

Federal Bureau of Prisons



Privacy Impact Assessment for the NIC System of Technical Assistance Requests (NIC STAR)

Issued by:
Sonya D. Thompson, CIO / SCOP

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

Date approved: [September 24, 2024]

(May 2022 DOJ PIA Template)

Section 1: Executive Summary

The Federal Bureau of Prisons (FBOP) National Institute of Corrections (NIC) provides training and technical assistance (TA) to federal, state, local, and tribal correctional agencies. Some requests can be fulfilled by NIC personnel, while others may require NIC to hire a Technical Resource Provider (TRP) to provide a specialized service or resource. Some requests involve training an agency's employees on a specific subject, and others allow members of one agency to visit another agency to observe and learn about a particularly promising program or practice. The resources provided in response to TA requests are funded through various means, including contracted services, cooperative agreements, micro-purchases, or reimbursement for travel-related expenses. The NIC's System of Technical Assistance Requests (NIC STAR) is a FedRAMP-certified Software-as-a-Service (SaaS) platform that allows NIC personnel to track, process, and capture information related to nearly every aspect of each request it receives. NIC STAR also allows correctional agencies to submit their requests via a public-facing website featuring an intuitive web-based request form, educational materials, and surveys to allow for end-user engagement and feedback. The NIC has prepared a Privacy Impact Assessment (PIA) for NIC STAR because this system collects, maintains, and disseminates information in an identifiable form about state, local, tribal, and federal requestors, training participants, and TRPs.

Individuals or federal, state, tribal, or local entities who wish to obtain TA services from NIC will voluntarily submit information about their agency and the nature of their assistance request through the external-facing NIC STAR web portal for approval. The individual or entity's point of contact (POC) will be required to submit their name along with her/his or the entity's telephone, address, and email contact information. Data is only obtained from individuals or entities who elect to obtain assistance services from NIC.

The NIC STAR web portal is housed on a webpage accessible from the main FBOP NIC website. Information submitted by participants and TRPs on the external-facing NIC STAR web portal will be transmitted to the internal-facing NIC STAR application where authorized NIC employees ("users") will access the information to verify the agency and approve or deny a request, using multi-factor authentication (MFA) and single sign-on (SSO). Users for NIC STAR are determined by need: FBOP NIC Administrative Officers with access to the NCIC system will have access to the background check information submitted through NIC STAR and FBOP Financial Department employees will have access to the financial information needed to reimburse NIC-related expenses. NIC STAR will also help NIC employees respond and track TA requests throughout the response process and internal approval levels (e.g., Supervisor confirming with NIC Unit Manager that a TA request falls within NIC's scope).

Many TA requests involve specialized training or subject matter expertise in a particular correctional subject. For these types of requests, NIC may utilize contracted personnel who specialize in a particular subject related to the request. These contractors are commonly referred to as TRPs. TRPs who wish to be considered for work providing technical assistance will voluntarily submit their contact information, including name, telephone, address, and email address for their firm or agency to the web portal. TRPs also provide their resume to help NIC identify which areas of expertise they possess. For those TRPs who are not employed with federal, state, local, or tribal correctional facilities, FBOP contracts with the individual and not the entity who employs the TRP.

The public-facing NIC website that will allow NIC to service TA requests from federal, state, local, and tribal requestors and will also include educational materials about NIC capabilities and answers to frequently asked questions (FAQ). The website will collect aggregated web analytics about the general location of user traffic, the type of browser and operating system used to access the site, the date and time of access, the internet address of the website from which users linked directly to the site (the only source for login is located on the main NIC webpage), and pages visited. This information is used to improve usage of the website and will be leveraged to measure future marketing efforts. The information of individual website visitors is not stored in the system and is not available to any system users.

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.

NIC STAR will transform NIC operations so that TA requests, funding sources, and training-related logistics can be tracked in one centralized, secure location, creating several business efficiencies. Requestors can provide their contact information and request details so that NIC has the necessary information to assign prioritization to and complete each request. After a requestor submits their information, an NIC employee will manage all information in NIC STAR to consistently track and service the request. Requestors will be able to view the status of their requests and receive email communications about their requests throughout the process (receipt, identify solution, prepare solution). Requestors are unable to edit the information they submitted through NIC STAR, but they are able to contact NIC and an authorized user can include a note with the necessary corrections to accompany the initial submission per the request of the initial requestor.

NIC STAR will also collect information to reimburse participants for travel-related expenses, which includes the individual's name, SSN, email address, mailing address, and banking information (routing number, account number, and account type). For participants or TRPs that require a background investigation prior to entering a FBOP institution, NIC STAR will collect the participant's or TRP's name, SSN, mailing address, telephone number, date of birth, sex, race, height, weight, eye and hair color, and place of birth. For participants or TRPs who are not traveling or entering FBOP facilities, NIC STAR will collect first and last names and email addresses. SSNs are used to conduct NCIC background checks for participants who attend training at FBOP facilities without an agency-issued badge. SSN is also required to enter participant travel reimbursement information into the Unified Financial Management System (UFMS). While all information in NIC STAR will be encrypted in transit and at rest, financial information and SSNs will be further encrypted in transit *and* at rest using a deterministic encryption scheme. Once the information from the participant or TRP is submitted into the external-facing web portal, the system will make the information available in the internal-facing application for NIC use and processing (background checks or financial reimbursement).

Prior to implementation of NIC STAR, participant travel reimbursement information (account type, routing number, and account number) is collected via encrypted email. Upon implementation, the NIC STAR will provide a secure weblink for participants to provide their banking information for

reimbursement. The link will direct the individual to a secure portal to provide the required information, which will then be sent to the internal-facing application for authorized NIC Financial Department to review. Information collected by NIC STAR will be populated into UFMS to issue financial compensation.

Analytics tools are used to capture non-identifiable aggregated web analytics, supported by Google Analytics, that will be used to improve usage of the website, measure NIC efforts, and prioritize future enhancements to optimize the user experience (UX). These tools do not capture name, email address, IP address, or any other PII.

The information regarding federal, state, local and tribal requestors can only be retrieved by authorized personnel with access to the system using approved authentication mechanisms, including multifactor authentication. Approved FBOP contractors are involved with the design and development of the information system and will continue to provide maintenance and administrative services on the production environment after the information system is deployed.

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. §§ 4351-4352
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.*

Federal Bureau of Prisons/NIC System of Technical Assistance Requests

(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, B, C, D	Individual requestor, participant, TRP, and NIC employee name
Date of birth or age	X	A, B, C, D	Participant and TRP date of birth
Place of birth		A, B, C, D	Participant and TRP place of birth
Gender	X	A, B, C, D	Participant and TRP gender
Race, ethnicity, or citizenship	X	A, B, C, D	Participant and TRP race
Religion			
Social Security Number (full, last 4 digits or otherwise truncated)	X	A, B, C, D	Participant and TRP SSN
Tax Identification Number (TIN)	X	A, B, C, D	TRP Tax ID number on request for purchase
Driver's license			
Alien registration number			
Passport number			
Mother's maiden name			
Vehicle identifiers			
Personal mailing address	X	A, B, C, D	Participant and TRP mailing address
Personal e-mail address	X	A, B, C, D	Participant and TRP email address
Personal phone number	X	A, B, C, D	Participant and TRP phone and business fax number
Medical records number			
Medical notes or other medical or health information			
Financial account information	X	A, B, C, D	Participant banking information
Applicant information			
Education records	X	A, B, C, D	TRP resume (document)
Military status or other information	X	A, B, C, D	May be included on TRP resume (document), as determined by the individual submitting the resume
Employment status, history, or similar information	X	A, B, C, D	TRP resume (document)
Employment performance ratings or other performance information, e.g., performance improvement plan			
Certificates			
Legal documents			
Device identifiers, e.g., mobile devices			

Department of Justice Privacy Impact Assessment
Federal Bureau of Prisons/NIC System of Technical Assistance Requests
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
Web uniform resource locator(s)	X	A, B, C, D	Collects internet address of the website from which users linked directly to the site, and pages visited for all NIC users (this information is not PII)
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	X	A, B, C, D	Request for Purchase Form
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			
- Scars, marks, tattoos			
- Vascular scan, e.g., palm or finger vein biometric data			
- DNA profiles			
- Other (specify)			
<i>System admin/audit data:</i>			

(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
- User ID	X	A	System admin / audit data and User ID of authorized FBOP personnel.
- User passwords/codes	X	A	System admin / audit data and User ID of authorized FBOP personnel.
- IP address	X	A	System admin / audit data and User ID of authorized FBOP personnel.
- Date/time of access	X	A	System admin / audit data and User ID of authorized FBOP personnel.
- Queries run	X	A	System admin / audit data and User ID of authorized FBOP personnel.
- Contents of files	X	A	System admin / audit data and User ID of authorized FBOP personnel.
Other (please list the type of info and describe as completely as possible):	X	A, B, C, D	The agency request portal will capture audience acquisition and behavior metrics for web analytics.

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	X	Email	X		
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 FBOP personnel, such as NIC employees and contractors using enterprise authentication mechanisms. Ad hoc requests (audit, Privacy Act access or amendment, or FOIA requests) will be sent to system owners to determine need and the minimum information required to satisfy the request.
DOJ Components	X		X	Status information for TA requests may be shared to the individual that submitted the request, such as U.S. Marshal Services employees. Some examples include notifications that the request has been received or the request is under review.

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.
				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			Status information for TA requests may be shared to the individual that submitted the request, such as employees with Department of Defense and Department of Homeland Security. Some examples include notifications that the request has been received or the request is under review. 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.
State, local, tribal gov't entities	X			Status information for TA requests may be shared to the individual that submitted the request. Some examples include notifications that the request has been received or the request is under review.

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.
Public	X			Members of the public may request access to their information through NIC STAR or by submitting a Privacy Act access request to FBOP. The information the individual will receive is limited to only their information in the system (if it exists).
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.*

Specific notice to individuals will be provided to individuals via the Privacy Act (e)(3) notice that will be provided to requestors on all pages of the application when populating and submitting information required for opportunities. A link to the FBOP’s privacy notice/policy will be made available on the footer of all pages for view by requestors when NIC STAR is made available to the public.

Generalized notice is provided to individuals in the following System of Records Notices published in the Federal Register cover the records in this system:

- FBOP's National Institute of Correction Technical Resource Provider Record System, Justice/BOP-101, published on March 2, 2000 (65 FR 11342) and last modified on May 25, 2017 (82 FR 24147) and published here: <https://www.gpo.gov/fdsys/pkg/FR-2000-03-02/pdf/00-4973.pdf>.
- FBOP's National Institute of Corrections Academy Record System, Justice/BOP-103, published on Dec. 16, 1999 (64 FR 70286) and last modified on May 25, 2017 (82 FR 24147) and published here: <https://www.gpo.gov/fdsys/pkg/FR-2017-05-25/pdf/2017-10780.pdf>. DOJ's DOJ Computer Systems Activity & Access Records, Justice/DOJ-002, published on December 30, 1999 (64 FR 73585) and last modified on Jul. 14, 2021 (86 FR 37188) and published here: https://www.justice.gov/d9/pages/attachments/2021/08/02/2021-14986_-_doj-002_sorn_update.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 voluntarily submit requests. By submitting information, requestors are voluntarily agreeing to participate in the collection and use of information in the 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.*

Individuals may follow FBOP protocols to receive or amend information collected or stored by FBOP through a Privacy Act or FOIA request. Additional information will be available in the [NIC STAR Privacy Statement](#) and the relevant SORNs (see Section 7 below). While individual requestors are unable to edit their TA requests themselves, they can contact NIC and authorized personnel may add a note to accompany the requestor's information in NIC STAR per the individual's request.

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): BOP-NICSTAR was authorized to operate on 12/5/24. 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: No outstanding POAMs.
	This system is not subject to the ATO processes and/or it is unclear whether NIST privacy controls have been implemented and assessed. Please explain:
X	This 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: The system was assigned Moderate based on the highest classification across all relevant information types for Availability, Confidentiality, and Integrity.
X	Monitoring, testing, or evaluation has been undertaken to safeguard the information and prevent its misuse. Specify: FBOP will conduct testing of security controls to ensure 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: The system captures an audit of user account modifications and system events that will be reviewed by system administrators on a quarterly basis. Additional auditing of transactional data will be captured and maintained to align with records and information management requirements. A subset of approved internal users (e.g., employees, contractors) have been identified as system administrators to support organization-defined configuration, security, and access control.
X	Contractors that have access to the system are subject to information security, privacy and other provisions in their contract binding them under the Privacy Act, other applicable laws, and as required by DOJ policy.
X	Each Component is required to implement foundational privacy-related training for all Component personnel, including employees, interns, and contractors, when personnel on-board and to implement refresher privacy training annually. Indicate whether there is additional training specific to this system, and if so, please describe:

NIC STAR users are required to complete annual NIC STAR system-specific training; and training materials are readily available for reference purposes when needed.
--

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?*

Accounts are created for a subset of identified internal users (e.g., employees, contractors). Access to NIC STAR is granted through single sign-on (SSO) and multi-factor authentication (MFA) using enterprise services. Inbound requests to the internal application are restricted to a subset of IP ranges and monitored for usage.

Approved FBOP employees and contractors are designated as system administrators to support organization-defined configuration, security, and access control. The account managers periodically review accounts to identify personnel that no longer need access. Account managers will add new users, remove existing users, or modify existing users. Accounts will be modified or deactivated to ensure that access privileges are promptly altered (e.g., termination, transfer, and/or change in responsibilities) mitigating potential security risks. Automatic account management will be applied to inactivate accounts that have not logged into the system for a specified period. The system incorporates security controls to identify and restrict unsuccessful login attempts. Additional password complexity, reset duration, and reset reuse have been implemented to align with FBOP standards.

NIC STAR utilizes industry best practices for data encryption, including encryption at rest and in transit. All information in NIC STAR will be encrypted in transit and at rest, and financial information and SSNs will be further encrypted in transit and at rest. Once the information from the participant or TRP is submitted into the external-facing web portal, the system will make the information available in the internal-facing application for NIC use and processing (background checks or financial reimbursement).

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.)*

Information in NIC STAR is maintained by FBOP for approximately 8 years, pursuant to N1-129-04-002, NIC Registrar Database. This information may also be destroyed when the information is superseded when new or updated information replaces the current information for personal, class or registration records. Information may be deemed obsolete when NIC no longer provides completed file records beyond the 8-year retention or class information.

N1-129-04-002: NIC Registrar Database

The system helps administer the daily activities of training, administration, and to keep track of training histories. Three main types of records:

- **Personal Records:** Includes information on applicants and trainees, including job titles, agencies, addresses, telephone numbers, types of corrections agencies for which they work, etc.
- **Class Records:** Include information about course title, course description, dates and times, location, number of participants, etc.
- **Registration Records:** Include information that tie the person and class records together to indicate that a person applied for a particular class and was either selected or rejected. If an applicant was rejected, the reason for rejection is entered into the system.

Temporary: Deleted or shredded, depending on the medium, when data is superseded or obsolete.

N1-129-10-003: Records of Director and Deputy Director (NIC)

#5: Technical Assistance Files: Case files documenting short-term assistance provided to state and local correctional agencies via private-sector subject matter experts paid by NIC. Records include the initial request, correspondence and memoranda regarding logistics and expenses, supporting documentation from the presenter (journal articles, bibliographies, etc.), final report, expense report, and the recipient's evaluation to the presenter.

Temporary: Destroy 8 years after case is closed.

#6: Technical Assistance Management Information System: Electronic edition of the TA files, which also functions as a tracking system. Information includes number dates, requesting agency, names of contact people, staff assigned, and the subject area. The program will make selections matching the clients' goal(s) with the consultant's expertise. The system has a financial component which automatically obligates funds. Reporting categories include division, individual staff workload, project status, and requests.

Temporary: Delete 8 years after case is closed.

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:*

BOP-101: National Institute of Correction Technical Resource Provider Record System. Last published in full at 64 FR 11343 (Mar. 2, 2000), available at:

<https://www.govinfo.gov/content/pkg/FR-2000-03-02/pdf/00-4973.pdf>.

BOP-103: National Institute of Corrections Academy Record System. Last published in full at 64 FR 70286 (Dec. 16, 1999), available at: <https://www.gpo.gov/fdsys/pkg/FR-1999-12->

[16/pdf/99-32617.pdf](https://www.justice.gov/d9/pages/attachments/2021/08/02/2021-14986_-_doj-002_sorn_update.pdf).

DOJ-002, DOJ Computer Systems Activity & Access Records. Last published in full at 86 Fed. Reg. 37188 (Jul. 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?

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 NIC STAR. 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 STAR. 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. Additionally, FBOP employees and contractors undergo training where they learn how to properly handle PII, which includes collecting information for only necessary purposes; sign a DOJ Rules of Behavior agreement that informs and requires the personnel to only use FBOP systems, including NIC STAR, for FBOP mission-related purposes; and undergo Ethics training, which requires FBOP personnel to ethically handle and safeguard PII used in the course of the individual's employment.

There is also a potential privacy risk arising from collecting information of inadequate quality on each individual. To mitigate this, NIC STAR 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 as a footer on all webpages where information is collected, which includes information on Information Collected, How Personal Information Is Used, Child Privacy, Cookie Usage, External Sites, and Security.

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, such as MFA-required access to systems, SSO, and data encryption. These safeguards include the maintenance of records and technical equipment in restricted areas.

b. Potential Risks related to the Use of Information

Potential threats to privacy arising from FBOP's use of NIC STAR information includes the risk of unauthorized use of information and threats to the integrity of the information arising

from unauthorized access or improper disposal of information. FBOP ensures information is provided only to those individuals who require access to perform their official duties as a way to mitigate the risk of unauthorized access through the implementation of data access controls. Additionally, to address the threats to the integrity of the data from unauthorized access, only specifically authorized FBOP employees and contractors are permitted access to the internal NIC STAR system; no personnel from the larger DOJ community are authorized. 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 STAR.

Employees are also required to complete annual training that addresses how to properly handle sensitive information, which helps to mitigate the risks arising from improper use or disposal of the information. FBOP also maintains updated record retention schedules that govern the durations for how long FBOP is authorized to retain NIC STAR records. The information disposition date is based upon when business use ceases in accordance with FBOP data storage and retention policies.

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, as well as risks resulting from unauthorized data modification and misuse. FBOP mitigates these risks by enforcing access controls, utilizing data encryption for all NIC STAR information, and routinely auditing user and system administration activities. Data transmission, both within and outside the system, is encrypted using the TLS protocol.

Information may be shared with other DOJ components, other federal entities, or Congress, as authorized by law for auditing, reporting, or evaluative purposes to help identify the most needed course topics. Each TA request is evaluated to determine need and the minimum information required to satisfy the request. FBOP legal employees will evaluate the request prior to it being exported or sent, as necessary. FBOP will aggregate data and remove all personal identifiers as necessary and appropriate when it is required to share data with other DOJ components. These measures help reduce the risk of disclosure of information to unauthorized individuals.