 (Apr. 8, 2002), available at https://www.gpo.gov/fdsys/pkg/FR-2002-04-08/pdf/02-8424.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.

Inmates must request and are provided the Visitor Information form #BP-A0629 to send to potential visitors (e.g. friends and family). Inmates must consent to the collection of their information in order to request a visitor. Potential visitors fill out the form and submit it to the BOP for approval. Completion of the form is voluntary, however, if an inmate's intended visitor does not complete the form, they will not be authorized to visit the inmate.

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.

The information entered into the system is either provided by members of the public or retrieved from other BOP systems. Individuals seeking to update information about themselves may provide a new Visitor Information form. Additionally, they 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 BOP's public website.

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):**

	BOPNet authorization date: 9/22/2022; exp date 3/24/2023 **If an ATO has not been completed, but is underway, provide status or expected completion date:** N/A **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:** BOP IT staff and contractors monitor system traffic to ensure the traffic is only via approved paths and to approved sites. BOP IT staff and contractors also perform user acceptance of any modification of the system prior to deployment.
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 routinely reviewed by system administrators. Additional auditing of transactional data will be captured and maintained to align with records & information management requirements.
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 training is conducted.

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?

Access to the system and data is limited to those persons who have an appropriate security clearance and are authorized to review such information for their official duties. Such access is regularly reviewed. User access is restricted to those staff who need to view and upload data, and user roles are defined to limit capability (e.g. only unit management staff are authorized to revise and update visiting lists). System access is web-based using a unique user ID and password. Access to the network requires two-factor authentication. All transmissions of data

are encrypted using the Transport Layer Security (TLS) encryption protocol. Data is also encrypted at rest through hardware encryption.

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.)

Disposition Authority: DAA-0129-2019-0004-0019- Item 19- Front Entrance Visitor Logs; Temporary; Destroy 5 years after cutoff.

The Visitor Information form #BP-A0629 is placed in the inmate's Case file, however, relevant information from the form is entered into IVIS. Once the information is entered into the system and validated, the paper copy of the form is destroyed. Disposition Authority: DAA-0129-2017-0002-0001- Institution Inmate Case File; Temporary; Destroy 10 years after expiration of sentence.

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:

DOJ/BOP-005, Inmate Central Records System, last published in full at 84 Fed. Reg. 19808 (May 6, 2019), available at https://www.govinfo.gov/content/pkg/FR-2019-05-06/pdf/2019-09204.pdf.

DOJ/BOP-010, Access Control Entry-Exit System, last published in full at 67 Fed. Reg. 16760 (Apr. 8, 2002), available at https://www.gpo.gov/fdsys/pkg/FR-2002-04-08/pdf/02-8424.pdf.

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

A potential privacy risk arising from IVIS is the over-collection of PII beyond what is necessary to accomplish BOP's official duties. The unnecessary collection of data poses a risk of the loss of personal information to potential visitors, BOP staff, and inmates due to the sensitivity of the data involved, such as Drivers' License numbers, passport numbers, and criminal history 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 IVIS. 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 on individuals that is inaccurate or outdated. To mitigate this, IVIS collects information directly from the potential visitor about whom the information pertains to the greatest extent practicable through the Visitor Information form. This information is further verified through appropriate background investigations. Paper forms are entered into the IVIS system manually by BOP staff and then destroyed to prevent any potential unauthorized access to the information through the paper form.

In order to mitigate the risk of unauthorized access or use, collected information is safeguarded in accordance with Bureau rules and policy governing 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 IVIS include the risk of unauthorized access to 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. 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. The duration of time to retain information is determined when business use ceases in accordance with BOP data storage/retention policy. Additionally, in order to address the threats to the integrity of the data from unauthorized access, there are no outside users, other than authorized contractors, who are permitted access to IVIS, 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's access to IVIS-specific information.

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 from 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. Additionally, the data in IVIS is segregated by location, limiting staff's ability to update visitor or inmate data unless the associated inmate is physically located/assigned to the local site. 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.