Office of Justice Programs

Privacy Impact Assessment
for the
Public Safety Officer Medal of Valor

Issued by:

Maureen A. Henneberg

Senior Component Official for Privacy

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

Date approved: May 29, 2025

(March 2025 DOJ PIA Template)

Section 1: Executive Summary

Provide a high-level overview of the project or information technology (e.g., application, tool, automated process) in non-technical terms that describes the project or information technology, its purpose, how the information technology operates to achieve that purpose, the general types of information involved, how information may be used and shared, and why a Privacy Impact Assessment was conducted. (Note: this section is an overview; the questions below elicit more detail.)

Created by Congress under the Public Safety Officer Medal of Valor Act of 2001, the Public Safety Officer Medal of Valor (MOV) award recognizes extraordinary acts of heroism and bravery on the part of our nation's public safety officers. To support the workflow of this prestigious award process, the Office of Justice Programs (OJP) MOV website, managed by the Bureau of Justice Assistance (BJA), both accepts and manages the review of nominations.[1]

To receive the Medal of Valor, public safety officers are nominated by the chief executive officer of their employing agencies, recommended by the bipartisan Congressional Medal of Valor Review Board (Medal of Valor Review Panel), and cited by the Attorney General. The MOV system manages the workflow of the nomination records to support the nomination process. The MOV system's website is made of two components: 1) nomination submission and 2) award processing. (*Note:* The nomination submission process guidelines are identified here.)

External users (i.e., members of the public) act as nominators; nominators submit personally identifiable information (PII) about individual nominees (i.e., public safety officers) for this award by completing an online nomination form on the MOV system, with supporting documentation. The online nomination applications contain PII about individual nominator and nominees.

Authorized internal users of the MOV system have the capability to receive, maintain, and review electronic nomination applications for vetting and awarding. Authorized internal users are BJA and OJP staff members who have a need to know (i.e., Designated Federal Officer, information security staff, BJA as needed) and the 9-12 members of the Medal of Valor Review Panel. Nomination application records containing nominees' PII will be maintained for the purpose of determining eligibility for this award. Once recommended by the Medal of Valor Review Panel, the recommended candidates titles, names, agency and summary of the courageous act are disseminated from the MOV website by OJP BJA to the Attorney General and the Office of the President for their review and approvals.

Upon completion of all necessary approvals, the public safety officer will receive the Medal of Valor award. The cycle for the process occurs annually.

---

[1] The MOV website is an application on OJP's Bureau of Justice Assistance's website. The BJA's website is hosted within OJP's Digital Experience (Dex) Content Management System (CMS) on the Aquia platform, an OJP FedRAMP certified Cloud Service Provider (CSP) that routs OJP's DEx CMS.

Section 2: Purpose and Use of the Information Technology

2.1 Explain in more detail than above the purpose of the project or information technology, the type of technology used (e.g., databases, video conferencing, artificial intelligence, machine learning, privacy enhancing technologies), 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 Medal of Valor website is designed to support OJP by capturing online applications for the Medal of Valor award. It allows members of the public to submit MOV applications through the publicly-accessible section of the site.

The Medal of Valor also consists of internal authorized user functions to provide a workflow for reviewing and managing submitting applications. The internal records in the MOV website include the following:

- Information about the nominee: a) title; b) full name; c) home address; d) email; e) phone number; and f) the Authorization For Release Of Information Form (the Form is only viewable by DOJ personnel)
- Information about the nominator: nominator's title, name, agency name and address and contact information, event summary; and any supporting documents that the nominator uploads in support of the nominee.
- Ability to search active MOV applications by Application ID or a combination of the following: Applicant/Nominator/Witnesses, First Name, Last Name, Gender, City, State, Date Range of Event, and/or Summary.

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	28 U.S.C. § 530C, Authority to use available funds; 34 U.S.C. § 10102, Duties and functions of the Assistant Attorney General; 15 U.S.C. § 2214, Public safety awards; 42 U.S.C. § 15201, Authorization of Medal
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

3.1 Indicate below what types of information that may be personally identifiable in Column (1) will foreseeably be collected, handled, disseminated, stored and/or accessed by this information technology, regardless of the source of the information, whether the types of information are specifically requested to be collected, and whether particular fields are provided to organize or facilitate the information collection. Please check all that apply in Column (2) and indicate to whom the information relates in Column (3). Note: This list is provided for convenience; it is not exhaustive. Please add to "other" any other types of information.

(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	Full name of nominators, nominees, federal, state and local public safety officers and other persons relevant to the nominations (such as, but not limited to, witnesses, references, supervisors)..
Date of birth or age			
Place of birth			
Sex	X	A, B & C	The nominee's sex.
Race, ethnicity, or citizenship			
Religion			
Social Security Number (full, last 4 digits or otherwise truncated)	X	A, B & C	The SSN is captured within an image file of the Authorization for Release of Information Form (Form 85P) that must be completed and uploaded in connection with the submitted MOV nomination.
Tax Identification Number (TIN)			
Driver's license			
Alien registration number			
Passport number			
Mother's maiden name			
Vehicle identifiers			

(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
Personal mailing address	X	A, B & C	Personal mailing addresses of nominators, nominees, federal, state and local public safety officers and other persons relevant to the nominations (such as, but not limited to, witnesses, references, supervisors).
Personal e-mail address	X	A, B & C	Personal e-mail addresses of nominators, nominees, federal, state and local public safety officers and other persons relevant to the nominations (such as, but not limited to, witnesses, references, supervisors).
Personal phone number	X	A, B & C	Personal phone numbers of nominators, nominees, federal, state and local public safety officers and other persons relevant to the nominations (such as, but not limited to, witnesses, references, supervisors).
Medical records number			
Medical notes or other medical or health information	X	A, B & C	MOV nominee candidate's health information about injuries sustained or resulting disabilities during the act of bravery may be included.
Financial account information			
Applicant information	X	A, B & C	Nominee's Title, Full Name; Gender; Home Address; Email; and Contact Number, Nominator's Title, First and Last Name; Agency Address; Email; and Contact Number, Bravery Event Information: Date of Event; City, County or Township; State; and Summary of Act of Bravery.
Education records			
Military status or other information			
Employment status, history, or similar information	X	A, B & C	Consist of the name of the public safety agency that the nominee works for.
Employment performance ratings or other performance information, e.g., performance improvement plan			
Certificates			

(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
Legal documents	X	A, B & C	If a guardian is appointed by a court and completes the Authorization for Release of Information form, then the court document confirming the guardianship must be submitted.
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			
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	A, B, & C	The submission of supporting documents which may include news articles, photos, and videos depending on their size, etc.
- **Video containing biometric data**			
- **Fingerprints**			
- **Palm prints**			
- **Iris image**			
- **Dental profile**			
- **Voice recording/signatures**			
- **Scars, marks, tattoos**			

(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
- **Vascular scan, e.g., palm or finger vein biometric data**			
- **DNA profiles**			
- **Other (specify)**			
System admin/audit data:			
- **User ID**	X	A	The following information is collected and stored for internal OJP users who access the system: user ID, date/time of last access, email address, status (active/inactive), and role. The system connects with DIAMD for account authorization, so no password data is collected and stored.
- **User passwords/codes**			
- **IP address**			
- **Date/time of access**	X	A	The following information is collected and stored for internal OJP users who access the system: user ID, date/time of last access, email address, status (active/inactive), and role. The system connects with DIAMD for account authorization, so no password data is collected and stored.
- **Queries run**			
- **Contents of files**			
Other (please list the type of info and describe as completely as possible):			

3.2 Indicate below the Department's source(s) of the information. (Check all that apply.)

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

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

Non-government sources:					
Members of the public	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	N/A	X	To complete required vetting, MOV nominees complete and submit an Authorization For Release Of Information form. This record is shared by secured email with the federally designated officer within the component who eventually transmits the record to the FBI Enterprise for background vetting. OJP staff can also directly access records within the component as needed for review of nomination records.

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.**
DOJ Components	X	N/A		To complete required vetting, specific information is pulled from MOV nomination records and their completed Authorization For Release Of Information forms. That specific information is transmitted to the FBI Enterprise for background vetting.
Federal entities	X		X	Information from the system may be shared with the MOV Review Board members associated with other Federal entities. Each MOV nomination committee reviewer receives direct access to view (but not edit) nomination records to which they are assigned.
State, local, tribal gov't entities	X		X	Information from the system may be shared with the MOV Review Board members associated with other state local or tribal government entities. Each MOV nomination committee reviewer receives direct access to view (but not edit) nomination records to which they are assigned.
Public	X		X	Information from the system may be shared with the MOV Review Board members who can be members of the public. Each MOV nomination committee reviewer receives direct access to view (but not edit) nomination records to which they are assigned.
Counsel, parties, witnesses, and possibly courts or other judicial tribunals for litigation purposes	N/A	N/A	N/A	
Private sector	N/A	N/A	N/A	

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.**
Foreign governments	N/A	N/A	N/A	
Foreign entities	N/A	N/A	N/A	
Other (specify):				

4.2 If the information will be released to the public for "Open Data" purposes, e.g., on data.gov (a clearinghouse for data from the Executive Branch of the federal government), and/or for research or statistical analysis purposes, explain whether—and, if so, how—the information will be de-identified, aggregated, or otherwise privacy protected.

N/A

Section 5: Notice, Consent, Access, and Amendment

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

There is a Privacy Act 552a(e)(3) notice (Privacy Act Notice) on the system's site. The Privacy Act Notice specifies the authority to collect the PII involved in this system as well as provide notice that the disclosure of the information in the system is voluntary. An applicable SORN has been published in the Federal Register and is listed in Section 7.

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.

Users are presented with a link to the Privacy Act 552a(e)(3) notice. The notice complies with all subsection (e)(3) requirements, including stating that providing information in this system is voluntary, and outlines the potential effects of not providing all or any part of the requested information. Users are therefore provided the information necessary to choose whether to consent to the collection and use of their information.

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.

As provided in the OJP Awards Systems System of Records Notice (SORN), individuals seeking to contest or amend records maintained in this system of records must direct their requests to the address indicated in the "Record Access Procedures" paragraph in the SORN. All requests to contest or amend records must be in writing and the envelope and letter should be clearly marked "Privacy Act Amendment Request." All requests must state clearly and concisely what record is being contested, the reasons for contesting it, and the proposed amendment to the record. Some information may be exempt from the amendment provisions. An individual who is the subject of a record in this system of records may contest or amend those records that are not exempt. A determination of whether a record is exempt from the amendment provisions will be made after a request is received. More information regarding the DOJ's procedures for amending or contesting records in accordance with the Privacy Act can be found at 28 CFR § 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) (if the system operates under an Authorization to Use (ATU) or other authorization mechanism, provide related details wherever an ATO is referenced):** ATO granted 12/16/2022 and expires 12/22/2025. **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:** N/A
	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: N/A
X	**This information or information 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 NIST SP 800-60 v.2 rev.1, Guide for Mapping Types of Information and Information Systems to Security**

	Categories: Appendices. Specify and provide a high-level summary of the justification, which may be detailed in the system security and privacy plan: The actual elements of information within the MOV have been assigned a FIPS security categorization of Moderate, pursuant to the "high water mark" standard. This categorization is based on universal categorization of Moderate assessments in Confidentiality, Integrity, and Availability for both its Personal Identity and Authentication as well as its Official Information Dissemination Information Types.
X	**Monitoring, testing, or evaluation has been undertaken to safeguard the information and prevent its misuse. Specify:** The MOV website is subject to an annual internal assessment of OJP's defined Core Controls conducted throughout the course of the Fiscal Year. DOJ's annual Core Control assessment includes the testing and evaluation of the security and privacy controls safeguarding the information within the system. In addition, OJP observes the monthly continuous monitoring submissions from Aquia, an OJP FedRAMP certified Cloud Service Provider (CSP) that routs the MOV website through OJP's DEx Content Management System (CMS)
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:** This system has been integrated with the OJP Security Information & Event Management (SIEM) tool Splunk, which forwards logs to Splunk for auditing purposes. The audit trail captures any changes to the MOV users' data by DOJ personnel. OJP Cybersecurity teams monitor logs in accordance with DOJ security control requirements, which require monitoring on a weekly basis.
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**. All DOJ contracts that implicate PII, including contracts by which the Department obtains embedded contract personnel who process users' PII implicated by MOV, are required under DOJ Acquisition Procurement Notice APN-21-07A to include the DOJ-02 Contractor Privacy Requirements clause, which satisfies the relevant requirements of the Privacy Act and other applicable law, regulation, and 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: There is no additional training specific to this system.

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. MOV application is defined and configured to provide access based on the principles of Least Privilege, only approved privileged users are provided access to the MOV with roles in the application based on least privilege access needed to perform function. MOV leverages the organization's identity management system DIAMD to provide password security which 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 using OJP SIEM Splunk.

Privacy risks are also minimized with physical controls. MOV is hosted within the Aquia platform, an OJP FedRAMP certified Cloud Service Provider (CSP) that routs the MOV website through OJP's DEx Content Management System (CMS) and houses the website's servers and infrastructure as well as 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, if available.) If the project involves artificial intelligence and/or machine learning, indicate if the information is used for training AI models, and if so, how this will impact data retention and disposition.

Records in this system are retained and disposed of in accordance with the National Archives and Records Administration, General Records Schedule 5.7: "Administrative Management and Oversight Records" for records about administrative management activities in Federal agencies.

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:

OJP-019, OJP Award Nomination System, last published in full at 89 Fed. Reg. 83906 (Oct. 18, 2024), available at https://www.govinfo.gov/content/pkg/FR-2024-10-18/pdf/2024-23950.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? For projects involving the use of artificial intelligence and/or machine learning, identify the privacy risks uniquely associated with the use of AI/ML, and how those risks are being mitigated, for example the risk of output inaccuracies and mitigations in the form of testing, continuous monitoring, training, secondary review, etc.

- There is a privacy risk arising from the collection of inaccurate or outdated information on individuals. In order to mitigate this risk, the MOV system collects information from a variety of sources, including:
    - The person nominating a person for an award
    - The person(s) being nominated for an award
    - The FBI and other DOJ components for results of background vetting
    - MOV Review Board members for nomination input and result

- There is a privacy risk of collection of information without proper consent. In order to ensure that individuals provide informed consent to the collection of personal information, users of the MOV system are presented with a link to the Privacy Act 552a(e)(3) notice.

- There is a privacy risk of potential unauthorized access to PII in the system and loss of access to data. In order to mitigate these risks, OJP maintains several security and privacy administrative, technical, and physical controls over the information, including:
    - Secure transmission and storage: This information is captured via web forms which are transmitted over HTTPS into the DEx BJA website. The system leverages cloud service providers that maintain an authority to operate in accordance with applicable laws, rules, and policies, including Federal Risk and Authorization Management Program (FedRAMP) requirements. Internet connections are protected by multiple firewalls.
    - Access controls: Once captured, this data is only visible to site managers within the given site. In addition to the site manager role, the user must also authenticate via DIAMD (two-factor authentication) in order to access this data. The demographics metadata is protected by both a security role in DEx (site manager) as well as DIAMD (two-factor authentication).

- Backups: Backup information will be maintained in accordance with a government contract that requires adherence to applicable laws, rules, and policies.
- Vulnerability scans: Security personnel conduct periodic vulnerability scans using DOJ-approved software to ensure security compliance and security logs are enabled for all computers to assist in troubleshooting and forensics analysis during incident investigations.