

Federal Bureau of Prisons



Privacy Impact Assessment for the Inmate Education Systems

Issued by:

Michael Rogers
Acting SCOP

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

Date approved: [Component to insert date of PIA approval]

(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) offers opportunities for inmates to acquire literacy and marketable skills so they can obtain employment after release in accordance with the Bureau's mission and federal law. In the effort to provide inmates with education to prepare for their successful reentry into society, the FBOP utilizes a network of systems that enable facilities to distribute educational materials, conduct standardized testing, and develop career-oriented skills. To meet the needs of a functional education network, the inmate education systems collect education information, system administration and audit information, and personally identifiable information (PII) that connects an inmate to their account for testing purposes.

Appendix A to this PIA lists and briefly summarizes the systems and applications that comprise the “Inmate Education Systems” under the control of the FBOP. PII for the systems listed in Appendix A have been accounted for in the PII table in Section 3.1. Any additional education systems procured at a future date will be addressed in their own initial privacy assessments and added to the appendix.

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.

The Inmate Education System’s primary purpose is to provide educational opportunities for federal inmates in the custody of the FBOP to complete the Bureau’s mission of preparing individuals for successful reentry into the public. To serve this purpose, education systems collect, maintain, and disseminate information accordingly, including analytics, reports, trends in course related documents, and other specific application information detailed in the appendix, to provide an education program for federal inmates. The core infrastructure of the inmate education network is built on a VMware Cloud Software-Defined Data Center (SDDC) with a Windows Domain environment utilizing Active Directory for identity management.

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, 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. The First Step Act of 2018 (FSA; Public Law 155-391) that requires the DOJ to provide convicted individuals in federal custody with opportunities to take evidence-based recidivism reducing programs, as well as allow them to participate in productive activities.
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.*

Department of Justice Privacy Impact Assessment
Federal Bureau of Prisons / Inmate Education Systems
Page 3

(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 Detainees; 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
<i>Example: Personal email address</i>	<i>X</i>	<i>B, C and D</i>	<i>Email addresses of members of the public (US and non-USPERs)</i>
Name	X	A, C, and D	First and last names of inmates (US and non-USPERs) and FBOP employees and contractors.
Date of birth or age	X	C and D	Date of birth of inmates (US and non-USPERs).
Place of birth			
Sex	X	C and D	Sex of inmates (US and non-USPERs).
Race, ethnicity, or citizenship	X	C and D	Race and ethnicity of inmates (US and non-USPERs).
Religion			
Social Security Number (full, last 4 digits or otherwise truncated)			
Tax Identification Number (TIN)			
Driver's license			
Alien registration number			
Passport number			
Mother's maiden name			
Vehicle identifiers			
Personal mailing address			
Personal e-mail address			
Personal phone number			
Business contact information, e.g., email address, phone number, address of a business	X	A	Facility location and business email address of FBOP employees and contractors.
Medical records number			
Medical notes or other medical or health information	X	C and D	Medical accommodation information for testing purposes of inmates (US and non-USPERs), if applicable.
Financial account information			
Applicant information			
Education records	X	C and D	Education information, to include student score reports, user testing, and activity information of inmates (US and non-USPERs).
Military status or other information			
Employment status, history, or similar information			

Department of Justice Privacy Impact Assessment
Federal Bureau of Prisons / Inmate Education Systems

Page 4

(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
Employment performance ratings or other performance information, e.g., performance improvement plan			
Certificates	X	C and D	Education completion certificates of inmates (US and non-USPERs).
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			
Proprietary or business information			
Location information, including continuous or intermittent location tracking capabilities			
<i>Biometric data:</i>			
- Photographs or photographic identifiers			
- Video containing biometric data			
- Fingerprints			
- Palm prints			
- Iris image			
- Dental profile			
- Voice recording/signatures			

Department of Justice Privacy Impact Assessment
Federal Bureau of Prisons / Inmate Education Systems

Page 5

(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 Detainees; 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			
- Vascular scan, e.g., palm or finger vein biometric data			
- DNA profiles			
- Other (specify)			
<i>System admin/audit data:</i>			
- User ID	X	A, C and D	User IDs for FBOP employees, contractors, and inmates.
- User passwords/codes	X	A, C and D	Passwords for FBOP employees, contractors, and inmates.
- IP address	X	A	IP addresses of FBOP employees and authorized contractors.
- Date/time of access	X	C and D	Tracks date and time of access of inmate activities.
- Queries run	X	A	Queries run of FBOP employees and authorized contractors.
- Contents of files	X	A, C and D	Content of files for user activity of FBOP employees, contractors, and inmates.
Other (please list the type of info and describe as completely as possible):	X	C and D	Register numbers of inmates that serve as account IDs. Facility location of inmates (US and non-USPERs).

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	X
Phone		Email			
Other (specify):					

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

Non-government sources:				
Members of the public		Public media, Internet		Private sector X
Commercial data brokers				
Other (specify): "Private sector" refers to education program vendors listed in the appendix.				

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	Authorized education employees will be assigned role-based permissions. Sharing with employees outside of FBOP inmate education services will be done on a need-to-know basis.

Department of Justice Privacy Impact Assessment
Federal Bureau of Prisons / Inmate Education Systems
 Page 7

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.
				Per the relevant contract, ALS contractors set up and verify configuration of the system and the inmate coursework. PearsonVue provides access to the GED test information, maintains the system and provides system support when needed for administering a GED examination. A Pearson VUE partnership with the American Council of Education (ACE) allows the ACE to maintain the inmate's official diploma and transcripts, as well as the inmate's register number. The handling of data as part of the process is included in the FBOP contracts, which include privacy clauses requiring privacy training, PII handling regulations, breach reporting, and other privacy protections as prescribed in DOJ-02 and DOJ-05.
DOJ Components				
Federal entities				
State, local, tribal gov't entities				
Public			X	Federal inmates have log-in access for coursework assigned to them along with completed coursework. Inmates are only able to access their own education information.
Counsel, parties, witnesses, and possibly courts or other judicial tribunals for litigation purposes				
Private sector				
Foreign governments				

Department of Justice Privacy Impact Assessment
Federal Bureau of Prisons / Inmate Education Systems

Page 8

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 entities				
Other (specify):				

- 4.2 *If the information will be released to the public for “[Open Data](#)” purposes, e.g., on data.gov (a clearinghouse for data from the Executive Branch of the federal government), and/or for research or statistical analysis purposes, explain whether—and, if so, how—the information will be de-identified, aggregated, or otherwise privacy protected.*

N/A

Section 5: Notice, Consent, Access, and Amendment

- 5.1 *What kind of notice, if any, will be provided to individuals informing them about the collection, use, sharing or other processing of their PII, e.g., a Privacy Act § 552a(e)(3) notice? Will a System of Records Notice (SORN) be published in the Federal Register providing generalized notice to the public? Will any other notices be provided? If no notice is provided to individuals or the general public, please explain.*

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

DOJ’s Inmate Central Records System, Justice/BOP-005, 84 Fed. Reg. 19808 (May 6, 2019), available at: <https://www.govinfo.gov/content/pkg/FR-2019-05-06/pdf/2019-09204.pdf>

DOJ’s Department of Justice Information Technology, Information System, and Network Activity and Access Records, Justice/DOJ-002, 64 FR 73585 (Dec. 12, 1999) and last modified 86 FR 37188 (July 14, 2021), available at: https://www.justice.gov/d9/pages/attachments/2021/08/02/2021-14986_-_doj-002_sorn_update.pdf

Additionally, 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*

Department of Justice Privacy Impact Assessment
Federal Bureau of Prisons / Inmate Education Systems

Page 9

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 inmate education 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, the coursework in this system helps prepare the inmates in GED testing. See 18 U.S.C. § 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 are provided the opportunity to take GED preparation coursework through the ALS. Since the primary purpose of the system is to provide secure and controlled access to these applications, there are no provisions for individuals to directly consent to the collection or specific uses of their information within the inmate education environment. User authentication data, such as passwords, are required for security and access purposes, and this information is provided by the users themselves as part of the authentication process.

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 can see real time information on their individual accounts and results while completing the coursework. Inmates may request to review their educational records, including any testing results, stored in the FBOP inmate case management system. They receive notification of these procedures and how to amend or correct information retained by FBOP 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) (if the system operates under an Authorization to Use (ATU) or other authorization mechanism, provide related details wherever an ATO is referenced): The Inmate Education systems are authorized to operate under two separate ATO's: BOP-ICEN- authorized on 9/30/24 and expires on 9/30/27. BOP-ALS- authorized on 9/29/25 and expires on 9/28/28. If an ATO has not been completed, but is underway, provide status or expected completion date: 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:
	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:
X	Monitoring, testing, or evaluation has been undertaken to safeguard the information and prevent its misuse. Specify: Each system includes monitoring capabilities, including routine review of the traffic for each system to ensure the traffic is only via approved paths. FBOP IT employees and contractors conduct testing; review traffic, access, and security logs; and test and evaluate the security of inmate workstations dedicated to inmate education services. FBOP IT employees 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 privileges are completed. Enterprise audits

Department of Justice Privacy Impact Assessment
Federal Bureau of Prisons / Inmate Education Systems

Page 11

	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: FBOP employees and contractors administering the inmate education system receive privacy-related training as part of their normal duties, including annual training as to how to protect and process PII. 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 is strictly limited to authorized inmate workstation to complete their assigned courses and programs based on enrollments and access permissions.

Data regarding FBOP inmate education employees and contractors to access inmate education systems, administer programs and testing, transmit data, and grant access for FBOP IT employees and contractors to configure, update, and monitor system information 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 inmate education employees are authorized to review education reports). Administrative access to the network for FBOP employees, inmates, and authorized contractors requires two-factor authentication. All transmissions of data are encrypted using TLS encryption. All data is also encrypted at rest and in transit. The systems are configured with appropriate security settings to prevent unauthorized access, protect data transmission, and secure the system. This includes monitoring capabilities, including routine review of the traffic to and from the systems to ensure the traffic is only approved paths 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.) 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.

Records related to ALS and Pearson VUE do not retain inmate information beyond 60 days at the completion of the coursework. The completion of the coursework is keyed into the FBOP's inmate management system, for which a separate privacy impact assessment is maintained and available on the FBOP's Freedom of Information Act webpage [Freedom Of Information](#). Records related to ICEN does not include inmate information. Records in ALS and Pearson VUE are retained in accordance with General Records Schedule 5.2, Item 010: Transitory Records and can only be deleted and purged by authorized FBOP employees. FBOP user information in ICEN is handled in accordance with General Records Schedule 3.1: General Technology Management Records Item #020, which orders to retain records 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).*

_____ 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:*

DOJ's Inmate Central Records System, Justice/BOP-005, 84 Fed. Reg. 19808 (May 6, 2019), available at: <https://www.govinfo.gov/content/pkg/FR-2019-05-06/pdf/2019-09204.pdf>

DOJ's Department of Justice Information Technology, Information System, and Network Activity and Access Records, Justice/DOJ-002, 64 FR 73585 (Dec. 12, 1999) and last modified 86 FR 37188 (July 14, 2021), available at: https://www.justice.gov/d9/pages/attachments/2021/08/02/2021-14986_-_doj-002_sorn_update.pdf

Section 8: Privacy Risks and Mitigation

When considering the proposed use of the information, its purpose, and the benefit to the Department of the collection and use of this information, what privacy risks are associated with the collection, use, access, dissemination, and maintenance of the information and how are those risks being mitigated? For projects involving the use of artificial intelligence and/or machine learning, identify the privacy risks uniquely associated with the use of AI/ML, and how those risks are being mitigated, for example the risk of output inaccuracies and mitigations in the form of testing, continuous monitoring, training, secondary review, etc.

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

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

a. Potential Risks Related to Information Collection

Collecting and maintaining more personal information than necessary to accomplish FBOP's official duties is a potential threat to privacy arising from inmate education systems. The FBOP mitigates this risk by only collecting the data that is required to complete the authorized and necessary functions. Additionally, the FBOP mitigates risks to confidentiality through the implementation of data access controls to this system, ensuring that information is provided only to those who require access and have been trained on how to perform their official duties.

b. Potential Risks Related to the Use of Information

Potential threats to privacy arising from FBOP's use of the information in inmate education systems 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, FBOP employees and contractors are annually trained on how to properly handle personally identifiable 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,

Department of Justice Privacy Impact Assessment
Federal Bureau of Prisons / Inmate Education Systems

Page 14

and the required use of proper passwords and user identification codes to access the system. Only those Bureau personnel and contract support employees 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 the authorized inmate workstation to complete their assigned coursework, including authentication mechanisms, role-based access permissions, conducting regular security audits, and monitoring access logs for any suspicious activities.

c. Potential Risks Related to the Dissemination of Information

There is a privacy risk to individuals arising from the potential disclosure of 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 an employee's ability to update inmate data unless the inmate is physically located/assigned to the local site. Data at rest and in transit, both within and outside the system, is also encrypted.

APPENDIX A: FBOP Inmate Education Systems

This appendix lists the systems and applications collectively referred to as the “Inmate Education Systems” throughout this PIA.

1. **The Aztec Learning System (ALS)** - A Software as a Service (SaaS) application that provides content for adult education. ALS will be utilized by the inmate population to provide supplemental educational material for the literacy program (GED) and content for FBOP-assigned recidivism reduction programs and productive activities. ALS serves as the classroom environment application accessed through ICEN (see below) and will offer FBOP employee teachers a tool to benchmark and track inmate mastery levels and monitor student progress in assigned curricula. The system will provide detailed reports and analytics for the instructor to monitor and respond to inmate progress, completion, questions answered incorrectly, ineffective questions, and to develop academic remediation plans, as needed. Consistent with its privacy policy, Aztec LLC analyzes data related to user activity to identify areas for improvement, such as questions answered incorrectly or ineffective questions, among other uses. Aztec uses data analytics for the purpose of ascertaining trends on course related data input by the inmates. This information is used to measure the administration of courses more effectively. The trends are determined by monitoring and responding to inmate progress, completion of courses, questions answered incorrectly, ineffective questions, and to assist in the development of customized academic remediation plans, as needed. ALS does utilize artificial intelligence for ascertaining trends and identifying improvements for coursework, but the FBOP does not utilize those capabilities. Additionally, the reports provide insights into inmate students’ activities, performance, and system usage. ALS will collect first and last names of inmates and FBOP employees and contractors, federal register numbers, inmate education information, FBOP employee and contractor email addresses, and user IDs.
2. **Fair Shake** – The FBOP provides reentry resources to incarcerated individuals to support their transition back into society. Inmates can log into their ICEN account to access the Fair Shake portal for assistance with reentry needs. The Fair Shake portal offers tools and support for inmates regarding employment, housing, and community integration via a resource directory. This website does not collect any information on the user when they navigate the application.
3. **The Inmate Consolidated Education Network (ICEN)** - An FBOP on-premises private cloud datacenter designed to facilitate secure access for users to various inmate education applications hosted on third-party cloud platforms for the FBOP’s inmate education initiatives. ICEN’s primary purpose is to provide seamless and secure access to essential applications. These applications, including ALS, Pearson VUE GED Certification Testing, and Reentry Programs, are crucial for education, certification, and reintegration efforts. For the operation of the system, the user authenticates their identity when logging into the ICEN ecosystem, users are then presented with a user dashboard containing URL

Department of Justice Privacy Impact Assessment
Federal Bureau of Prisons / Inmate Education Systems

Page 16

links to the third-party cloud-hosted applications. This process ensures that only authenticated users gain access to the applications they require. The system primarily collects and uses user authentication data, such as usernames and passwords, along with application usage and various security logs for auditing purposes. Information within the ICEN system is used solely for the purpose of granting authorized access to the ICEN platform and authorized applications. No data is shared externally; all operations are confined within the on-premises private cloud datacenter.

4. **JSTOR** – This website provides a sustainable platform whose features are designed to meet the evolving needs of the educational employees at the FBOP. The tools include a vast digital library of journals, books, images, primary sources, audio files, and video sources that assist FBOP inmate education employees in planning courses for inmate students. This website leverages generative AI to continually improve and enhance the user experience and expand discovery. This website does not collect any PII when a user navigates the application.
5. **Pearson VUE** – Pearson VUE is an online testing platform used to provide prep materials and to administer the test exams for the GED certification. Pearson Vue will provide preparation materials and administer test exams for the GED certification, and to accomplish its purpose, the system will collect information of FBOP education employees to include first and last names, FBOP resource mailbox email addresses, and facility information (address and phone number). Additionally, inmate information is entered into the GED Testing Service Manager to create an inmate user profile to schedule GED® testing through Pearson VUE. The unofficial GED test results are emailed to an FBOP resource mailbox. Official test results are physically mailed to the facility and provided to the inmate. These test results are not maintained in Pearson VUE beyond 60 days after transmittal.