Office of Justice Programs

Privacy Impact Assessment
for the
Bureau of Justice Assistance
(BJA) National Training
Technical Assistance
Center (NTTAC)

Issued by:
Maureen Henneberg

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

Date approved: March 20, 2025

(May 2022 DOJ PIA Template)

Section 1: Executive Summary

The mission of the Office of Justice Programs (OJP) is to increase public safety and improve the fair administration of justice across America through leadership and programs. Through OJP, and in coordination with the Bureau of Justice Assistance (BJA), the National Training Technical Assistance Center (NTTAC) will provide governments and leaders across the federal, state, local, and tribal levels with expert training and technical assistance (TTA) to help maintain their communities' safety and work to strengthen the national criminal justice system at large.

The goal of BJA NTTAC is to improve America's criminal justice system by providing communities nationwide with expert, coordinated, research-driven or evidence-based justice-related technical assistance and training that ultimately supports communities in improving local justice system responses. To do so, BJA NTTAC collects and shares data about TTA relevant to OJP's BJA, including data from individuals and organizations that may be providing or requesting TTA, as well as associated events and deliverables.

BJA NTTAC leverages FedRAMP AWS Gov Cloud SCN to deliver information and services. This PIA is being conducted because BJA NTTAC contains information in identifiable form about members of the public that is contained in an IT system.

Section 2: Purpose and Use of the Information Technology

The BJA NTTAC website (https://bjatta.bja.ojp.gov/) collects and shares data about TTA relevant to OJP's BJA, including data from individuals and organizations that may be providing or requesting TTA, as well as associated events and deliverables. The site also assists TTA providers in creating a semiannual report that they can submit to JustGrants.

In addition, the BJA NTTAC website supports BJA NTTAC's mission of strengthening the capacity of public safety agencies through the delivery of cost-free training, evidence-based resources, and customized expertise. In particular, the website provides communities nationwide with rapid, expert, coordinated, research-driven or evidence-based justice-related TTA that supports communities in improving local justice system responses. OJP provides cloud infrastructure for BJA NTTAC and scans for vulnerabilities. A contractor is responsible for building, updating, and maintaining the BJA NTTAC website and manages user engagement while also providing technical support and accomplishing any necessary remediation.

The BJA NTTAC website is a web-based application and is divided into three sub-sections: Working with NTTAC (WWN), TTA Collaboration Portal (TTA CP), and TTA Reporting Portal (TTARP). Each section collects information dependent on its purpose.

WWN is primarily used as a public facing website for BJA NTTAC to share information with the public. Information collected from users includes the following:

- **TTA Request** – Information is collected from the requesting organization ("requestor") regarding the type of training or technical assistance sought, the problem faced in the community, and the expected outcome from receiving the TTA. This information helps the BJA NTTAC TTA Coordinator to understand the scope of the request and to determine whether BJA NTTAC can help deliver the requested TTA. The requestor also includes a point of contact (POC) for the recipient agency (to include name, email, and phone number).

- **Provider Application** – Individuals or organizations that would like to be considered a TTA Provider for BJA NTTAC may submit an application that contains their service area preferences, a POC, two references (to include name and either email or phone number), business address, and a description of the organization. For individuals there is also a question on citizenship, eligibility to work in the U.S., and an optional question on race.
- **User Profiles** – Individuals who register an account on the website must complete a User Profile which includes name and email. In addition, individuals may provide optional, additional information, such as a professional title and profile picture and information on their demographics, experience, education, and location.
- **Justice Community Mailing List** – Users of the BJA NTTAC website can sign up for this mailing list by providing the following information: name, email, organization, and title.

TTA CP allows authenticated users to share the following information voluntarily:

- **Posts** – Users can share information voluntarily with the community through 'posts' which contain a title and body field, for the purpose of sharing, collaborating, or seeking assistance.

TTARP collects the following information from authenticated users:

- Information on BJA TTA awards (grants and cooperative agreements), award activities, and performance metrics for the purposes of allowing BJA NTTAC to manage and report out on BJA TTA grantee work. The information collected covers TTA services developed, worked on, or provided under a BJA TTA grant or cooperative agreement.

The BJA NTTAC website is hosted in the Secure Cloud Network which resides in Amazon Web Services (AWS) GovCloud. It is isolated from other tenants in its own Virtual Private Cloud (VPC).

2.1 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	34 U.S.C. § 10142(3) and (4); 28 U.S.C. 530C
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

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, D	Required for all users, and POCs for TTAs and awards
Date of birth or age			
Place of birth			
Sex	X	C, D	Submission is voluntary for BJA NTTAC providers and applicants
Race, ethnicity, or citizenship	X	C, D	Citizenship to determine contractor's work eligibility. Race submission is voluntary for BJA NTTAC providers and applicants
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	C, D	Required for BJA NTTAC providers and applicants
Personal e-mail address	X	A, B, C, D	Required for all users, and of POCs for TTAs and awards.
Personal phone number	X	C, D	POCs for TTAs and awards, and BJA NTTAC providers and applicants
Medical records number			
Medical notes or other medical or health information			
Financial account information			
Applicant information			
Education records			
Military status or other information			
Employment status, history, or similar information	X	C, D	Submission is voluntary for BJA NTTAC providers and applicants
Employment performance ratings or other performance information, e.g., performance improvement plan			
Certificates			
Legal documents			
Device identifiers, e.g., mobile devices			
Web uniform resource locator(s)			Required for organizations, not individuals

(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
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			
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, C, D	Required for user registration
- **User passwords/codes**	X	A, B, C, D	Required for user registration
- **IP address**			
- **Date/time of access**	X	A, B, C, D	Required for logs and audits
- **Queries run**			

(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
- **Contents of files**			
Other (please list the type of info and describe as completely as possible):			

3.1 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	X	Email	X		
Other (specify):					

Government sources:					
Within the Component	X	Other DOJ Components		Other federal entities	
State, local, tribal	X	Foreign (identify and provide the international agreement, memorandum of understanding, or other documented arrangement related to the transfer)			
Other (specify): Grant award information is sourced from the DMRA and imported into the NTTAC website.					

Non-government sources:					
Members of the public	X	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	Certain BJA staff with user accounts can access information with direct log-in access. Otherwise, information is shared within the component as requested.
DOJ Components				
Federal entities				
State, local, tribal gov't entities			X	Users can access a limited amount of information upon direct log-in. Users are only able to access information of other users who post, comment, or share resources upon signing in.
Public			X	Users can access a limited amount of information upon direct log-in. Users are only able to access information of other users who post, comment, or share resources upon signing in.
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.

No information from BJA NTTAC will be released for Open Data purposes.

Section 5: Notice, Consent, Access, and Amendment

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

The BJA NTTAC website provides a link to the DOJ Privacy Policy. The Training and Technical Assistance Center Records (TTAC) SORN has been published in the Federal Register to cover those uses not already covered by existing systems of records notices, and a Privacy Act § 552a(e)(3) notice for individuals will be placed on electronic forms used to collect PII.

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.

The use of BJA NTTAC, including the creation of a user account, is voluntary, however failure to provide such information would limit the user's ability to request and receive TTA. A user's name may appear in relation to their company or governmental entity, and may be visible to others (*i.e.*, colleagues). Additionally, a shared resource such as a TTA document or presentation, may likewise be credited to that user's name, voluntarily. User accounts are automatically locked after 90 days of inactivity. While the user may no longer appear in a list of users related to a company or particular training resource, they may still be credited on the resource itself (*i.e.,* a PDF with their name as one of the authors).

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.

Users can amend and modify their own information or can request access and amendment in accordance with the System of Records Notice and 28 C.F.R. § 16.46, "Requests for Amendment or Correction of Records."

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).

	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):** September 8, 2023; expires September 8, 2026. **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:**
	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 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:** BJA NTTAC is categorized as a Moderate impact system in accordance with guidance provided in FIPS 199 based on the type of information collected and stored to maintain the confidentiality, integrity, and availability of information in the system.
×	**Monitoring, testing, or evaluation has been undertaken to safeguard the information and prevent its misuse. Specify:** OJP has implemented IT security continuous monitoring, a critical part of the risk management process, where security controls and risks are assessed and analyzed by BJA NTTAC and validated by OJP at a frequency sufficient to support risk-based security decisions to adequately safeguard the information. In addition, DOJ/OJP monitors the monthly continuous monitoring submissions from Cloud Service Providers (CSPs) for all Cloud Service Offerings (CSOs) supporting BJA NTTAC in accordance with FedRAMP Continuous Monitoring requirements.
×	**Auditing procedures are in place to ensure compliance with security and privacy standards. Explain how often system logs are reviewed or auditing procedures conducted:** Application audit logs are ingested by Splunk and reviewed in accordance with Department and Component policies and procedures.
×	**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**.
	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: No, consultants on contract with BJA NTTAC are not required to take any privacy-related training specific to this website.

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?

BJA NTTAC employs separations of duties in order to prevent users from having more than one task, thus increasing the security posture of the system. Any potential conflicts will be documented, to include processes and procedures in the event a waiver is needed.
This system leverages FedRAMP AWS Gov Cloud Secure Cloud Network (SCN), ensuring access requests are managed through a central point. Role-based access controls are employed to limit users to those privileges that are necessary to complete their assigned tasks. Only System Administrators are allowed privileged access to system components.

OJP has implemented physical and logical security controls that comply with department standards and policies regarding protection of sensitive information in digital and non-digital form. BJA-NTTAC adheres either directly or through inherited hybrid controls the suite of

Access Control (AC), Audit and Accountability (AU), Identification and Authentication (IA), Risk Assessment (RA), System and Communications Protection (SC), and System and Information Integrity (SI).
Of these, the implemented controls are as follows:

- AC-03: Access Enforcement
- AC-06: Least Privilege
- AC-11(1): Pattern-hiding Displays
- AC-17: Remote Access
- AC-17(2): Protection of Confidentiality and Integrity Using Encryption
- AU-03(3): Limit Personally Identifiable Information Elements
- IA-02(1): Multi-factor Authentication to Privileged Accounts
- IA-02(2): Multi-factor Authentication to Non-privileged Accounts
- IA-06: Authentication Feedback
- IA-07: Cryptographic Module Authentication
- IA-08: Identification and Authentication (non-organizational Users)
- RA-05: Vulnerability Monitoring and Scanning
- SC-02: Separation of System and User Functionality
- SC-07: Boundary Protection
- SC-07(3): Access Points
- SC-08: Transmission Confidentiality and Integrity
- SC-12: Cryptographic Key Establishment and Management
- SC-18: Mobile Code
- SC-23: Session Authenticity
- SC-39: Process Isolation
- SI-02: Flaw Remediation
- SI-04(2): Automated Tools and Mechanisms for Real-time Analysis
- SI-07(1): Integrity Checks

Additionally, OJP has issued the OJP IT Security Program instruction and additional SOPs that defines types of digital and/or non-digital media requiring restricted access and provides guidelines for the secure processing, transmission, and storage of OJP sensitive information.

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.)

Records in this system are retained and disposed of in accordance with the National Archives and Records Administration, General Records Schedule 1.2, Item 020: "Grant and Cooperative Agreement Case Files." This schedule covers records relating to individual grant or cooperative agreements. Pursuant to this schedule, records will be destroyed after 10 years after final action is taken on the file but may be retained longer if required for business use.

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, Department of Justice Information Technology, Information System, and Network Activity and Access Records, last published at 86 Fed. Reg. 37188 (July 14, 2021), available at https://www.justice.gov/d9/pages/attachments/2021/08/02/2021-14986_-_doj-002_sorn_update.pdf.

OJP-010, Technical Assistance Resource Files, last published in full at 53 Fed. Reg. 40530 (Oct. 17, 1988), available at: https://www.justice.gov/opcl/docs/53fr40530.pdf.

OJP- 018, Training and Technical Assistance Center Records (TTAC), last published in full at 89 Fed. Reg. 84199 (Oct. 21, 2024), available at https://www.govinfo.gov/content/pkg/FR-2024-10-21/pdf/2024-23952.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?

There is a privacy risk associated with the overcollection of PII. In order to mitigate this risk, the BJA NTTAC program periodically reviews the types of information collected on its various applications to ensure that only the minimum necessary information is collected from its applicants.

There is also a risk that information collected on individuals may be inaccurate or out-of-date. In order to mitigate this risk, information collected by BJA NTTAC is obtained directly from the individual completing any respective form, and that information is only used or shared in TTA engagements or for BJA special projects. Users will be presented with a Privacy Act Statement by the system software that describes their rights under the Privacy Act of 1974.

There is a privacy risk associated with unauthorized access to the information within the system. In order to mitigate this risk, BJA NTTAC utilizes several security controls. For example, only a select few NTTAC team members with public trust clearance have access to the information collected. Additionally, data is not shared outside of the website unless it is for the purpose of fulfilling TTA engagements or completing special projects as directed by BJA.