



**Privacy Impact Assessment**  
*Embassy Rangoon Guest  
Identification Network*

## 1. Contact Information

**Department of State Privacy Coordinator**

Sheryl L. Walter  
Bureau of Administration  
Global Information Services  
Office of Information Programs and Services

## 2. System Information

- (a) Date PIA was completed: Feb. 14, 2012
- (b) Name of system: Embassy Rangoon RSO Dubern Park Guard Booth Guest Identification Network
- (c) System acronym: ER-GIN (not official)
- (d) IT Asset Baseline (ITAB) number:
- (e) System description (Briefly describe scope, purpose, and major functions):

The Embassy Rangoon RSO Dubern Park Guard Booth Guest Identification Network (ER-GIN) supports RSO Rangoon's Mission Facilities Access Policy by facilitating a system to identify heretofore unknown guests of American Embassy Rangoon Association (AERA) Club members (direct-hire as well as affiliate and associate members). This club is a recreational building inside a U.S. government-owned and occupied residential compound. Identifying individuals entering the club is particularly important as the AERA board has seen fit to extend AERA Club membership to non-embassy employee foreign nationals who do not receive the same level of background investigation as full-time embassy employees. These non-embassy employees could present significant security risks particularly in the realm of counterintelligence and theft/vandalism.

- (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):

- (h) Date of previous PIA (if applicable):

## 3. Characterization of the Information

The system:

- does NOT contain PII. If this is the case, you must only complete Section 13.
- 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?**

The RSO Rangoon Dubern Park guards will require for entry into the compound a government-issued identifying document (generally a passport or national ID card) from any adult guest under escort by a member. The guest is the source of the PII. The guards will then scan a copy of the identifying document via a scanner to store on the Open Net system in a drive accessible to RSO Rangoon personnel only. The document will then be returned to the guest. The scanned copies of the documents will be sorted by date/time of scan for potential investigative purposes and deleted after three months time if not used for investigative action.

Guests whose information is collected in ER-GIN are predominantly foreign nationals, but some U.S. citizen's identification is collected, as well. PII that could be collected in the identifying documents includes:

- Name
- Date/Place of birth
- Address
- ID documentation number (e.g., passport number, driver's license number, national registration card)
- Photo

**b. How is the information collected?**

As described in section 3(a), information is collected by the guest providing in person a government-issued identifying document. The document is scanned and stored in ER-GIN.

**c. Why is the information collected and maintained?**

The information is collected and maintained for RSO Rangoon to meet its mission of providing a safe and secure environment on the USG-owned-occupied residential/American Embassy Recreational Association compound. Collection of the information is necessary to effect a robust counterintelligence program and enable RSO personnel to investigate any hostile intelligence or criminal act that occurs on the compound and that could be attributed to an AERA Club member's guest.

**d. How will the information be checked for accuracy?**

Any suspect document will be referred to DS agents working in RSO Rangoon for appropriate follow-up with Burmese law enforcement.

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

- Public Law 99-399 (Omnibus Diplomatic Security and Antiterrorism Act of 1986, as amended);
- Public Law 107-56 (USA Patriot Act – Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism)

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

The nature of the information collected, processed, and maintained resulted in an overall security categorization of **Moderate**. The information collected in ER-GIN is the minimal amount to fulfill the purpose of facilitating the potential investigation of criminal activity in the club. Embassy Rangoon needs to know who is visiting its facilities, and ER-GIN allows them to do this.

#### **4. Uses of the Information**

##### **a. Describe all uses of the information.**

The copies of guests' identifying documents are not used unless criminal activity needs to be investigated. The information is stored on OpenNet for a short period of time until it is no longer needed. If criminal activity is detected, the identifying information of guests of the AERA Club can be sent to DS agents working in RSO Rangoon.

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

No analysis of the information collected in ER-GIN is performed. Instead, it is merely used for identification purposes in the event identification of guests is necessary.

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

No commercial information, publicly available information, or information from other Federal agency databases is used in ER-GIN.

##### **d. Is the system a contractor used and owned system?**

No.

##### **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.**

Information collected in ER-GIN is used for a very limited purpose: the potential identification of guests who could be involved in criminal activity while on the AERA Club premises. The information is not otherwise analyzed. Privacy risks from usage are minimal due to the very limited nature of the use of information.

#### **5. Retention**

##### **a. How long is information retained?**

Identification materials collected in ER-GIN are only maintained in OpenNet for three months before they are deleted, unless it is determined that the materials need to be retained due to the individual's potential involvement in criminal activities at the AERA Club. This retention schedule is standard among posts checking guests' identities.

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

Risks from the retention of PII in ER-GIN are mitigated by the very short retention schedule outlined in 5(a). After three months, the scanned documents of individuals' identifying documents are deleted from OpenNet.

## **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?**

In the event of the discovery of criminal activity or counterintelligence efforts that have taken place at the AERA Club, DS agents at RSO Rangoon are alerted and provided with the identities of suspected guests who were present at the time of the occurrence. Copies of the scanned documents are provided to allow the DS agents to coordinate with local Rangoon authorities to identify the criminals.

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

Information obtained in 6(a) above may be shared by either electronic (OpenNet email attachment internal with PII designation) or hard copy internal use by RSO Rangoon personnel and other embassy personnel deemed necessary to share this information. RSO Rangoon will safeguard all information collected in DS prescribed enclosures for 3 months unless material is required for an on-going investigation.

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

Information in ER-GIN is only shared with DS agents in the event of criminal activity or possible counterintelligence. This limited internal sharing is controlled and only done when necessary, so privacy risks are limited.

## **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 information obtained through ER-GIN will be shared outside of RSO channels except in the event of imminent danger, attack or other exigent circumstance that would require the information be released to Host Nation authorities to protect life or property.

(This would have to be a DS policy regarding sharing investigative evidence or collected information with a foreign government.)

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

The sharing described in 7(a) will have to be decided by DS agreements with a foreign Government or local law enforcement agency. If it is shared, it will be by either electronic (OpenNet email attachment with PII designation) or hard copy.

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

Information in ER-GIN is only shared with local governments or authorities in the event of imminent danger, attack or other exigent circumstance that would require the information be released. This limited external sharing is controlled and only done when necessary, so privacy risks are limited.

## 8. Notice

The system:

contains information covered by the Privacy Act.

Provide number and name of each applicable systems of records:

Security Records, State-36

does NOT contain information covered by the Privacy Act.

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

Individuals who provide their identifying documents to the security guard on duty are notified verbally that certain information is required to obtain access to the club and why it is collected. Additionally, the publication of State-36, mentioned above, notifies individuals that the Department will, at times, collect their information for purposes such as those in ER-GIN.

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

Yes. Any individual who declines to provide information may not be granted entry to the club.

### 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?

No. Information must be provided or entry to the club may be denied.

### 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.

The notice provided by the guard as to the collection of PII to gain admittance to the club mitigates the risk that individuals could be unaware of the collection. Additionally, the publication of State-36 provides individuals with notice of the type of collection in ER-GIN.

## 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?

The nature of the collection of scanned copies of the individuals' identifying documents does not allow for redress mechanisms. Information is only used for identification purposes, and any attempts to alter the information on identifying documents could be seen as forgery.

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

Due to the nature of the collection in ER-GIN, redress is not possible. Therefore, no privacy risk stems from this category.

## **10. Controls on Access**

**a. What procedures are in place to determine which users may access the system and the extent of their access? What monitoring, recording, and auditing safeguards are in place to prevent misuse of data?**

Only authorized users of the Department's OpenNet system may potentially have access to ER-GIN. OpenNet has access controls, such as username/password protection and audit logs, to ensure that improper access is not granted. In addition, only employees at RSO Rangoon with a need-to-know are granted access to ER-GIN.

RSO Rangoon shared folders located on embassy servers have security controls in place to ensure only those personnel required to access RSO Rangoon information can do so. These restrictions are set by individual folder security options.

**b. What privacy orientation or training for the system is provided authorized users?**

Per 13 FAM 360 training is now required of all Foreign Service and locally employed staff who handle personally identifiable information (PII) while performing their official department duties.

**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.**

Privacy risks associated with access are mitigated by maintaining the information in ER-GIN in a shared folder with security controls in place to ensure only those with a need-to-know have access. Additionally, this folder is located inside the Department's OpenNet, which is also access controlled.

## **11. Technologies**

**a. What technologies are used in the system that involve privacy risk?**

ER-GIN operates as a folder on OpenNet, so no technology with additional privacy risk is utilized.

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

No privacy risk results from the use of privacy-sensitive technology.

## **12. Security**

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

A C&A was determined to not be necessary for ER-GIN.