Federal Bureau of Prisons

Privacy Impact Assessment
for the
Mailfast

Issued by:

Michael Rogers
RIM Chief / SCOP

Approved by: Victoria Garcia
Counsel
Office of Privacy and Civil Liberties
U.S. Department of Justice

Date approved: July 16, 2026

(March 2025 DOJ PIA Template)

Section 1: Executive Summary

Provide a high-level overview of the project or information technology (e.g., application, tool, automated process) in non-technical terms that describes the project or 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 Mailfast system is designed for law enforcement purposes to monitor, verify, and facilitate the delivery of incoming and outgoing inmate physical mail.[1] This system also assists in tracking whether an inmate has been released, is on restricted mail status, or is approved for inmate-to-inmate correspondence, and whether an inmate's mail requires monitoring for investigative purposes. Pursuant to the privacy provisions of the E-Government Act of 2002, the Federal Bureau of Prisons (FBOP) has prepared and will publish a Privacy Impact Assessment (PIA) for this system because it collects, maintains, and disseminates information in identifiable form of members of the public, namely inmates housed in FBOP custody.

Section 2: Purpose and Use of the Information Technology

2.1 Explain in more detail than above the purpose of the project or information technology, the type of technology used (e.g., databases, video conferencing, artificial intelligence, machine learning, privacy enhancing technologies), 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.

Mailfast displays information from other FBOP systems, primarily CICLOPS.[2] The systems for which information is displayed in Mailfast are the systems of records. The displayed information is live CICLOPS data, and anytime information is updated in CICLOPS, it automatically updates in Mailfast. FBOP Mailfast users may manually enter information into the system for approved inmate-to-inmate correspondence and mail monitoring status. The information entered into a specific record in Mailfast is copied from the record's originating systems of records. Mailfast is currently maintained on an on-premises solution and is being upgraded to the Amazon Web Services (AWS) GovCloud platform.

The information collected, maintained, used, and disseminated within Mailfast includes

---

[1] The Mailfast system includes the collection, use, processing, dissemination, storage, and access of information for the processing of physical mail to and from inmates. Electronic correspondence, such as emails, is covered in separate privacy compliance documentation and not maintained in this system.
[2] Privacy considerations concerning CICLOPS is evaluated in in separate privacy compliance documentation.

inmates' names, federal register numbers, facility housed, admission and release code, housing unit/quarters location, and start/end dates of mail monitoring, restricted mail status, and inmate-to-inmate correspondence approvals. This information is used to facilitate the delivery of incoming and outgoing inmate mail. For example, internal FBOP employees use the system to determine in which housing unit the inmate resides when processing physical mail to and from inmates.

Mailfast is only used to sort mail by typing in the inmates' register number. The FBOP employee processing the mail only uses Mailfast to check the inmate's register number, their location, whether a restricted mail status exists, and whether the inmate is approved to receive or send mail to another inmate. Based on the findings in Mailfast, additional steps may be taken, such as sending the mail to FBOP's Investigative Unit and physical checks conducted on the piece of mail for safety and security purposes. Information related to the forwarding or checks, however, is not documented in Mailfast.

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 (federal inmates), 5003 (state inmates) and Section 11201 of Pub. L. 105-33; 111 Stat. 740 (DC Offenders)
Executive Order	
Federal regulation	28 CFR part 540
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	C and D	First and last names of inmates being housed in federal facilities.
Date of birth or age			
Place of birth			
Sex			
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			
Vehicle identifiers			
Personal mailing address	X	C&D	Inmate facility and housing unit/quarters location, which serves as inmate's personal mailing address while in FBOP custody.
Personal e-mail address			
Personal phone number			
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			

(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
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			
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	FBOP employee User IDs

(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
- **User passwords/codes**			
- **IP address**			
- **Date/time of access**			
- **Queries run**			
- **Contents of files**			
Other (please list the type of info and describe as completely as possible):	X	C and D	Federal register numbers, restricted mail status, and inmate-to-inmate correspondence approvals of inmates housed in federal facilities.

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		Online	
Phone		Email			
Other (specify):					

Government sources:					
Within the Component	X	Other DOJ Components		Other federal entities	
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		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 FBOP employees who require access to perform their official duties and such access is further refined via the user 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				
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 kind of notice, if any, will be provided to individuals informing them about the collection, use, sharing or other processing of their PII, e.g., a Privacy Act § 552a(e)(3) notice? Will a System of Records Notice (SORN) be published in the Federal Register

providing generalized notice to the public? Will any other notices be provided? If no notice is provided to individuals or the general public, please explain.

The DOJ has published a System of Records Notice in the Federal Register which applies to the collection of inmate data:

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.

Additionally, inmates are also provided a general notice regarding the collection of their information when they are initially incarcerated as part of the inmate's Admission and Orientation. *See* FBOP Program Statement 5290.14, "Admission and Orientation Program," (April 3, 2003), available at: https://www.bop.gov/policy/progstat/5290_014.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.

Pursuant to 28 C.F.R. § 540.12, federal inmates are able to provide consent to send and receive general correspondence (physical mail). Inmates are notified that if they wish to send or receive physical mail, FBOP will open the inmate's mail prior to delivery to the inmate. If the inmate does not consent to FBOP opening their mail prior to their receipt, the inmate is notified that their mail will be returned to the Postal Service and the inmate will not receive their mail.

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.

Because inmate records are exempt from disclosure under the Privacy Act (see 28 CFR 16.97), inmate requests for records under the Privacy Act will be processed in accordance with the FOIA. 28 C.F.R. §§ 513.50; *see* 28 C.F.R. §§ 513.61-513.68.

Inmates are provided the opportunity to review their documents upon request. Inmates can submit a request by completing the *Request to Staff Member* form (Form BP-A0148) and submitting it to their housing unit team staff, providing any documentation they may have as to why the data needs to be corrected or amended. They receive notification of these procedures (how to amend or correct information) during their initial incarceration at Admission and Orientation, which every inmate is required to attend and every time they are transferred to another facility.

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) (if the system operates under an Authorization to Use (ATU) or other authorization mechanism, provide related details wherever an ATO is referenced):** **If an ATO has not been completed, but is underway, provide status or expected completion date:** Mailfast is currently authorized pursuant to the CICLOPS ATO, which was approved on 12/30/2025 and will expire on 12/29/2028. **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	**This information or information system has been assigned a security category as defined in Federal Information Processing Standards (FIPS) Publication 199, Standards for Security Categorization of Federal Information and Information Systems, based on the information it contains and consistent with NIST SP 800-60 v.2 rev.1, Guide for Mapping Types of Information and Information Systems to Security Categories: Appendices. Specify and provide a high-level summary of the justification, which may be detailed in the system security and privacy plan:** Mailfast maintains inmate-to-inmate correspondence approvals and mail monitoring status. All other information used in Mailfast is live SENTRY/CICLOPS data. If a loss of availability, integrity, or confidentiality regarding this information were to occur, the worst-case scenario would be that unauthorized disclosure might assist criminals to perpetrate fraud and result in an adverse effect on public confidence in the FBOP. Under NIST SP800-60 Volume 2, Rev 1, this information properly falls under federal correctional activities and community and social services, with default categorization of moderate, and special factors listed that could result in higher or lower impact level. Based on the specific use and information maintained in Mailfast, there are no aggravating or special factors that require a higher impact level. Therefore, based on the guidance in SP 800-60, a moderate impact level.
X	**Monitoring, testing, or evaluation has been undertaken to safeguard the information and prevent its misuse. Specify:** FBOP IT employees and contractors manage and maintain compliance of configuration changes required for maintenance, vulnerability management,

	and all continuous monitoring aspects of the system. They also perform configuration changes to improve the security posture when necessary. These activities include updating configuration baselines to remediate vulnerabilities, applying all security patches and editing of continuous monitoring profiles to increase auditing capabilities.
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:** Mailfast follows the Audit and Accountability (AU) controls by NIST 800-53 Rev. 5 Security and Privacy Controls for Information Systems and Organizations. Auditing by the system administrator provides visibility into important security events via log files and suspicious activities are forwarded to the FBOP for correlation, reporting, and archiving on a regular basis. Audit and accountability procedures are reviewed annually, and audit and accountability policies are reviewed every three years.
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 responsible for complying with the applicable policies and procedures in accordance with the security posture established by senior management and with applicable contracts with the FBOP. FBOP requires basic security and privacy awareness training for employees and contractors that support the operation of the contractor systems. Those who have additional access will have information security technical training for them to understand their information system security roles.
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:** There is no additional training for Mailfast.

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 FBOP employees who are authorized to review such information for their official duties. Such access is reviewed on a regular basis as defined in the Mailfast System Security and Privacy Plan. User access is restricted to employees who need to view and upload data, and user roles are defined to limit capability (e.g. only housing unit management employees are authorized to revise and update approved inmate to inmate mail lists). System access is web-based using a unique user ID and password. Access to the network requires two-factor authentication.

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.) If the project involves artificial intelligence and/or machine learning, indicate if the information is used for training AI models, and if so, how this will impact data retention and disposition.

Mailfast displays information that is maintained in other FBOP systems, such as CICLOPS. When information is manually entered into Mailfast, the entered information is updated in the record's originating system and the information entered into Mailfast is deleted from Mailfast. Therefore, the records in Mailfast are considered transitory as they contain real-time data from the inmate management system and information keyed into the system from other systems.

Records in Mailfast fall under General Records Schedule 5.2, item 010: Transitory Records. This includes records that meet the following conditions:

- They are required for only a short time (generally less than 180 days), and
- They are not required to meet legal or fiscal obligations, or to initiate, sustain, evaluate, or provide evidence of decision-making.

The disposition instructions are to destroy the records when no longer needed for business use, or according to an agency predetermined time period of business rule.

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/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.

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? For projects involving the use of artificial intelligence and/or machine learning, identify the privacy risks uniquely associated with the use of AI/ML, and how those risks are being mitigated, for example the risk of output inaccuracies and mitigations in the form of testing, continuous monitoring, training, secondary review, etc.

Note: When answering this question, please specifically address privacy risks and mitigation measures in light of, among other things, the following:

- ***Specific information being collected and data minimization strategies, including decisions made to collect fewer data types and/or minimizing the length of time the information will be retained (in accordance with applicable record retention schedules),***
- ***Sources of the information,***
- ***Type of technology employed (e.g. AI/ML),***
- ***Specific uses or sharing,***
- ***Privacy notices to individuals, and***
- ***Decisions concerning security and privacy administrative, technical, and physical controls over the information.***

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 Mailfast. FBOP mitigates this risk by only collecting the data that is required to complete the authorized and necessary functions. The risk of collecting erroneous or inaccurate information on inmates is also mitigated by only collecting what is necessary because FBOP employees are able to focus on a small set of data for mail processing to ensure accuracy. Mailfast connects directly to the inmate management system to obtain real-time data when processing the inmate mail.

b. Potential Risks Related to the Use of Information

Potential threats to privacy arising from FBOP's use of the information in Mailfast include erroneously misidentifying an individual. To mitigate this risk, FBOP employees are annually trained on how to properly handle sensitive information. There are also inherent checks within the process that prevent misidentification of an individual For example, if the FBOP employee uses Mailfast and determines mail needs to be forwarded to FBOP's Investigative Unit for further consideration of an investigation, authorized Investigative Unit employees review the material sent to them before starting or updating an investigation and the Investigative Unit can flag any erroneous misidentifications. Since Mailroom and Investigative Unit employees need to enter the inmate's register number, there are two instances where Mailfast information is checked against the unique inmate register number. This helps prevent misidentification.

c. Potential Risks Related to the Unauthorized Access of Information

There is a privacy risk to individuals arising from the potential unauthorized access to Mailfast information. This risk is mitigated by enforcing access controls and encryption at rest and in transit (as described above) and by providing auditing of user and system administration activities in accordance with DOJ security requirements, such as access permissions, account management, and data access.

Additionally, FBOP employees are annually trained on how to properly handle sensitive information. Administrative access to the system is limited to those persons who have a need-to-know based on job function. User access is reviewed on a regular basis as defined in the Mailfast System Security and Privacy Plan. Information is safeguarded in accordance with Bureau rules and policy governing automated information systems security and access. These safeguards include employee requirements concerning maintenance of records and technical equipment in restricted areas, and the required use of proper passwords and user identification codes to access the system. Only those Bureau personnel who require access to perform their official duties may utilize information in the system.