

PRIVACY IMPACT ASSESSMENT

Post Bangkok Business Applications

1. Contact Information

A/GIS Deputy Assistant Secretary

Bureau of Administration
Global Information Services

2. System Information

- (a) **Date of completion of this PIA:** June 2022
(b) **Name of system:** Post Bangkok Business Applications
(c) **System acronym:** PBBA
(d) **Bureau:** EAP
(e) **iMatrix Asset ID Number:** 325222
(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:**

Post Bangkok Business Application (PBBA) is the SQL-based application suite that serves business operations for the Bangkok Embassy Sections that have signed up for International Cooperative Administrative Support Services (ICASS) with the Bangkok Information Resource Management/Information System Center (IRM/ISC). PBBA consists of locally developed applications that enable Section customers to access and use the applications electronically on desktops, Go Virtual and Go Desktop platforms within the OpenNet network and infrastructure. This suite of collective applications stores

administrative, security, financial, utilities, customs and shipping, items inventory, and Diplomatic Notice (DipNote) information and records. The PBBA provides the services for the Management, Information System Center (ISC), Information Programs Center (IPC), Regional Human Resources (RHR), Bangkok Customer Service Center (BCSC), Financial Management Center (FMC), General Services Office (GSO), and Area Telecommunications Office – Asia (ATO-Asia) sections.

The Post Bangkok Business Application (PBBA) system consists of:

(1) **MVO DipNote Visa Request**: Bangkok Mission Visitors Office (MVO) is an online application that GSO Mission Visitors Office (GSO/MVO) uses to prepare and manage the Third Country Visas requests for Embassy personnel who take official trips to other countries. The DipNote Visa Request application allows users to fill out their information and submit the request electronically for supervisor approval. The application works collaboratively with the Mission Thailand DipNote Request application to obtain the DipNote reference number. The application also helps the GSO/MVO Team to keep track of ICASS workload counts for each agency.

(2) **Bangkok DipNote Request**: Bangkok DipNote Request application generates Diplomatic Note numbers for all mission's correspondence between the U.S. Government and the Thailand government. The user submits a request for a DipNote number and uploads the chronological (Chron) files to the application's database for official record. This application consists of three major functions - User, Application Owner, and Reminder. The User function enables employees to create or cancel their Diplomatic Note requests, upload Chron File(s) or track their request status and detail. The Application Owner function allows authorized and designated section staff to track all requests statuses and details, cancel requests or upload Chron File(s). The Reminder function within the Bangkok DipNote Request application automatically sends an email reminder to the requester to upload the Chron file if not already done.

(3) **Bangkok ATO-Asia Bill of Material (BOM) Request**: Bangkok ATO-Asia BOM Request Application is an inventory management system that the ATO-Asia team uses to manage and track the projects and their associated bill of material. The ATO-Asia creates projects and fills them with assigned equipment, parts, and BOM. This inventory management tool has a robust function that enables the ATO-Asia team to search, edit\add, scan barcode as well as monitor and refill stock. The application stores project owners' contact information.

(4) **Bangkok FMC System**: Bangkok FMC System consists of three applications that the Financial Management Center use to manage the travel voucher, bill payment, and bill collection processes. The applications track transactions of billing, payment, and voucher; maintain records; and generate reports, which help the FMC staff to perform their work more efficiently.

- The Voucher Logbook - generates and tracks Embassy vouchering information.
- The FMC Phone Tracking - manages the bills from the local telephone service providers and allocates appropriate fund cite (government fiscal year funding appropriation) for the telephone billing payments.

- FMC Bill of Collection - tracks and manages the bill collection from employees, such as overpaid per diem and health insurance.

(5) **Bangkok Customs and Shipping Tracking System**: The Bangkok Customs and Shipping Tracking System is a web-based application that manages and tracks the inbound and outbound of all diplomatic shipments through the Thai Customs. The reporting feature of the application automatically generates the Diplomatic Note references and 66 other official forms and reports to help the GSO team process the Mission's import and export of the diplomatic shipments in Thailand. Additionally, this application's many useful functions and features enable the GSO team to perform the annual ICASS workload counts, evaluate the shipping companies, and conduct costs saving analysis.

This online customs and shipping tracking system automates, streamlines, and standardizes the Embassy import/export shipment workflows. It is a management tool that modernizes the manual work done on pen and paper.

(6) **Bangkok Utilities Tracking System**: The Utilities Tracking System is an application used to monitor, analyze, and report the consumption of electricity, water and gas usage and costs for the Embassy offices and employee's residences. The GSO team feeds the monthly utility data into the application to form a data repository that enables the Green Team and Facility team to oversee the utility usage and costs for all properties. The application has robust searching and reporting features that allow sending emails to the employees depending on their utility consumptions for the month. The application's platform is an effective and transparent utilities and energy conservation tool for cost saving on the business and residential properties of the Embassy.

(7) **Bangkok eForm System**: Bangkok eForm System is a web-based application that automates the collection and management of several of Post's dedicated forms into a single platform and improves operational efficiency. Namely, the BCSC New Arrival Request forms (includes E2 New User Form, DS-4211, Notification of New Arrival for Check-In/Accreditation to Thailand Ministry of Foreign Affairs, DS-3064, and SF-1190), IRM OpenNet Account Access Request form (DS-7667), ClassNet Account Request form (DS-7667) and Electronic Mobile Computing and Data Storage Request form (DS-7642).

(8) **Bangkok RHR System**: Bangkok Regional Human Resources (RHR) System is a web-based application that provides record keeping and useful functionalities to help the RHR staff manage awards and other official documents more efficiently. This system is used to manage two programs:

- RHR Awards - manages and tracks employees' awards and has robust reporting function.
- RHR Diplomatic Accreditation & Privileges (DAP) - manages and tracks the American Direct Hire employee's diplomatic ID, passport expiration date, Thailand visa and driver's license. The RHR DAP reminder feature is also used by the RHR DAP staff to auto-generate emails from the RHR System providing employees with advanced notice and guidance on expiring important documents. All the agreements and handouts are

sent automatically in the PDF format that allow the employee to put the digital signatures.

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

- Name
- Personal Phone Number
- Personal Email Address
- Personal Address
- Partial Social Security Number (SSN)
- Local Employee Payroll Number
- Passport Number
- National ID (for non-US citizens)
- Date of Birth
- Place of Birth
- Citizenship
- Personnel/Employment
- Family Member Information and Contact: Last Name, First Name, MI, Date of Birth, Relationship, Gender, SSN4Digits, Nationality, Hometown, Email, Home Leave Address, Family member's emergency contact and relationship
- Emergency Point of Contact Information: Last Name, First Name, MI, Relationship, Email, Phone, Home Leave Address
- Vehicle License registered plate Number, Vehicle Identification Number, and Vehicle Engine Number
- Employee Badge Numbers
- Local Staff's Employee ID
- Business Contact: Work Email, Work Title, Work Phone Number, Work Address
- Other Business Contact PII Elements: Application-defined Username and Password, OpenNet Logon ID and Full name, Agency Fund Cite Codes

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

22 U.S.C. 2651a (State Department Basic Authorities Act of 1956)
 22 U.S.C. 3921 (Management of service)
 22 U.S.C. 2656 (Management of foreign affairs)

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

Yes, provide:

- SORN Name and Number:

Human Resources Records (STATE-31)
 Global Financial Management (STATE-73)

Network User Account Records (STATE-56)
 Personnel-Payroll Records (STATE-30)

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

Human Resources Records (STATE-31) - July 19, 2013
 Global Financial Management (STATE-73) - July 15, 2008
 Network User Account Records (STATE-56) - December 12, 2017
 Personnel-Payroll Records (STATE 30) – 02/11/1998

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)):
 - B-02-001-01: Financial Management and Reporting Administrative Records
 - B-02-001-02: Financial Transaction Records
 - B-02-002-10: Employee Management Administrative Records
 - B-02-002-11: Employee Incentive Award Records
 - B-02-003-04: Information Technology Operations and Maintenance Records
 - B-02-003-11: System Access Records
 - B-02-004-01: Tracking and Control Records

- Disposition Authority Number:
 - DAA-GRS-2013-0003-0001 (GRS 1.1, item 001)
 - DAA-GRS-2013-0003-0001 (GRS 1.1, item 010)
 - DAA-GRS-2017-0007-0001 (GRS 2.2, item 010)
 - DAA-GRS-2017-0007-0003 (GRS 2.2, item 030)
 - DAA-GRS-2013-0005-0004 (GRS 3.1, item 020)
 - DAA-GRS-2013-0006-0003 (GRS 3.2, item 031)
 - DAA-GRS-2013-0002-0016 (GRS 4.1, Item 010)

- Length of time the information is retained in the system:

GRS 1.1, Item 001 - Destroy when 3 years old

GRS 1.1, Item 010 - Destroy 6 years after final payment or cancellation
 GRS 2.2, Item 010 - Destroy when 3 years old
 GRS 2.2, Item 030 - Destroy when 2 years old or 2 years after award is approved or disapproved
 GRS 3.1, Item 020 - Destroy 3 years after agreement, control measures, procedures, project, activity, or transaction is obsolete, completed, terminated, or superseded
 GRS 3.2, item 031 - Destroy 6 years after password is altered or user account is terminated
 GRS 4.1, Item 010 - Destroy when no longer needed

- Type of information retained in the system:

Financial Management and Reporting
 Financial Transaction Records
 Employee Management Administrative Records
 Employee Incentive Awards Records
 Information Technology Operations and Maintenance Records
 System Access Records
 Tracking and Control Records

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?

22 U.S.C. 2651a (State Department Basic Authorities Act of 1956)
 22 U.S.C. 3921 (Management of service)
 22 U.S.C. 2656 (Management of foreign affairs)

Partial Social Security Number (SSN) is collected for internal business processes. eForms collects this information to assist Bangkok Customer Service Center (BCSC), HR and FMC, as part of the check in services package preparation at post.

(d) How is the PII collected?

(1) **MVO DipNote Visa Request**: The information collected for this system is obtained directly from the employees or the responsible sponsors via SharePoint user interface. Responsible sponsors include U.S. Direct Hire (USDH) colleagues or supervisors who assist newcomers to check-in prior to their arrival. The application will generate the diplomatic letters and reports.

(2) **Bangkok DipNote Request**: Employees enter and submit requests for Diplomatic Note reference numbers for their section's correspondence between the U.S. Government and the Thailand government via SharePoint user interface on the Bangkok SharePoint home page.

(3) **Bangkok ATO Asia BOM Request**: The ATO-Asia Application Owners manually enter the project requester's (internal employees who are POCs for the projects) information and the project details into the application via SharePoint user interface. The ATO-Asia Team will coordinate with the requester to provide and confirm their business contact information and the project details.

(4) **Bangkok FMC System (FMC Voucher Logbook, FMC Bill of Collection, and FMC Phone Tracking System)**: Bangkok FMC Team receives data directly from employee using the employee arrival check-in, direct Bangkok deposit form, Permanent Change of Station (PCS) travel orders and claims, and E2 travel. FMC staff manually enters the data into the system through a desktop Visual Basic or Visual Basic.Net user interface.

(5) **Bangkok Customs and Shipping Tracking**: The GSO Custom and Shipping Team manually receives employee's information from the employee's official documents and directly from employees — assignment cable, check-in form, copy of passport, and Thailand vehicle registration. GSO team manually enters data into the system via the SharePoint user interface.

(6) **Bangkok Utilities Tracking System**: The GSO Housing Team receives employee information through the Department official assignment orders and travel portals (TMONE, TMFOUR, and the PCS Portal) in myServices, and reviews the information from their internal housing master list stored in a spreadsheet and the arrival and departure details provided by employee. The GSO team manually enters this information and the electricity usage bills provided by the electricity service providers into the application via a SharePoint user interface.

(7) **Bangkok eForm System**: Employees or sponsors enter PII and data via a SharePoint user interface or submit PDF forms. The data include the employee and employee's family member(s) or the dependents. This application generates the following forms:

- a. BCSC New Arrival Request
 - i. BCSC: E2 New User Form
 - ii. RHR: DS-4211 Leave Accounting For American Employees Returning From Home Leave Or Transferring To Post
 - iii. RHR - Notification of New Arrival For Check-in/Accreditation to Thai MFA
 - iv. RHR: DS-3064 Foreign Service Emergency Locator Information
 - v. FMC: SF-1190 Foreign Allowances Application, Grant and Report
- b. IRM OpenNet Account Access Request (DS-7667)
- c. ClassNet Account Request form (DS-7667)
- d. Electronic Mobile Computing and Data Storage Request (DS-7642)

(8) **Bangkok RHR System (RHR Awards and RHR DAP)**: HR staff manually review and enter employee's information into both applications from a desktop Visual Basic or Visual Basic.Net user interface. They reference and use the employee's data from the Department's Overseas Personnel System (OPS). For RHR DAP, HR staff also receive data from the BCSC New Arrival Request. For RHR Award, HR staff receives the information from standard award nomination forms such as JF66 submitted by supervisors for awards.

(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.

All application database records are stored on Bangkok's servers on OpenNet and all databases are encrypted.

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

(1) **MVO DipNote Visa Request**: The information collected for this application is obtained directly from the employees or the responsible sponsors via SharePoint user interface. The MVO team verifies the accuracy of data entered.

(2) **Bangkok DipNote Request Application**: Users or Application Owners enter the information into the Bangkok DipNote Request application and are responsible for accuracy of PII information.

(3) **Bangkok ATO-Asia Bill of Material (BOM) Request**: The ATO-Asia Team coordinates with the requester to confirm their business contact information and the project details.

(4) **Bangkok FMC System (FMC Voucher Logbook, FMC Bill of Collection, and FMC Phone Tracking System)**: FMC Team manually enters employee data into this system and verifies the accuracy of the PII from the employee direct deposit form and official cables.

(5) **Bangkok Customs and Shipping Tracking System**: The GSO Custom and Shipping Team manually verifies employees' information from the employees' official documents and directly from employees — assignment cable, check-in form, copy of passport, and Thailand vehicle registration.

(6) **Bangkok Utilities Tracking System**: The GSO Housing Team reviews and ensures accuracy of information they entered in the application by comparing information from the Department online application, MeterNet, and PCS check-in/check-out portals submitted by employees in myServices, and TMONE and TMFOUR to make sure that the occupant information is accurate. MeterNet enables the Department to monitor its energy, gas, and water consumption and identify ways to conserve resources and reduce operational costs.

(7) **Bangkok eForm System**: The information entered into this system is obtained directly from the employee, and/or the responsible sponsor during the arrival process, and they are thus responsible for accuracy. The Customer Service Center Team reviews the overall entries to ensure that the required PII is filled appropriately for the business process and reports. If not, the Customer Service Center will coordinate with the employee or the responsible sponsor to provide the required PII.

(8) **Bangkok RHR System**: HR Awards Team are responsible for manually entering and verifying the accuracy of the employee's PII every time they process the nominations for the award. For the RHR DAP Reminder, the RHR DAP staff manually enter and verify the accuracy of the PII.

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

The information in the database is updated by the individual offices directly any time their information changes or needs to be updated (e.g., change of address); therefore, it is up to the individual offices who own the information to keep it current. Supervisors will review and sign off on all documents and paperwork generated through the PBBA applications. It is the responsibility of application owners and supervisors to ensure currency. Users can make changes to their information in the eForm System and the Bangkok DipNote Request application. The rest of PBBA applications require the application owners to ensure the information remains current.

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

The system does not get information from commercial sources or information that is publicly available.

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

The full SSN is no longer collected. The database has been cleared and cleaned up to ensure that no reference to full SSNs are present. As such, amount of PII collected was reduced to the minimum needed to fulfill the system's function.

5. Use of information

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

The information collected and maintained within the system will be used to support the activities required for arrival check-ins, official travel orders, cashier services, and bill collections. Contact information of individuals including both personal and official addresses, e-mails, and phone numbers will be used to complete mission specific forms. Employee's partial Social Security numbers will be used for security checks and to provide appropriate access to post systems. Family members and vehicle information are both provided during new employees' check-in/check-out using PCS portal in my Services.

(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 provide information sharing and business continuity for embassy operations in Bangkok. This collective system of applications stores administrative and security information related to employee, financial, utilities, customs, inventory, and DipNote records which require the PII to function. No collateral uses exist for the information collected by the system.

(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: Information is not shared internally.

External: Information may be shared with the Thailand Ministry of Foreign Affairs, other Embassies, and local shipping companies.

(b) What information will be shared?

Internal: N/A

External: Name and passport number may be shared with the Thailand Ministry of Foreign Affairs and Embassies of other countries in Bangkok. Name and address may be shared with local shipping companies.

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

Internal: N/A

External: PII shared with the Thailand Ministry of Foreign Affairs is used to process Diplomatic ID and Import of Household Effects and Vehicles. PII shared with other Embassies is used to obtain the third country visa for official travel. PII shared with local shipping companies is used for delivery and pack-out.

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

Internal: N/A

External: Diplomatic Notes are used to send PII to the Thailand Ministry of Foreign Affairs. The original hard copy of Diplomatic notes is delivered to the Thailand Ministry of Foreign Affairs in a locked and sealed bag by the Embassy Motor Pool service. The Diplomatic Notes in PDF format are uploaded to Thailand Ministry of Foreign Affairs' ePrivilege system. In urgent matters, Diplomatic Notes are sent via Department email to Thailand Ministry of Foreign Affairs. Designated motor pool employees also hand-carry

documents in a locked and sealed bag to other Embassies. The GSO Customs and Shipping Team contacts the shipping companies via email and telephone to schedule pack out/delivery related services.

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

Internal: N/A

External: Diplomatic Notes are tracked and protected as official records. All documents sent to the Ministry of Foreign Affairs or other Embassies are packaged according to Department protocol. This includes using sealed envelopes, cover sheets, and locked bags. All packages are tracked and recorded to ensure receipt. All passports are secured and kept in a locked area.

Shipping companies are verified at the time of contact, and only the absolute minimum PII is shared to allow for the pack out/delivery services.

7. Redress and Notification

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

Yes, there are two Privacy Act statements (PAS) with one for PBBA applications collecting general PII and another for applications collecting SSNs. These PASs provide the user with notice of what authorizes the Department to collect the information, why the information is being collected, with whom that information will be shared, and whether the information is mandatory.

(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?

A Privacy Act statement is visible for all applications. The record subjects have the opportunity to decline to provide the PII. Providing the information is voluntary. Failure to provide the information requested may result in delays due to performing manual completion of those services.

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

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

Most of the applications, with the exception of the three below, are business processes that record subjects do not have a need-to-know to the information, only the application owners can access the information.

Three of the PBBA applications, eForm System, DipNote Visa Request, and the Bangkok DipNote Request, have a built-in feature that enable users (record subjects) to view their data records entered in the applications. The rest of the other PBBA applications only allow the application owners to see and manage data records.

Record subjects may also request access to their information through procedures detailed in one of the applicable System of Records Notices in 3(f).

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

Yes No

If yes, explain the procedures.

Three of the PBBA applications, eForm System, DipNote Visa Request, and the Bangkok DipNote Request, have a built-in feature that enable users to view and cancel their data record entered in the applications.

Except the above three applications, to correct inaccurate or erroneous information in other PBBA applications, users need to contact the application owners to make any change or correction to their records. Record subjects may also follow redress procedures as detailed in one of the applicable System of Records Notices listed in 3(f).

If no, explain why not.

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

It is mandatory for all newcomer employees and their families to check-in in person at the Bangkok Customer Service Center (BCSC).

Further, users can request to see their own records by submitting a service request to the corresponding sections associated with the PBBA applications. Application owners will contact record subjects to verify or correct their information.

BCSC staff will verify all information on eForm apps entered or provided by employees with their travel orders (TMONE, TMFOUR) and diplomatic passports.

BCSC will contact record subjects to collect missing or clarify incorrect information via OpenNet email.

The same procedure applies to all other PBBA applications. Application owners are responsible for accuracy of the information entered into the applications. They contact employees (record subjects) to correct missing and incorrect information.

The Department provides several centrally managed information repositories for overseas posts. For example, Application Owners use HR Online, Overseas Personnel System (OPS), PCS portal in myServices, travel orders (TMONE and TMFOUR, diplomatic passports to verify and validate employee's information.

Individuals are further notified of procedures to correct their information in one of the applicable System of Record Notices in 3(f).

8. Security Controls

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

All applications and data are located on OpenNet, the Department's Sensitive But Unclassified internal network that is secured by the Department of State security policies and baselines. These policies and baselines follow the requirements laid out in the Federal Information Security Management Act, the National Institute of Standards and Technology Guidelines, the Foreign Affairs Manuals, the Foreign Affairs Handbook, and the Department Assessment and Authorization process.

These policies and baselines include:

- Encryption of data at rest for all databases
- Multi-factor authentication (MFA), which is implemented for the Users, the Application Owners and the System Administrators to get access to the applications
- The use of MFA with RSA tokens, Department of State badges, and the Microsoft Authenticator app for users who have enrolled the GO Virtual program

(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).

Users – Access to this system is restricted to the U.S. Embassy employees who have an OpenNet account and are direct hire Americans, EFMs, LE staff, and contractors. Three of the PBBA applications, eForm System, Bangkok DipNote Request, and Visa DipNote Request require a user account to access and enter their own information. Users are unable to access any information that is not their own.

Application Owners – Application Owners are designated section employees who operate the business applications. They create, manage, and maintain data records, and therefore have access to all the PII collected in the data records within their specific applications. The Application Owners roles are defined and set up in all applications. Application owners submit IT services request with a supervisor's approval to the ISC team for obtaining access to the applications and any technical support

System Administrators – System administrators (ISC staff) provide technical support to all business applications. They are responsible for creating user and application owner accounts and managing roles. They grant and remove the Users and the Application Owners’ access to the system. They also perform routine maintenance, install, upgrade, troubleshoot, backup, monitor application health and database administration. The System Administrator audits the user accounts and application performance on a schedule. System administrators have access to the PII of all business applications, including any PII in 3(d).

(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.

All users who have an OpenNet accounts are granted access to three PBBA applications — eForm System, DipNotes Visa Request, and the Bangkok DipNote Request, and do not have access to other PBBA applications. The approval is based on a need-to-know basis. All access is enforced by the permitted login IDs stored in the SQL Database. All access must be through Department approved web browsers and desktop application from an OpenNet workstation. All access is restricted through MFA authentication and requires a PIV card and PIN code.

Supervisors approve Application Owners for accessing their applications based on position as well as a need-to-know. All ISC System Administrators can access the applications due to their role. ISC System Administrators routinely monitor application owners and system admin accounts.

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

Users – The access to three of the PBBA applications, eForm System, DipNotes Visa Request, and the Bangkok DipNote Request, is automatically granted to the U.S. Embassy employees who have OpenNet account and are direct hire Americans, EFMs, LE staff, and contractors. User access includes the ability to access their profile information and the ability to submit, review, and cancel the request.

Application Owners – The access includes the ability to create, manage, and maintain data records, and therefore have the access to all data records. The access is granted when the Section Chief authorizes and approves the access to their section application for their staff. The Section Chief will work collaboratively with the System Administrators to ensure that the access is granted properly.

System Administrators – The System Administrators maintain full administrative access to the system. All ISC staff’s administrator accounts are automatically added to this group. The ISC System Administrators use the Account Request form on SharePoint site to manage and process the PBBA access accounts.

Application owners are required to fill out and submit the Account Request form. The Supervisor reviews these requests and makes decision for approval. Once the request is approved, ISC staff update the request details with creating, updating, or deleting an account. ISC System Administrators also use credential reports to monitor user accounts, send to Application Owner every 90 days to identify those who no longer need to access as Application Owner. The SOP is shared and available for review on the Mission Thailand SharePoint site.

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

Server Monitoring and Auditing — ISC System Administrators monitor server activities and review audit logs on daily basis. All the servers are in the secured server room.

Application Owner Accounts — ISC System Administrators use a continuous monitoring program that includes ongoing security control assessments in accordance with the organizational continuous monitoring strategy.

Credential reports are used to monitor user accounts and are sent to an Application Owner's Point of Contact every 90 days to identify those who no longer have a need to access the application. Any unused credentials are disabled or deleted after the inactive accounts or unused credentials are identified.

(f) Are procedures, controls, or responsibilities regarding access to data in the system documented?

Yes No

All procedures, controls, and responsibilities are described in the Standard Operating Procedure (SOP) of the Post Bangkok Business Application. The document provides guidance and instruction pertaining to the responsibilities and actions expected from each role. The document describes the Roles and Responsibilities, the Ownership, Creating and maintaining local application, and the Local application user accounts.

(g) Explain the privacy training provided to each role identified in 8(b) that has access to PII other than their own.

In regard to all of the roles identified in 8b that have access to the PII in this system, mandatory security (PS800 - Cyber Security Awareness) and privacy (PA318 - Protecting Personally Identifiable Information) training are required for all authorized users to ensure they understand the proper protocols for protecting the vast amounts of PII they have access to. In order to retain access, each user must annually complete the Cyber Security Awareness Training, which has a privacy component. PA-318 is a biennial requirement.