

Federal Bureau of Prisons



Privacy Impact Assessment for the BOP Government Website (BGW)

Issued by:
Michael Rogers
Acting RIM Chief / SCOP

Approved by: Andrew J. McFarland
Senior Counsel, Office of Privacy and Civil Liberties
U.S. Department of Justice

Date approved: September 18, 2025

(May 2019 DOJ PIA Template)

Section 1: Executive Summary

The Federal Bureau of Prisons (FBOP) Government Web (BGW) (formerly called BOP.GOV or BOPCloud) is the FBOP's public-facing website, which is hosted in Amazon GovCloud, a FedRAMP-certified environment. Information in the system includes descriptions of FBOP facilities, programs and services for federally incarcerated persons, FBOP career and employment opportunities, contracting processes, FBOP policies and forms, news stories, and applications such as Inmate Locator, Voicing a Concern regarding an inmate, and Privacy Act access and Freedom of Information Act (FOIA) Requests.

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 Government Website (BGW) provides members of the public with access to publicly available information regarding the FBOP and persons in its custody and care. BGW receives nightly uploads from the SENTRY system for inmate locator data. It enhances the FBOP's ability to communicate with the public, increases government transparency, promotes public participation and collaboration and facilitates a more efficient, streamlined process of information dissemination to the public. When sending a concern related to a FBOP matter or individual, members of the public may opt to provide their email address or complete a Privacy Act or FOIA request online using the public access link (PAL) instead of mailing a hard copy request. This data is not stored on the website; instead, it is transmitted to the FBOP FOIA Office via email. Once the request is received, it is then manually entered into the FBOP's FOIA case management system. Information in the BGW locator system may include:

- Inmate names, federal register numbers, District of Columbia Department of Corrections (DCDC) numbers, FBI or alien registration numbers, age, race, sex, physical housing location, and release date.
- Members of the public can opt to provide their names, mailing address, phone number, fax number, or email address.

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. §§ 3621, 4042, 5003 and section 11201 of Chapter 1 of Subtitle C of Title XI of the National Capital Revitalization and Self-Government Improvement Act of 1997; 5 U.S.C. §§ 552 (FOIA), 552a (Privacy Act).
Executive Order	

	Federal Regulation	
	Agreement, memorandum of understanding, or other documented arrangement	
	Other (summarize and provide copy of relevant portion)	Federal Cloud Computing Strategy ; OMB Memorandum M-10-06, Open Government Directive (December 8, 2009); OMB Memorandum M-10-22, Guidance for Online Use of Web Measurement and Customization Technologies (June 25, 2010); OMB Memorandum M-11-24, Streamlining Service Delivery and Improving Customer Service; OMB Memorandum M-17-06, Policies for Federal Agency Public Websites and Digital Services.

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
<i>Example: Personal email address</i>	<i>X</i>	<i>B, C and D</i>	<i>Email addresses of members of the public (US and non-USPERs)</i>
Name	<i>X</i>	<i>A, C and D</i>	Federally incarcerated persons, FBOP employees, and members of the public first and last names (US and non-USPERs)
Date of birth or age	<i>X</i>	<i>C and D</i>	Federally incarcerated persons (US and non-USPERs) dates of birth
Place of birth			
Sex	<i>X</i>	<i>C and D</i>	Federally incarcerated persons (US and non-USPERs) sex

Department of Justice Privacy Impact Assessment
Federal Bureau of Prisons/BOP Government Website (BGW)

Page 3

(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 Detainees; 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	C and D	Federally incarcerated persons (US and non-USPERs) race and ethnicity
Religion			
Social Security Number (full, last 4 digits or otherwise truncated)			
Tax Identification Number (TIN)			
Driver's license			
Alien registration number	X	C and D	Federally incarcerated persons (US and non-USPERs) alien registration number, if applicable
Passport number			
Mother's maiden name			
Vehicle identifiers			
Personal mailing address	X	C and D	Members of the public (US and non-USPERs) mailing address, if provided
Personal e-mail address	X	C and D	Members of the public (US and non-USPERs) email address, if provided
Personal phone number	X	C and D	Members of the public (US and non-USPERs) phone number (to include personal and fax), if provided
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			
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			

Department of Justice Privacy Impact Assessment
Federal Bureau of Prisons/BOP Government Website (BGW)
Page 4

(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
Criminal records information, e.g., criminal history, arrests, criminal charges	X	C and D	Scheduled federal execution dates have a posted notice which includes their publicly available offense information.
Juvenile criminal records information			
Civil law enforcement information, e.g., allegations of civil law violations			
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	X	C and D	Federally incarcerated persons (US and non-USPERs) FBOP facility location
Biometric data:			
- Photographs or photographic identifiers	X	A, B, C and D	Photos of federally incarcerated persons (US and non-USPERs), employees, and members of the public may be included in headline news articles, publications or recruitment videos posted on the site. Such publication only occurs with their documented consent.
- 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	Employee user IDs
- User passwords/codes	X	A	Employee user passwords

(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 Detainees; 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
- IP address	X	C and D	Internet domain, IP addresses, and type of browser of the user
- Date/time of access	X	C and D	When the user logged into the site
- Queries run	X	C and D	Webpages accessed by users and visitors
- Content of files accessed/reviewed			
- Contents of files			
Other (please list the type of info and describe as completely as possible):	X	C and D	Federally incarcerated persons (US and non-USPERs) federal register numbers, DCDC number, and/or FBI number.

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		Online	X
Phone		Email			
Other (specify):					

Government sources:					
Within the Component	X	Other DOJ Components	X	Online	
		Foreign (identify and provide the international agreement, memorandum of understanding, or other documented arrangement related to the transfer)			
State, local, tribal	X				
Other (specify): A website visitor can enter an inmate's alien registration number to find the inmate into the inmate locator page.					

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	Administrators within the FBOP have access to update the system and enter public information for the external facing website.
DOJ Components				
Federal entities				
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.

Generalized public notice is provided in the published SORN and privacy policy posted on the website:

- DOJ-002, Department of Justice Information Technology, Information System, and Network Activity and Access Records, 86 FR 37188 (July 14, 2021), available at: https://www.justice.gov/d9/pages/attachments/2021/08/02/2021-14986_-_doj-002_sorn_update.pdf.
- FBOP-005, Inmate Central Records System, 84 FR 24147 (May 6, 2019), available at: <https://www.govinfo.gov/content/pkg/FR-2019-05-06/pdf/2019-09204.pdf>.
- FBOP Privacy Policy, available at: https://www.bop.gov/website/privacy_policy.jsp.

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.*

Users may opt to provide their information, but it is not required for visiting the site. However, users are notified in the Privacy Policy that failure to provide the requested contact information may prevent FBOP from addressing their question or concern.

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 seek access or amendment to their information by submitting a FOIA or Privacy Act request, which is accessible on the FBOP website (<https://www.bop.gov/foia>) and in accordance with the procedures listed in SORNs DOJ-002 and BOP-005.

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): Granted under BOP-BGW 10/30/2020, last authorized 10/30/25, and expires on 10/30/2028. 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: N/A
	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: Access and roles within the system is limited to those persons who have an appropriate security clearance, which is reviewed annually, and is determined by their position description. Information is safeguarded by use of approved multi-factor authentication methods to access the system. System logs are monitored and analyzed on a regular basis, using authorized DOJ and FBOP methods.
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 and system administrator activities are regularly audited to ensure employee roles are current. Access controls are maintained daily and are routinely audited.
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. Contractors are screened, receive commensurate security clearances and complete training to understand their responsibilities under federal law and DOJ/FBOP 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: No additional privacy training is provided specific to this system; however, system administrators use internal procedures to determine what information is appropriate when adding information to BGW.

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?

Employees are given specific role-based access dependent on job roles. Data transmission

is encrypted, and employees must have valid credentials and authorization to access the system. User and system administration activities are regularly audited to ensure employee roles are current and access attempts are legitimate. Once an employee is transferred to another facility, transfers roles, or separates from the FBOP, their access is modified and/or terminated.

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.)*

BGW information will be held according to the applicable record schedule, GRS 6.4, Item 020-Public correspondence and communications not requiring formal action. Temporary. Destroy when 90 days 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:*

- DOJ-002, Department of Justice Information Technology, Information System, and Network Activity and Access Records, 86 FR 37188 (July 14, 2021), available at: https://www.justice.gov/d9/pages/attachments/2021/08/02/2021-14986_-_doj-002_sorn_update.pdf.
- BOP-005, Inmate Central Records System, 84 FR 24147 (May 6, 2019), available at: <https://www.govinfo.gov/content/pkg/FR-2019-05-06/pdf/2019-09204.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

Collecting and maintaining more personal information than necessary to accomplish FBOP’s official duties is a potential threat to privacy arising from BGW. Additional risks to privacy are inherent when the personal data is particularly sensitive or if the information is not

maintained securely.

The unnecessary collection of data poses a risk of the loss of personal information for inmates. FBOP mitigates this risk by only collecting and displaying data that is required to complete the authorized and necessary functions of BGW.

Collected information is safeguarded in accordance with Bureau 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 FBOP's use of the information in BGW include the risk of unauthorized access to information, threats to the integrity of the information arising from unauthorized access or improper disposal of information.

FBOP mitigates this risk 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.

FBOP employees are provided information security awareness training with regards to privacy, information security, and technical and physical controls over sensitive information on an annual basis. When an FBOP employee departs from the FBOP or transitions to a new position, the FBOP takes appropriate measures to deactivate the user's access to BGW.

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. 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. Additionally, information posted to the website is fully reviewed and approved to be placed on the BGW prior to releasing the information online.