Federal Bureau of Prisons

Privacy Impact Assessment
for the
Electronic Inmate Central File (eICF)

Issued by:
Sonya D. Thompson, Assistant Director/SCOP

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

Date approved: April 30, 2021

Section 1: Executive Summary

The Electronic Inmate Central File (eICF) datastore assists the BOP in meeting statutory responsibilities for the safekeeping, care and custody of offenders housed in federal custody. BOP has prepared a Privacy Impact Assessment for the eICF datastore because this system collects, maintains, and disseminates information in identifiable form about individuals. Specifically, eICF serves as a repository for storing and managing collections of data on pretrial offenders, convicted inmates, former inmates, and inmate visitors.

The information is used by BOP staff to carry out mission critical functions of the agency such as sentence computations, designation decisions, and documentation of inmate progress reports, assignments, correspondence, investigatory and discipline reports, transfer paperwork, and release and referral documents. The eICF datastore replaces the management of the paper file system by migrating business workflows and storage of paper files to an electronic storage and retrieval system. The eICF datastore also includes the following subsystems: the Insight system, the Discipline and Administration Reintegration Tracking System (DARTS), and the Residential Reentry Referral Management (R3M) system.

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 eICF datastore is a centralized role-based system. Each facility has access to data that pertains to the offenders housed at their location. eICF receives real time data updates from the SENTRY system, to include the offender's profile, housing assignments, medical care level, work detail, case management information, and education information. The system includes information critical to the continued safety and security of federal prisons and the public such as information and supporting documentation related but not limited to:

- Sentence computations (judicial orders and sentence impact documentation, and information concerning present offense, prior criminal background, and identification data);
- Designation decisions (separation orders and judicial recommendations);
- Work and payroll records, educational data, and physical and mental health data;
- United States Parole Commission orders, actions and related forms;
- Physical correspondence;
- Information relating to inmate contacts (to include background investigations of persons wishing to physically visit an inmate);
- Personal property records;
- Safety reports and rules;
- Media interview requests;
- Litigation-related records;
- Referrals of non-federal inmates to Bureau custody and/or referrals of Bureau inmates

to state custody;
- Documentation of inmate progress reports, assignments, and correspondence;
- Documentation concerning pending charges and wanted status including warrants;
- Requests from other federal and non-federal law enforcement agencies for notification prior to release;
- Investigatory and discipline reports (to include records of the allowance, forfeiture, withholding and restoration of good time); and
- Transfer paperwork; and release and referral documents.

The system also consists of subsystems or applications that collect, use, maintain, and disseminate information consistent with the following assessment of eICF below. The following subsystems or applications within eICF utilize the data in the eICF datastore to assist in various BOP functions:

Insight System: The Insight System, which includes a suite of applications (Insight, Insight Feedback, Release/Referral Application), was created to assist Unit Team staff in developing and managing individualized program and reentry plans for inmates, to include Program Reviews, Progress Reports, Residential Reentry Center/Home Confinement referrals, and transfer and release packets. The system enables program disciplines (Education, Psychology, Religious Services, and Health Services) the opportunity to provide case management staff with recommendations regarding needed programs to address criminogenic risks and written reports of the inmate's progress toward established goals or progress in completing recommended programs.

DARTS: The DARTS application is used to initiate, track, and document the Disciplinary Process from incident reporting to case disposition. DARTS allows staff the ability to create, search, investigate, upload, and complete documentation related to Unit Disciplinary Committee and Disciplinary Hearing Officer proceedings. The inmate discipline program is an essential tool in the management of the inmate population as it promotes a safe and orderly environment for inmates and staff.

R3M: The R3M solution automates the referral workflow between the Bureau and the Residential Reentry Centers (RRCs) and provides greater security, improved productivity and improved quality assurance. Prior to R3M, community confinement referrals were sent by fax or U.S. mail. Health services specialists also use R3M to review and determine precertification for inmate medical care requests submitted by RRCs. RRCs which receive inmate information from BOP are required to safeguard the data under their contracts with BOP.

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 U.S.C. §§ 3621, 4042, 5003 and section 11201 of Chapter 1 of Subtitle C of Title XI of the National Capital Revitalization and Self-Government Improvement Act of 1997.
	Executive Order	

Authority		Citation/Reference
	Federal Regulation	
	Agreement, memorandum of understanding, or other documented arrangement	
	Other (summarize and provide copy of relevant portion)	

Section 3: Information in the Information Technology

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

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to: A. DOJ/Component Employees, Contractors, and Detailees; B. Other Federal Government Personnel; C. Members of the Public - US Citizens or Lawful Permanent Residents (USPERs); D. Members of the Public - Non-USPERs	(4) Comments
Example: Personal email address	*X*	*B, C and D*	*Email addresses of members of the public (US and non-USPERs)*
Name	X	C and D	Names of pretrial offenders, convicted inmates, former inmates within eICF and all subsystems. Names of inmate visitors within eICF and Insight.
Date of birth or age	X	C and D	Dates of birth of pretrial offenders, convicted inmates, former inmates within eICF and all subsystems. Dates of birth of inmate visitors within eICF and Insight.
Place of birth	X	C and D	Places of birth of pretrial offenders, convicted inmates, and former inmates within eICF and Insight.
Gender	X	C and D	Gender of pretrial offenders, convicted inmates, former inmates,

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to: A. DOJ/Component Employees, Contractors, and Detailees; B. Other Federal Government Personnel; C. Members of the Public - US Citizens or Lawful Permanent Residents (USPERs); D. Members of the Public - Non-USPERs	(4) Comments
			and inmate visitors within eICF, Insight, and R3M.
Race, ethnicity or citizenship	X	C and D	Race, ethnicity and/or citizenship of pretrial offenders, convicted inmates, former inmates, and inmate visitors within eICF and Insight.
Religion	X	C and D	Religion of pretrial offenders, convicted inmates, and former inmates within eICF and Insight.
Social Security Number (full, last 4 digits or otherwise truncated)	X	C and D	Social Security Numbers of pretrial offenders, convicted inmates, former inmates, and inmate visitors within eICF and Insight.
Tax Identification Number (TIN)			
Driver's license	X	C and D	Driver's license information on pretrial offenders, convicted inmates, former inmates, and inmate visitors within eICF and Insight.
Alien registration number	X	C and D	Alien registration numbers of pretrial offenders, convicted inmates, former inmates, and inmate visitors within eICF and Insight.
Passport number	X	C and D	Passport numbers of pretrial offenders, convicted inmates, former inmates, and inmate visitors within eICF and Insight.
Mother's maiden name	X	C and D	Mother's maiden name of pretrial offenders, convicted inmates, and former inmates within eICF and Insight.
Vehicle identifiers			
Personal mailing address	X	C and D	Personal mailing addresses of pretrial offenders, convicted inmates, former inmates, and inmate visitors

(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
			within eICF, Insight, and R3M.
Personal e-mail address			
Personal phone number	X	C and D	Personal phone numbers of inmate visitors within eICF and Insight.
Medical records number			
Medical notes or other medical or health information	X	C and D	Basic health information of pretrial offenders, convicted inmates, and former inmates within eICF, Insight, and R3M.
Financial account information			
Applicant information			
Education records	X	C and D	Education records, to include diploma, GED, certificates, apprenticeships of pretrial offenders, convicted inmates, and former inmates within eICF and Insight.
Military status or other information			
Employment status, history, or similar information	X	C and D	Work assignment, payroll and history of pretrial offenders, convicted inmates, and former inmates within eICF and Insight.
Employment performance ratings or other performance information, e.g., performance improvement plan	X	C and D	Convicted inmates and former inmates as part of work assignments within eICF and Insight.
Certificates	X	C and D	Convicted inmates and former inmates as part of work assignments within eICF and Insight.
Legal documents	X	C and D	Legal documents of pretrial offenders, convicted inmates, and former inmates within eICF and Insight.
Device identifiers, e.g., mobile devices			
Web uniform resource locator(s)			
Foreign activities			
Criminal records information,	X	C and D	Criminal records

(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
e.g., criminal history, arrests, criminal charges			information on pretrial offenders, convicted inmates, former inmates, and inmate visitors within eICF and Insight.
Juvenile criminal records information	X	C and D	Juvenile criminal records information on pretrial offenders, convicted inmates, former inmates, and inmate visitors within eICF and Insight.
Civil law enforcement information, e.g., allegations of civil law violations			
Whistleblower, e.g., tip, complaint or referral			
Grand jury information			
Information concerning witnesses to criminal matters, e.g., witness statements, witness contact information			
Procurement/contracting records			
Proprietary or business information			
Location information, including continuous or intermittent location tracking capabilities	X	C and D	Prison, residential reentry, or home confinement location information of pretrial offenders, convicted inmates, and former inmates within eICF, Insight, and R3M.
Biometric data:			
- **Photographs or photographic identifiers**	X	C and D	Photographs of pretrial offenders, convicted inmates, and former inmates within eICF and all subsystems.
- **Video containing biometric data**			
- **Fingerprints**			
- **Palm prints**			
- **Iris image**			
- **Dental profile**			
- **Voice recording/signatures**			
- **Scars, marks, tattoos**	X	C and D	Recorded scars, marks, and tattoos of pretrial offenders, convicted

(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
			inmates, and former inmates within eICF and Insight.
- **Vascular scan, e.g., palm or finger vein biometric data**			
- **DNA profiles**		C and D	Testing status of pretrial offenders, convicted inmates, and former inmates within eICF.
- **Other (specify)**	X	C and D	Internal disciplinary records of pretrial offenders, convicted inmates, and former inmates within eICF, Insight, and DARTS.
System admin/audit data:			
- **User ID**	X	A	User IDs of DOJ users and administrators
- **User passwords/codes**			
- **IP address**			
- **Date/time of access**	X	A	Date/time of access log information on DOJ users and administrators
- **Queries run**			
- **Content of files accessed/reviewed**			
- **Contents of files**			
Other (please list the type of info and describe as completely as possible):			

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		Email	X		
Other (specify):					

Government sources:					
Within the Component	X	Other DOJ Components	X	Online	X

Government sources:					
State, local, tribal	X	Foreign (28 CFR § 0.96b allows for the Director of the BOP to receive from a foreign country, certifications and reports required under a treaty. A list of participating countries on the International Prisoner Treaty Unit list may be accessed through the website: http://www.justice.gov/criminal/oeo/iptu.)	X		
Other (specify): Military, Veterans Affairs					

Non-government sources:					
Members of the public	X	Public media, Internet		Private sector	X
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 and data within eICF and its subsystems is limited to BOP staff who require access to perform official duties. Data in eICF and its subsystems is access controlled and segregated, limiting staff's ability to update inmate data. Real time information from SENTRY is transmitted to eICF and its subsystems. Data from eICF is leveraged by its subsystems, Insight Suite, DARTS, and R3M, for inmate transfer, disciplinary data, progress reviews, and release purposes. Data created by the Insight Suite, and DARTS are uploaded into eICF and/or SENTRY.
DOJ Components	X	X		Sharing with DOJ law enforcement entities only as needed in accordance with established agreements via secure e-mail or physical mail. Documents in eICF are directly transferred to the U.S. Marshals Service system for the transfer of offenders.
Federal entities	X			Data sharing from eICF or all of its subsystems with Federal law enforcement entities only as needed and authorized in accordance with established agreements via secure e-mail or physical mail.

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.**
State, local, tribal gov't entities	X			Sharing of data maintained in eICF and its subsystems with state, local and tribal law enforcement entities only as needed and authorized in accordance with established agreements via secure e-mail or physical mail. The Transfer requests and inmate information from state entities and the DC Department of Corrections are sent to BOP either via e-mail or physical mail.
Public				
Counsel, parties, witnesses, and possibly courts or other judicial tribunals for litigation purposes	X			Sharing of data maintained in eICF and/or all of its subsystems with Federal Courts only as needed for litigation purposes, via secure e-mail, physical mail, or in-person during court appearances.
Private sector				
Foreign governments	X			Sharing with foreign law enforcement entities only as needed and authorized in accordance with established agreements via secure e-mail or physical mail. Transfer requests and inmate information from foreign entities are sent to BOP either via e-mail or physical mail.
Foreign entities				
Other (specify):	X			Sharing of relevant data maintained in eICF and its subsystems with contracted RRCs using R3M.

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.

BOP has published a System of Records Notice in the Federal Register which applies to eICF and its subsystems: DOJ's Inmate Central Records System, Justice/BOP-005, last published in full on May 6, 2019 (84 Fed. Reg. 19808).

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.

Federal inmates do not have the right to decline to provide the information while in federal custody. Individuals must provide identifiable information so that they can be uniquely identified in the system for purposes of managing their custody. Members of the public who request to enter an institution for physical visitation with an inmate are required to consent to the collection and use of their PII for background investigation checks prior to visitation.

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.

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 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. The public is advised of the opportunity and method to access their information via applicable System of Records Notice(s) (see Section 7.2 below). These procedures apply to information maintained in eICF and its subsystems.

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):** Incorporated into the SENTRY ATO. Authorized on 6/21/2018. **If an ATO has not been completed, but is underway, provide status or expected completion date:** N/A **Unless such information is sensitive and release of the information could pose risks to the component, summarize any outstanding plans of actions and milestones (POAMs) for any privacy controls resulting from the ATO process or risk assessment and provide a link to the applicable POAM documentation:** N/A
	This system is not subject to the ATO processes and/or it is unclear whether NIST privacy controls have been implemented and assessed. Please explain:
X	**Monitoring, testing, or evaluation has been undertaken to safeguard the information and prevent its misuse. Specify:** The system traffic is being monitored. Testing and user acceptance of any modification is performed prior to deployment.
X	**Auditing procedures are in place to ensure compliance with security and privacy standards. Explain how often system logs are reviewed or auditing procedures conducted:** User rights are reviewed frequently, including annual certification.
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:** BOP provides annual privacy-related training that covers its use of eICF, in addition, there istraining to applicable staff on the use and protection of the data.

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 eICF and its subsystems along with the data is limited to those persons who have an appropriate security clearance and are authorized to review such information for their official duties. Such access is regularly reviewed. User access is restricted to those staff who need to

view and upload data, and user roles are defined to limit capability (e.g. only case management staff are authorized to revise and update progress reports).

BOP staff with access to the system are annually trained on how to properly handle sensitive information. Individuals outside of BOP, including personnel from the larger DOJ community. are not permitted access to eICF or its subsystems. 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 eICF-specific information.

System access is web-based using a unique userID and password. Access to the network requires two-factor authentication. All transmissions of data are encrypted using the Transport Layer Security (TLS) encryption protocol. Additionally, the data in eICF and its subsystems is segregated by location, limiting staff's ability to update inmate data unless the inmate is physically located/assigned to the local site.

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.)

The eICF datastore and its subsystems follow Disposition Authority DAA-0129-2017-0002-0001. Applicable records are destroyed 10 years after expiration of sentence (which includes parole, probation, or supervision).

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).

Yes, information in eICF and its subsystems can be retrieved by a personal identifier, namely the inmate name or register number. Information on visitors is connected to the inmate they are visiting and is retrieved by the inmate's identifiers.

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), https://www.govinfo.gov/content/pkg/FR-2019-05-06/pdf/2019-09204.pdf.

Section 8: Privacy Risks and Mitigation

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 eICF and its subsystems. Additional

risks to privacy are inherent when the personal data is particularly sensitive, such as social security numbers (SSNs) or health information, and the potential threat is that the information is not maintained securely. For example, BOP collects and maintains a large amount of sensitive information on inmates within eICF and its subsystems such as social security numbers, health information, and criminal information, including PII, which is used for the administration of the inmates. Furthermore, BOP collects identification and criminal history information on individuals wishing to visit inmates at BOP facilities in order to facilitate appropriate background investigations.

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

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, such as documentation provided by members of the public, 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 eICF and its subsystems 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.

Staff are annually trained on how to properly handle sensitive information. There are no outside users who are permitted access to eICF or its subsystems, including personnel from the larger DOJ community. When a BOP employee departs from the BOP or transitions to a new position, the BOP takes appropriate measures to deactivate the user's access to eICF-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 eICF and its subsystems 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 eICF and its subsystems is shared with external entities as outlined in Section 4.1. In order to mitigate this risk, RRCs, which receive inmate information from BOP, are required to safeguard the data under the terms of their contracts with BOP. Additionally, sharing with external law enforcement agencies is done on a case-by-case basis in accordance with established agreements.