Federal Bureau of Prisons

Privacy Impact Assessment
for the
Inmate Management System (CICLOPS)

Issued by:
Sonya D. Thompson
Assistant Director / CIO

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

Date approved: August 3, 2023

(May 2019 DOJ PIA Template)

[This PIA should be completed in accordance with the DOJ Privacy Impact Assessments Official Guidance (and any supplemental guidance) at https://www.justice.gov/opcl/file/631431/download.] The following questions are intended to define the scope of the information in the information technology, specifically the nature of the information and the sources from which it is obtained. The responses should be written in plain language and should be as comprehensive as necessary to describe the information technology.]

Section 1: Executive Summary

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

The Inmate Management System (Centralized Inmate Case Logistics Operations and Planning System - CICLOPS) is a real-time information system consisting of various applications for processing sensitive but unclassified (SBU) inmate information and property management. BOP has prepared a Privacy Impact Assessment for CICLOPS because this system collects, maintains, and disseminates information in identifiable form about individuals. Data collected, maintained, and stored in CICLOPS includes information relating to the care, classification, subsistence, protection, discipline, and programs of incarcerated persons being housed in federal custody, as well as for criminal law enforcement purposes and intelligence activities.

CICLOPS is the modernization of the Sentry Inmate Case Management System that was developed and implemented in 1981. CICLOPS is a cloud-based system used to manage all aspects of an Inmate's incarceration. CICLOPS also supports data extracts for the Law Enforcement Information Sharing (LEIS)/Law Enforcement Officer (LEO) Data Integration Network (DIN), the Medical Claims Adjudication (MCA), the Management Analysis Portal (MAP), and other Law Enforcement Partners. CICLOPS is also used to facilitate the collection and transmission of inmate biometric data to the FBI via the Rapid Biometric Identification Data (RaBID) application.

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 information is collected to assist the Attorney General and the BOP in meeting statutory responsibilities for the safekeeping, care, and custody of incarcerated persons, including those sentenced to terms of imprisonment and those in pre-trial custody. It serves as the primary record system on these individuals and includes information critical to the continued safety and security of federal prisons and the public. The data collected is used to generate various daily, weekly, and monthly rosters to assist the institutions, regions and Central Office in the management of the BOP. CICLOPS also supports data extracts for various approved government entities and the following systems:

Data Integration Network (DIN): The DIN system is a cloud-based service used to facilitate the exchange of inmate data with the BOP's federal government law enforcement partners. The DIN service extracts data from CICLOPS on a periodic basis based on external agency requirements documented in an approved Memorandum of Agreement or Memorandum of Understanding. DIN does not store any data or have a user interface. The data disseminated includes demographic information about specific offenders based on defined criteria, e.g. demographic, discipline, education and sentencing data for the U.S. Probation Office is provided for inmates within two years of release.

Medical Claims Adjudication (MCA): The MCA system is a Commercial Off-the-Shelf (COTS) system used for facilitating the adjudication of medical billing and invoices generated by the BOP's outside health care service providers through a contract with a Comprehensive Medical Contractor (CMC). Federally incarcerated persons names, federal register numbers, dates of birth, and location data are generated in a daily electronic feed through CICLOPS which is securely shared with MCA. MCA also collects medical, lab, radiology and psychological claim information, i.e., treatment codes, provider name, service dates and locations.

Management Analysis Portal (MAP): The MAP system extracts information from CICLOPS and other sources and provides a collection of extensive statistical aggregate level information on each BOP institution, region, security level, and the BOP nationally. This data includes information about rated capacity, admissions and discharges, average daily population, inmate demographics, security designation, custody classification, urine surveillance, assaults, escapes, discipline, inmate grievances, education, and staff demographics. This allows BOP Executive Staff to compare institutions, analyze trends over time, and make management decisions based on such metrics.

Select authorized staff have additional access to view specific inmate data, such as federal register numbers, inmate name, age, criminal offense information, and COVID testing status.

Rapid Biometric Identification Data (RaBID): The RaBID system is used to communicate with the FBI's Criminal Justice Information Services to verify the identity of inmates being admitted or transferred within BOP custody using biometric data.

DOJ Joint Automated Booking System (JABS): The JABS is an information-sharing system as well as a conduit for sending inmate data directly to the Federal Bureau of Investigation's (FBI's) Integrated Automated Fingerprint Identification System (IAFIS) for identification and retrieval of criminal history. The following data is collected and transferred to JABS through RaBID: Incarcerated persons photos, fingerprints, federal register numbers, and inmate names.

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, 4003, 4042, 4082 and 5003 (state inmates), Section 11201 of Chapter 1 of Subtitle C of Title XI of the National Capital Revitalization and Self-Government Improvement Act of 1997 (Pub. L. 105-33; 111 Stat. 740)

	Executive Order	
	Federal Regulation	
	Agreement, memorandum of understanding, or other documented arrangement	Memorandums of understanding with: AOUSC, ARMY, Court Services and Offender Supervision Agency, Criminal Division, EOUSA, FBI, ICE, DEA, OIG, Parole Commission, Prisoner Transport Division, USMS, and Office of the Pardon Attorney.
	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 name of incarcerated persons in and released from the BOP. First initial of first name and last name of case management staff.
Date of birth or age	X	C and D	Dates of birth/age of incarcerated persons in and released from federal custody.
Place of birth	X	C and D	Place of birth of incarcerated persons in federal custody.
Gender	X	C and D	Gender of incarcerated persons in federal custody.
Race, ethnicity or citizenship	X	C and D	Race, ethnicity, and citizenship of incarcerated persons in federal custody.
Religion	X	C and D	Religious preferences, to include religious background and special religious dietary requirements of incarcerated persons in federal custody.

Social Security Number (full, last 4 digits or otherwise truncated)	X	C and D	Full SSN's of incarcerated persons in federal custody.
Tax Identification Number (TIN)			
Driver's license	X	C and D	Driver's license numbers (if available) of incarcerated persons in federal custody.
Alien registration number	X	C and D	Alien registration numbers of incarcerated persons in federal custody.
Passport number	X	C and D	Passport numbers of incarcerated persons in federal custody.
Mother's maiden name			
Vehicle identifiers			
Personal mailing address	X	C and D	Release address of incarcerated persons in federal custody.
Personal e-mail address			
Personal phone number			
Medical records number			
Medical notes or other medical or health information	X	C and D	Medical classification, physical and mental health data of incarcerated persons in federal custody.
Financial account information	X	C and D	Financial obligations owed to the federal courts of incarcerated persons in federal custody.
Applicant information			
Education records	X	C and D	Education participation records, including industrial and vocational of incarcerated persons in federal custody.
Military status or other information	X	C and D	Prior military status of incarcerated persons in federal custody.
Employment status, history, or similar information	X	C and D	Work detail assignments, and payroll records of incarcerated persons in federal custody.
Employment performance ratings or other performance information, e.g., performance improvement plan	X	C and D	Program selections, assignments, skills assessments, and performance or progress reports of incarcerated persons in federal custody.
Certificates	X	C and D	Certificates completed of incarcerated persons in federal custody.
Legal documents			

(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
Device identifiers, e.g., mobile devices			
Web uniform resource locator(s)			
Foreign activities			
Criminal records information, e.g., criminal history, arrests, criminal charges	X	C and D	Criminal history, arrests, criminal / pending charges, warrants, current sentencing and supporting information, sentence computations (federal, military, state, DC, and foreign), institution conduct records including information concerning disciplinary actions and reviews, participation in escapes, assaults, and disturbances, federal parole information, notifications to other federal and non-federal law enforcement agencies, release processing information of incarcerated persons in federal custody.
Juvenile criminal records information	X	C and D	Juvenile criminal records of incarcerated persons in federal custody.
Civil law enforcement information, e.g., allegations of civil law violations	X	C and D	Civil commitment orders about incarcerated persons in federal custody
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			

(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
Location information, including continuous or intermittent location tracking capabilities	X	C and D	Institution designation, transfer information, to include referrals of non-federal incarcerated persons to BOP custody and/or referral to BOP incarcerated persons to state custody, and housing assignments of incarcerated persons in federal custody.
Biometric data:			
- **Photographs or photographic identifiers**	X	C and D	Photographs of incarcerated persons in federal custody.
- **Video containing biometric data**			
- **Fingerprints**	X	C and D	Fingerprints of incarcerated persons in federal custody.
- **Palm prints**			
- **Iris image**			
- **Dental profile**			
- **Voice recording/signatures**			
- **Scars, marks, tattoos**	X	C and D	Scars, marks and tattoos of incarcerated persons in federal custody.
- **Vascular scan, e.g., palm or finger vein biometric data**			
- **DNA profiles**	X	C and D	Indication that the DNA profile was completed or needed of incarcerated persons in federal custody. Actual DNA profiles not stored in the system.
- **Other (specify)**			
System admin/audit data:			
- **User ID**	X	A	User IDs
- **User passwords/codes**			
- **IP address**	X	A	IP Address of system used
- **Date/time of access**	X	A	Date and time of user access
- **Queries run**	X	A	Transaction tracking
- **Content of files accessed/reviewed**			
- **Contents of files**			

(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
Other (please list the type of info and describe as completely as possible):	X	C and D	Federal register, FBI, DC Dept of Corrections, and State ID numbers of incarcerated persons in federal custody. Drug testing, test results and analysis records, physical descriptions of incarcerated persons in federal custody. Mail and visiting records, administrative remedy records, and investigatory information of incarcerated persons in federal custody.

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	
Phone	X	Email	X		
Other (specify):					

Government sources:					
Within the Component	X	Other DOJ Components	X	Online	
State, local, tribal	X	Foreign (identify and provide the international agreement, memorandum of understanding, or other documented arrangement related to the transfer)	X		
Other (specify): Federal Sentencing Courts; Foreign sources would only apply in connection with a treaty transfer inmate. The inmate's foreign sentencing information, which is provided by the foreign country, is entered into CICLOPS for designation and sentencing purposes.					

Non-government sources:					
Members of the public	X	Public media, Internet		Private sector	
Commercial data brokers					

Other (specify): Educational Institutions and health care providers.

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	Access to the system is limited to BOP staff who require access to perform official duties. Data is access controlled and segregated, limiting staff's ability to update inmate data. Data from the system is extracted for statistical purposes and placed into the BOP's internal statistical Management Analysis Portal (MAP) application for institution, regional, and Central Office use. Data extracts are also placed in the BOP's intelligence system for investigative purposes.

Recipient	How information will be shared			
	Case-by-case	**Bulk transfer**	**Direct log-in access**	**Explain specifics of the sharing, as well as how these disclosures will support and are compatible with the purposes of the collection.**
DOJ Components	X	X	X	Access is provided to DOJ Law Enforcement components in furtherance of criminal investigations or to facilitate prisoner operations. FBI, DEA, ATF, USMS, EOUSA, Criminal Division, U.S. Parole Commission, and Office of Inspector General have access on an individual query case-by-case basis, or thru approved MOUs, BOP enables bulk transfers of select datasets utilizing direct log-in, data extracts, and/or through the DIN. Data disseminated includes demographic information about specific offenders based on defined criteria, as well as specific information, e.g. discipline, education, and sentencing data.

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.**
Federal entities		X		Sharing with the Administrative Offices of the U.S. Courts for pre-release planning; sharing with the Criminal Justice Coordinating Counsel for the administration of admission or release of offenders from the District of Columbia; the Social Security Administration, the Veterans Administration, the Department of State Passport Services, and the Internal Revenue Service receive bulk transfer of inmate demographic and custody information, to include projected release dates, to facilitate benefits fraud detection via the DIN system or direct file transfers. Sharing with the U.S. Probation Office for inmates within two years of release through DIN.
State, local, tribal gov't entities	X			On a case-by-case basis for state, local, and tribal law enforcement entities, sentencing information and release dates on individual incarcerated persons may be shared for law enforcement purposes.

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.**
Public	X	X		Public inmate information is downloaded and transferred to a file which is uploaded onto the BOP's public facing Government website (BGW), which can be queried by members of the public using the inmate's name, federal register number, D.C. Department of Corrections (DCDC) number, alien registration number, or FBI number. Obtainable information includes the inmate's name, age, race, sex, current facility, and release date. On a case-by-case basis, members of the public may request information via the Freedom of Information Act. Any data which is releasable, without necessary signed consent from an inmate as required by the Privacy Act, will be provided.
Counsel, parties, witnesses, and possibly courts or other judicial tribunals for litigation purposes	X	X		Sharing with Federal Courts for court-related purposes in criminal prosecutions, civil court actions or regulatory Proceedings, through email or in-person.
Private sector		X		Medical data and billing information is downloaded and transferred to a file which is transmitted to the BOP's contract medical claim adjudication system.
Foreign governments	X			On a case-by-case basis, information may be shared with foreign and international law enforcement agencies for law enforcement purposes.
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:

BOP-004, Inmate Administrative Remedy Record System, last published in full at 67 FR 57244 (Sep. 9, 2002), available at: https://www.gpo.gov/fdsys/pkg/FR-2002-09-09/pdf/02-22792.pdf.

BOP-005, Inmate Central Records System, last published in full at 67 FR 31371 (May 9, 2002), available at: https://www.gpo.gov/fdsys/pkg/FR-2002-05-09/pdf/02-11578.pdf.

BOP-007, Inmate Physical and Mental Health Record System, last published in full at 67 FR 11712 (Mar 15, 2002), available at: https://www.gpo.gov/fdsys/pkg/FR-2002-03-15/pdf/02-6205.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. Incarcerated persons do not have the right to decline to provide the information while in federal custody. Incarcerated persons must provide identifiable information so they can be uniquely identified in the system for purposes of managing their custody.

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.

Under various provisions of the BOP Program Statement, incarcerated persons are provided the opportunity to request copies of and review their documents. They receive notification of these procedures, including how to amend or correct their information, during their incarceration after arriving at their designated institution. Inmates can submit a request by completing the Request to Staff Member form (Form BP-A0148) and submitting it to their unit team staff, providing any documentation they may have as to why the data needs to be corrected or amended. The public is advised of the opportunity and method to access their information via applicable System of Records Notices (see Section 7.2 below).

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):** CICLOPS ATO pending. **If an ATO has not been completed, but is underway, provide status or expected completion date:** Anticipated completion Q3 FY23. **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:** Access and roles within the system are limited to those persons who have an appropriate security clearance which is reviewed annually. Information is safeguarded by use of approved multi-factor authentication methods to access the system. System logs are monitored on a regular basis.
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 administration activities are regularly audited to ensure staff 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 all applicable IT security parameters 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 privacy training is provided.

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 controls are utilized by segregating the data inside the system and by limiting staff's ability to access/update inmate data. Staff are given specific role-based access dependent on job roles and location. Data transmission is encrypted and staff must have valid credentials and authorization to access the system. User and system administration activities are regularly audited to ensure staff roles are current and access attempts are legitimate. Once a staff member is transferred to another facility, transfers roles, or separates from the BOP, 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.)

Data is retained permanently. Records are transferred to NARA 60 years after record creation in CICLOPS or when records are no longer needed for agency use and purposes, whichever is later. The approved retention schedule is N1-129-04-007.

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:

BOP-004, Inmate Administrative Remedy Record System, last published in full at 67 FR 57244 (Sep. 9, 2002), available at: https://www.gpo.gov/fdsys/pkg/FR-2002-09-09/pdf/02-22792.pdf.

BOP-005, Inmate Central Records System, last published in full at 67 FR 31371 (May 9, 2002), available at: https://www.gpo.gov/fdsys/pkg/FR-2002-05-09/pdf/02-11578.pdf.

BOP-007, Inmate Physical and Mental Health Record System, last published in full at 67 FR 11712 (Mar 15, 2002), available at: https://www.gpo.gov/fdsys/pkg/FR-2002-03-15/pdf/02-6205.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?

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,***
- ***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 BOP's official duties is a potential threat to privacy arising from CICLOPS. Additional risks to privacy are inherent when the personal data is particularly sensitive or if the information is not maintained securely. For example, BOP collects and maintains a large amount of sensitive information on inmates within CICLOPS such as social security numbers, health information, and criminal history information, including PII, which is used for the administration of the inmates.

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

There is also a potential privacy risk arising from collecting information of inadequate quality on each individual. To mitigate this, a decision was made to collect data from a number of sources who could provide different perspectives regarding the individual as well as information based on their professional interaction and technical assessment.

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 BOP's use of the information in CICLOPS 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 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.

BOP staff 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 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 CICLOPS-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 CICLOPS is segregated by location, limiting staff's ability to update inmate data unless the 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.

There is additional privacy risk related to potential unauthorized access when information is shared with external entities. Some information in CICLOPS is shared with external entities as outlined in Section 4.1. In order to mitigate this risk, sharing with external law enforcement agencies is done on a case-by-case basis in accordance with established agreements.

Federal Bureau of Prisons

Privacy Impact Assessment Addendum
for the
Inmate Management System (CICLOPS)

Issued by:
Michael Rogers
RIM Chief / SCOP

Approved by: Peter A. Winn
Director
Office of Privacy & Civil Liberties
U.S. Department of Justice

Date approved: August 20, 2026

(October 2024 DOJ PIA Template)

This Addendum to the Privacy Impact Assessment (PIA) of the Centralized Inmate Case Logistics Operations and Planning System (CICLOPS) documents the addition by the Federal Bureau of Prisons (FBOP) of certain new features to CICLOPS. The original PIA for CICLOPS was signed by the Office of Privacy and Civil Liberties on August 1, 2023.[1]

The new changes to CICLOPS include:

1. Additional federal and state entities who receive data extractions;
2. Collection of records showing that the employees of direct recipients (federal agency partners) have completed required background investigations, training, and signed DOJ's Rules of Behavior for General Users prior to accessing CICLOPS or its associated systems; and
3. Direct connection between CICLOPS and Bed Book, Work Detail, and Inmate Labels (BWI) system and CICLOPS and the Facility Inmate Housing Display (FIHD) system.

FBOP has added more federal and state entities as data extract recipients than those originally identified in the CICLOPS PIA. These recipients receive CICLOPS data through the CICLOPS Secure File Transfer Protocol (SFTP), as well as multiple internal FBOP systems/applications that connect to and auto-populate inmate data from the CICLOPS database. Additional recipients include Department of Treasury, Department of Homeland Security (DHS) to include its law enforcement subcomponents, and the Federal Aviation Administration for the Federal Bureau of Prisons (FBOP) Inmate Case Management System (CICLOPS). See the information sharing table below, which clarifies changes made to the system since the PIA was originally signed on August 1, 2023.

CICLOPS now also collects records related to the required background investigations, training, and signed DOJ's Rules of Behavior for General User of direct recipients' employees' prior to accessing CICLOPS or its connected system is collected in CICLOPS.

Additionally, CICLOPS directly connects and provides live data to two additional FBOP systems: Bed Book, Work Detail, and Inmate Labels (BWI) and Facility Inmate Housing Display (FIHD). The two systems only display live CICLOPS data; the systems do not maintain or create new records.

BWI provides FBOP employees with information related to the identification, custody, and control of inmates or detainees while housed and/or assigned to a work detail in federal custody. Information in the BWI displays CICLOPS information that can be filtered by:

- Individual inmate name or register number,

[1] Although a new feature is being added to CICLOPS, the feature does not change the types of organizations that FBOP will share information with or information shared among users. The FBOP conducted a privacy analysis on the new feature and determined that the privacy risks and mitigations addressed in the existing CICLOPS Privacy Impact Assessment (PIA), which the Department of Justice (DOJ) approved on August 1, 2023, continue to apply to the new feature for the additional CICLOPS data recipients. Since the privacy risks have not changed, the PIA for CICLOPS does not need to be updated other than with this summary alerting the public to the new feature and that the current mitigations apply equally to the new feature. This document serves as a summary of the pertinent information for the purposes of Section 208 of the eGovernment Act of 2002, regarding a privacy evaluation similar to a PIA.

- Inmate work assignment,
- Inmate callouts (any scheduled appointment within the institution for each day, i.e., inmate medical appointment) entered in the inmate management system,
- Inmates' custody levels (community, out, in, or maximum based on criminal history, instant offense, and institutional adjustment),
- Inmates' medical care levels (Care 1 through 4 depending on health care needs), and
- All inmates who reside in specific housing unit and quarters within an institution.

Inmate custody and care levels dictate the degree of employee supervision and medical care needed. CICLOPS users can generate inmate labels by inputting the inmate's federal register number into the search field, and BWI will then produce a picture of the inmate, their full name, register number, date of birth, age, and sex. These labels are used by FBOP employees to verify the identity of the inmates.

FIHD provides the FBOP case management employees with information needed to determine, monitor, and manage facility, unit, housing, and work assignments for inmates and detainees while housed in federal custody.

Information in FIHD also displays information from CICLOPS, rather than create new records, and users can filter information by an inmate's specific institution, housing unit, or quarters assignments. This filtering quickly informs case management employees of access what beds are open and available for inmate cell or housing unit assignments (includes which housing unit inside the institution along with the range and cells inside each housing unit and which bed is assigned inside each cell), and inmate work assignments in each housing unit. Case management users can also filter FIHD information by the inmate population's age range, race, cell/unit, and work assignments.

The records associated with the additional changes identified in this Addendum are materially similar to the records described in the SORNs listed in the existing CICLOPS PIA, which include:

- JUSTICE/BOP-004,
- JUSTIC/BOP-005, and
- JUSTICE/BOP-007.

These changes do not affect the types of users with access to CICLOPS or to the information maintained within CICLOPS,[2] nor does the new feature substantially change any other privacy risks or mitigations addressed in the approved CICLOPS PIA.

[2] This Addendum notes that CICLOPS will provide new recipients with extracts of CICLOPS data not previously identified in the CICLOPS PIA. While added recipients include federal and state entities, only federal partners will receive direct access capabilities to CICLOPS and its associated systems. FBOP does not provide state entities with direct access to CICLOPS or its associated systems.

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	Access to the system is limited to BOP staff who require access to perform official duties. Data is access controlled and segregated, limiting staff's ability to update inmate data. Data from the system is extracted for statistical purposes and placed into the BOP's internal statistical Management Analysis Portal (MAP) application for institution, regional, and Central Office use. Data extracts are also placed in the BOP's intelligence system for investigative purposes.
DOJ Components	X	X	X	Access is provided to DOJ Law Enforcement components in furtherance of criminal investigations or to facilitate prisoner operations. FBI, DEA, ATF, USMS, EOUSA, Criminal Division, U.S. Parole Commission, and Office of Inspector General have access on an individual query case-by-case basis, or thru approved MOUs, BOP enables bulk transfers of select datasets utilizing direct log-in, data extracts through SFTP. Data disseminated includes demographic information about specific offenders based on defined criteria, as well as specific information, e.g. discipline, education, and sentencing data.

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.**
Federal entities		X		Sharing with the Administrative Offices of the U.S. Courts for pre-release planning; sharing with the Criminal Justice Coordinating Counsel for the administration of admission or release of offenders from the District of Columbia; the Social Security Administration, the Veterans Administration, the Department of State for Passport Services, the Internal Revenue Service (in accordance with 26 U.S.C. § 6116), and new information sharing with the DHS, the Department of Treasury, and the Federal Aviation Administration receive bulk transfer of inmate demographic and custody information, to include projected release dates, to facilitate benefits fraud detection via SFTP through direct file transfers. Sharing with the U.S. Probation Office for inmates within two years of release through STFP.
State, local, tribal gov't entities	X			On a case-by-case basis for state, local, and tribal law enforcement entities, sentencing information, and release dates on individual incarcerated persons may be shared for law enforcement purposes.

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.**
Public	X	X		Public inmate information is downloaded and transferred to a file which is uploaded onto the BOP's public facing Government website (BGW), which can be queried by members of the public using the inmate's name, federal register number, D.C. Department of Corrections (DCDC) number, alien registration number, or FBI number. Obtainable information includes the inmate's name, age, race, sex, current facility, and release date. On a case-by-case basis, members of the public may request information via the Freedom of Information Act. Any data which is releasable, without necessary signed consent from an inmate as required by the Privacy Act, will be provided.
Counsel, parties, witnesses, and possibly courts or other judicial tribunals for litigation purposes	X	X		Sharing with Federal Courts for court-related purposes in criminal prosecutions, civil court actions or regulatory proceedings, through email or in-person.
Private sector		X		Medical data and billing information is downloaded and transferred to a file which is transmitted to the BOP's contract medical claim adjudication system.
Foreign governments	X			On a case-by-case basis, information may be shared with foreign and international law enforcement agencies for law enforcement purposes.
Foreign entities				
Other (specify):				