PRIVACY IMPACT ASSESSMENT

Safety and Accountability For Everyone System PIA

1. Contact Information

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

2. System Information

(a) Date of completion of this PIA: January 24, 2022
(b) Name of system: Safety and Accountability for Everyone
(c) System acronym: SAFE
(d) Bureau: Information Resource Management (IRM)
(e) iMatrix Asset ID Number: 260359
(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:

Formally known as SafeState Emergency Notification and Accountability solution, this system was renamed to Safety and Accountability for Everyone (SAFE). SAFE is an

enterprise emergency notification and accountability system for all overseas Chief of Mission (COM) personnel and Direct Hire domestic employees. The purpose of the system is to collect contact information for U.S. Government employees (State Department and other government employees), their family members, contractors (U.S. and host nation), and Locally Employed Staff to be used for mass notification during times of emergency. The PII collected and stored in the system is necessary to the Department's mission due to the requirement of protecting life and safety in the event of an emergency or natural disaster by providing vital notifications, to all modalities, in a timely and efficient process, and collecting safety status responses from recipients.

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

Full Name
Personal Telephone Number
Personal Email Address
City (USP)
State (USP)
Zip Code (USP)

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

5 U.S.C 301 – Management of the Department of State
22 U.S.C. 2581 – General Authority of Secretary of State
22 U.S.C 2651a – Organization of the Department of State
22 U.S.C. 3927 – Chief of Mission Authority
22 U.S.C. 4802 – Secretary of State Security Responsibilities

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

☒Yes, provide:

- SORN Name and Number:
  State 40 – Employee Contact Records

- SORN publication date (found under the Volume Number and above the Public Notice Number on the published SORN):
  April 24, 2018

☐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)):
  NARA General Records Schedule 5.3, Item: 020

- Disposition Authority Number:
  DAA-GRS2016-00040002

- Length of time the information is retained in the system:
  Destroy when superseded or obsolete, or upon separation or transfer of employee.

- Type of information retained in the system:
  Employee and Chief of Mission emergency contact information. Records used to account for and maintain communication with personnel during emergencies, office dismissal, and closure situations. Records include name and emergency contact information such as telephony devices and general office location.

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?

PII records are primarily collected voluntarily from the SAFE End Users (the person of record) who can update their contact information via the SAFE User Portal. Each overseas posts has Human Resources representatives that have access to the SAFE Management Console and can update additional information on behalf of the user, such as Organizational Hierarchy, Telephony Devices, Post Section, and Embassy or Consulate designation. Domestically, PII records are collected voluntarily from the SAFE End Users and validated by the Bureau Executive Directors. The minimum required data to establish an End User is their official email address and name.

(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.

Information is stored in a BlackBerry AtHoc FedRAMP-approved cloud infrastructure.

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

The information that is entered into this system is obtained directly from the person of record during onboarding processes. The information is cross referenced against similar information and database platforms belonging to the Department of State (MyProfile and Active Directory) to ensure the highest levels of accuracy.

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

Yes, the information in the system is current. To ensure that the information remains current, Department employees with administrative permissions review and update as needed. Additionally, this system has an automated notification every 90 days to inform individuals to log in and validate and/or update their contact information. Individuals are also able to make updates to their user profile at any time.

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

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

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

During the requirements analysis phase of the system design, it was determined that information that did not directly relate to notifying personnel (and family members) in times of emergencies was not needed in the system. As such, we were able to minimize

the amount of PII collected to fulfil the system's function. The only PII collected and stored in the system is necessary for the requirement of protecting life and safety in the event of an emergency or natural disaster.

5. Use of information

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

The intended use of the PII is to allow for rapid targeting and notification to all record subjects in specific locations during emergencies.

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

The purpose of this system is to notify individuals in times of emergencies. The PII collected is necessary and only kept so that the system can perform the functions that it was designed to do.

(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?

(2) Does the analysis result in new information?

(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: All domestic bureaus have access to view all PII elements for their personnel (and related family members) only. Information will only be shared with personnel of the specific domestic bureaus or the overseas Chief of Mission.

External: No information will be shared outside of the Department of State regarding Department of State employees. Other government agencies will have view of

their agency personnel (and family members) only. While other agencies can access the system, information from this system is not exported or shared with any external entities. Information on access is discussed in section 8.

(b) What information will be shared?

Internal: Domestic bureaus will have access to view all PII elements for their personnel (and family members) only. Overseas Chief of Mission administrators will have access to view all, or parts based on restrictions, of the PII elements for their specific location(s).

External: N/A

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

Internal: The purpose for information sharing is for data validation and sanitization. Domestically, Executive Directors validate their bureau personnel, often providing corrections to personnel that have moved to another Bureau or are no longer employed by the Department.

External: N/A

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

Internal: Data are exported to a comma-separated values (CSV) file and transmitted electronically.

External: N/A

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

Internal: When sharing information, only designated personnel have access to the system with the use of role-based permissions and only those users can export/import the CSV user data. When CSV files are transferred, all information is marked PII and is transferred to specific individuals across the Sensitive But Unclassified (SBU) OpenNet platform.

External: N/A

7. Redress and Notification

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

The splash page of the administrative and user web portals identify that the individual is accessing a U.S. Government information system and that by using this information

system, the individual understands and consents that they should have no reasonable expectation of privacy regarding any communication or data transiting or stored on this information system and must click the "acknowledge" button to proceed.

(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?

All data elements within the User Portal are adjustable and can be removed by the user if they no longer wish to share the information. Granting consent consists of adding additional information into the information system that was not previously captured or leaving reported information in the system when prompted to review and validate.

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

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

This information system has a customer facing user portal that can be accessed on a Department of State machine or personal device and users can add, remove, or change any of their existing data within the system.

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

☒Yes ☐No

If yes, explain the procedures.

Individual users have the capability to make corrections and modifications to their data. This system makes use of pull-down selections to keep the information consistent. Every 90 days, the system will prompt the record subject to review and validate entered information and provides guidance on how to edit/add/remove information.

If no, explain why not.

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

The established protocol is for the system Administrators to inform the person of record of the ability to edit the information at any time using the End User portal. The SAFE system is mentioned in the Regional Safety Officer (RSO) briefing and users are instructed to update their profile based on new TDY phones and/or local phone numbers when on Temporary Duty Assignment (TDY) status or during Permanent Change of Station (PCS) moves. In addition, the system has an automated notification every 90 days to inform individuals to log in and validate or update their contact information.

8. Security Controls

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

This information system is secured in a BlackBerry AtHoc FedRAMP-approved cloud infrastructure for both data in transit and at rest. The FedRAMP security follows all applicable NIST security controls. Individual access is controlled via two-factor authentication. Administrative access is controlled via role-based authentication, along with two-factor authentication.

(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 – End users have access to the Self-Service portal only and can only access their information and the information of family members associated with them.

- SAFE Data Managers – This role has administrative access to all PII; however, access is restricted to personnel based on bureau, office, or other restrictive factors deemed necessary by Chief of Mission (COM) security authority. Administrators include representatives that fall under COM but are outside the Department of State with access to only their organizations' data.

- SAFE Managers (specific to post) – This role has administrative access to all PII; however, access is restricted to post specific data. Managers are responsible for sending notifications to all individuals under their Chief of Mission security authority. They have the capability to respond on behalf of others to update accountability status, as required.

- SAFE Org Admins (specific to post) – This role has administrative access to all PII; however, access is generally reserved for the Regional Security Officer (RSO) for control of this Emergency Notification and Accountability tool. This individual is considered a super user with access to everything under the post specific instance for Chief of Mission security responsibility.

(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.

Administrators (Department of State employees or other agency representatives) for this information system are required to fill out, sign, and return an authorized user agreement and are then provided training and access by the Enterprise administrators. Role-based determinations will be applied to limit what all users can see and do within this information system (end-users and administrators).

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

Role-based assignments vary. Domestically, theyare determined by Bureau Executive Directors. At posts, they are dependent on the unique security policies created by the RSO.t. As post identifies the user role assignments, the SAFE program office assigns the appropriate role-based permissions.

- End User – Every use in the system has end user capabilities.
- SAFE Data Managers –Requires supervisor approval.
- SAFE Managers (specific to post) – Requires RSO or post Emergency Action Committee Approval.
- SAFE Org Admins (specific to post) –Reserved role for post system admins identified in system deployment, limited to RSO or IRM office staff.

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

The information in this system is highly restricted based on respective role-based requirements. Posts' Information Systems Security Officers (ISSO) have oversight of their post instance in the system and their view is restricted to their user community. They do not have access to any PII in the system. At the enterprise level, the system ISSO can view and access all system and user audit logs. The auditing data are integrated into the Department's enterprise monitoring tool, SPLUNK, for greater oversight and to identify suspicious anomalies.

(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.

While role-based training does not exist for the roles mentioned in 8(b), each role is required to take the annual Cybersecurity Awareness training (PS800) and the biennial Protecting Personally Identifiable Information training (PA318). Administrators for this system are also required to review and sign an acceptable use agreement and are provided training by the SAFE program office to enforce the importance and sensitivity of the data they are responsible for. Annual access review and training is provided.