Federal Bureau of Prisons

Privacy Impact Assessment
for the
Themis (BOP-Themis)

Issued by:

Michael Rogers

RIM Chief / SCOP

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

Date approved: May 22, 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 Federal Bureau of Prisons (FBOP) protects society by confining offenders in the controlled environments of prisons, and community-based facilities that are safe, humane, and appropriately secure, and which provide work and other self-improvement opportunities to assist offenders in becoming law-abiding citizens. FBOP's electronic legal case management system, BOP-Themis (Themis) collects and stores information regarding legal and administrative claims and disputes between the FBOP and incarcerated inmates, FBOP employees, and members of the public.

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.

Themis enables FBOP legal employees to track and manage litigation materials. Themis is made of the seven modules below. Themis and its modules currently run on IBM's Content Manager platform and is being migrated and upgraded to the Enterprise Cloud Platform (ECP) on the AWS Cloud platform.

Themis modules include:

- Civil Litigation (CIV): collects and stores civil and criminal litigation case files.
- Administrative Tort Claims (TRT): collects and stores documents and information regarding administrative tort claims under the Federal Tort Claims Act (FTCA), Military and Civilian Employees Claims Act (CECA) and Bureau of Prisons Claims Act (BOPCA).
- Commercial Law Branch (CLB): collects and stores government contract dispute case files.
- Legal Hold Notice (LHN): collects and stores notices to hold documents pursuant to legal process.
- Labor Law (LLB): collects and stores legal and administrative claims and disputes between the Federal Bureau of Prisons and current and former employees.
- Real Estate and Environmental Law (REL): collects and stores legal information

regarding compliance with environmental laws and acquisition of property for correctional facilities.

The system is used to store legal claims or case-related documents including pleadings, administrative claims, contracts, court documents (such as court orders, Pre-Sentence Investigation reports, etc.), discovery requests and materials, correspondence, etc., for the FBOP's Office of General Counsel (OGC). The system is designed to assist legal employees in tracking and monitoring all aspects of case and claim processing. Information is retrieved from the system by authorized legal employees only, via values such as case name, case number, FBOP region, FBOP institution, and claimant name.

Access to each module is limited to those employees who have an appropriate security clearance and are authorized to review such information for their official duties, The supervisor for each of the OGC workstreams is responsible for reviewing and ensuring employee information is accurate and access is necessary. The supervisor then sends the employee information to the system administrator, who then grants access to the user. The supervisor is also responsible to share any updates needed for access or removal to the system administrator. User access is restricted to those employees who need to view and upload specific module data, and user roles are defined to limit capability.

At present, CIV and TRT modules are inter-connected so that administrative claim files can be joined with litigation files if an appeal of the administrative claim is pursued in federal court. There is also an inter-connection between Themis and the FBOP's inmate case management system that shares information, such as the inmate's name and current facility location, from the inmate case management system to Themis.

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, 4082 and 5003 (state incarcerated inmates), Section 11201 of Pub. L. 105-33; 111 Stat. 740 (DC felons); 31 USC § 3721 (CECA); 31 USC 3722 (BOPCA); 28 U.S.C. § 1346(b); 28 U.S.C. § 2671-2680, (Tort Claims Procedure); and 44 U.S.C. § 3518 (c)(1).
Executive Order	
Federal regulation	28 C.F.R. Part 14 and 543 (FTCA)
Agreement, memorandum of understanding, or other documented arrangement	
Other (summarize and provide copy of relevant portion)	

Section 3: Information in the Information Technology

3.1 Indicate below what types of information that may be personally identifiable in Column (1) will foreseeably be collected, handled, disseminated, stored and/or accessed by this information technology, regardless of the source of the information, whether the types of information are specifically requested to be collected, and whether particular fields are provided to organize or facilitate the information collection. Please check all that apply in Column (2) and indicate to whom the information relates in Column (3). Note: This list is provided for convenience; it is not exhaustive. Please add to "other" any other types of information.

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to: A. DOJ/Component Employees, Contractors, and Detailees; B. Other Federal Government Personnel; C. Members of the Public - US Citizens or Lawful Permanent Residents (USPERs); D. Members of the Public - Non-USPERs	(4) Comments
Example: Personal email address	*X*	*B, C and D*	*Email addresses of members of the public (US and non-USPERs)*
Name	X	A, C and D	First and last name and aliases for inmates in custody and released from the FBOP, FBOP employees, or members of the public.
Date of birth or age	X	A, C and D	Date of birth and age of FBOP employees, members of the public, or inmates in custody or released from FBOP may be contained within documents gathered during course of proceedings.
Place of birth			
Sex	X	A, C and D	Sex of FBOP employees, members of the public, inmates in custody or released from FBOP may be contained within documents gathered during course of proceedings.
Race, ethnicity, or citizenship	X	A, C and D	Race, ethnicity, or citizenship of FBOP employees, members of the public, or inmates in custody or released from FBOP s may be contained within documents gathered during course of proceedings.
Religion			
Social Security Number (full, last 4 digits or otherwise truncated)	X	A, C and D	Full social security numbers of FBOP employees, members of the public, or inmates in custody or released from FBOP may be contained within documents gathered during course of proceedings.

(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
Tax Identification Number (TIN)	X	C	Bid protests include TIN, which is collected by the Commercial Law Branch and will be stored in the CLB module.
Driver's license	X	A, C and D	Driver's licenses of FBOP employees, members of the public, or inmates in custody or released from FBOP may be contained within documents gathered during the course of proceedings.
Alien registration number			
Passport number			
Mother's maiden name			
Vehicle identifiers	X	A, C and D	Vehicle information on employees or members of the public may be contained within documents gathered during the course of proceedings.
Personal mailing address	X	A, C and D	Personal mailing address of FBOP employees, released inmates or members of the public relevant to the matter or proceeding.
Personal e-mail address	X	A, C and D	Personal e-mail address of FBOP employees, released inmates or members of the public relevant to the matter or proceeding.
Personal phone number	X	A, C and D	Personal phone number of FBOP employees, released inmates or members of the public relevant to the matter or proceeding.
Medical records number	X	A, C, and D	Medical records numbers may be included in documents relevant to BOPCA claims.
Medical notes or other medical or health information	X	A, C and D	Medical notes or health information may be contained within documents gathered during the course of proceedings for FBOP employees, members of the public, or inmates in custody or released from FBOP.
Financial account information			
Applicant information	X	A, C and D	Various employment applications may be considered relevant to a matter or proceeding and contained within documents gathered during the course of proceedings for FBOP employees or members of the public.

(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
Education records	X	A, B, C and D	Education information may be contained within documents gathered during the course of proceedings for FBOP employees, members of the public, or inmates in custody or released from FBOP.
Military status or other information	X	A, C and D	Military status may be contained within documents gathered during the course of proceedings for FBOP employees or members of the public.
Employment status, history, or similar information	X	A	FBOP employees' work numbers, job title, email address, work address.
Employment performance ratings or other performance information, e.g., performance improvement plan	X	A, B, C and D	Employment information may be contained within documents gathered during the course of proceedings for FBOP employees, other Federal government personnel, or incarcerated/released inmates.
Certificates			
Legal documents	X	A, B, C and D	Legal documents are gathered throughout the course of proceedings and may relate to FBOP employees, other Federal government personnel, members of the public, or inmates in custody or released from FBOP.
Device identifiers, e.g., mobile devices			
Web uniform resource locator(s)			
Foreign activities			
Criminal records information, e.g., criminal history, arrests, criminal charges	X	A, C and D	Criminal records information concerning FBOP employees, members of the public, or inmates in custody or released from FBOP may be collected throughout the course of proceedings.
Juvenile criminal records information	X	A, C and D	Juvenile criminal records information may be contained within documents gathered during the course of proceedings on FBOP employees or inmates in custody or released from FBOP.
Civil law enforcement information, e.g., allegations of civil law violations	X	A, C and D	Civil law enforcement information may be contained within documents gathered during the course of proceedings for FBOP employees, members of the public, or inmates in custody or released from FBOP.

(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
Whistleblower, e.g., tip, complaint, or referral	X	A, B, C and D	Whistleblower information may be contained within documents gathered during the course of proceedings for FBOP employees, members of the public, or inmates in custody or released from FBOP.
Grand jury information			
Information concerning witnesses to criminal matters, e.g., witness statements, witness contact information	X	A, B, C and D	Witness information may be contained within documents gathered during the course of proceedings for FBOP employees, members of the public, or inmates in custody or released from FBOP.
Procurement/contracting records			
Proprietary or business information			
Location information, including continuous or intermittent location tracking capabilities			
Biometric data:			
- **Photographs or photographic identifiers**	X	A, C and D	Photographs may be contained within documents gathered during the course of proceedings for FBOP employees, members of the public, or inmates in custody or released from FBOP.
- **Video containing biometric data**			
- **Fingerprints**			
- **Palm prints**			
- **Iris image**			
- **Dental profile**	X	A, C and D	Dental information may be contained within documents gathered during the course of proceedings for FBOP employees or inmates in custody or released from FBOP.
- **Voice recording/signatures**	X	A, C and D	Voice recordings or signatures may be contained within documents gathered during the course of proceedings for FBOP employees, members of the public, or inmates in custody or released from FBOP.

(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
- **Scars, marks, tattoos**	X	C and D	No metadata fields specifically collecting such data. Scars, marks and/or tattoos may be contained within documents gathered during the course of proceedings for inmates in custody or released from FBOP..
- **Vascular scan, e.g., palm or finger vein biometric data**			
- **DNA profiles**			
- **Other (specify)**	X	C and D	Federal Register numbers of inmates in custody or released from FBOP.
System admin/audit data:			
- **User ID**	X	A	User IDs of FBOP employees.
- **User passwords/codes**			
- **IP address**			
- **Date/time of access**	X	A	Date/time of employee access.
- **Queries run**	X	A	Queries ran by employees.
- **Contents of files**	X	A	Record of modified file, date of modification, and modification action.
Other (please list the type of info and describe as completely as possible):	X	A, B, C and D	Due to the unpredictability of proceedings that are covered within Themis, it is possible the documents gathered in the course of proceedings and stored in Themis may include more information than what is identified in the Chart above.

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	Other federal entities	X

Government sources:					
State, local, tribal	X	Foreign (identify and provide the international agreement, memorandum of understanding, or other documented arrangement related to the transfer)			
Other (specify):					

Non-government sources:					
Members of the public	X	Public media, Internet		Private sector	
Commercial data brokers					
Other (specify): Parties to a proceeding, which may include attorneys representing FBOP employees in employment matters or other entities related to the different modules within Themis.					

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	Case information is shared within FBOP to authorized employees with direct need to know based on their employment requirements.

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			FBOP shares information to DOJ components who are representing the agency in legal proceedings. These litigating components receive data on a case-by-case basis when authorized FBOP employees share the information by downloading the data to their FBOP computers and then emailing or printing and providing the litigating components hard copies of the information contained in Themis.
Federal entities	X			FBOP may share Themis information with the U. S. Department of Homeland Security and its components relating to immigration proceedings.
State, local, tribal gov't entities				
Public				
Counsel, parties, witnesses, and possibly courts or other judicial tribunals for litigation purposes	X			FBOP employees may share Themis information as part of legal proceedings, including to the presiding court. FBOP shares Themis information by downloading the data to their FBOP computers, and then emailing or printing and providing the counsel, party, witness, or court hard copies of the information contained in Themis. Themis information is often shared with parties associated in accordance with or required by a discovery request or other court order.
Private sector				

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.**
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.

Notice is provided to the public via the System of Records Notices identified in Section 7.2.

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.

In most instances, the public does not have an opportunity or right to decline to provide information in Themis-related cases because claims could not be appropriately investigated or processed without such information. However, members of the public may have the ability to decline or expressly consent to providing their information at the initial point of collection, depending on the information collection (applications, government forms, etc.). Individuals may also have the opportunity to challenge information pertaining to them in the course of proceedings, such as with motions to suppress information or evidentiary challenges.

5.3 What, if any, procedures exist to allow individuals to gain access to information in the system pertaining to them, request amendment or correction of said information, and receive notification of these procedures (e.g., Freedom of Information Act or Privacy Act procedures)? If no procedures exist, please explain why.

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

Section 6: Maintenance of Privacy and Security Controls

6.1 The Department uses administrative, technical, and physical controls to protect information. Indicate the controls below. (Check all that apply).

X	**The information is secured in accordance with Federal Information Security Modernization Act (FISMA) requirements, including development of written security and privacy risk assessments pursuant to National Institute of Standards and Technology (NIST) guidelines, the development and implementation of privacy controls and an assessment of the efficacy of applicable privacy controls. Provide date of most recent Authorization to Operate (ATO) (if the system operates under an Authorization to Use (ATU) or other authorization mechanism, provide related details wherever an ATO is referenced):** The system is currently authorized pursuant to the BOPNet ATO, which was granted on 12/8/2025 and will expire on 12/8/2028. Based on the platform upgrade to the FBOP's AWS GovCloud, FBOP is in the process of creating a new ATO for BOP-Themis, which is to be finalized upon completion of privacy documentation. **If an ATO has not been completed, but is underway, provide status or expected completion date:** The new BOP-Themis ATO will be finalized upon completion of privacy documentation. **Unless such information is sensitive and release of the information could pose risks to the component, summarize any outstanding plans of actions and milestones (POAMs) for any privacy controls resulting from the ATO process or risk assessment and provide a link to the applicable POAM documentation:** No outstanding POAMs.
	This system is not subject to the ATO processes and/or it is unclear whether NIST privacy controls have been implemented and assessed. Please explain:
X	**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: Themis maintains Legal Defense, Investigation, Prosecution and Litigation, Resolution Facilitation, Labor Rights Management, Labor Relations, Central Records and Statistics Management, Inspections and Auditing, and Permits and Licensing. If a loss of availability, integrity, or confidentiality regarding this information were to occur, the worst-case scenario would be that individuals may suffer unauthorized disclosure of criminal or personal information, or the FBOP may suffer an adverse effect on public and inmate confidence. Under NIST SP800-60 Volume 2, Rev 1, this information properly falls under Litigation and Judicial Activities, Human Resource and Workforce Management, Regulatory Compliance and Enforcement, and General Government, with default categorization of High, and special factors listed that could result in higher or lower impact level. Themis does not present special factors. Based on the specific facts of this scenario, there are no mitigating, aggravating factors, or special factors because the information type categorizations held within Themis are sufficient, resulting in High impact level.
X	**Monitoring, testing, or evaluation has been undertaken to safeguard the information and prevent its misuse. Specify:** The system use is monitored and audited on a routine basis by FBOP's Cybersecurity Office. Testing of any modification is performed prior to deployment. In coordination with the supervisor of the FBOP employee attempting to gain access to Themis, the Cybersecurity Office ensures the employee's access authorization is limited and based on the employee's need to know that is listed in his/her specific position description (see Section 6.2 for more information).
X	**Auditing procedures are in place to ensure compliance with security and privacy standards. Explain how often system logs are reviewed or auditing procedures conducted:** The system tracks user account modifications and system events that will be reviewed by system administrators on a quarterly basis. Additional auditing of transactional data will be captured and maintained to align with records and information management requirements. A subset of approved internal users have been identified as system administrators to support organization-defined configuration, security, and access control.
X	**Contractors that have access to the system are subject to information security, privacy and other provisions in their contract binding them under the Privacy Act, other applicable laws, and as required by DOJ policy**.
X	**Each component is required to implement foundational privacy-related training for all component personnel, including employees, interns, and contractors, when personnel on-board and to implement refresher privacy training annually. Indicate whether there is additional training specific to this system, and if so, please describe:** Themis-specific training is conducted for authorized users within the FBOP.

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?

System roles and privileges are assigned based on need to know, in accordance with user's specific job description. Authorized legal supervisors must request user access by affirming that Themis access is required for the performance of the user's duties. User access for a contractor is requested by the applicable program/project manager. Access to certain sensitive information requires specific authorization by the employee's supervisor and is limited to select personnel. The ability to review, input, and modify legal claim data is restricted to those that directly process claims or have a need-to-know. Users receive Themis-specific training that explains to users the sensitive nature of the data within the modules and reminds users of the need to strictly control the visibility and sharing of the Themis data to those who have an authorized need-to-know. FBOP users receive annual training that addresses how to handle sensitive information and reminds users of their information security and privacy requirements and responsibilities. All employees who are involved in the management, operation, programming, maintenance, or use of a DOJ information system are made aware of the threats to and vulnerabilities of those systems and their responsibilities regarding privacy and information security. All contractors who access FBOP information or systems are also required to attend annual security awareness and privacy training.

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.

All records will be disposed of in accordance with the following records retention schedules:

- N1-129-88-001: Tort Claims: OGC Federal Tort Claims, Adjudication and Settlement Case Files- Case files maintained by office of record. Transfer to FRC 3 years after close of case. Destroy 12 years after close of case.

- N1-129-88-002: Litigation Case Files: Case files maintained by office of record. "These files result from litigation involving the Federal Bureau of Prisons and its employees. Case files are accumulated by BOP legal offices in their respective District Courts and by the Office of General Counsel in cases appealed to the United States Circuit Courts and the Supreme Court. Some of the documentation in a case file is duplicative of files maintained by the United States Attorney's Offices and other Department of Justice offices, but the BOP case file contains the necessary material for the Bureau's internal needs." These files include all electronic data associated with the case. The Office of General Counsel also maintains files regarding litigation cases considered for settlement. Transfer to FRC 3 years after close of case. Destroy 10 years after close of case.

- N1-129-09-020: Labor Law Content Management System: Digital Labor Law-related case content including PDF, word processing files, video, still images, audio files in a variety of electronic formats. Delete 5 years after final adjudication or when no longer needed for reference purposes, whichever is later.

- N1-129-09-021: Commercial Law Branch Content Management System:

  1. Digital content including PDF, word processing files, video, still images, audio files in a variety of electronic formats. (1) All content except content containing legal briefs and litigation reports. Delete 12 years after close of case. (2) Legal briefs and litigation report content. Delete 20 years after entry or when no longer needed for reference purposes, whichever is later.
  2. Jurisdiction File. The branch is responsible for determining whether the federal government will have exclusive jurisdiction over an institution (i.e., only federal laws shall apply), or whether jurisdiction will be shared between federal and state governments. Files consist of memoranda on individual institutions, plus memoranda and background information on the laws of various states. Destroy 5 years after close of institution.
  3. Subject Files. Background material accumulated on topics of continuing interest to staff members. Documentation includes correspondence, memoranda, legal publications, reports, journal articles, and publications from other agencies. Topics include alternative dispute resolution, drug abuse act, Lorton takeover, new employee orientation, and GAO rules and regulations. A. BOP-authored materials. Destroy when 5 years old or when no longer needed for reference purposes, whichever is later. B. External Publications. Destroy or when no longer needed for reference purposes, whichever is later.

- N1-129-09-022: Litigation Support Content Management System:

  - 1.C.1. All legal content, except legal briefs and litigation reports. Delete 12 years after close of the case.
  - 1.C.2. Legal briefs and litigation reports. Delete 20 years after entry or when no longer needed for reference purposes, whichever is later.

- N1-129-09-037: Commercial Law Content Management:

  1. CLB-CM Contract Advice Files - Data- scanned and/or electronic content concerning agency protests, bonds, common law employee statement of work reviews, dispute decisions, novation, change of name agreements, other than full and open competition, ratification of unauthorized commitments, terminations for default, utilities, and other required or discretionary contract advice. Document flow includes correspondence between parties, memoranda, and/or documents received from parties concerned. Copies of reference materials from legal journals or Westlaw

may also be added as well as other related papers. Destroy 15 years after date of contract advice issuance or when no longer needed for reference, whichever is later.

2. CLB-CM General Advisory Matter Files- Data- scanned and/or electronic content concerning appropriations, use of the Bureau seal, allegations of fraud, intellectual property, PCAP, Randolph-Sheppard, tax, or other non-contract advisory matters. Document flow includes correspondence between parties, memoranda, and/or documents received from parties concerned. Copies of reference materials from legal journals or Westlaw may also be added as well as other related papers. Destroy 20 years after date of contract advice issuance or when no longer needed for reference, whichever is later.
3. CLB-CM Policy Review Files- Data- scanned and/or electronic content pertaining to policy review files. Include executive staff paper reviews, initial program statement reviews, 10-day program statement reviews, or any other review of Bureau policy. Document flow includes correspondence between parties, memoranda, and/or documents received from parties concerned. Copies of reference materials from legal journals or Westlaw may also be added as well as other related papers. Destroy 10 years after date of policy advice issuance to the client, or when no longer needed for reference, whichever is later.
4. CLB-CM Agreement Files- Data- scanned and/or electronic content consisting of funded and unfunded agreements between the Bureau and another governmental entity, regarding facilities, fire/EMS assistance, housing BOP inmates, housing state inmates, medical, military, publications/software, staff, training for staff, transportation, utilities, and other funded agreements; canine searches, CST meeting areas, data sharing, emergency assistance, fire/EMS assistance, firing range, medical student preceptorship, public works projects, SENTRY access, training for inmates, training for staff, vending machines, and other unfunded agreements. Content consists of correspondence between parties; memoranda, copies of agreements or prior agreements between parties; copies of agreements or prior agreements on the same subject area; documents received from the parties. Copies of reference materials from legal journals or Westlaw may also be added as well as other related papers. Destroy 3 years after termination or expiration of the agreement, or when no longer needed for reference, whichever is later.
5. CLB-CM Contract Protests Case Files- Data- scanned and/or electronic content consisting of Contract case files arising from protests, appeals or other litigation before the Government Accountability Office, Court of Federal Claims, Court of Appeals for the Federal Circuit, and Civilian Board of Contract Appeals or other Board. Content consists of notices; responses; complaints; opinions; orders, correspondence between parties;

memoranda; copies of contracts, plans, specifications, exhibits, change orders, and amendments; transcripts of hearings; documents received from parties concerned; and final decisions, Copies of reference materials from legal journals or Westlaw may also be added as well as other related papers. Destroy 10 years after the closing of a case, or when no longer needed for reference, whichever is later.

6. CLB-CM Contract Case Files- Data- scanned and/or electronic content storing contract case files arising from appeals or other litigation before the Court of Federal Claims, Court of Appeals for the Federal Circuit, Federal district Courts, Federal Circuit Courts of Appeals, and Civilian Boards of Contract Appeals or other Boards. Content consists of notices; responses; complaints; opinions; orders; correspondence between parties; memoranda; copies of contracts, plans, specifications, exhibits, change orders, and amendments; transcripts of hearings; documents received from parties concerned, and final decisions. Copies of reference materials from legal journals or Westlaw may also be added as well as other related papers. a. Board of Contract Appeals Case Content - Data: Destroy 20 years after the closing of a case, or when no longer needed for reference purposes, whichever is later. b. Other Contract Case Content Assign to Non-CLB Attorneys - Data: Destroy 10 years after the contract file closes, or when no longer needed for reference purposes, whichever is later.
7. CLB-CM Other Litigation Case Files- Data- scanned and/or electronic case file content, other than those listed in Item #1, arising from proceedings before any court or 5th administrative tribunal, examples include Bankruptcy, Class Action, Amendment Takings, Fraud, Touhy/Non-Party, or other litigation. Content consists of notices, responses; complaints; opinions; orders; correspondence between parties; memoranda; copies of contracts, plans, specifications, exhibits, change orders, and amendments; transcripts of hearings; documents received from parties concerned; and final decisions. Copies of reference materials from legal journals or Westlaw may also be added as well as other related papers. Destroy 10 years after final resolution of the case, or when no longer needed, whichever is later.
8. CLB-CM Administrative Matters- Data- scanned and/or electronic records accumulated that relate to the internal administration or housekeeping activities of the office rather than the functions for which the office exists. In general, these records relate to the office organization, staffing, procedures, and communications, including facsimile machine logs; the expenditure of funds, including budget records; day-to-day administration of office personnel including training and travel; supplies and office services and equipment requests and receipts, and the use of office space and utilities. They may also include copies of internal activity and workload reports (including work progress, statistical, and narrative reports prepared in the office and forwarded to higher levels) and other

materials that do not serve as unique documentation of the programs of the office. Destroy when 3 years old, or when no longer needed, whichever is later.

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-004, BOP's Inmate Administrative Remedy Record System, , 67 FR 57244 (Sep. 9, 2002), last modified at 82 FR 24147 (May 25, 2017), and published at: https://www.gpo.gov/fdsys/pkg/FR-2002-05-09/pdf/02-11578.pdf;

JUSTICE/BOP-005, BOP's Inmate Central Records System, 48 FR 23711 (June 7, 1984),last modified at 84 FR 19808 (May 6, 2019), and published at: https://www.govinfo.gov/content/pkg/FR-2019-05-06/pdf/2019-09204.pdf;

JUSTICE/BOP-009, BOP's Administrative Claims Record System, p67 FR 41453 (June 18, 2002), last modified at 82 FR 24147 (May 25, 2017), and published at: https://www.gpo.gov/fdsys/pkg/FR-2017-05-25/pdf/2017-10780.pdf

JUSTICE/DOJ-002, DOJ Computer Systems Activity & Access Records, 86 FR 37188 (July 14, 2021), available at: https://www.justice.gov/opcl/page/file/1419896/download;

JUSTICE/DOJ-008, DOJ Grievance Records, 68 FR 61696 (Oct. 29, 2003), and last modified at 72 FR 3410 (Jan. 25, 2007), and published at: https://www.gpo.gov/fdsys/pkg/FR-2003-10-29/pdf/03-27194.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.***

Themis information is collected and retained in accordance with federal requirements, and no additional information is requested or retained. The information is collected in relation to pending and active administrative and judicial claims or investigations and used to support the processing of such claims and litigation by the Department of Justice. However, there are risks associated with FBOP's use of Themis that FBOP has attempted to mitigate as follows.

There is a privacy risk related to the inadvertent disclosure of information to people not authorized to receive it. While FBOP uses Themis as a case management system, there are various reasons the information contained in Themis is shared to others in FBOP or outside of FBOP, such as to DOJ litigators representing FBOP in a particular matter or to parties to a proceeding in accordance with an appropriate court order. To mitigate this risk, Themis users receive annual training on how to properly handle sensitive information and manage the data maintained in the Themis modules. FBOP also limits access to the system to those persons who have an appropriate security clearance which is regularly reviewed, need to know determined by job function, and completion of training on how to handle data within Themis and DOJ required annual privacy and cybersecurity training. The data is also segregated, limiting an employee's ability to update data they are not authorized to view or modify. Data transmission is also encrypted at rest and in transit.

There is also a risk of 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. Users who have access to modify or input data into case files are also limited to those users with a need to make such modifications, such as legal supervisors and employees who are responsible for managing the individual cases. There are also no outside users who have direct access to Themis or its modules, including the larger DOJ community. Additionally, when a FBOP employee departs from the FBOP or transitions to a new position, the FBOP takes appropriate measures to deactivate the user's access to Themis-specific information.

Lastly, there is a risk of mistaken name association with the case information in Themis. As in most cases where a record associates a person or entity with a criminal or civil investigation, the mere presence of a name in the system can generate the assumption of

involvement with unsavory activity or other damage to reputation. For this reason, there is no automated dissemination of information from this system outside of OGC. Any dissemination must be done pursuant to proper authority and management review (as indicated in Section 4.1).