Federal Bureau of Prisons

# Privacy Impact Assessment
for the
*National Institute of Corrections Learning Center - (NIC LC)*

Issued by:
Sonya D. Thompson
Assistant Director / SCOP

Approved by: Brian A. Young
Chief, Law Enforcement and National Security Unit
Office of Privacy and Civil Liberties Officer
U.S. Department of Justice

Date approved: [November 8, 2024]

***(May 2022 DOJ PIA Template)***

## Section 1: Executive Summary

The Federal Bureau of Prisons (FBOP) National Institute of Corrections (NIC) is directed to provide training, technical assistance, and information services to the field of corrections, which includes federal, state, tribal, and local corrections agencies and individuals. NIC uses the National Institute of Corrections Learning Center (NIC LC) to provide state-of-the-art e-learning courses, classroom event registration, and other resource materials to various federal, state, tribal, and local corrections agencies and individuals. NIC LC facilitates the management of participant registration, delivers online course content and training completion certificates, and allows users to review transcripts online.

A Privacy Impact Assessment was conducted to account for the personally identifiable information concerning DOJ and external corrections employees that is collected, maintained, and disseminated through this system. The information gathered from the system such as, name, home address, phone numbers, email address, and employment information is used to verify users and approve or deny account access. Certain data fields, such as number of years of correctional experience and job title, are used to determine appropriate placement into a classroom program. Data is also used to capture operational information participation information, such as number of courses completed and which courses have the highest rate of completion. Finally, NIC uses sanitized statistical information (no personal or account information) for analytical purposes and review by FBOP's NIC Executive Employees and Advisory Board meetings.

## 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.***

As mentioned above, FBOP NIC is tasked with training federal, state, local, and tribal correctional employees. NIC LC helps NIC facilitate online courses and expand the training audience to those who are unable to take in-person training. NIC uses analytics[1] to determine which courses to offer. As a result, NIC courses include Nalozone Narcan training to help stop overdoses, Prison Rape Elimination Act (PREA) training, and standardized courses concerning leadership, training methodology, screening, trauma sensitivity, and suicide prevention. NIC LC includes a public-facing web portal that is linked from the main NIC website. Participants register for a user account through this portal, using an approved federal, state, local, or tribal correctional entity-provided email address and creating a username and password, which they then use to access the online trainings hosted on the portal. The e-learning trainings allow participants to access courses in different formats, including hybrid (in-person and online), online, and in-person. NIC LC also allows NIC administrators to manage administrative needs for in-person, online, and hybrid courses. NIC LC administrators

[1] FBOP uses Google analytics for website analytics and LMS-specific software included in the LMS platform for LMS analytics.

upload course and instructor data, track the start and end of a course, and manage certificates.

User account information is collected during initial user account creation, which consists of:

- Usernames and passwords;
- Registration information including first name, last name, email address, address (street, city, state, zip code), job title, agency/organization name, current position level in the field of corrections, and primary area of responsibility. Data responses occur via open-ended responses or dropdown/multiple choice selections;
- Home address, day and mobile phone numbers, and email which are used for 1) participant selection criteria and 2) to schedule travel if necessary
- User account details such as date created, date joined, date last access, and date updated fields;
- Training history and transcripts including learning activity started, learning activity in process, and learning activity completed; records of completion and current completion certificates.

NIC LC also sends standard system messages to users, such as when they enrolled in, dropped, or completed a program. NIC LC collects certain information from these messages, including subject text, message text (the only PII related information is first and last name), and PDF attachments such as learning assignments and curriculum.

***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 USC §§ 4042, 4351, 4352; Public Law 93-41.5 (establishes NIC) |
| Executive Order | |
| Federal regulation | 28 CFR § 0.95(m) |
| 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, B, C, and D | First and last name for Federal and non-Federal Corrections employees only. Non-USPERs may possibly enter their information into the system. |
| **Date of birth or age** | | | |
| **Place of birth** | | | |
| **Gender** | | | |
| **Race, ethnicity, or citizenship** | | | |
| **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** | X | A, B, C, and D | Mailing address for Federal and non-Federal Corrections employees only. Non-USPERs may possibly enter their information into the system. |
| **Personal e-mail address** | X | A, B, C, and D | Home email address for Federal and non-Federal Corrections employees only. Non-USPERs may possibly enter their information into the system. |
| **Personal phone number** | X | A, B, C, and D | Home and mobile phone numbers for Federal and non-Federal Corrections employees only. Non-USPERs may possibly enter their information into the system. |
| **Medical records number** | | | |
| **Medical notes or other medical or health information** | | | |
| **Financial account 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:<br>A. DOJ/Component Employees, Contractors, and Detailees;<br>B. Other Federal Government Personnel;<br>C. Members of the Public - US Citizens or Lawful Permanent Residents (USPERs);<br>D. Members of the Public - Non-USPERs | (4) Comments |
|---|---|---|---|
| **Applicant information** | | | |
| **Education records** | X | A, B, and C | Training history and transcripts from this system are also saved. |
| **Military status or other information** | X | A, B, and C | May be provided, as determined as necessary by the individual registering with NIC LC |
| **Employment status, history, or similar information** | X | A, B, C, and D | Employment information including: current position, number of years employed, and primary area of responsibility for Federal and non-Federal Corrections employees only.<br>Non-USPERs may possibly enter their information into the system. |
| **Employment performance ratings or other performance information, e.g., performance improvement plan** | | | |
| **Certificates** | X | A, B, and C | Completion of Training |
| **Legal documents** | | | |
| **Device identifiers, e.g., mobile devices** | | | |
| **Web uniform resource locator(s)** | X | A, B, C | Collects internet address of the website from which users linked directly to the site, and pages visited for all NIC users |
| **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** | X | A, B, and C | Business name, address, and phone number for non-profit and for-profit organizations |

| (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:<br>A. DOJ/Component Employees, Contractors, and Detailees;<br>B. Other Federal Government Personnel;<br>C. Members of the Public - US Citizens or Lawful Permanent Residents (USPERs);<br>D. Members of the Public - Non-USPERs | (4) Comments |
|---|---|---|---|
| **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, B, and C | Usernames, passwords, and user account details for Federal and non-Federal Corrections employees, as well as NIC employees, contractors, and vendor employees |
| - **User passwords/codes** | X | A, B, and C | Usernames, passwords, and user account details for Federal and non-Federal Corrections employees, as well as NIC employees, contractors, and vendor employees |
| - **IP address** | X | A, B, and C | User IP addresses are captured. |
| - **Date/time of access** | X | A, B, and C | Usernames, passwords, and user account details for Federal and non-Federal Corrections employees, as well as NIC employees, contractors, and vendor employees |
| - **Queries run** | | | |
| - **Contents of files** | X | | Message content and assignments. |
| **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 | | Hard copy: mail/fax | | Online | X |
| Phone | | Email | | | |
| Other (specify): | | | | | |

| **Government sources:** | | | | | |
|---|---|---|---|---|---|
| Within the Component | X | Other DOJ Components | X | Other federal entities | X |
| 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 | | Public media, Internet | | Private sector | |
| 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 | | X | Login access is granted to approved (authorized and trained) FBOP personnel such as NIC employees and contractors using enterprise authentication mechanisms to manage accounts and the participation in NIC courses. |

| Recipient | How information will be shared | | | |
|---|---|---|---|---|
| | **Case-by-case** | **Bulk transfer** | **Direct log-in access** | **Explain specifics of the sharing, as well as how these disclosures will support and are compatible with the purposes of the collection.** |
| DOJ Components | X | | X | Participants will have a unique ID and password to access their specific information in NIC LC.<br><br>Reporting information for DOJ auditing or FBOP's efforts to measure success may be shared on a case-by-case basis with other DOJ components, such as USMS.<br><br>Information may be shared with other DOJ components, in support of ad hoc requests for unforeseen events, including but not limited to litigation. Ad hoc reporting requests (audit, Privacy Act access or amendment, or FOIA requests) will be sent to system owners, evaluated to determine need, and the minimum information required to satisfy the request will be exported or sent as needed. |
| Federal entities | X | | X | Participants will have a unique ID and password to access their specific information in the NIC LC.<br><br>Information may be shared with other federal entities, in support of ad hoc requests for unforeseen events, including but not limited to litigation. Ad hoc reporting requests (audit, Privacy Act access or amendment, or FOIA requests) will be sent to system owners, evaluated to determine need, and the minimum information required to satisfy the request will be exported or sent as needed. |

| 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 | Participants will have a unique ID and password to access only their specific information in the NIC LC. |
| Public | | | | |
| Counsel, parties, witnesses, and possibly courts or other judicial tribunals for litigation purposes | | | | |
| Private sector | | | | |
| 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, 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.***

FBOP will display a Privacy Act Statement to individuals who register for NIC LC accounts. A link to the FBOP's privacy notice and website privacy notice will be provided upon a user logging into NIC LC: https://nicic.gov/privacy-statement-and-disclaimers.

General guidance is provided to the public in the following SORNS:

- DOJ-002, DOJ Information Technology, Information System, and Network Activity and Access Records, last published in full at 86 Fed. Reg. 37188 (Jul. 14, 2021), https://www.justice.gov/opcl/page/file/1419896/download; and
- BOP-103, National Institute of Corrections Academy Record System, last published in full at 82 FR 24147 (5-25-2017), https://www.gpo.gov/fdsys/pkg/FR-2000-03-02/pdf/00-4973.pdf.

***5.2 What, if any, opportunities will there be for individuals to voluntarily participate in the collection, use or dissemination of information in the system, for example, to consent to collection or specific uses of their information? If no opportunities, please explain why.***

Visitors to the public-facing website are not required to submit requests. However, users who seek access to the training services must provide the requested information and complete the online registration. By completing the online registration, requestors are voluntarily agreeing to participate in the collection and use of information in the system. Individuals are notified that the submission of information is mandatory if they wish to obtain NIC courses.

***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.***

As part of the registration process, participants will create a unique ID and password to access or modify their own information in the NIC LC.

Individuals may also access or amend information collected or stored by NIC through a Privacy Act or FOIA request. Additional information will be available at NIC LC Privacy Notice and the relevant SORNs (see Section 7 below).

## Section 6: Maintenance of Privacy and Security Controls

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

| | |
|---|---|
| X | **The information is secured in accordance with Federal Information Security Modernization Act (FISMA) requirements, including development of written security and privacy risk assessments pursuant to National Institute of Standards and Technology (NIST) guidelines, the development and implementation of privacy controls and an assessment of the efficacy of applicable privacy controls. Provide date of most recent Authorization to Operate (ATO):**<br><br>**If an ATO has not been completed, but is underway, provide status or expected completion date:** The ATO for NIC LC is pending approval of privacy document.<br><br>**Unless such information is sensitive and release of the information could pose risks to the Component, summarize any outstanding plans of actions and milestones (POAMs) for any privacy controls resulting from the ATO process or risk assessment and provide a link to the applicable POAM documentation:** |
| | **This system is not subject to the ATO processes and/or it is unclear whether NIST privacy controls have been implemented and assessed. Please explain:** |
| X | **This 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 FIPS 199. Specify and provide a high-level summary of the justification, which may be detailed in the system security and privacy plan:**<br>FBOP determined the information contained in the system warrants a Moderate classification because some of the information can have severe adverse impacts for the individuals for whom the information pertains if the information was released or exposed in an unauthorized manner to unauthorized personnel. |
| X | **Monitoring, testing, or evaluation has been undertaken to safeguard the information and prevent its misuse. Specify:** Thorough testing of security controls will be undertaken to ensure the proper implementation, monitoring and safeguarding of 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:** System administrators will review the system audits logs weekly to assure security standards are being met, including reviews to determine whether any unusual or inappropriate activities have taken place. |
| 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:**<br>FBOP and NIC employees, contractors, and detailees are required to complete cybersecurity and privacy training. FBOP employees, contractors, and detailees are also required to review and sign the DOJ Cybersecurity and Privacy Rules of Behavior for General Users, which details the responsibilities for DOJ users and includes instructions about how to safeguard and safely manage DOJ information and PII. |

***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?***

The security risks associated with maintaining data in an electronic environment have been mitigated through administrative, technical, and physical safeguards. The safeguards in place are commensurate with the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of the data.

Administrative Controls: NIC LC System Administrators have the sole ability to create accounts for a subset of identified internal users (e.g., employees, contractors), referred to as account managers. Account managers access NIC LC using single sign-on (SSO) and multi-factor authentication (MFA) using enterprise services, including PIV-card access. Account managers support organization-defined configuration, security, and access control, as well as periodically review accounts to identify personnel who no longer need access due to change in

job descriptions or inactivity. Account managers are able to add new users, remove existing users, and modify existing users. Access is restricted to only personnel required to perform job duties and exposure to unencrypted PII data is limited to a minimum number of personnel. Employees also receive and maintain access to DOJ computers and equipment by completing initial and annual cybersecurity awareness and Privacy Act training in the operation of security policies, as well as review and sign for the DOJ Cybersecurity and Privacy Rules of Behavior for General Users. Additionally, individuals requiring access to sensitive information are processed for access authorization in accordance with personnel security policy.

Technical Controls: NIC LC utilizes industry best practices for data encryption, including encryption at rest and in transit. Requests from users are sent to the internal application and are restricted to a subset of IP ranges and monitored for usage, which ensures only NIC administrators have access to the internal NIC application. This control helps prevent unauthorized users or actors from accessing the internal NIC application where personal information can be accessed. Devices that display or output sensitive information in readable form are positioned to deter unauthorized individuals from reading the information and are located in 24x7 physically secured locked area. The application is located on servers and cloud capability provided within Amazon Web Services (AWS) GovCloud datacenters in the United States. Automatic account management will be applied to inactivate accounts that have not logged into the system after 30 days. The system incorporates security controls to identify and restrict unsuccessful login attempts. Additional password complexity, reset duration, and reset reusage have been implemented to align with FBOP standards. The servers are only accessible to authorized customer personnel, SaaS vendor personnel, and AWS personnel.

Physical Controls: NIC LC is located on servers and cloud capability provided within Amazon Web Services (AWS) GovCloud datacenters in the United States.

***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.)***

Pursuant to record retention schedules approved by NARA, NIC LC records (DAA-060-2017-0009-0001 through DAA-060-2017-0009-0004) include law enforcement training records, which are temporary records with a retention period of 25 years after date of last action; administration of justice technical skills training records, which are temporary records with a retention period between 6 years and 10 years after cutoff; and training administration records, which are temporary records with a retention period of 6 years after cutoff.

## 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-002, DOJ Information Technology, Information System, and Network Activity and Access Records, last published in full at 86 Fed. Reg. 37188 (July 14, 2021), https://www.justice.gov/opcl/page/file/1419896/download; and

BOP-103, National Institute of Corrections Academy Record System, last published in full at 82 FR 24147 (May 25, 2017), https://www.gpo.gov/fdsys/pkg/FR-2000-03-02/pdf/00-4973.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?***

### a. Potential Risks Related to Information Collection

Collecting and maintaining more personal information than necessary to accomplish FBOP official duties is a potential threat to privacy arising from NIC LC. The unnecessary collection of data poses a risk of the loss of personal information due to the sensitivity of the data involved, such as names and email addresses. FBOP mitigates this risk by implementing measures to limit the collection of data to that which is required to complete the authorized and necessary functions of NIC LC. These measures include creating certain defined data fields where required information can be inserted and evaluating each step, form, and field to determine need and minimize the amount of information collected. NIC LC utilizes industry best practices for data encryption, including encryption at rest and in transit.

There is also a potential privacy risk arising from collecting information of inadequate quality on each individual. To mitigate this, NIC LC collects information directly from the requestor about whom the information pertains to the greatest extent practicable. A link to the FBOP privacy notice and policies is available on the footer of all pages for requestors which includes information on Information Collected, How Personal Information Is Used, Child Privacy, Cookie Usage, External Sites, and Security. Additionally, FBOP provides a Privacy Act Notice to all individuals registering with NIC LC.

To mitigate the risk of unauthorized access or use, the collected information is safeguarded in accordance with FBOP rules and policy governing automated information systems security and access. These safeguards include the maintenance of records and technical equipment in restricted areas. System Administrators and Account Managers also regularly monitor accounts to identify user accounts that can be deleted due to a change of job descriptions or inactivity.

**b. Potential Risks related to the Use of Information**

Potential threats to privacy arising from FBOP's use of the information in NIC LC includes the risk of unauthorized use of information, threats to the integrity of the information arising from unauthorized access or improper disposal of information. FBOP mitigates the risk of unauthorized access through the implementation of data access controls, ensuring information is provided only to those individuals who require access to perform their official duties.

Employees are annually trained on how to properly handle sensitive information to mitigate the risks arising from improper use or disposal of the information. The duration of time to retain information is determined when business use ceases in accordance with FBOP data storage and retention policies. Additionally, to address the threats to the integrity of the data from unauthorized access, there are no outside users who are permitted access to the internal LMS besides the authorized NIC administrators. When a FBOP employee departs from FBOP or transitions to a new position, the FBOP takes appropriate measures to deactivate the user access and accounts to NIC LC.

**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 and by providing auditing of user and system administration activities. 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 FBOP mission.

Reporting information for auditing or measuring success may be shared on a case-by-case basis with other DOJ components and Federal agencies. Each request is evaluated to determine need, and the minimum information required to satisfy the request will be exported and/or sent as needed. All data shared with other DOJ components for reporting purposes will be aggregated and will have personal identifiers removed. These restrictions help address the risk of disclosure of information to unauthorized individuals both inside and outside FBOP.

FBOP and NIC employees, contractors, and detailees also complete required annual privacy and cybersecurity training, as well as reviews and signs the DOJ Cybersecurity and Privacy Rules of Behavior for General Users. These measures train and explain employees, contractors, and detailees of their responsibility to safeguard information, which includes proper handling of information to prevent unauthorized disclosure of the information.