Office of Justice Programs

Privacy Impact Assessment
for the
Public Safety Officers' Benefits 2.0 (PSOB 2.0) System

Issued by:
Maureen Henneberg

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

Date approved: August 20, 2018

(May 2015 DOJ PIA Template)

EXECUTIVE SUMMARY

The Public Safety Officers' Benefits 2.0 (PSOB 2.0) system is an Office of Justice Programs (OJP) operated automated case management system that supports the U.S. Department of Justice (DOJ), Office of Justice Programs, Bureau of Justice Assistance's (BJA) Public Safety Officers' Benefits (PSOB) program. The PSOB Program provides benefits to eligible fallen or totally and permanently disabled public safety officers and their families. The PSOB 2.0 system is a major web application and its purpose is to store and process PSOB benefit claims applications and enable collaborative processing by PSOB 2.0 users. The PSOB 2.0 system collects and maintains the following information in identifiable form (IIF) depending on the type of PSOB application or claim: name, date of birth, mailing addresses, telephone number, email address, Social Security Number (SSN) of the deceased or injured public safety officer (officer) , marital status of the officer, date of death, or injury information about the officer (including medical records), and education history.

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 Public Safety Officers' Benefits 2.0 (PSOB 2.0) system is an Office of Justice Programs (OJP) operated major application that supports the U.S. Department of Justice, Office of Justice Programs, Bureau of Justice Assistance's (BJA) Public Safety Officers' Benefits (PSOB) Program. The PSOB program provides benefits to eligible fallen or totally and permanently disabled public safety officers and their families (beneficiaries).[1] PSOB 2.0 enables the storage and processing of benefit claims applications submitted by potential or existing PSOB beneficiaries.

(b) Listed below are the types of application and claims processing supported by PSOB 2.0 for the delivery of the PSOB Program.

- Death and Disability Application Processing
- Death and Disability Claim Processing
- Education Benefits Application Processing
- Education Benefits Claim Processing

[1] Benefits are pursuant to the Public Safety Officers' Benefits Act of 1976 , 34 U.S.C. §10281 et seq.

- Death and Disability Claim Appeal Application
- Hearing Officer Process
- BJA Director Claim Appeal Application Process
- BJA Director Claim Review Process

Each type of application or claims processing has a defined set of users with limited data access, dependent upon their role. All user interactions occur either via a web-based portal for external users or via web-based case management system Microsoft Dynamics 365 for internal users. The Dynamics 365 is a component of Microsoft Office 365 cloud based Software-as-a-Service (SaaS) solution for Customer Relationship Management (CRM). The Dynamics 365 along with SharePoint Online, a component of the same Office 365 SaaS cloud solution, stores the data and documents associated with PSOB applications and claims, and enables collaborative processing by PSOB 2.0 users.

(c) PSOB 2.0 collects the following data depending on the type of PSOB application or claim : name, date of birth, mailing addresses, telephone number, email address, social security number of the deceased or injured public safety officer (officer), marital status, date of death or injury information about the officer (including medical records), and education history.

(d) Both (1) OJP employees and contractors, and (2) registered external users, including officers and beneficiaries, will have access to PSOB 2.0. In PSOB 2.0, the access roles defined within the system determine what data the users will be privy to. Authorized OJP employees and contractors will have limited data access, dependent upon their role. Registered external users will have access to their own, or assigned claim records, based on the type of external user. For example, an injured officer will have access to his or her own records, while a deceased officer's beneficiary will have access to records about the relevant decedent.

(e) OJP employees and contractors will retrieve claim information by name, case (or claim) number, and by Public Safety Officer's SSN. External users will use their login credentials to access PSOB 2.0 and ascertain the status of their claim.

(f) PSOB 2.0 is a web based application and all communication between the users and the system happens via secure communication protocol (HTTPS).

(g) PSOB 2.0 does not interconnect with any other system.

(h) PSOB 2.0 is a major web application.

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	
Taxpayer ID		Driver's license		Financial transaction	
Employee ID		Passport		Patient ID	
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		Financial info	
Alias		Home address	X	Medical information	X
Gender		Telephone number	X	Military service	
Age	X	Email address	X	Physical characteristics	
Race/ethnicity		Education	X	Mother's maiden name	

Other general personal data (specify):

- Marital status
- Marriage Date
- Officer's spouse, children, or other beneficiaries, including designated PSOB beneficiaries, designated life insurance beneficiaries, parents, and adult children:
  - Name
  - Date of Birth (children only)

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					
User ID	X	Date/time of access	X	ID files accessed	
IP address	X	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):					

Non-government sources					
Members of the public		Public media, internet		Private sector	
Commercial data brokers					
Other (specify): • Private Non-profit Public Safety Agencies					

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.)

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 PSOB applicant data by government and contractor personnel. To mitigate the possible misuse of PSOB data, a DOJ background check is performed on all DOJ personnel, employees, contractors, and Medical Reviewers[2], working on PSOB. In addition to the background check, all DOJ personnel are required to complete annual computer security awareness training and adhere to Rules of Behavior (ROB) that includes rules for safeguarding Personally Identifiable Information (PII). Medical Reviewers are required to sign non-disclosure agreements.

OJP has made the following choices in the redesigned PSOB 2.0 system to reduce the privacy risks associated with the collection of SSNs and individuals' bank information:

- Except for the collection of Public Safety Officer's SSN pertaining to the claim(s), SSNs are not collected from claimants.
- Bank information is not collected from the claimants in the PSOB 2.0 system.
- Minimized collection of unnecessary data through streamlined and logic-based questionnaire.

[2] Medical Reviewers (BJA Director appointees who review multiple claims for PSOB) will receive a DOJ background check.

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 determine eligibility for PSOB Program death, disability, and education benefits under the PSOB Act and implementing regulations, and to facilitate and record payments made to such beneficiaries.		

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.

OJP uses the collected information associated with Public Safety Officer's deaths and disabilities to determine whether claims are to be awarded or denied to the beneficiaries.

• Public Safety Officers' Death Benefits Application: The Public Safety Officer's Death Benefits Application allows the applicant and agency to assert that the decedent was a public safety officer, and that his or her injury occurred in the line of duty. The Public Safety Officer's Death Benefits Application lists the officer's survivors and ensures that eligible beneficiaries are considered for PSOB purposes. The information on these forms is not readily available from sources other than the applicant(s) and former employing agency. Changes to the form have been made in an effort to streamline the application process and eliminate requests for information that are either extraneous or being collected by other means.

• Public Safety Officers' Disability Benefits Application: The information collected is pursuant to the PSOB Act to determine the eligibility of permanently and totally disabled public safety officers for the payment of benefits. The application includes information necessary to determine that the circumstances that led to the disability meet the requirements established by law. Changes to the form have been made in an effort to streamline the application process and eliminate requests for information that are either extraneous or being collected by other means.

• Public Safety Officers' Educational Assistance Application: This information is collected to confirm the eligibility of applicants seeking PSOEA benefits. Eligibility is dependent on several factors, including the applicant's having received a portion of the PSOB Death Benefit, or having a spouse or parent who received the PSOB Disability Benefit. OJP also considers the applicant's age (if a child)

and the schools attended. The application form has been created in an effort to streamline the application process and eliminate requests for information that are either extraneous or being collected by other means.

• Public Safety Officers' Appeal Request Application: This information is collected to allow claimants to appeal a previous death, disability, or education benefit determination. The application includes information necessary to determine the validity of the appeal request. Respondents who complete the application may be disabled public safety officers, or claimants of fallen officers, including but not limited to spouses, children, PSOB designees, life insurance beneficiaries, parents, and adult children.

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	• Public Safety Officers' Benefits Act of 1976 , 34 U.S.C. § 10281 et seq. •
	Executive Order	
X	Federal Regulation	• PSOB Program's implementing regulations at 28 C.F.R. part 32
	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 PSOB records electronically is currently being developed with the National Archives and Records Administration. Under OJP's current record disposition authority, OJP Handbook 1330.2A, records within the PSOB database have been classified as permanent.

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 PSOB applicant data by government and contractor personnel, and the possible unauthorized modification of application information. To ensure the information is handled, retained, and disposed appropriately, OJP has put the following controls into place:

- A DOJ background check is performed on all DOJ personnel, employees, contractors, and Medical Reviewers, working on PSOB. In addition to background check, all DOJ personnel are required to complete annual computer security awareness training and sign "DOJ Cybersecurity and Privacy Rules of Behavior (ROB) for General Users" that includes rules for safeguarding PII. Medical Reviewers 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 applicant's information. The audit trail captures any change to applicant data by DOJ personnel.
- Each type of application or claims processing has a defined set of users with data access limited by their role.
- PSOB 2.0 is a web-based application where public user interactions are allowed only through an external facing portal. Internal users interact with the system and collaborate using a web based case management system based on Microsoft Dynamics 365. The Dynamics 365 is a component of Microsoft's Office 365 cloud based Software-as-a-Service (SaaS) solution for CRM. The Dynamics 365 is a FedRAMP compliant solution implementing necessary security controls at Federal Information System Modernization Act (FISMA) of 2014 Moderate level.
- PSOB 2.0 is a secure system that features user identification and password access control.
- In the PSOB 2.0 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 happens via secure communication protocol (HTTPS) which provides confidentiality and integrity of sensitive data transmitted between a user's web browser and the web server.
- Transparent Data Encryption (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		X	
Federal entities	X		X	
State, local, tribal gov't entities	X		X	
Public	X		X	aggregated information
Private sector	X		X	
Foreign governments				
Foreign entities				
Other (specify):				

Note: The direct access information sharing is via the PSOB 2.0 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 (including applicants and deceased or disabled officer's employing agencies) will have direct access to their own, or assigned claim records, based on the type of external user.

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

- BJA PSOB Office / Staff
- BJA Hearing Officers
- BJA 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
  DOJ September 11th Victim Compensation Fund (VCF). OJP shares information with VCF to implement the offset required by law at 34 U.S.C. § 10281(f)(3).

Federal entities.

- Federal Public Safety Agencies. Information is shared with the deceased or disabled officer's employing agency (*e.g.*, Federal Bureau of Investigation, Drug Enforcement Administration, and Forest Service) for purposes of verifying eligibility for benefits.
- Department of Labor / Workers Compensation. Information is shared with the Department of Labor's Office of Workers' Compensation Programs for purposes of verifying eligibility for benefits and to implement the offset required by law at 34 U.S.C. § 10281(f)(2).
- 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 function.

State, local, tribal gov't entities.

- State, Local, Tribal Government Public Safety Agencies. Information is shared with the deceased or disabled officer's employing public safety agency for purposes of verifying eligibility for benefits. Examples of such agencies include police departments, sheriffs' offices, county constables, primary state law enforcement agencies including state police, special jurisdiction law enforcement agencies (*e.g.*, Fish and Wildlife Conservation), fire departments, volunteer fire departments, ambulance crews, and rescue squads.
- Line of Duty Benefits Programs. Information is shared with the deceased or disabled officer's state-level administrative agency for purposes of verifying eligibility. Examples of such agencies include the Texas Employee Retirement System, which administers the Texas line of duty death benefit, and the Ohio Police and Fire Pension Fund, which administers disability retirement for certain local police officers and firefighters in Ohio.
- Workers Compensation. Information is shared with the deceased or disabled officer's state or municipal workers' compensation program for purposes of verifying eligibility for benefits.

Public

- Claimants / Claimants Representatives. Information is shared with claimants and their appointed representatives for purposes of developing information necessary to determine the claim, verifying eligibility for benefits, and complying with the Privacy Act.
- Freedom of Information Act Requests. Information is shared with the public for purposes of complying with the Freedom of Information Act, unless disclosure would constitute a clearly unwarranted invasion of personal privacy, or another FOIA exemption applies.
- Public. Pursuant to 34 U.S.C. § 10285(e), the Bureau of Justice Assistance publishes reports on its website with information about the processing of claims e.g., the number of claims pending before the agency. No personally identifying information is included in these reports.
- Physicians. Information is provided to the deceased or disabled officer's physician and other medical care providers for purposes of developing information necessary to determine the claim and verifying eligibility for benefits.

Private sector

- Private Agencies Filing PSOB Claims. Information is shared with a claimant's appointed representatives for purposes of developing information necessary to determine the claim and verifying eligibility for benefits.

- National Public Safety Organizations. Upon request of claimants and their appointed representatives, information is shared with national public safety organizations, for purposes of developing information necessary to determine the claim and verifying eligibility for benefits.

Additional disclosures may be made in accordance with the applicable System of Records Notices, available at 64 FR 25,070 (May 10, 1999), 66 FR 8,425 (January 31, 2001), and 82 FR 2,4147 (May 25, 2017).

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 component/Department leadership. Claim specific data is shared with the entities listed in section 4.1 via PSOB 2.0 with appropriate access controls, secure email, 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: PSOB Privacy Act Statement and Certification of Application
	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: Message or call the PSOB office and decline to provide information
	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.

X	Yes, individuals have an opportunity to consent to particular uses of the information.	Specify how: Individuals have the opportunity to consent, on the application certification screen, to the use of the information by the Department of Justice during the certification of the application to determine eligibility of an Applicant/Claimant for PSOB Program benefits. To verify eligibility for benefits; the information provided is subject to investigation and may be disclosed to federal, state, tribal, and local agencies.
	No, individuals do not have the opportunity to consent to particular uses of the information.	Specify why not:

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 the applicants start their application, they are provided with a Privacy Act 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. Applicants are also provided with a link to the Department of Justice Privacy Policy on all pages in the footer section of the website. Finally, applicants are presented with a Certification of Application, which, like the Privacy Act Statement, explains the purpose for the collection, how the Department of Justice will use that information to determine the applicant/claimant's eligibility for PSOB Program benefits, and how the information will be disclosed to federal, state, tribal, and local agencies to verify eligibility for benefits. The Certification of Application requires applicants 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 this claim may be grounds for non-payment of benefits or for prosecution for a false statement under 18 U.S.C. § 1001. Applicants are required to affirm that they have read and understand the Certification of Application.

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: 09/26/2017 If Certification and Accreditation has not been completed, but is underway, provide status or expected completion date:	
X	A security risk assessment has been conducted.	
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) have been identified, implemented, and assessed for PSOB 2.0.	
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 risks 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 applicant 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.

PSOB 2.0 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 applicant's information. The audit trail captures any change to applicant data by DOJ personnel. Moreover, OJP is leveraging the Microsoft Dynamics 365 cloud service. As such, PSOB 2.0 users receive the benefit of a FedRAMP compliant solution implementing necessary security controls at FISMA Moderate level. PSOB 2.0 utilizes HTTPS which provides confidentiality of sensitive data via secure communication between a user's web browser and the web server and features user identification and password access control. Transparent Data Encryption (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: - 64 FR 25070 (5-10-1999)* - 66 FR 8425 (1-31-2001) - 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.

OJP personnel can retrieve a case file by a personal identifier, like name, case (or claim) number, and Public Safety Officer's SSN, for example.