Federal Bureau of Prisons

Privacy Impact Assessment
for the
Inmate Consolidated Education Network (ICEN)

Issued by:
T. R. Craig, Acting Assistant Director

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

Date approved: [December 7, 2021]

(May 2019 DOJ PIA Template)

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 Consolidated Education Network (ICEN) is the Bureau of Prison's (BOP's) inmate network infrastructure to facilitate computerized Learning Management System (LMS) programming and General Educational Development (GED) testing for inmates required by the National GED Testing Service. The BOP has a contract with the National GED testing service who subcontracts with Pearson VUE to facilitate electronic GED testing. BOP has prepared a Privacy Impact Assessment for ICEN because this system collects and disseminates information in identifiable form about individuals. Specifically, it is used to collect names and GED examination responses from inmates, which is transmitted to Pearson VUE for scoring purposes. The ICEN system also collects system administration information to monitor usage of the 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.

ICEN enables the BOP to be able to administer the National GED testing service via the ICEN local area networks at each BOP institution, which are certified GED test sites. ICEN also provides the potential capability to deliver standardized, computer-based educational and vocational training for inmates in the future. ICEN local area networks at each institution are integrated into a wide area network to facilitate content delivery, support and troubleshooting of the system.

The ICEN system collects responses to the GED exam questions from the inmate, but the system does not store this information. The inmate's test-related information is stored with the National GED testing service. The ICEN system is administered by BOP Education and IT staff, as well as contract IT support staff. BOP Education staff login to the Pearson VUE website to schedule testing for inmates who are prepared to take the GED exam. Once the exam is scheduled, the Education staff proctor/administer the test to the inmates locally on the ICEN system. Once the exam is completed, the Education staff synchronize the results from ICEN to Pearson VUE. During this process, the exams taken by the inmates are uploaded through Pearson VUE to the National GED testing service and no inmate test data is retained in the ICEN system. The results of the inmate's tests are stored in the BOP's Inmate Central File.

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 11202 of Chapter 1 of Subtitle C of Title XI of the national Capital Revitalization and Self-Government Improvement Act of 1997.
	Executive Order	
	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	A, C, and D	BOP Employees / Contractors, Convicted Inmates
Date of birth or age			
Place of birth			
Gender			
Race, ethnicity or citizenship			
Religion			
Social Security Number (full, last 4 digits or otherwise truncated)			

(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)			
Driver's license			
Alien registration number			
Passport number			
Mother's maiden name			
Vehicle identifiers			
Personal mailing address			
Personal e-mail address			
Personal phone number			
Medical records number			
Medical notes or other medical or health information			
Financial account information			
Applicant information			
Education records	X	C and D	Convicted Inmates
Military status or other information			
Employment status, history, or similar information			
Employment performance ratings or other performance information, e.g., performance improvement plan			
Certificates			
Legal documents			
Device identifiers, e.g., mobile devices			
Web uniform resource locator(s)			
Foreign activities			
Criminal records information, e.g., criminal history, arrests, criminal charges			
Juvenile criminal records information			
Civil law enforcement information, e.g., allegations of civil law violations			
Whistleblower, e.g., tip, complaint or referral			
Grand jury information			
Information concerning witnesses to criminal matters, e.g., witness statements, witness contact information			
Procurement/contracting records			

(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
Proprietary or business information			
Location information, including continuous or intermittent location tracking capabilities			
Biometric data:			
- **Photographs or photographic identifiers**			
- **Video containing biometric data**			
- **Fingerprints**			
- **Palm prints**			
- **Iris image**			
- **Dental profile**			
- **Voice recording/signatures**			
- **Scars, marks, tattoos**			
- **Vascular scan, e.g., palm or finger vein biometric data**			
- **DNA profiles**			
- **Other (specify)**			
System admin/audit data:			
- **User ID**	X	A	BOP Employees / Contractors
- **User passwords/codes**	X	A	BOP Employees / Contractors
- **IP address**	X	A	BOP Employees / Contractors
- **Date/time of access**	X	A	BOP Employees / Contractors
- **Queries run**	X	A	BOP Employees / Contractors
- **Content of files accessed/reviewed**	X	A	BOP Employees / Contractors
- **Contents of files**	X	A	BOP Employees / Contractors
Other (please list the type of info and describe as completely as possible):	X	C and D	Inmate register numbers that serve as account IDs

3.2 Indicate below the Department's source(s) of the information. (Check all that apply.)

Directly from the individual to whom the information pertains:

In person	X	Hard copy: mail/fax		Online	
Phone		Email			
Other (specify):					

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

Non-government sources:					
Members of the public		Public media, Internet		Private sector	X
Commercial data brokers					
Other (specify): "Private sector" refers to Pearson VUE. Pearson VUE, as a subcontractor to the National GED testing service, with which BOP as a contract, provides the secure GED test to the BOP GED Coordinator. After the inmate takes the exam, it is uploaded to Pearson VUE, the test is scored and the results are e-mailed to the BOP GED Coordinator for input into the Inmate Central File.					

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	ICEN syncs to Pearson VUE for GED test results and reports which are disseminated to BOP sites. Education staff will login to synchronize tests with Pearson VUE for final results and BOP site reports. Once the inmate has tested and results are received, the information is manually input into the BOP inmate management system.
DOJ Components				
Federal entities				
State, local, tribal gov't entities				
Public				
Counsel, parties, witnesses, and possibly courts or other judicial tribunals for litigation purposes				
Private sector			X	BOP contractors setup and verify configuration of ICEN (e.g. synchronization of tests with Pearson VUE for final results and BOP site reports). Pearson VUE is a sub-contractor with the National GED testing service who facilitates electronic testing. The handling of data as part of the testing process is prescribed by National GED Testing Service requirements and DOJ security clauses included in the BOP contract. The BOP contract includes privacy clauses requiring privacy training, PII handling regulations, breach reporting, and other privacy protections.
Foreign governments				
Foreign entities				

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.
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.

The information is not released to the public for Open Data purposes.

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.

The DOJ has published a System of Records Notice in the Federal Register which applies to the collection of DOJ user data: Department of Justice Information Technology, Information System, and Network Activity and Access Records: DOJ/002 last published in full on 7/14/2021 (86 FR 37188). Additionally, DOJ users are informed of the collection of their computer usage information when they utilize a DOJ device. Inmates are also provided a general notice regarding the collection of their information when they are initially incarcerated.

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 are required to provide identifiable information so that they can be uniquely identified in ICEN and other BOP systems for purposes of managing their custody, including educational records. Inmates who have not obtained a high school diploma or GED (and are mentally capable of doing so) are required to participate in the GED program. (See 18 USC § 3624(f)). Inmates may decline to participate in the literacy program but doing so may affect their earning of good conduct time and access to other privileges. Inmates taking the GED do so through the ICEN system.

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.

Testing information on inmates is not retained in ICEN after responses are transmitted to Pearson VUE and the National GED testing service; however, inmates may request to review their educational records, including GED testing results, stored in the BOP inmate management system. They receive notification of these procedures (how to amend or correct information retained by BOP) at the Admission and Orientation program, which every inmate is required to participate in upon initial incarceration and every time they are transferred to another facility.

Section 6: Maintenance of Privacy and Security Controls

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

X	**The information is secured in accordance with Federal Information Security Modernization Act (FISMA) requirements, including development of written security and privacy risk assessments pursuant to National Institute of Standards and Technology (NIST) guidelines, the development and implementation of privacy controls and an assessment of the efficacy of applicable privacy controls. Provide date of most recent Authorization to Operate (ATO):** January 22, 2022 **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 ICEN system includes monitoring capabilities, including routine review of the traffic to and from the system to ensure the traffic is only via approved paths and to approved sites (e.g. the secure path to Pearson VUE testing). BOP IT staff and contractors perform testing of such traffic and access; review security logs; and test and evaluate the security of GED test workstations. BOP IT staff and contractors also perform user acceptance of any modification of the system 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:** Monthly certification of user rights are completed. Enterprise audits include review of access permissions, account management, system configuration, and data access.

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 staff and contractors administering the system receive privacy-related training as part of their normal duties, including annual training as to how to protect and process sensitive information. No additional privacy training is conducted (e.g. end-user training for inmates who use the system).

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?

Inmate access to the system is strictly limited to their testing workstation to complete their assigned GED testing. Inmates cannot log into the GED system or have access to GED Data and the latter data is transmitted by a Pearson VUE certified GED Coordinator (BOP staff member) from a restricted secure administrative terminal.

Access to the system and data for BOP Education staff to administer testing and transmit data, and access for BOP IT staff and contractors to configure, update and monitor the system is limited to those persons who have an appropriate security clearance and are authorized to access such information for their official duties. All such access is regularly reviewed.

User roles are defined to limit capability (e.g. only Education staff are authorized to revise and update education reports). Administrative access to the network for BOP staff and contractors requires two-factor authentication. All transmissions of data are encrypted using TLS encryption. The system is configured with appropriate security settings to prevent unauthorized access, protect data transmission, and secure the system. Only GED certified test administrators deliver and proctor GED testing using credentials provided by Pearson VUE. The ICEN system includes monitoring capabilities, including routine review of the traffic to and from the system to ensure the traffic is only via approved paths and to approved sites (e.g. the secure path to Pearson VUE testing) in accordance with DOJ policy and NIST standards.

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.)

No inmate information is being retained in ICEN beyond the end of each testing session. The results of the inmate's tests are stored in the BOP's inmate management system, for which a separate privacy impact assessment is maintained, available on BOP's Freedom of Information

Act webpage: https://www.bop.gov/foia/#tabs-4. DOJ user information is handled in accordance with General Records Schedule 3.1: General Technology Management Records Item #20 (retain record for three years after activity date).

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).

System admin/audit data pertaining to DOJ users is retrievable by User ID. However, inmate information collected is not retained in ICEN beyond each testing session and is therefore not retrievable within the system. After the inmate takes the exam, it is uploaded to Pearson VUE, the test is scored and the results are either emailed to BOP education staff or BOP staff log into the Pearson VUE website to retrieve the scores for their respective sites. None of the inmate GED scores are stored anywhere in the ICEN infrastructure.

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:

The DOJ has published a System of Records Notice in the Federal Register which applies to the collection of DOJ user data: Department of Justice Information Technology, Information System, and Network Activity and Access Records: DOJ/002 last published in full on 7/14/2021 (86 FR 37188).

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 ICEN. BOP mitigates this risk by only collecting the data that is required to complete the authorized and necessary functions of ICEN. Additionally, BOP mitigates risks to confidentiality through the implementation of data access controls to ICEN, ensuring that information is provided only to those who require access to perform their official duties.

b. Potential Risks Related to the Use of Information

Potential threats to Privacy arising from BOP's use of the GED testing information in ICEN include the risk of unauthorized access to information and threats to the integrity of the information arising from unauthorized access or improper disposal of information. To mitigate this risk, staff are annually trained on how to properly handle sensitive information. Administrative 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. 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. Only those Bureau personnel and contract support staff who require access to perform their official duties may administer testing and transmit information using the system. There is also a privacy risk of unauthorized access or modification of data in the system by the inmate users. In order to mitigate this risk, inmate access to the system is strictly limited to their testing workstation to complete their assigned GED testing. Inmates cannot log into the GED system or have access to GED Data and the latter data is transmitted by a Pearson VUE certified GED Coordinator (BOP staff member) from a restricted secure administrative terminal.

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 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 in accordance with DOJ security requirements, such as access permissions, account management and data access. Further security is provided via data segregation and 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 also encrypted.