PRIVACY IMPACT ASSESSMENT

Safety Health and Environmental Management (SHEM) Risk Management System (SRMS)

1. Contact Information

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

2. System Information

(a) Date of completion of this PIA: August 2022
(b) Name of system: Safety Health and Environmental Management (SHEM) Risk Management System (SRMS)
(c) System acronym: SRMS
(d) Bureau: Overseas Buildings Operations (OBO)
(e) iMatrix Asset ID Number: 116361
(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 SHEM Risk Management System (SRMS) is a web-based application that supports OBO/OPS/SHEM mission requirements by enabling overseas posts to electronically report and manage mishaps, per 15 FAM 954. A “mishap” is any unplanned, unexpected, or undesirable event causing injury, disease or illness, death, material loss or property

damage, or incident causing environmental contamination, including improper pesticide application, and leaking underground or above-ground storage tanks.

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

- Name (of the person involved with the mishap)
- Date of birth (of the person involved with the mishap if an employee)
- Medical PII (Nature of injury or occupational illness such as lacerations, heat stress, etc. and affected body parts (e.g., knees, leg, arm))

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

- 29 U.S.C. 688 – Section 19 of the Occupational Safety and Health Act of 1970 (Public Law 91-596);
- Executive Order 12196 – Occupational Safety and Health Programs for Federal Employees;
- 29 CFR 1960 – Basic Program Elements for Federal Employee Occupational Safety and Health Programs;
- 29 CFR Parts 1904 – Recording and Reporting Occupational Injuries and Illness, Occupational Safety and Health Standards; and

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

☒Yes, provide:

- SORN Name and Number:
  Contractors Records, STATE-45

- SORN publication date (found under the Volume Number and above the Public Notice Number on the published SORN):
  October 26, 2006

☐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):

- Schedule number (e.g., (XX-587-XX-XXX)):
  N/A

- Disposition Authority Number:
  DAA-0059-2020-0019-0004

- Length of time the information is retained in the system:
  Cutoff at the end of the calendar year. Destroy 30 year(s) after cutoff.

- Type of information retained in the system:
  Location information including Post Name and location type, time of incident, vehicle information, injured person information, property information and corrective actions.

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?

(d) How is the PII collected?

The information is entered directly into the SRMS (which is an electronic version of the DS-1663/1664 Mishap Report forms) by OBO personnel, Post personnel (usually the Post Occupational Safety and Health Officer (POSHO) and or POSHO assistant (APOSHO), or by the involved party, if the involved party is a U.S. Government employee. If the involved party is a Member of the Public, Contractor or Other without access to SRMS, the information is collected by the POSHO, APOSHO or a U.S.

government employee using the paper or pdf DS-1663/1664 forms and they will then enter the data in SRMS.

(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.

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

The PII (Name and DOB) is added and provided directly by the involved party to SRMS, and therefore the involved party is responsible for the accuracy of the information.

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

Yes, the SRMS data are collected from the record subjects, and are therefore current at the time of collection. Data are maintained in order to meet statutory mishap reporting requirements, to track corrective actions, to provide safety and health performance metrics to Department of State management, and to reduce hazards at overseas posts. Data are not kept current beyond this point, as SRMS is for reporting data from the time of the mishap.

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

No information from commercial sources or publicly available information is used.

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

The PII collected by the system is the minimum required for reporting mishaps as required by OSHA recordkeeping regulations. DOB is only collected for employees with work related injuries and is no longer being collected for other record subjects.

5. Use of information

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

PII (Name and DOB) is collected to report work-related injuries or illnesses involving employees or Department facilities as required by the Department of Labor.

(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. PII (Name and DOB) is collected to be aligned with the Department of Labor minimum reporting requirements for work-related mishaps.

(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?
Click or tap here to enter text.

(2) Does the analysis result in new information?
Click or tap here to enter text.

(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.

6. Sharing of PII

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

Internal: Limited summary information could be shared internally with the Designated Agency Safety and Health Official (DASHO)'s office in the Bureau of Medical Services (MED), upon their request.

External: PII is shared with OSHA/the Department of Labor (DOL) as required by the annual report for occupational injury and illnesses, as required by 29 CFR 1904.

(b) What information will be shared?

Internal: The entire mishap report (which as stated above, would include the person's name, DOB, and medical information) could be shared with MED personnel who do not have direct access to SRMS or the data, if needed.

External: PII (name, DOB, and medical information) is shared with OSHA representatives and the Department of Labor as required by the annual report for occupational injury and illnesses (29 CFR 1904).

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

Internal: Information is shared so that MED is able to follow up with the Department of State employee regarding their medical care, workers compensation claim, and/or benefits and return to work.

External: Information is shared to meet requirements set by Department of Labor in the Department's Safety and Occupational Health Annual Report, and to meet requirements set forth in 29 CFR 1904.

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

Internal: The mishaps reports or any other data are provided by SHEM via internal Department of State email communication using pdf.

External: The information maybe be part of the annual report submitted to the Department of Labor via an electronic system designed and owned by the Department of Labor.

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

Internal: The information is protected by the safeguards of the Department's internal email system.

External: The annual report is a CSV file created outside SRMS, then it is uploaded to the DOL. To upload the CSV file into the Department of Labor system, a point of contact provides a personalized link to the Department of State designated person. There will be only one designated person in the Department of State with access to upload the CSV file. The process is protected by the Department of State data housing safeguards. There is no direct data sharing or transfer between SRMS and the DOL electronic system.

7. Redress and Notification

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

Yes. Prior to access, the SRMS login screen displays a Privacy Act statement. Information provided by non-Government employees is voluntary. In all instances, their information is initially collected on the hard or pdf copy DS-1663/1664 form that contains the Privacy Act statement.

(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 injured party has the option to decline to provide their PII, however there are additional steps taken to minimize PII when possible. The common practice is for the injured person to create the mishap report either in the SRMS or DS-1663/1664 forms. The affected person will be adding the name and DOB as PII, the person has the option to provide the age instead of the DOB and in some limited and specific cases the name is not required either. The person is identified by a designated case number. In some cases, the POSHO could ask the involved person for the PII data in order to complete the report.

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?

Individuals could have access to their information in SRMS if they created/authored the report in the system. They can generate PDF summary form in SRMS. There are no individuals outside of authorized Department users that have access to the system. If subjects do not have ready access to the system, they can request a copy of their records from an authorized user, usually the local POSHO, APOSHO, or SHEM.

Record subjects can also follow procedures laid out in the SORN Contractor Records, State-45.

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

☒Yes ☐No

If yes, explain the procedures.

Individuals who have created a record can go in and correct the information. If the mishap report is under “accepted”, “reported”, or “closed” status only those with Admin role (SHEM) or POSHO role can go back into the system to do edits. Amendments can be requested through any of these persons by marking up a copy of the DS-1663/1664 and submitting the DS-1663/1664 copy with the corrected information to the person who authored the SRMS report.

Record subjects can also follow procedures laid out in the SORN Contractor Records, State-45.

If no, explain why not.

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

Record subjects are provided the means for correcting their information using the system’s User’s Guide instructions. Record subjects can also go through the Post Safety Officer. Due to the nature of the reporting, record subjects outside of the Department without access to SRMS would not know of the accuracy of their information and would

not know to correct it, however, as noted above in 7c and 7d, they would be able to request a copy from the POSHO, APOSHO, or SHEM, and submit an update in order to correct their information.

8. Security Controls

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

The application system information is secured based on system role-based security and encryption mechanisms. User access is limited/controlled by their role within the system, so they only have access to information that is necessary for their job responsibilities and role. Encryption is enforced by methods discussed in 8(e) below, ensuring that data at rest and data in-transit use approved cryptography methods required by various Department of State, FedRamp, and NIST controls.

(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).

Roles are assigned in the system based on user needs to implement an effective program. Applicable to all the roles - To get SRMS access the employee must have a state.gov email account. There are thirteen possible roles for post personnel:

1. Author: Authors are able to draft and submit mishap reports in SRMS. Authors can see all PII listed in 3d for reports they have authored.
2. MED Author: MED Authors draft and submit initial injury mishap reports, which are shorter than full mishap reports. MED Authors can see all PII listed in 3d for reports they have authored.
3. Post Reader: The Post Reader role is intended for post senior management. Post Reader role can view the data in SMRS and run analysis on the data. Post Reader role can see all PII listed in 3d.
4. POSHO: The POSHO role reviews and edits mishap reports and submits mishap reports to SHEM. The POSHO role can see all PII listed in 3d.
5. Reviewer: The Reviewer role reviews and edits mishap reports and submits mishap reports to the POSHO. The Reviewer role can see all PII listed in 3d.
6. Motor Vehicle Accident (MVA) Reviewer: The MVA Reviewer accesses and edits all the motor vehicle mishap reports only. MVA Reviewer can see all PII listed in 3d.
7. Motor Post Supervisor: The Motor Post Supervisor accesses and edits all the motor vehicle mishap reports for their assigned post. They are also responsible for review of motor vehicle mishap reports for their assigned post. The Motor Post Supervisor role can see all PII listed in 3d.
8. Regional Facility Manager (RFM) – RFM role reviews and edits mishap reports for their assigned posts. They also submit mishap reports to SHEM for their assigned posts. The Regional Facility Manager role can see all PII listed in 3d.
9. Construction Management (CM) Reader – CM Reader is a read only role and the access is limited to reports classified in SRMS as OBO Construction-managed.

CM Readers help manage the safety program of the overseas construction projects. Construction Management Reader role can see all PII listed in 3d.

10. CM Author – The CM Author role creates, edits, and submits reports for overseas construction projects. The role access is limited to reports classified in SRMS as OBO Construction-managed. CM Author role can see all PII listed in 3d.
11. HQ Author -– The HQ Author role creates, edits, and submits mishap reports to SHEM. This role is obsolete, as it was originally used when Post Authors were unable to access the system. The HQ Author role can see all PII listed in 3d.
12. HQ Reader -– The HQ Reader role is for area managers and allows them to view and run data analysis on all assigned posts. HQ Reader role can see all PII listed in 3d.
13. Administrator – The Administrator role can create and edit mishap reports. The Administrator role assign roles to other users. This is an internal SHEM role that provides access to all other roles. The Administrator role is able to see all PII listed in 3d.

(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.

Access to SRMS is restricted by OBO/OPS/SHEM staff that manage the OBO's mishap investigation and reporting program and assigned post personnel responsible for managing and reporting mishaps based on their role. Only the Author role does not require SHEM approval. Reviewer role requires additional approval by the Post Safety Officer. All other roles require SHEM approval. The main access control is by limiting users to view data based on their role in the system. The system Administrators are the only users with direct access to the entire database for the purpose of performing maintenance, and for performing trends analysis to strategize risk-management efforts. In addition, to get access (any role) to SRMS the employee must have a state.gov email account.

SRMS requires an active Open Net account, and access is disabled due to 90 days of inactivity, requiring re-approval for access from SHEM. If an individual who has an account moves to a new Post, they are required by business process to disable their access to current post and gain new approval for the new Post.

Access to State Department data is only available to State Department employees (OBO/SHEM and Post personnel responsible for mishap reporting) and is centrally controlled by staffers in Washington D.C within SHEM which is the business owner for this data.

- Every post has a combination of authors, reviewers, and supervisors responsible for managing and reporting the mishaps at those posts.
- No employee from one post can access data from another post.

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

Access is based on a 'need to know' rationale, job title/description and roles are limited to the greatest extent possible and in compliance with requests from all users at post, as described below.

The primary process in which access is managed is through inactivity. If an individual does not log into SRMS for >90 days the account becomes inactive. The user will not have access to SRMS. The user will need to reach out to SHEM Administrators for their account to be reactivated. This usually happens when someone leaves posts for any reason. If they go to a new post they must send a request to SHEM Administrators to get access to the new post. In some other cases, if SHEM knows when the employee will depart when their role is given, that expiring date is set to rescind access from the day they are first given access.

1. Author: Anyone at post who registers for a SRMS user account, is automatically granted access to the system as an Author. To get access the employee must have a state.gov email account.
2. MED Author: The MED Author role is automatically given access to SRMS when a post user registers for a SRMS user account and checks the "I am member of Health Unit" box. If a post user with the MED Author role requests the Post Reader role, the POSHO must grant access as a Post Reader by editing the user profile. MED Author may only access records that they have created, and only as long as it is in MED Author draft status.
3. Post Reader: The Post Reader role is intended for post senior management and is granted by the POSHO or the administrator (SHEM). Post Reader can access all the mishap reports for the assigned post. This is a read only role and the access is limited to their assigned post(s).
4. POSHO: The POSHO role is granted by the Administrator (SHEM). Records are limited to their assigned post(s). The POSHO can access and edit all the mishap reports for their assigned post.
5. Reviewer: Granted by the Administrator (SHEM) or the POSHO. The Reviewer can access and edit all the mishap reports for their assigned post. Records are limited to their assigned post(s).
6. Motor Vehicle Accident (MVA) Reviewer: Administrator (SHEM) and POSHO grants or promotes user's author role to MVA Reviewer. The MVA Reviewer can access and edit all the motor vehicle mishap reports only. Records are limited to their assigned post(s).
7. Motor Post Supervisor: requested by the user in SRMS and granted by the Administrator (SHEM) or the POSHO. The Motor Post Supervisor can access and edit all the motor vehicle mishap reports for their assigned post. Records are limited to their assigned post(s).
8. Regional Facility Manager (RFM): requested by the user in SRMS and granted by the Administrator (SHEM). The Reviewer can access all the mishap reports for their assigned post.
9. Construction Management (CM) Reader: requested by the user and granted by the Administrator (SHEM). This is a read only role and the access is limited to reports classified in SRMS as OBO Construction-managed.

10. CM Author: requested by the user and granted by the Administrator (SHEM). The role access is limited to reports classified in SRMS as OBO Construction-managed.
11. HQ Author: granted by the Administrator (SHEM). Only granted to SHEM staff. They have access to all mishap reports, regardless of post assignment. Can edit only those reports they authored.
12. HQ Reader: granted by the Administrator (SHEM). Only granted to SHEM staff or the Office of the Inspector General. This is a read only role with access to all the mishaps reports in SRMS regardless of post assignment.
13. Administrator: Can create and edit reports. This is an internal SHEM role that provides access to all other roles. They have access to all mishap report, regardless of post assignment.

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

All users who login to SRMS must have a valid Department of State email address, access to OpenNet, and register in the system. All privacy-related security controls have been documented. In addition, all system users complete mandatory annual training covering the agencies PII pre-established processes. The system logs activity and status changes for each mishap report providing information on when and who performed the edits, which can be used to trace and identify potential misuse. These processes provide oversight and accountability to ensure mechanisms are in place to make certain that individuals are held accountable for implementing these controls. SRMS uses role-based permissions to limit unauthorized access to specific system functionality and reduce the misuse of the information.

In addition, all privacy-related security controls have been documented in the System Security Plan. These controls limit unauthorized access to the system and reduces the chance of misuse of the information. For instance, all SRMS data are encrypted both during transmission and while stored in our database management system based on NIST controls SC 8 and SC 28.

(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.

There is no specific role-based training; however, all roles/OpenNet users are required to take PS800-Cybersecurity Awareness Training, which has a privacy component, annually and PA318-Protecting Personally Identifiable Information on a biennial basis.