*Mishap Reporting System (MRS)*

## 1. Contact Information

Department of State Privacy Coordinator

Margaret P. Grafeld
Bureau of Administration
Global Information Services
Office of Information Programs and Services

## 2. System Information

A. Date PIA was completed: 2/12/2009

B. Name of system: Mishap Reporting System

C. System acronym: MRS

D. IT Asset Baseline (ITAB) number: 4321

E. System description (Briefly describe scope, purpose, and major functions):

The Mishap Reporting System (MRS) is a web-based application that supports OBO/OPS/SHEM mission requirements by enabling overseas post to electronically report and manage mishaps in accordance with 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. The term “mishap” is used instead of “accident” or “occupational illness” and includes motor vehicle accidents.

The MRS workflow is designed to ensure that post safety officers (POSHOs) are included in the reporting process and that SHEM conducts a final review before committing the mishap record to the database. The system collects the mishap data using various data entry forms, a drawing applet for diagrams and a file attachment module for photos or documents associated with the mishap. The system contains a number of important report listings and summaries to analyze mishap trends and meet federal injury and illness reporting requirements.

The System is designed to provide the user at post (government employees or Foreign Service national (FSN)) the capability to input data regarding reportable mishaps in which they are either a witness or an involved party. These incidents could normally be submitted on up to three different forms submitted through the POSHOs and then consolidated by the SHEM and MED offices for tracking and further Federal reporting. This consolidated reporting System will also allow POSHOs to be aware of all incidents involving their post and create a historical reference for SHEM.

F. Reason for performing PIA:

☒ New system
□ Significant modification to an existing system
□ To update existing PIA for a triennial security re-certification

G. Explanation of modification (if applicable): N/A

H. Date of previous PIA (if applicable): N/A

## 3. Characterization of the Information

The system:

☐ Does NOT contain PII. If this is the case, you must only complete Section
☒ Does contain PII. If this is the case, you must complete the entire template.

### A. What elements of PII are collected and maintained by the system? What are the sources of the information?

- Name, gender, age and date of birth;
- Home address and phone numbers;
- Post Safety Officer name and government supervisor's e-mail address; and
- Vehicle data.

The following table shows the typical information gathered from persons involved:

| | GOV Employees | Injured non-employees | Witnesses |
|---|---|---|---|
| Name | Yes | Yes | Yes |
| Gender | Yes | Yes | No |
| DOB | Yes | No | No |
| Age | Calculated | Yes | No |
| Address | No | No | Yes |
| Phone # | No | No | Yes |

In most cases, the personally identifiable information (PII) is collected from the injured individual, vehicle driver or witnesses to the mishap. This information could contain PII on Department employees, family members, Foreign Service nationals or other U.S. citizens if they were involved in the mishap while in a government vehicle, on government property, or while engaging in government business. If an injured party is incapacitated, a supervisor or family member provides the information. All non-personal information in the mishap report (vehicle data, mishap location, corrective action) is provided by post personnel.

### B. How is the information collected?

Information is collected through completion of electronic forms that include Form DS-1663, "Report of Mishap"; Form DS-1664, "Overseas Motor Vehicle Mishap Report"; and Form SF-91, "Motor Vehicle Accident Report". The information and form fields required on these documents have been modified and adapted within a MRS application.

### C. Why is the information collected and maintained?

The MRS data is collected and maintained in order to meet statutory mishap reporting requirements, track corrective actions, provide safety and health performance metrics to DOS management, and to reduce hazards at posts abroad.

### D. How will the information be checked for accuracy?

MRS has a validation process which checks to ensure that required fields have been entered. Mishap records are routed to a post safety officer and to OBO/OM/SHEM for verification and coding. The System ensures that the data collected is concerning Department of State personnel only. In the event a visitor is injured on Department property or as a result of a U.S. Government mishap, the MRS will collect the non-government person's name, gender and age. If they were a witness, MRS can collect name, address and phone number.

### E. What specific legal authorities, arrangements, and/or agreements define the collection of information?

- 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
- 15 FAM 960 – Safety, Occupational Health, and Environmental Management (SHEM) Program Requirements.

### F. Privacy Impact Analysis: Given the amount and type of data collected, discuss the privacy risks identified and how they were mitigated.

In order to best protect MRS data, precautions have been taken to ensure that all the information is handled appropriately and processed according to the outlined procedures for processing the current forms. Data collected is the minimum amount required to satisfy reporting requirements.

The nature of the PII collected and maintained in MRS resulted in a security categorization of "moderate" for the application. The security categorization establishes a specific set of security controls required to be in place before operation of the application system. The controls are subject to rigorous testing, a formal certification and accreditation (C&A) process, and the authority to operate as authorized by a senior agency official. Moreover, controls are reviewed annually and accredited every three years or sooner if the system has implemented major changes, as defined by OMB Circular A-130. Only authorized users with a "need to know" are granted access to the application. Users are periodically reminded by both the Department and the Bureau of Diplomatic Security of their responsibilities in protecting the data in the MRS.

## 4. Uses of the Information

### A. Describe all uses of the information.

MRS data has the following uses:

- To report and file mishap reports from posts abroad to the Bureau of Overseas Building Operations (OBO)'s Office of Safety, Health and Environmental Management (SHEM);

- To track the investigation of serious mishaps and review by OBO/OM/SHEM;
- To track post's corrective actions on all mishaps to prevent reoccurrences;
- To provide quarterly summaries of mishap data to Department management; and
- To analyze trends in accident types, sources and injuries in order to develop proactive mishap prevention programs and tools (SHEM management can analyze Department trends while post can only analyze their own).

### B. What types of methods are used to analyze the data? What new information may be produced?

Reports for SHEM management are run from the MRS system via the report screen utilizing criteria designated for retrieval. Only authorized users have access to these reports and the compiled information. Reports are generated for management through the built-in queries within the MRS after a user selects filters (e.g., FY, bureau) and groupings (e.g., type of accident, body part injured). It does not generate new information; it only summarizes and categorizes the data in the system.

### C. If the system uses commercial information, publicly available information, or information from other Federal agency databases, explain how it is used.

If an individual did provide the necessary information during the mishap, publicly available information may be used to verify an individual's identity. In order to obtain information on Department employees, MRS uses the global address listing. Additionally, addresses from local listings may be utilized to obtain information regarding local individuals involved in an incident.

### D. Is the system a contractor used and owned system?

No, MRS is a U.S. Government-owned and operated system.

### E. Privacy Impact Analysis: Describe the types of controls that may be in place to ensure that information is handled in accordance with the above uses.

MRS performs basic internal analytical functions on the PII but does not create new information about the record subject. MRS uses statistical reports to analyze trends in accident types, and sources and injuries to develop proactive mishap prevention programs and tools, none of which create new information about the record subject. Thus, there are adequate safeguards in place to preserve data accuracy or integrity and avoid faulty determinations or false inferences about the record subject, thereby mitigating privacy risk. There is also no risk of "function creep," wherein with the passage of time, PII is used for purposes for which the public was not given notice. Based on these specific uses that do not create additional information about the record subject, there is minimal privacy risk.

## 5. Retention

### A. How long is information retained?

DOS regulation 15 FAM 966 requires records to be maintained for at least five years past the end of the calendar year in which the mishap occurred. Records beyond this date may be deleted from the system or retained depending on the Department Records Disposition Schedule.

**B. Privacy Impact Analysis: Discuss the risks associated with the duration that data is retained and how those risks are mitigated.**

Historically, paper mishap reports had been submitted by post and retained indefinitely in a secure file room. With the release of MRS, paper reports are no longer filed, which reduces privacy risk by eliminating unnecessary paper records. The system will be backed-up in accordance with current ESOC procedures and maintained at a SBU facility.

## 6. Internal Sharing and Disclosure

**A. With which internal organizations is the information shared? What information is shared? For what purpose is the information shared?**

Information may be shared with the DASHO office in MED, upon their request. This typically refers only to serious mishaps in which there is a medical need-to-know (those resulting in hospitalization or a fatality).

**B. How is the information transmitted or disclosed? What safeguards are in place for each sharing arrangement?**

Information would be transmitted within the Department's SBU OpenNet system or by hard copy to the person(s) with a need to access the information.

**C. Privacy Impact Analysis: Describe risks to privacy from internal sharing and disclosure and describe how the risks are mitigated.**

A log is created for any hard copies delivered, where the copy number and recipient's name/org symbol are listed. Hard copies are hand carried to the recipient.

## 7. External Sharing and Disclosure

**A. With which external organizations is the information shared? What information is shared? For what purpose is the information shared?**

No PII is shared externally; please refer to the comments in 2E.

**B. How is the information shared outside the Department? What safeguards are in place for each sharing arrangement?**

Not applicable, as information is not shared outside the Department.

**C. Privacy Impact Analysis: Describe risks to privacy from external sharing and disclosure and describe how the risks are mitigated.**

Not applicable.

## 8. Notice

The system:

□ Contains information covered by the Privacy Act.
Provide number and name of each applicable systems of records.
(visit *www.state.gov/m/a/ips/c25533.htm* for list of all published systems):

☒ Does NOT constitute a system or records covered by the Privacy Act.

### A. Is notice provided to the individual prior to collection of their information?

Prior to access, the MRS login screen displays the same Privacy Act statement that is printed on the paper form. This statement reminds the user that they are subject to privacy policy when utilizing MRS.

Additionally, the PIA published on the Department website, as required by the E-Government Act, provides a degree of notice to the individual.

### B. Do individuals have the opportunity and/or right to decline to provide information?

Public individuals have the right to decline to provide information. However, federal employees are required to disclose information in order to facilitate an investigation regarding any motor vehicle accident per compliance with the Privacy Act of 1974. Those involved are the users completing the forms and creating documentation.

### C. Do individuals have the right to consent to limited, special, and/or specific uses of the information? If so, how does the individual exercise the right?

Conditional consent is not applicable to the official purpose of MRS.

### D. Privacy Impact Analysis: Describe how notice is provided to individuals and how the risks associated with individuals being unaware of the collection are mitigated.

Notice is provided on the documents which are used to collect the initial information regarding the incident. The same warnings are printed on the forms displayed prior to utilizing the application on OpenNet requiring the users to adhere to the same rules.

## 9. Notification and Redress

### A. What are the procedures to allow individuals to gain access to their information and to amend information they believe to be incorrect?

Individuals are not able to gain access to their information in MRS. There are no individuals outside of authorized Department users that have access to the system. However, subject users can correct their own data until the mishap is "accepted' within the system by amending the reports. After acceptance, amendments to submitted reports can be made through the relevant POSHO or through the SHEM office with administrative control.

### B. Privacy Impact Analysis: Discuss the privacy risks associated with notification and redress and how those risks are mitigated.

Limiting individuals who have access to the system allows for more control and validity of the submitted documents and record information. The users are the same individuals who previously submitted Form DS 1663/1664 and are aware of the Privacy Act authority regulating those forms. This Privacy Act statement is also part of the initial login screen in MRS.

## 10. Controls on Access

### A. What procedures are in place to determine which users may access the system and the extent of their access?

Procedures in place to determine access include the following:

- System users must have a valid Department of State e-mail address;
- Database administrators and developers must have SHEM approval prior to receiving access; and
- System administrators have access by default based on security configuration guidelines established by the Bureau of Diplomatic Security.

### What monitoring, recording, and auditing safeguards are in place to prevent misuse of data?

Data access is restricted by application roles which include the following:

- The "author" grants access to the records that he/she created within MRS at their current post abroad. This role covers the majority of the system users and provides the fewest privileges of all the application roles;
- The "POSHO" and "reviewer" roles grant access to all records for a single post abroad; and
- "Headquarters" roles provide access to records for all posts abroad. They are reserved for OBO/OM/SHEM and M/MED employees.

All user accounts are assigned the "author" role by default. All other roles must be granted by a user with a higher level role. When a user with the POSHO role leaves his/her post, the user's account is temporarily locked until a system administrator has reviewed the requested change and unlocks the account. When a user with the reviewer role leaves his/her post, the user's role is changed to author.

### B. What privacy orientation or training for the system is provided authorized users?

When an individual registers for access to the system they are required to sign a security agreement. The agreement describes the nature of the information captured by the system and the appropriate use of the system. Additionally, all DOS employees must complete an annual cyber computer security and privacy awareness training in order to retain network access.

### C. Privacy Impact Analysis: Given the sensitivity of PII in the system, manner of use, and established access safeguards, describe the expected residual risk related to access.

Access is granted at the lowest level, as described above. When access is deemed no longer necessary, a system administrator updates the user's role accordingly. The system owner conducts audits and checks to ensure that users have the appropriate level of use at six month intervals, which is in accordance with organizational policy.

Additionally, individual MRS users may request a user logon from SHEM headquarters through their POSHO. The system will only allow access to system records if the individual has created a specific entry or if an entry involves them as reviewers (POSHOs) at their post. This allows for more control over the submitted documents and record information.

## 11. Technologies

### A. What technologies are used in the system that involve privacy risk?

No technologies known to elevate privacy risk are employed in MRS.

### B. Privacy Impact Analysis: Describe how any technologies used may cause privacy risk, and describe the safeguards implemented to mitigate the risk.

Not applicable.

## 12. Security

## A. What is the security certification and accreditation (C&A) status of the system?

The Department of State operates MRS in accordance with information security requirements and procedures required by Federal law and policy to ensure information is appropriately secured. The Department has conducted a risk assessment of the system, identified appropriate security controls to protect against that risk, and implemented the controls. The Department performs monitoring, testing, and evaluation of security controls on a regular basis to ensure that the controls continue to work properly. In accordance with the Federal Information Security Management Act (FISMA) provision for the triennial recertification of this system, MRS is currently going through certification and accreditation as of April 2009.