Office of Justice Programs

Privacy Impact Assessment
for the
International Terrorism Victim Expense Reimbursement Program
(ITVERP) – Web Application

Issued by:
Maureen Henneberg

Approved by: Peter A. Winn, Acting Chief Privacy and Civil Liberties Officer, Department of Justice

Date approved: April 18, 2019

(May 2015 DOJ PIA Template)

EXECUTIVE SUMMARY

The International Terrorism Victim Expense Reimbursement Program (ITVERP) is a unique federal program that provides financial reimbursement for qualifying expenses to eligible U.S. citizens and U.S. government employees who suffered direct physical or emotional injury from an act of international terrorism while outside the United States. ITVERP is administered by the Office for Victims of Crime (OVC) within the Office of Justice Programs (OJP), U.S. Department of Justice (DOJ). Through ITVERP, reimbursement is provided to victims of international terrorism and their families for expenses related to medical and mental healthcare, funeral and burial, repatriation of the victim's remains, property loss, and miscellaneous expenses such as emergency travel. The ITVERP web application system will assist in processing ITVERP claims from initial receipt of the claim through approval for payment. The ITVERP system collects and maintains information in identifiable form (IIF), which may include, but is not limited to: claimant name, address, gender, date of birth, Social Security Number, employer information, medical information, financial records, marriage certificates, birth certificates, property loss expenses, mental health expenses, income tax information, insurance information, and funeral and burial expenses.

Section 1: Description of the Information System

Provide a non-technical overall description of the system that addresses:

(a) the purpose that the records and/or system are designed to serve;
(b) the way the system operates to achieve the purpose(s);
(c) the type of information collected, maintained, used, or disseminated by the system;
(d) who has access to information in the system;
(e) how information in the system is retrieved by the user;
(f) how information is transmitted to and from the system;
(g) whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects); and
(h) whether it is a general support system, major application, or other type of system.

(a) The International Terrorism Victim Expense Reimbursement Program (ITVERP) provides financial reimbursement for qualifying expenses to eligible U.S. citizens and U.S. government employees who suffered direct physical or emotional injury from an act of international terrorism while outside the United States. Through ITVERP, reimbursement is provided to victims of international terrorism and their families for expenses related to medical and mental health care, funeral and burial, repatriation of the victim's remains, property loss, and miscellaneous expenses such as emergency travel. The ITVERP web application will handle ITVERP claims from the initial receipt of a claim through the final claim determination.

(b) The web-based claims management system will accomplish intake, data management, reporting, and business flow management. External users of this system (claimants), will be allowed to submit and track their claims online. ITVERP claimants will be offered real-time access to their

claim status information and will be able to upload supporting documentation electronically into the ITVERP document repository. Once the claimant submits the application and supporting documents for processing, the claimant will no longer have access to modify the application, but will be able to modify their system profile information. Internal users (OVC program staff and contractors with a need-to-know) will have access to the claim application and the supporting documentation that will be used to adjudicate claims for reimbursement. During this process, OVC reviews the terrorist incident designation, the claimant's expenses incurred, and supporting documentation for legal sufficiency. After approval by the Director of OVC, the approved claimant expenses are manually sent to the Office of the Chief Financial Officer (OCFO), where payments are executed through OCFO's Treasury system. The ITVERP system will also permit OVC to compile weekly, monthly, and annual internal reports, as well as an annual report for Congress.

The ITVERP application will be deployed within Microsoft Azure and Dynamics 365 (Dynamics 365). Dynamics 365 is a cloud-based solution for Customer Relationship Management (CRM) offered by Microsoft. Dynamics 365 provides a secure website for user's access, and utilizes Hyper Text Transfer Protocol Secure (HTTPS) and Transport Layer Security (TLS) 1.2 to secure data in transmission. Transparent Data Encryption (TDE) is used to encrypt data at rest. Dynamics 365 is also Federal Information Processing Standards (FIPS) 140-2 compliant.

(c) The data fields and supporting documents collected directly from the claimant by the system include[1] the following:

- Name
- Address
- Telephone Number
- Email Address
- Gender
- DOB/Age
- Place of Birth
- SSN
- Driver's License Number
- Passport Number
- Military Service
- Occupation
- File/Case/Claim ID
- Patient ID
- Income Tax Information/ Taxpayer ID Number
- Banking Information, including account number, financial account transaction number

[1] The information collected from each claimant will vary depending on the expenses for which they are seeking reimbursement, and may include additional information input into free-text fields. However, OVC will not request any additional data elements from claimants.

- Employment Status Information, including employee ID, employed part/full time, work related injury
- Insurance Information
- Relationship Verification Information, including marital status, marriage date, marriage certificate, birth certificate, power of attorney, will, health care directive, etc.
- Terrorist incident date, location, and lead investigative agency
- Description of terrorist incident and verification of victims' injuries
- Supporting documents related to an incident, including police report, news articles, pictures, etc.
- Death Information, including date of injury or death, funeral and burial records, death certificate
- Medical and mental health records
- Property valuation, such as receipts, photographs, credit card statements or other documentation that shows the cost of the property at the time it was purchased.
- System administration/audit data, including user ID and date/time of access

(d) The system will be accessible to both external and internal users. The external users (claimants) do not reside on the ITVERP domain; they use their email address and create a username and password. Internal users reside on the @ojpitverp.onmicrosoft domain. Dynamics 365 stores the account information for both internal and external users. The ITVERP system employs Microsoft Azure's Active Directory as the users' Identity and Account Management system. Active Directory supports strong authentication, authorization, and auditing of user access activities in accordance with Federal mandates and standards.

Claimants must register for an account prior to gaining access to the ITVERP application. Once registered and validated for approval, claimants can complete an application, upload supporting documents and submit their claim for expense reimbursement.

Internal users must have a valid OJP clearance, job duties, need-to-know, and supervisory approval to perform the ITVERP internal job functions within the system. ITVERP employs separate roles and functions and uses "least privilege" to govern internal user access and permissions. ITVERP has the following 7 roles for internal users: System Administrator, ITVERP Case Manager, ITVERP Program Manager, ITVERP OGC, ITVERP OVC Leadership, ITVERP OCFO, and ITVERP Web Form Customizer.

(e) The ITVERP application is web-based and public facing for internal and external users. Claimants will have limited search and retrieval functionality, limited to viewing their application inputs, profile information, and supporting documents. Claimants are unable to conduct searches for their own information using elements of Personally Identifiable Information (PII) elements within the system database. Internal users' search functions will be governed by the system user roles, permitting searches for claimant information using PII stored within the system database records. Internal users will also have printing, document storage,

and data extraction capabilities. This system will completely replace the former paper-based system, including the formerly paper-based processing and storage of claims, and the formerly paper-based information retrieval process.

(f) ITVERP data workflow is transmitted over an Internet-based system accessible by Uniform Resource Locator (URL) web address. The URL supports both OJP badged internal users and external users. All application activities and data input transmissions will be handled at the dedicated website application and backend database system. The claimant information submitted is reviewed and processed by internal users according to their access roles. Once a claim is approved, the payment request is processed offline and transmitted to the Treasury Department for reimbursement. All ITVERP transactions are transmitted over a HTTPS secure network connection.

(g) ITVERP does not interface with other external agencies or entities.

(h) ITVERP is a major web application. ITVERP resides within the MS Azure Infrastructure as a Service (IaaS) Government cloud, which is physically located within the continental U.S. The MS Azure Platform received a FedRAMP Provisional Authority to Operate (ATO) from the Joint Authorization Board, dated September 30, 2013. Per Section 208 of the E-Government Act, because ITVERP collects, processes, and, when appropriate, disseminates information in personally identifiable form, a Privacy Impact Assessment (PIA) is required. Additionally, because records within ITVERP are retrieved by personal identifiers, a Privacy Act System of Records Notice (SORN) is required.

Section 2: Information in the System

2.1 Indicate below what information is collected, maintained, or disseminated. (Check all that apply.)

Identifying numbers					
Social Security	X	Alien Registration		Financial account	X
Taxpayer ID	X	Driver's license	X	Financial transaction	X
Employee ID	X	Passport	X	Patient ID	X
File/case ID	X	Credit card			
Other identifying numbers (specify):					

General personal data					
Name	X	Date of birth	X	Religion	
Maiden name		Place of birth	X	Financial info	X
Alias		Home address	X	Medical information	X
Gender	X	Telephone number	X	Military service	X
Age	X	Email address	X	Physical characteristics	
Race/ethnicity		Education	X	Mother's maiden name	
Other general personal data (specify): - Marital status - Marriage Date					

Work-related data					
Occupation	X	Telephone number	X	Salary	
Job title	X	Email address	X	Work history	
Work address	X	Business associates			
Other work-related data (specify): - Employment Status (Full-Time, Part-Time, etc.) - Work related injury or death information including date of injury or death					

Distinguishing features/Biometrics					
Fingerprints		Photos		DNA profiles	
Palm prints		Scars, marks, tattoos		Retina/iris scans	
Voice recording/signatures		Vascular scan		Dental profile	
Other distinguishing features/biometrics (specify):					

System admin/audit data

System admin/audit data					
User ID	X	Date/time of access	X	ID files accessed	
IP address		Queries run		Contents of files	
Other system/audit data (specify):					

Other information (specify)

2.2 Indicate sources of the information in the system. (Check all that apply.)

Directly from individual about whom the information pertains					
In person		Hard copy: mail/fax		Online	X
Telephone		Email			
Other (specify):					

Government sources					
Within the Component		Other DOJ components	X	Other federal entities	X
State, local, tribal	X	Foreign			
Other (specify): Any agency that has employees overseas which could be susceptible to a terrorist attack.					

Non-government sources					
Members of the public		Public media, internet		Private sector	X
Commercial data brokers					
Other (specify): Any company that has employees overseas that could be susceptible to a terrorist attack.					

2.3 Analysis: Now that you have identified the information collected and the sources of the information, please identify and evaluate any potential threats to privacy that exist in light of the information collected or the sources from which the information is collected. Please describe the choices that the component made with regard to the type or quantity of information collected and the sources providing the information in order to prevent or mitigate threats to privacy. (For example: If a decision was made to collect less data, include a discussion of this decision; if it is necessary to obtain information from sources other than the individual, explain why.)

OVC collects the minimum information necessary to adjudicate and process claims for payment under the ITVERP program. Information, including PII, is collected from either the claimant, medical provider, or other entities defined in section 4.1. Any provided third party information is compared to the claim information to validate the accuracy of the claim information. With the collection of information as identified in section 2.1, there exists a potential threat to privacy where there is a possibility of misuse of ITVERP data by government and contractor personnel. To mitigate the possible misuse or unauthorized disclosure of ITVERP data, all data is encrypted in transmission and at rest. Further, a DOJ background check is performed on all DOJ personnel, employees, and contractors working on ITVERP. In addition to the background check, all DOJ personnel are required to complete the annual computer security awareness training and adhere to Rules of Behavior (ROB) that includes rules for safeguarding PII.

Section 3: Purpose and Use of the System

3.1 Indicate why the information in the system is being collected, maintained, or disseminated. (Check all that apply.)

Purpose			
	For criminal law enforcement activities		For civil enforcement activities
	For intelligence activities		For administrative matters
	To conduct analysis concerning subjects of investigative or other interest		To promote information sharing initiatives
	To conduct analysis to identify previously unknown areas of note, concern, or pattern.		For administering human resources programs
	For litigation		
X	Other (specify): To adjudicate claims for financial reimbursement under the ITVERP program and to facilitate and record payments made to claimants.		

3.2 Analysis: Provide an explanation of how the component specifically will use the information to accomplish the checked purpose(s). Describe why the information that is collected, maintained, or disseminated is necessary to accomplish the checked purpose(s) and to further the component's and/or the Department's mission.

OVC uses the collected information to confirm the eligibility of claimants seeking reimbursements under ITVERP. The application includes information necessary to determine that the claimant (1) is an eligible person under ITVERP rules, (2) was injured or deceased in a Department of Justice, National Security Division (NSD) designated terrorist attack, and that (3) the expenses claimed are eligible for reimbursement by OVC. In addition, OVC uses the collected information to ensure that the claimant was not paid or reimbursed by a third party and is not otherwise submitting duplicative claims.

3.3 Indicate the legal authorities, policies, or agreements that authorize collection of the information in the system. (Check all that apply and include citation/reference.)

Authority		Citation/Reference
X	Statute	34 United States Code (U.S.C.) subtit. II, ch. 201, subch. I; 34 U.S.C. § 20106; 44 U.S.C. 3103
	Executive Order	
X	Federal Regulation	28 C.F.R. Part 94, Subpart A.
	Memorandum of Understanding/agreement	
	Other (summarize and provide copy of relevant portion)	

3.4 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.)

A retention schedule for retaining ITVERP records electronically is currently being developed. Until a records retention schedule is defined with the National Archives and Records Administration (NARA), ITVERP records are retained indefinitely for the purpose of processing new claims that may be related to existing records.

3.5 Analysis: Describe any potential threats to privacy as a result of the component's use of the information, and controls that the component has put into place to ensure that the information is handled, retained, and disposed appropriately. (For example: mandatory training for system users regarding appropriate handling of information, automatic purging of information in accordance with the retention schedule, etc.)

OJP has worked to mitigate the privacy risks associated with the use of the information. There is a possibility of misuse of ITVERP data by government and contractor personnel, and the possible unauthorized modification of claimant's information. To ensure the information is handled, retained, and disposed of appropriately, OJP has the following controls in place:

- A DOJ background check is performed on all DOJ personnel, employees, and contractors working on ITVERP. In addition to the background check, all DOJ personnel are required to complete annual computer security awareness training and sign the "DOJ Cybersecurity and Privacy Rules of Behavior (ROB) for General Users" that includes rules for safeguarding PII. Medical Reviewer contractors are required to sign non-disclosure agreements.
- Auditing features of the system allow for the reconstruction or review of actions taken by an individual including unauthorized modifications to claimant's information. The audit trail captures any change to claimant data by DOJ personnel.
- Each type of application or claims processing has a defined set of users with data access limited by their role.
- ITVERP is a web-based application where external user interactions are allowed only through an external facing website. Internal users interact with the system and collaborate using a web based case management system based on Dynamics 365. Dynamics 365 is a component of Microsoft's Office 365 cloud based Software-as-a-Service (SaaS) solution for CRM. Dynamics 365 is a FedRAMP compliant solution implementing necessary security controls at FISMA Moderate level.
- ITVERP is a secure system that features user identification and password access control.
- In the ITVERP system, the access roles defined within the system determine what data the users will be privy to. The authorized OJP employees and contractors will have access to the data based on their assigned roles within the Dynamics 365 CRM solution. The registered external users will have access to only their own or assigned claim "records."

- All communication between the users and the system is encrypted via HTTPS, which provides confidentiality and integrity of sensitive data transmitted between a user's web browser and the web server.
- TDE is employed to protect data at rest by encrypting database files.

Section 4: Information Sharing

4.1 Indicate with whom the component intends to share the information in the system and how the information will be shared, such as on a case-by-case basis, bulk transfer, or direct access.

Recipient	How information will be shared			
	Case-by-case	Bulk transfer	Direct access	Other (specify)
Within the component	X		X	
DOJ components	X			
Federal entities	X			
State, local, tribal gov't entities	X			
Public	X			
Private sector	X			
Foreign governments				
Foreign entities				
Other (specify):				

Note: The direct access information sharing is via the ITVERP system with appropriate access controls. Authorized employees and contractors will have limited direct data access dependent upon their assigned privileges within the system. Registered external users will have direct access to their own claim records.

Within the component: Information is shared within the Office of Justice Programs (OJP) for purposes of application processing, supervision, payment, system development and maintenance, auditing, communication, and program oversight.

- OVC ITVERP Office/Staff
- OVC Director
- OJP Office of the Assistant Attorney General
- OJP Office of the Chief Financial Officer
- OJP Office of the Chief Information Officer
- OJP Office of Audit, Assessment, and Management
- OJP Office of the General Counsel
- OJP Office of Communications

DOJ components: Information is shared within the Department for purposes of supervision, auditing, communication, and program oversight.

- DOJ Leadership
- DOJ Civil Division
- DOJ Office of the Inspector General

Federal entities:

- Treasury Department. Information is shared with the Treasury Department for purposes of paying benefits and collecting debts.
- Congress. Information is shared with Congress pursuant to constituent inquiries and oversight functions. This may include information such as claim status, incident information, and whether or not a reimbursement payment has been made.

State, local, and tribal government entities:

- Victim Compensation Programs. Information may be shared with a state victim compensation program for purposes of verifying whether the claimant has applied for and/or received any benefits under the state program for the same event.

Members of the public:

- Freedom of Information Act (FOIA) Requestors. Information is shared with the public for purposes of complying with the FOIA.
- Medical Providers. A request to verify expenses incurred in connection to the terrorism event may be sent to the claimant's medical provider to validate the claim's accuracy.
- Other Members of the Public. Information is shared with the public for purposes of complying with statutory reporting requirements, *e.g.*, 34 U.S.C. § 20106(c).

Private sector:

- Private Companies. Private companies listed in the claim application may be contacted to validate application details.

4.2 Analysis: Disclosure or sharing of information necessarily increases risks to privacy. Describe controls that the component has put into place in order to prevent or mitigate threats to privacy in connection with the disclosure of information. (For example: measures taken to reduce the risk of unauthorized disclosure, data breach, or receipt by an unauthorized recipient; terms in applicable MOUs, contracts, or agreements that address safeguards to be implemented by the recipient to ensure appropriate use of the information – training, access controls, and security measures; etc.)

To reduce the risk to privacy, data is shared as aggregate data or claim-specific data on a case-by-case basis as listed in Section 4.1. The aggregate data does not contain PII and is produced in the form of reports to stakeholders, such as Congress, the public, and Department leadership. Claim-specific data is shared with the entities listed in section 4.1 via ITVERP using secure email, telephone, or U.S. Mail.

Section 5: Notice, Consent, and Redress

5.1 Indicate whether individuals will be notified if their information is collected, maintained, or disseminated by the system. (Check all that apply.)

X	Yes, notice is provided pursuant to a system of records notice published in the Federal Register and discussed in Section 7.	
X	Yes, notice is provided by other means.	Specify how: ITVERP Privacy Act (e)(3) Statement and Certification of Application, as approved by OPCL.
	No, notice is not provided.	Specify why not:

5.2 Indicate whether and how individuals have the opportunity to decline to provide information.

X	Yes, individuals have the opportunity to decline to provide information.	Specify how: Users have the option to decline to provide information through not submitting the information and messaging the ITVERP team through the portal as to why the information cannot be provided. However, failing to provide the requested information may result in delays in processing a claim or a claim being denied based on insufficient evidence.
	No, individuals do not have the opportunity to decline to provide information.	Specify why not:

5.3 Indicate whether and how individuals have the opportunity to consent to particular uses of the information.

	Yes, individuals have an opportunity to consent to particular uses of the information.	Specify how:
X	No, individuals do not have the opportunity to consent to particular uses of the information.	Specify why not: Individuals do not have the opportunity to consent to the particular use of the information; however, claimants consent to the use of their information by the DOJ prior to completing and submitting their application.

5.4 Analysis: Clear and conspicuous notice and the opportunity to consent to the collection and use of individuals' information provides transparency and allows individuals to understand how their information will be handled. Describe how notice for the system was crafted with these principles in mind,

or if notice is not provided, explain why not. If individuals are not provided the opportunity to consent to collection or use of the information, explain why not.

Before claimants start their application, they are provided with a Privacy Act (e)(3) Statement specifying the authority for OJP to solicit the information and whether disclosure of such information is mandatory or voluntary; the principal purpose for which the information is intended to be used; the Privacy Act routine uses which may be made of the information; and the effects on individuals, if any, of not providing all or any part of the requested information. Individuals are also provided with a link to the Department of Justice Privacy Policy on all pages in the footer section of the website. Users are also required to consent to the use of their information by the Department of Justice prior to completing and submitting their application, as noted in the Privacy Act Statement provided at the start of their application.

Immediately after claimants log into the application, they are provided with the Terms and Conditions specifying the penalties of not providing all or any part of the requested information, and the penalties for unauthorized or improper use of this system. Upon completion of their claim, claimants are presented with a Consent and Certification page. The Consent and Certification page requires claimants to certify that all of the information provided is correct and complete to the best of their knowledge and that they understand that knowingly and willfully making a false or incomplete statement or failing to fully disclose pertinent information concerning their claim may be grounds for non-payment of benefits or for prosecution for a false statement under 18 U.S.C. § 1001. Claimants are required to affirm that they have read and understand the Consent and Certification page.

Section 6: Information Security

6.1 Indicate all that apply.

X		The information is secured in accordance with FISMA requirements. Provide date of most recent Certification and Accreditation: April 15, 2019 If Certification and Accreditation has not been completed, but is underway, provide status or expected completion date:
X		The risk assessment has been conducted. April 15, 2019
X		Appropriate security controls have been identified and implemented to protect against risks identified in security risk assessment. Specify: Required controls for a FISMA moderate system and DOJ Cybersecurity Standard (Unclassified Security Control Matrix) will be identified, implemented, and assessed by April 15, 2019 for ITVERP. This includes customer responsible controls from the Microsoft Azure Platform as a Service, and the Dynamics 365 Software as a Service.
X		Monitoring, testing, or evaluation has been undertaken to safeguard the information and prevent its misuse. Specify: During the development of the system, the user stories (i.e., high level system requirements) are tested to ensure they are functioning as intended, including safeguards for the information. Additionally, OJP has implemented IT Security continuous monitoring, a critical part of risk management process, where security controls and risk are assessed and analyzed at a frequency sufficient to support risk-based security decisions to adequately safeguard the information.
X		Auditing procedures are in place to ensure compliance with security standards. Specify, including any auditing of role-based access and measures to prevent misuse of information: The system's auditing features enable reconstruction or review of actions taken by an individual, including unauthorized modification or misuse of information. Also, the audit trail captures any change to claimant's data by DOJ personnel.
X		Contractors that have access to the system are subject to provisions in their contract binding them under the Privacy Act.
X		Contractors that have access to the system are subject to information security provisions in their contracts required by DOJ policy.
X		The following training is required for authorized users to access or receive information in the system:
		General information security training
		Training specific to the system for authorized users within the Department.
		Training specific to the system for authorized users outside of the component.
	X	Other (specify): General information security training for authorized users within the component.

6.2 Describe how access and security controls were utilized to protect privacy and reduce the risk of unauthorized access and disclosure.

ITVERP uses a role-based access control and implements the principle of least privilege to ensure that only authorized users have access to sensitive data. Auditing features of the system enable the collection of information which allows for the reconstruction or review of actions taken by an individual, including unauthorized modifications to claimant's information. The audit trail captures any changes to application data by DOJ personnel. OJP leverages the Dynamics 365 cloud service. ITVERP users receive the benefit of a FedRAMP compliant solution implementing necessary security controls at FISMA Moderate level. ITVERP utilizes encryption via HTTPS which provides confidentiality of sensitive data via secure communications between a user's web browser and the web server. It also features user identification and password access control. Additionally, TDE is employed to protect data at rest by encrypting database files.

Section 7: Privacy Act

7.1 Indicate whether a system of records is being created under the Privacy Act, 5 U.S.C. § 552a. (Check the applicable block below and add the supplementary information requested.)

X	Yes, and this system is covered by an existing system of records notice. Provide the system name and number, as well as the Federal Register citation(s) for the most recent complete notice and any subsequent notices reflecting amendment to the system: OJP-014 Victims of International Terrorism Expense Reimbursement Program • 71 FR 44709 (8-07-2006)* • 72 FR 3410 (1-25-2007) (rescinded by 82 FR 24147) • 82 FR 24147 (5-25-2017)
	Yes, and a system of records notice is in development.
	No, a system of records is not being created.

7.2 Analysis: Describe how information in the system about United States citizens and/or lawfully admitted permanent resident aliens is or will be retrieved.

The International Terrorism Victim Expense Reimbursement Program (ITVERP) is a system of records, OJP-014 "Victims of International Terrorism Expense Reimbursement Program," established to support the administration of the program to reimburse qualifying expenses to eligible U.S. citizens and U.S. government employees who suffered direct physical or emotional injury from an act of international terrorism while outside the United States. Information regarding a United States citizen or lawfully admitted permanent resident alien is retrieved in the same manner regardless of citizenship or immigration status. OJP personnel can retrieve a case file by a personal identifier; most commonly, name, claim number, or claimant SSN.