PRIVACY IMPACT ASSESSMENT

DSMDb

1. Contact Information

A/GIS Deputy Assistant Secretary
Bureau of Administration
Global Information Services

2. System Information

(a) Date of completion of this PIA: 10/2022
(b) Name of system: Diplomatic Security Memorial Database
(c) System acronym: DSMDb
(d) Bureau: Bureau of Diplomatic Security
(e) iMatrix Asset ID Number: 308723
(f) Child systems (if applicable) and iMatrix Asset ID Number: N/A
(g) Reason for performing PIA:

- ☒ New system
- ☐ Significant modification to an existing system
- ☐ To update existing PIA for a triennial security reauthorization

(h) Explanation of modification (if applicable): N/A

3. General Information

(a) Does the system have a completed and submitted data types document in Xacta?
☒Yes ☐No - Contact IRM/IA at IASolutionCenter@state.gov for assistance.

(b) Is this system undergoing an Assessment and Authorization (A&A)?
☒Yes ☐No

If yes, has the privacy questionnaire in Xacta been completed?
☒Yes ☐No

(c) Describe the purpose of the system:

The purpose of Diplomatic Security Memorial Database (DSMDb) is to provide a modernized nomination tracking application to manage nominations and approvals of DS Personnel who have lost their lives in the line of duty while in service to the Bureau of Diplomatic Security (DS).

The business process consists of the following stages starting with the nomination of an individual and the eventual acceptance and memorialization of the nominee.

- Nomination
- Data collection
- Committee reviews nomination
- Assistant Secretary review
- Update wall, kiosk, external web sites

(d) Describe the personally identifiable information (PII) that the system collects, uses, maintains, or disseminates:

The PII for DSMDb pertains to the information about the requestor nominating a deceased Department of State employee. DSMDb may collect the following PII on U.S. government employees, locally employed staff, and contractors who initiate the nomination process:

- Full Name
- Personal and/or work Email Address
- Job Title
- Office Name & Symbol

For non-Department of State nominators, including members of the public and non-U.S. persons, the following PII may be collected:

- Full Name
- DS Affiliation or relationship to DS, if any (e.g., former DS employee or contractor, friend, family member, or former colleague of the DS deceased employee, retired DS employee)
- Contact Information which may include:
    - Personal and/or work Email Address
    - Personal and/or work Phone Number
    - Personal and/or work Address

For the deceased being nominated, the following PII may be collected:

- Full Name
- City/Country of death
- Date of death
- Circumstances of death
- Date of Birth
- Other biographical information
- Work Title
- Personnel/Employment Information

The nomination form also has an option for nominators to provide contact information for survivors of the deceased. This contact information may include:

- Full Name
- Personal and/or work Phone Number

- Personal and/or work Email Address
- Personal and/or work Address

The remainder of this PIA will focus only on PII of U.S.-persons.

(e) What are the specific legal authorities and/or agreements that allow the information to be collected?

- 5 U.S.C. 301 (Departmental regulations)
- 18 U.S.C. 1114 (Protection of officers and employees of the U.S.)
- 22 U.S.C. 4802 (Responsibility of Secretary State)
- 44 U.S.C. 3101 (Records management by agency heads)
- Pub. L. 104-106, Section 5113 (Federal Information Security Act)

(f) Is the information searchable by a personal identifier (e.g., name or Social Security number, etc.)?

☒Yes, provide:

- SORN Name and Number:
  STATE-36, Security Records

  STATE-31, Human Resources Records

  SORN publication date (found under the Volume Number and above the Public Notice Number on the published SORN): June 15, 2018 and July 19, 2013

☐No, explain how the information is retrieved without a personal identifier.

(g) Does the existing SORN need to be amended to reflect the inclusion of this new or significantly modified system? ☐Yes ☒No

If yes, please notify the Privacy Office at Privacy@state.gov.

(h) Is there a records retention schedule submitted to or approved by the National Archives and Records Administration (NARA) for this system? ☒Yes ☐No
(If uncertain about this question, please contact the Department's Records Officer at records@state.gov.)

If yes provide (Consolidate as much as possible):

- Disposition Authority Number:
  DAA-0059-2018-0003-0006

- Length of time the information is retained in the system:

Temporary. Cut-off at end of calendar year of final action. Destroy/delete 3 years after cut-off but no later than 10 years if required for business use.

- Type of information retained in the system:
  Program Support Records

  Description: Records relating to the support of security and law enforcement programs and initiatives. Records include, but are not limited to, memoranda, memorandum of agreements (MOAs); memorandum of understandings (MOUs); correspondence; congressional request or inquiries; research; policies and procedures; activities, status, or other reports; requirements; surveys; drawings; waivers; plans; studies; and investigations covering accreditation, anti-terrorism, assessments, asset forfeiture, building construction, computer security, counterintelligence, countermeasures, cybersecurity, crisis management, contractors, courier services, debugging, demolition, defensive equipment, Government-owned and commercially leased motor vehicles, electronic security, emergencies covering U.S. citizens abroad, emanations, engineering, inspections, inventories, penetration, physical security, product certification, product evaluation, program reviews, protective detail, security incidents, shielding, special events, surveillance detection, systems development, Tempest, testing, training, travel schedules, zones of control, victim resource advocacy, employee work schedules and assignments, Law Enforcement Availability Pay (LEAP) and other law enforcement personnel related matters, and other related subjects.

4. Characterization of the Information

(a) What entities below are the original sources of the information in the system? Please check all that apply.

☒ Members of the Public
☒ U.S. Government employees/Contractor employees
☒ Other (people who are not U.S. Citizens or LPRs)

(b) On what other entities above is PII maintained in the system?

☐ Members of the Public
☐ U.S. Government employees/Contractor employees
☐ Other
☒ N/A

(c) If the system contains Social Security Numbers (SSNs), is the collection necessary?
☐Yes ☐ No ☒N/A

- If yes, under what authorization?
  N/A

(d) How is the PII collected?

PII is collected by three means that are outside the scope of DSMDb but are a part of the business process: (1) a public facing website for members of the public, (2) an internal SharePoint site for the Departments' employees and (3) other sources as outlined below.

1. **Public Facing Website**: The non-Department nominator fills out a nomination form application on the Department's public facing website. Then an employee from DS Public Affairs manually enters the PII into DSMDb.

2. **Department of State Internal SharePoint Site**: The Department nominator fills out a nomination form application found on the SharePoint site on OpenNet. Once complete, the nominator emails Public Affairs. An employee from DS Public Affairs manually inputs the information in DSMDb.

3. **Other sources**: Information is collected from the internet (e.g., obituaries listing next of kin); friends or colleagues who may be familiar with the family of, or contacts for, the deceased; internal DS documents (e.g., spot reports); U.S. embassy staff where the deceased worked; Diplomatic Security Foundation, which sometimes provides grants to the families of the deceased. The information obtained from other sources is copied or summarized and manually entered into DSMDb by a DS Public Affairs staff member.

(e) Where is the information housed?

☐ Department-owned equipment
☒ FEDRAMP-certified cloud-
☐ Other Federal agency equipment or cloud
☐ Other

- If you did not select "Department-owned equipment," please specify.

Department of State's Azure cloud environment.

(f) What process is used to determine if the PII is accurate?

There is no process in place to determine if the PII is accurate. The person who enters the PII into the nomination form application is doing so on behalf of the deceased Department employee and provides the information in good faith with understanding that the information is accurate.

(g) Is the information current? If so, what steps or procedures are taken to ensure it remains current?

The information is current as of the time of collection. There are no additional procedures to ensure the collected information remains current.

(h) Does the system use information from commercial sources? Is the information publicly available?

Yes, DS Public Affairs staff use commercials sources and public sources available to gather information on nominees such as books, news articles, information at public libraries, Ancestry.com etc.

(i) How was the minimization of PII in the system considered?

The application was designed to only gather the necessary PII regarding the nominator to support the nominations of the fallen DS employees. Other potential PII elements are not gathered because they are not necessary to support the mission.

5. Use of information

(a) What is/are the intended use(s) for the PII?

The PII will be used by DS Public Affairs (DS/PA) to contact the nominator if additional follow-up about the nominee is deemed necessary. PII is also used to contact nominator and invite them to the ceremony honoring the fallen DS employee if their nominee is selected.

(b) Is the use of the PII relevant to the purpose for which the system was designed or for which it is being designed?

Yes, DSMDb will only use the PII in section 3d to support honoring DS personnel who were killed in action. The PII is collected to support processing the nominee and provide a data point if information about the nominee needs additional verification. Additionally, the nominator's PII allows for DS Public Affairs to contact them in the event the nominee is selected to be honored as part of the DS Memorial ceremony.

(c) Does the system analyze the PII stored in it? ☐Yes ☒No

If yes:

(1) What types of methods are used to analyze the PII?
N/A

(2) Does the analysis result in new information?
N/A

(3) Will the new information be placed in the individual's record? ☐Yes ☐No

(4) With the new information, will the Department be able to make new determinations about the individual that would not have been possible without it?
☐Yes ☐No

(d) If the system will use test data, will it include real PII?

☐Yes ☐No ☒N/A

If yes, please provide additional details.

N/A

6. Sharing of PII

(a) With whom will the PII be shared internally and/or externally? Please identify the recipients of the information.

Internal:
There is no sharing of the PII internally.

External:
There is no external sharing of the PII externally.

(b) What information will be shared?

Internal:
N/A

External:
N/A

(c) What is the purpose for sharing the information?

Internal:
N/A

External:
N/A

(d) The information to be shared is transmitted or disclosed by what methods?

Internal:
N/A

External:
N/A

(e) What safeguards are in place for each internal or external sharing arrangement?

Internal:
N/A

External:
N/A

7. Redress and Notification

(a) Is notice provided to the record subject prior to the collection of his or her information?

Members of the Public, Department of State personnel, and Contractors: When a nominator enters information via the nomination form application, a Privacy Act statement is visible on to the form. If a nominator submits a nomination over the phone or via email a Privacy Act Statement is not provided.

(b) Do record subjects have the opportunity to decline to provide the PII or to consent to particular uses of the PII?

☒Yes ☐No

If yes, how do record subjects grant consent?

The nominator has the opportunity to decline to provide the information, however, that would potentially result in their not receiving any follow up communication regarding invitations to, for example a memorial ceremony honoring the deceased.

If no, why are record subjects not allowed to provide consent?

N/A

(c) What procedures allow record subjects to gain access to their information?

1. Department employees: Nominators may reach out to DS Public Affairs via email to gain access to their information.

2. Members of the Public: Nominators are able to contact DS Public Affairs at DSPublicAffairs@state.gov or submit a Privacy Act request to gain access to the information they provided.

(d) Are procedures in place to allow a record subject to correct inaccurate or erroneous information?

☒Yes ☐No

If yes, explain the procedures.

The nominator may reach out to DS Public Affairs via e-mail to address any information related concerns regarding their nomination at the following e-mail address: DSPublicAffairs@state.gov.

If no, explain why not.

(e) By what means are record subjects notified of the procedures to correct their information?

The record subjects are provided the procedures to address their nomination related concerns via the nomination website.

8. Security Controls

(a) How is all of the information in the system secured?

There are various layers used to secure data in the system:

- Network access to the system is controlled by firewall to only accept requests from the Department of State network.
- Logical access to the system is controlled by authentication through Azure Active Directory and authorization is controlled by role-based access controls.
- Data in transit is protected by SSL certificates and TLS 1.2 when users are using a web browser to interact with the web server. The data transfer between the web server and database server transmits over SSL.
- Data at rest is protected using SQL Server's Table Data Encryption feature.
- Static code analysis has been performed to assist the development team to uncover vulnerabilities in the software.
- Automated software testing executes in DevOps pipelines as the software is updated to ensure that no new vulnerabilities related to authentication or authorization are introduced.

(b) Explain the different roles that have been created to provide access to the system and the PII (e.g., users, managers, developers, contractors, other).

- End user – Read-only privileges to all PII
- Contributor – Read and write privileges to all PII
- Administrator – Read and write privileges to all PII

(c) Describe the procedures established to limit system and data access to only those individuals who have an "official" need to access the information in their work capacity.

To limit system and data access to only individuals who have an "official" need to know, individuals must submit a request through AccessDS to be assigned any of the roles described above in 8b.

Users' access to DSMDb will be revoked if they haven't logged into the system after 90 days. This ensures that those who no longer require access are removed and data access is limited to only those with a need-to-know.

(d) How is access to data in the system determined for each role identified above?

All user roles listed above submit an AccessDS application. The request includes the justification for access for each level as related to their job duties. The request is routed

to the government supervisor, system Information System Security Office (ISSO), and a representative from DS Public Affairs are included in this approval chain for privileged accounts.

(e) What monitoring, recording, auditing safeguards, and other controls are in place to prevent the misuse of the information?

There are several layers meant to prevent misuse of the information:

- Authentication to the system is controlled by Azure Active Directory and IRM monitors login attempts.
- The system logs application errors for operations review.
- The system collects audit data when records are saved to enable reporting on who created or updated a record and when those modifications occurred.
- The system audits privilege grants in the system to enable reporting on who has which roles and when those privileges were granted and by whom.
- The system automatically removes user privileges after 90 days of inactivity

(f) Are procedures, controls, or responsibilities regarding access to data in the system documented?

☒Yes ☐No

(g) Explain the privacy training provided to each role identified in 8(b) that has access to PII other than their own.

Users are required to complete the annual cybersecurity training PS800: Cybersecurity Awareness which includes a module on privacy. Users are also required to take the course PA318: Protecting Personally Identifiable Information biennially.