Office of Justice Programs

Privacy Impact Assessment
for the Office for Victims of Crime Training and Technical Assistance Center (OVCTTAC)

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 Office for Victims of Crime Training and Technical Assistance Center (OVC TTAC) website (https://www.ovcttac.gov/) offers specialized training and technical assistance (TTA) on a wide range of topics relevant to victim service providers and allied professionals. All TTA is designed to help build the capacity of victim assistance organizations across the county and improve the quality of services offered to victims of crime in a variety of settings.

OVC TTAC is a web-based application that receives and processes applications from a variety of agencies and institutions requesting help in building their capacity in a number of victim-focused areas. OVC TTAC also receives and processes applications from individuals seeking professional development scholarships.

Information is stored in the database which resides on the server at the NTT Global Data Centers America, Inc. Access is granted only for the people who have access to the Consultant Network backend in their TTAC permissions (which is granted to only those whose work requires access to it) and the OVC COR. Information will not be shared with other offices, components, agencies, entities, or individuals.

This PIA is being conducted because OVC TTAC 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

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.

The OVC TTAC website is divided into the following sections: "Contact Us," "Sign-Up," "MyTTAC," "Resources," "How We Can Help," "News," "About Us," and TTA Provider Community. The sections that collect information from users are "Sign-Up," "MyTTAC," and "How We Can Help."

In the "Sign-Up" section, user contact information is collected to enable the user to receive emails regarding OVC TTAC updates.

The "MyTTAC" and "How We Can Help" sections allow users to request TTA and apply for a Professional Development Scholarship. Generally, the information requested from applicants (*see table at 3.1*) enables OVC to evaluate such requests.

The objective of the OVC TTAC system is to automate and simplify making requests and applications for TTA, which include the TTA Application and Professional Development Scholarship applications. The centralized collection mechanism ensures more accurate and expeditious evaluations of requests and applications. The system operates out of the data center known as NTT Global Data Centers Americas, based in Ashburn, Virginia. The systems' servers and infrastructure are all housed within the data center.

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	34 U.S.C. §§ 20103(c)(3) and 20111(c)(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: . DOJ/Component Employees, Contractors, and Detailees; . Other Federal Government Personnel; . Members of the Public - US Citizens or Lawful Permanent Residents (USPERs); . Members of the Public - Non-USPERs	(4) Comments
Example: Personal email address	*X*	*B, C and D*	*Email addresses of members of the public (US and non-USPERs)*
Name	X	A & C	**TTA Application** First (mandatory), middle initial (optional), last (mandatory) **OVC Consultant Network Application** Prefix (optional), first (mandatory), last (mandatory), suffix (optional) **Professional Development Scholarship Application** First (mandatory), middle (optional), last (mandatory) Names of References; names of DOJ users
Date of birth or age			
Place of birth			
Sex	X	C	**/C Consultant Network Application** Sex (optional)
Race, ethnicity, or citizenship	X	C	**/C Consultant Network Application** Race/ethnicity
Religion			

(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: . DOJ/Component Employees, Contractors, and Detailees; . Other Federal Government Personnel; . Members of the Public - US Citizens or Lawful Permanent Residents (USPERs); . Members of the Public - Non-USPERs	(4) Comments
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	**TTA Application** – N/A **OVC Consultant Network Application** N/A **Professional Development Scholarship Application** Home address (mandatory), city (mandatory), state/territory (mandatory), zip code (mandatory), country (mandatory)
Personal e-mail address	X	C	**TTA Application** – N/A **OVC Consultant Network Application** home email (optional) **Professional Development Scholarship Application** email (mandatory)
Personal phone number	X	C	**TTA Application** – N/A **OVC Consultant Network Application** Home phone (optional), cell phone (optional) **Professional Development Scholarship Application** phone (mandatory), fax (optional)
Medical records number			

(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: . DOJ/Component Employees, Contractors, and Detailees; . Other Federal Government Personnel; . Members of the Public - US Citizens or Lawful Permanent Residents (USPERs); . Members of the Public - Non-USPERs	(4) Comments
Medical notes or other medical or health information	X	C	**TTA Application – N/A** **OVC Consultant Network Application** The system asks the question, "Please let us know what special accommodations you will need while providing training and TA for OVC?" (Check all that apply) (optional) • Personal care attendant • Wheelchair accessibility (transportation, meeting space, lodging, etc.) • Type of wheelchair: manual, electric • Sign language interpreter • Specify type of sign language • Accommodations for service animal Materials converted into sight- assistive technology • Specify type of technology preferred • Specific dietary needs • Other (please explain) • None **Professional Development Scholarship Application** – N/A
Financial account information			
Applicant information			
Education records	X	C	**/C Consultant Network Application** Formal education (required)
Military status or other information			
Employment status, history, or similar information	X	C	**OVC Consultant Network Application** Employment (optional)
Employment performance ratings or other performance information, e.g., performance improvement plan			
Certificates			
Legal documents			
Device identifiers, e.g., mobile devices			
Web uniform resource locator(s)			
Foreign activities			
Criminal records information, e.g., criminal history, arrests, criminal charges			
Juvenile criminal records information			

(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: . DOJ/Component Employees, Contractors, and Detailees; . Other Federal Government Personnel; . Members of the Public - US Citizens or Lawful Permanent Residents (USPERs); . Members of the Public - Non-USPERs	(4) Comments
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	X	C	Photos are requested for consultants
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)			
ystem admin/audit data:			
User ID	X	A & C	Username, password
User passwords/codes	X	A & C	Username, password
IP address			
Date/time of access			
Queries run			
Contents of files			
Other (please list the type of info and describe as completely as possible):	X	C	Biographical summaries and resumes may include other types of PII not listed above; travel/budget information

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

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

Non-government sources:					
Members of the public	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 OVC staff with user accounts can access information with direct log-in access for the analysis and approval of applications. Otherwise, information is shared within the component as necessary.
DOJ Components				
Federal entities				
State, local, tribal gov't entities				
Public				
Counsel, parties, witnesses, and possibly courts or other judicial tribunals for litigation purposes				
Private sector				
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 the OVC TTAC 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.

Privacy Act System of Records Notices have been published in the Federal Register as noted in Section 7 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 OVC TTAC, 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). Users are required to provide Personal Identity and Authentication data, including their name, email and password, to access the platform.

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).

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):** An Authorization to Operate (ATO) extension was granted on December 3, 2024 for OVC Training and Technical Assistance Center (OVCTTAC) until September 3, 2025. **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:** OVC TTAC has open POAMs for the Privacy Impact Assessment and the Privacy Certification Memo, both of which will be satisfied after the completion of this Privacy Impact Assessment.
	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: System has been assigned a moderate security categorization based on the Information Types included and Impact Levels from NIST SP 800-60 V1 and V2.
X	**Monitoring, testing, or evaluation has been undertaken to safeguard the information and prevent its misuse. Specify:** Monitoring, testing, and evaluation will be performed by a contractor using Amazon Web Services (AWS) and native environment tools in conjunction with DOJ policy.
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 logs will be ingested into the SPLUNK system. System log reviews and auditing procedures will be performed in accordance with DOJ policy.
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**.
	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:

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?

Access controls have been designed to preserve and protect PII. Role-based access is ensured in the system to minimize any role-based vulnerabilities. Password security has been implemented using OJP-specified complexity rules.

PII in transmission is protected by usage of HTTPS (to ensure secure communication between users and the relevant website(s)), and TLS (Transport Security Layer) cryptographic protocol, version 1.2 or better.

Automated auditing of all information access types will be provided by the operating system and application software.

Privacy risks are also minimized with physical controls. NTT Global Data Centers Americas houses the systems servers and infrastructure and has implemented physical security protocols to protect the business premises and information systems from unauthorized access, damage, and interference.

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 (NARA), 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.

7.1 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), 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 OVC TTAC 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 recorded by OVC TTAC is provided directly by the users of the system. The information collected is used for a comprehensive assessment of the applicant and/or their request and is only shared as necessary within OVC. 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, OVC TTAC utilizes several security controls. For example, only cleared personnel within OJP have access to information in the system. Also, complex password protection is used for secure access to the applications. The data is secured in a hardened data center facility that has been audited and certified by an independent assessor using NIST requirements with no exceptions/findings noted. HTTPS is used for encrypted communications and a secure ID of a web server. TLS version 1.2 is used for the secure transport of data. Passwords are encrypted in the database.