

## **Third Party Application Privacy Impact Assessment**

|   |
|---|
| <b>Department of State Privacy Coordinator</b><br>Sheryl Walter<br>Bureau of Administration<br>Global Information Services<br>Office of Information Programs and Services |
| <b>Name of Third Party Application: Duty Officer App</b><br><b>ITAB Number: 66706</b><br><b>Month and Year PIA was completed: June 2013</b>                               |

**1) Purpose of the Department of State’s use of a third-party website or application. (Henceforth, third-party website or applications will be referred to as third party applications.)**

**(a) Give a general description of the third party application.**

Amazon Web Services GovCloud is an Android or iOS application that will be used by Embassy Duty Officers to answer questions posed to them by callers after hours and on weekends. This application is on a tablet device and the backend data is on Amazon GovCloud (US). The tablet device is only accessible to the American Duty officer with a PIN sign on required to unlock the device. The backend website is only available to assigned State Department employees that are granted access by Information Resource Management (IRM) administrators.

**(b) What is the specific purpose for using the third-party application and how does this purpose assist in accomplishing the Department’s mission?**

The purpose of this application is to assist the Duty Officer in correctly answering a wide variety of questions from American Citizens regarding emergencies, arrests, etc. and to provide a consistent framework that can be used by all Embassies and Consulates. The app allows fast access to the hundreds of answers that individual posts have written for the various questions that are asked. This is currently in a paper or .pdf format and takes time to look up. The “logbook” portion of the app keeps an electronic record of interactions with American citizens and allows for review by designated Consular Affairs officers. This logbook is currently a paper based notebook, used until full, then stored for one year. The electronic logbook will be encrypted so if lost or stolen it cannot be read by unauthorized personnel.

**(c) Is the use of the third-party application consistent with all applicable laws, regulations, and policies?**

## **State Department Duty Officer App**

Yes

### **(d) What federal authorities permit the collection of information for the intended purpose of this application?**

The legal authorities as documented in STATE-05, Overseas Citizens Services Records, specific to the Duty Officer App, are as follows:

- 22 U.S.C. 3904 (Functions of the Foreign Service, including protection of U.S. citizens in foreign countries under the Vienna Convention on Consular Relations and assistance to other agencies)

## **2) Personally Identifiable Information (PII) available through the use of the third-party application.**

### **(a) What PII will be made available to the Department?**

Callers voluntarily provide information that is relevant to their situation. Personally identifiable information may include, but is not limited to, home address, phone numbers of relatives, name, and potentially sensitive medical conditions. No PII is required in a call. It is all dependent on the nature of the call and the information needed to help the caller.

### **(b) What are the sources of the PII?**

The source of this information is always a call to the current Duty Officer phone. Callers are American citizens or local officials who provide information about themselves, family members or American citizens.

### **(c) From which individuals is the information collected?**

Information is collected from American citizens or local government officials (i.e. Police).

### **(d) Does this collection of information require compliance with the Paperwork Reduction Act (PRA) and, if so, how will the Department comply with the statute?**

This does not constitute a collection under the Paperwork Reduction Act.

## **3) Intended or expected use of PII**

### **(a) How will the Department use the PII described in Section 2 above?**

Information provided by callers can be used for scheduling appointments, replacing passports and notifying family members of arrest, hospitalization, or death of an American citizen.

**(b) Provide specific examples of how the PII may be used.**

If an American Citizen is in an accident, the police may call and ask the Embassy or Consulate to inform the family back in the United States. The information is noted for the reference of the duty officer (name, passport number, ID number etc.). In another case, it may be a “welfare and whereabouts” call from the United States asking to locate a family member that has gone missing. It could also a child abduction case, or hospitalization or Embassy staff with an urgent maintenance problem. The only PII collected is in the notes taken by the duty officer in the moment in order for them to perform the task.

**4) Sharing or disclosing PII**

**(a) With what entities or persons inside or outside the Department will the PII be shared and for what purpose will the PII be disclosed?**

Personally identifiable information collected on the calls will be shared with contacts specified by the American citizen, but only with an oral or written privacy waiver from that individual.

**(b) How will the PII be transmitted or disclosed to internal or external entities or persons?**

Personally identifiable information will be disclosed or transmitted by either a phone call to the family or through a document courier service (FedEx etc.).

**(c) What safeguards will be in place to prevent uses other than those legally authorized and described in this PIA?**

All data captured by the application is encrypted to Advanced Encryption Standard (AES) 256. All communication between the application (on the tablet) and servers (at Amazon GovCloud) uses SSL connections. All data on the servers is FedRamp certified for HIPAA compliance, encrypted with AES 256 and is transmitted via FIPS 140-2 compliant endpoints.

In the United States, AES was announced by the NIST as U.S. FIPS PUB 197 (FIPS 197) on November 26, 2001. This announcement followed a five-year standardization process in which fifteen competing designs were presented and evaluated. It became effective as a federal government standard on May 26, 2002 after approval by the Secretary of Commerce. AES is included in the ISO/IEC 18033-3 standard. AES is the first publicly accessible and open cipher approved by the National Security Agency (NSA) for top secret information when used in an NSA approved cryptographic module.

**5) Maintenance and retention of PII**

## **State Department Duty Officer App**

### **(a) How will the Department maintain the PII and for what time period?**

On the tablet device, a 7 day period of the log book is stored. On the server site, the information is stored for a one to two week period. We are trying to get information from Consular Affairs (CA) as to the need of keeping the logs longer than 7 days. Currently the data is hand written into notebooks that are used until full then stored in the human resources office at post. For long term storage (1 year) the consular officer would copy the data from the GovCloud site, attach it to a SMART record email, using privacy tags, and then delete it from the GovCloud site.

### **(b) Is there a records disposition schedule covering this collection? If so, what is the retention period?**

According to Records Disposition Schedule B-02-001-03, DispAuthNo II-NN-3544, item 26, Duty Officer Logs are destroyed 1 year after date of last entry.

## **6) Securing PII**

### **(a) Will the Department's privacy and security officials collaborate to develop methods for securing PII?**

Meetings have already been had with the Office of Information Assurance (IA). They view the data as a moderate risk, which is the standard for anything containing PII, and approved of the storage and transmission scheme. D/CIO Janice Fedak arranged these meetings with IA and the Information Technology Change Control Board (ITCCB). The requisite forms (**E-Authorization risk Assessment Tool** and the **System Categorization Form**) are being sent to IA Solutions for approval. The data will be on approved devices for moderate level data

### **(b) Describe how a user will access the third party application.**

The Duty Officer will use a pin code assigned by Human Resources (HR) or Consular to access the Android or iOS tablet. Any lost device will be remotely wiped. The data for a post is only visible to assigned users at that post.

## **7) Identifying and mitigating other privacy risks**

### **What other privacy risks exist and how will the Department mitigate those risks?**

The risks are limited in that the only "interesting" data on the device is the log of calls. That "may" contain information about accident, hospitalizations, etc. that would be interesting reading, but not ultimately useful to a thief. The tablet is much more valuable. The new system would encrypt the data on the tablet. The data will only be viewable by the assigned Consular Officer at Post or the State Department Watch Officer. As the data is encrypted to the NSA AES 256 standard and transmitted in an encrypted form, even

**State Department Duty Officer App**

the loss of the tablet will not expose the data. To mitigate any loss, a tablet can be remotely wiped if lost, and the thief is more interested in erasing the device to erase any tracking software so it can be resold.

**8) Creating or modifying a system of records**

**(a) Is there an existing system of records to cover this collection of records as required under the Privacy Act of 1974?**

Yes, there is an existing system of records to cover this collection.

**(b) If “yes” to the question above, which system of records notice (SORN) covers this collection? (For a list of all Department published SORNS, go to [www.state.gov/m/a/ips/c25533.htm](http://www.state.gov/m/a/ips/c25533.htm)).**

The system of records that covers this collection is State-05, Overseas Citizens Services Records.

**If there is no existing Department SORN to cover this collection, one must be created. Please contact [SornTeam@state.gov](mailto:SornTeam@state.gov) for guidance.**

**(c) Is notice provided to the record subjects, other than through the SORN (e.g., through a Privacy Act statement or privacy notice)?**

Yes. Callers are informed that they need to sign waivers or give verbal authorization in order for their information to be relayed to family or designees. Additionally, notice will be provided through this PIA, which will be published on the public Department of State website.