PRIVACY IMPACT ASSESSMENT

PEGASYS 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: 06/2022
(b) Name of system: Post Emergency Guidance and Authoring System
(c) System acronym: PEGASYS
(d) Bureau: Diplomatic Security (DS)
(e) iMatrix Asset ID Number: 234636
(f) Child systems (if applicable) and iMatrix Asset ID Number: Not Applicable (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):

Not 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 Post Emergency Guidance and Authoring System (PEGASYS) is a web-based application that supports Department of State (Department) personnel responsible for the creation of Emergency Action Plans (EAP) for American embassies, posts, and consulates operating abroad. PEGASYS facilitates development, review, and approval of the mandated EAP via automated functions and allows an EAP to be easily updated on a frequent, as-needed basis. EAPs are living documents that are updated, maintained, and published using the application. PEGASYS retains post-specific information on how to plan for and respond to a crisis such as treaties, hospital capabilities, and crisis response plans. Approved EAPs are published via a separate read-only application, Post Emergency Reference Interactive Library (PERIL). PERIL is a software module in PEGASYS and is part of the system boundary. The purpose of PEGASYS for all users is to author a useable Emergency Action Plan for Department of State posts worldwide.

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

PII collected on EAP Contacts includes the following:

- Name (Given Name and Family Name)
- Personal Address
- Personal Email
- Personal Phone Number
- Work Address
- Work Email
- Work Phone Number
- Citizenship
- Personnel/Employment *

*Personnel/Employment only specific to non-Post employees. These are job categories for non-post employees; it is a field that one of the following options must be selected:

- Foreign Mission
- Host Country Based NGO
- Host Government
- Private Citizen/Company
- Third Country Based NGO
- U.S. Based NGO

There are EAP contacts who are U.S. Citizens and non-U.S. Citizens. Personnel/Employment category information is the only additional information collected on non-U.S. Citizens. The remainder of this PIA will focus on the PII collected from U.S. Citizens.

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

- Omnibus Diplomatic Security and Antiterrorism Act of 1986, 22 U.S.C. 4802
- Secure Embassy Counterterrorism and Construction Act, 22 U.S.C. 4865
- 5 U.S.C. 301 (Departmental Regulations)
- 22 U.S.C. 2651a(a)(4) (Organization of the Department of State)
- Federal Continuity Directive 1 (February 2008)

(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-40, Employee Contact Records

- SORN publication date (found under the Volume Number and above the Public Notice Number on the published SORN):
  - STATE-36, June 15, 2018
  - STATE-40, 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)):
  N/A

- Disposition Authority Number:
  DAA-GRS-2017-0003-0002 (GRS 5.2, item 020)

- Length of time the information is retained in the system:
  Temporary. Destroy upon verification of successful creation of the final document or file, or when no longer needed for business use, whichever is later. (Supersedes GRS 4.3, item 010; GRS 4.3, item 011; GRS 4.3, item 012; GRS 4.3, item 020; GRS 4.3, item 030, and GRS 4.3, item 031).

- Type of information retained in the system:
  The categories of information collected by PEGASYS address who to contact and how to contact that person or organization in each situation. Some examples of the information categories in the EAP include the following, but are not limited to:
  - Medical (Hospital, Clinics, Supplies)
  - Fire and Rescue
  - Local Police

- Hotels
- Mortuary Services
- U.S. Consulate or Embassy
- Destruction of Hazardous Materials
- Bomb Related Incidents
- Evacuation.

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?

For EAP Contacts, the PII collection process is determined at the post level and is unique to each location. Standardized processes are a future intent. There are 260 distinct posts and each post's EAP has 187 standard sections. PII may be collected in the following ways:

- In-person request
- Email request
- Direct entry into the system by an authorized EAP editor
- Copying of already provided PII from a post administrative document such as a contact roster

For PEGASYS Users who are also designated as EAP contacts, email, first and last name is imported from Active Directory and all other information in 3(d) is collected as stated above.

(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?

PEGASYS is internal to the Department of State for development of EAPs. The EAP Editor is the person who enters the information into the system and is responsible for verifying the accuracy of the collected information. Emergency Planning (DS/HTP/SP) provides the recommendation that posts update information at rotation/quarterly. Content is determined to be accurate after it goes through the approval process where people at post will check the accuracy of the content. The overall process is as follows:

1. EAP content is drafted by the Subject Matter Expert (ex: Medical Officer updates the medical information, Public Affairs handles that information, etc.) and all updated sections are pushed through the workflow approval process. The workflow approval process ensures that all updated sections are reviewed by an Emergency Action Committee (EAC) Chair (Alternate or Primary) before being published by someone in DC.
2. All EAP content must be verified and/or updated on an annual basis. During the Annual Certification process each posts' due date is set for 12 months following the previous certification.
3. If a section is over 1 year old, it automatically turns to a "Published (Needs Verification)" status for the SME to review. The SME would use their local processes, expertise, and contacts to ensure all information is viable (example: post has a new hospital, school, airport, etc.).

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

The Annual Certification process requires post to ensure that the information is checked and validated annually. The system tracks the date a contact was last verified. The EAC Chair Primary, typically the Deputy Chief of Mission (DCM) or Program Office (PO), is the official responsible. This is required by 12 FAH-1 H-036.

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

No, PEGASYS does not use information from commercial sources. The information is not publicly available.

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

The PII in Section 3d above is the minimum needed by PEGASYS to support the development of a useful EAP for use at all posts. EAP Editors collect PII in accordance with Department of State Guidance in 12 FAH 1, the Emergency Planning Handbook. As such, only data required by that guidance is collected. Only PII that is directly relevant and necessary to accomplish Emergency Action Planning is collected.

5. Use of information

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

The PII contained in PEGASYS will be used for personnel recall, location verification, and contact purposes. PEGASYS is developed and maintained by DS with the intent of providing American posts operating abroad the foundation and guidance needed to build and publish viable, accurate and usable EAPs.

(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, the use of the information is relevant for the design purpose. The information is collected and centralized to support EAPs.

(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.

The development team utilizes a pre-production environment for testing application modifications with real PII. Periodically the data in the pre-production database is updated with the data from the Production Database by the Operations Team to allow for this testing. The pre-production environment is accessible only on GoVirtual/OpenNet and testers access this environment the same way they would access the production environment. All testers must have advance authorization to access this pre-production environment. No PII a is contained in the test environment on the development network, which is a separate network.

6. Sharing of PII

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

Internal: Information in PEGASYS is occasionally shared with DSS Task Tracker (another DS Application).

External: N/A

(b) What information will be shared?

Internal: All information included in 3(d) is shared with DSS Task Tracker.

External: N/A

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

Internal: Information is shared with DSS Task Tracker when an audit is initiated by U.S. Government Accountability Office (GAO).

External: N/A

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

Internal: The information is shared via exported Excel spreadsheet that is then sent to DSS Task Tracker.

External: N/A

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

Internal: The email is sent via OpenNet by the PEGASYS Technical Team to DS/HTP (High Threat Posts), the administrators of DSS Task Tracker, properly marked as SBU/PII.

External: N/A

7. Redress and Notification

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

EAP contacts are not currently provided a Privacy Act Statement, but one is in development.

As a result of the PIA process, PEGASYS Management intends to implement recommended best practices for working with PII. This information will be included in future PEGASYS training.

(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?

EAP contacts can decline to provide PII; however, based upon their assigned duties, their PII is understood to be necessary for emergency purposes. These individuals work in roles that make their involvement key for successful emergency planning, response activities and personnel preservation.

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

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

An EAP contact would need to contact the person at post responsible for entering the information into PEGASYS to update or change the information.

If a PEGASYS user for a post is also an EAP contact for that Post, they would be able to edit their own contact information via logging into the PEGASYS application. They are not able to delete their own user information which is their email, first and last name.

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

☒Yes ☐No

If yes, explain the procedures.

EAP contacts would need to contact the person at post (EAP Editor) responsible for entering the information into PEGASYS to update or change the information.

If a PEGASYS user for a post is also an EAP contact for that Post, they can edit their own contact information via logging into the PEGASYS application.

If no, explain why not.

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

EAP contacts are informed during onboarding and know to notify their EAP editor when there is a contact information change, so that contact ensures that they are notified in the event of an emergency.

8. Security Controls

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

Access controls are in place for the back-end Oracle database, which are based upon role-based permissions configured for "least privilege." There are three role groups for PEGASYS described below in 8(b). They are:

- Post Roles
- EP Roles
- Application Roles

(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).

<u>Post Roles</u>:

- View Only User: Post role that can read EAP content.
- Post Administrator: This role cannot edit. It can add modify and delete post users.
- EAP Editor: Post role that has the ability to read EAP content, add/edit/delete EAP content, and add comments.
- EAC Member: Post role that can read EAP content, add/edit/delete EAP content, approve content, add comments, reject content, and certify chapters.
- EAC Chair (Alternate): The alternate post role can read EAP content, add/edit/delete EAP content, and add/delete custom annex data, approve content, add comments, add/delete a custom annex, reject content, and certify chapters.
- EAC Chair (Primary): Post role that can read EAP content, add/edit/delete EAP content, edit custom annex structure, approve content, add comments, add/delete a custom annex, reject content, and certify chapters.

<u>EP Roles</u>:

- View Only User: DC role that can read EAP content.
- DC Administrator: This role can read EAP content and administrative privileges for post user management and EP user management.
- DC Reviewer: This role can read EAP content, add/edit/delete EAP content, and approve EAP content.
- DC Certifier: This role can read EAP content, add/edit/delete content, approve content, assign due dates, and approve annual reviews.
- Suspended Post Viewer: This role can view suspended posts by name in the Post Picker.

Application Roles:

- Application Administrator: This role has privileges to read EAP content, manage posts and post users, manage EP users, and manage Foreign Affairs Handbook (FAH) content. The PEGASYS application administrator can run diagnostics such as data testing and FAH structure testing. Restricted to the Development Team and Operations Support.

(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.

Management approval is required for users with a "need-to-know" to access PEGASYS. Role-based access is in place for the PEGASYS application. General users are allowed to view EAPs generated by PEGASYS. The management and maintenance of data within the PEGASYS application system is the responsibility of authorized users consisting of cleared Department employees. Access DS is used to request elevated privileges with administrator roles as well as view only for domestic users. Post roles are granted by Post User Administrators. EP Roles are Granted by DC Administrators. For Administrative access – EP is notified via AccessDS after first level approval has been provided by the requestor's supervisor at post. EP validates user has been assigned to post prior to approving the request, once approved the request is fulfilled by the AccessDS Team.

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

Access is granted by management and is role-based. Post roles are determined by EAC Chair at individual Posts. EP roles are determined by the business owner. Application administrator roles are determined by Development Team Project Manager.

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

All users have been trained on proper usage, storage, and disposal of PII per the annual PS800 Cybersecurity Awareness Training. Chief Technology Office-managed systems are configured with Standard Operating Environment (SOE) settings that comply with the Diplomatic Security Configuration Guides. These settings include those for event auditing IAW 12 FAH-10 H-122.1 and are detailed by event ID for each user when the user was granted access, each time a user logs in, and the last time a user logged in to the application.

(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.

All PEGASYS users are required to complete the annual cybersecurity training PS800: Cybersecurity Awareness, which includes a module on privacy, and the biennial training PA318: Protecting Personally Identifiable Information.