PRIVACY IMPACT ASSESSMENT

Athens Business Application Suite

1. Contact Information

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

2. System Information

(a) Name of system: Athens Business Application Suite
(b) System acronym: ABAS
(c) Bureau: European and Eurasian Affairs
(d) iMatrix Asset ID Number: 346284
(e) Child systems and iMatrix Asset ID Number (if applicable): N/A
(f) Reason for performing PIA:

- ☒ New system
- ☐ Significant modification to an existing system
- ☐ To update existing PIA for a triennial security reauthorization

(g) Explanation of modification (if applicable):

3. Purpose

(a) Describe the purpose of the system.

Athens Business Application Suite is a collection of applications that covers multiple needs across the Mission Greece sections. The applications were built into a single system as a way to focus controls and efforts into a centralized space.

Description of each application as follows:

• **Regional Medical Office (RMO) Lab Records Application**: The RMO Lab Records Application is designed to track American employees and families' patient and lab records.

• **Earnings and Leave Statements Application (ELSA)**: The ELSA is a web-based solution, designed for Financial Management Center (FMC), to provide an interface to upload Local Employed Staff (LES) Earnings & Leave Statements and for users to be able to check their pay stubs per pay period per year.

• **Phone Billing Application (PBA)**: The PBA is designed for FMC and provides official mobile number billing management from a web interface for managers and users.

• **Information Systems Center (ISC) Feedback Application**: The ISC Feedback Application is a web-based solution designed for the Greece Information Systems Center providing an interface to collect feedback for all locally developed applications.

• **Regional Security Office (RSO) Foreign Service National Investigator (FSNI) Cases Application**: The RSO FSNI Cases Application provides LES subjects/cases handling tools with advanced reporting/filtering, enhanced calendar/notification features.

• **Telephone Directory Application**: The Telephone Directory Application is used by the Security Reception Unit (SRU) for data management. They handle house assignments, phone assignments etc. and system connects to the Log Incident Application.

• **Software License Manager Application (SLMA)**: SLMA provides control of Information Technology (IT) licensing which includes statistics of licenses usage and notifications before license expiration, control check for new licenses (when license is already assigned or if there are no licenses left from a registered product) and advanced filtering.

• **Information Systems Center (ISC) Assets Application**: The ISC Assets Application is designed for ISC and provides IT equipment registration with advanced live search/filtering, automated International Cooperative Administrative Support Services (ICASS) reports, and equipment mapping.

• **RSO Log Incident Application (LIA)**: The RSO LIA creates incident reports (security and/or safety related, alarm activations, demonstrations etc.); records information to share with other offices and/or agencies (consular incidents, maintenance issues etc.); records taxi reservations for U.S. Embassy's employees (personal & officials); modifies/updates SRU Data list for American employees and Eligible Family Members (EFM) and/or LES (Mobile Patrol Points (MPP) zones, personal information such as cellphone numbers, quick reference list etc.) in accordance with ISC's "Telephone Directory Application."

• **FMC Voucher Manager Application (VMA)**: The FMC VMA is designed for FMC and provides automatic voucher number handling combining details between voucher categories, voucher vendors, and ICASS codes.

• **Representational Expenses Calculator Form Application**: The Representational Expenses Calculator Form is designed for the FMC, and it's used for all Mission employees to be able to easily calculate representational expenses to be submitted to the E2 Solutions Travel and Authorization Voucher System.

• **Cellphone Manager Application**: The Cellphone Manager Application is a web repository to keep a track of all mobile numbers and devices assigned to the users. The application will keep a track on assignments, service providers, and data plans and it will automatically update the new version of the Telephone Directory Application and the Phone Billing Application.

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

- Name
- Home Address
- Personal Phone Number
- Date of Birth (DOB)
- Gender
- Business Email
- Personal Email
- Medical Information
- Employee ID
- Salary Information
- Business Mobile Number
- Nationality
- National Identification Number
- Marital Status
- Biometric (photo)
- Family Information (names, occupation for parents, siblings, spouses, children, parent's home addresses, sibling's home addresses)
- Identification papers (Official local IDs, military IDs, passports)
- Addresses of previous employers'
- Educational Information

(c) How is the PII above collected?

PII can be collected directly from the record subject or indirectly through another Athens Business Application Suite applications.

The following describes how PII is collected or obtained per application in ABAS:

1. **Regional Medical Office (RMO) Lab Records**: The MED unit collects PII with the employee present. They enter it into the system using the application's web interface.

2. **Earnings & Leave Statements Application**: Financial Management Center (FMC) payroll liaison downloads pay Stub files from Secure HTTP Internet File Transfer System (SHIFTS), a Bureau of the Comptroller and Global Financial Services system, and uploads it biweekly ELSA, automatically notifying the local staff about the new record. Each local staff is able to access their own pay stub files. For staff that don't have OpenNet access their managers can access their pay stub files. Files are uploaded into the system using the application's web interface.

3. **Phone Billing Application**: FMC downloads the official phone number records from the local service provider's website every month and uploads it into the system using the application's web interface. All employees are notified via email to check and verify their own records.

4. **ISC Feedback**: Employees submit a rating for applications inside ABAS. When the

employee rates the application, they can choose to keep it anonymous or not. If they choose not to keep the rating anonymous, the plugin collects their name and Department email address.

5. **RSO Foreign Service National Investigator (FSNI) Cases**: RSO Foreign Service National Investigators collects data from local employees, interns, and vendors to request recertification. Recertification occurs every 5 years and include background checks. This data is requested of the record subject via email or in person using the Authority to Release Information, Drug Certification, and Overseas Vetting Questionnaire forms. After their investigation, the application generates reports and paperwork for recertification. Investigators enter it into the system using the application's web interface.

6. **Telephone Directory Application**: RSO Receptionists collects PII during the security briefing or via phone/email when employees arrive at Post. They enter it into the system using the application's web interface.

7. **Software License Manager**: When requested, the ISC adds all software assignments. PII is collected during the software request. ISC enters PII into the system using the application's web interface.

8. **Information Systems Center (ISC) Assets**: When an employee submits a myServices ticket to ISC, their information is contained within that ticket. ISC installs all equipment installed into the Embassy compounds. They use ISC Assets for equipment monitoring and for ICASS counts. They pull the PII from the myServices ticket and enter it into ISC Assets using the application's web interface if the ticket involves assigning equipment/software license to the user.

9. **Log Incident Application (LIA)**: Regional Security Office (RSO) Security Receptionist Unit (SRU) collects PII when anyone reports something. This is done via telephone, email, or news from TV/web, and may include incidents that were witnessed in person. These reports can include things like a suspicious vehicle moving around an officer's house, a demonstration occurring, or a robbery that has occurred at an officer's home. The receptionists enter it into the system using the application's web interface.

10. **Voucher Manager**: FMC Voucher unit enters data with vendors transactions using the application's web interface.

11. **Representational Expenses Form**: An employee submits the Representational form, and the system automatically saves the form's details under the submitter's name and Department email address.

12. **Cellphone Manager**: An IMO's assistant retrieves phone numbers from a service provider and assigns the number to a new employee once they arrive at Post. The phone numbers are added to the application using the web interface.

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

PII is collected for Mission Greece operational processes per section as described below:

1. **RMO Lab Records**: The MED unit is using the PII for the primary purpose of keeping a track of scheduling lab records and gathering results.

2. **Earnings & Leave Statements Application**: The Payroll Liaison of local Financial Management Center (FMC) collects PII in order to distribute it to the LE Staff to be aware of their paystubs.

3. **Phone Billing Application**: The FMC collects PII in order to inform employees that exceeded the free-of-charge threshold and be able to identify personal calls and pay for any outstanding bills that have to do with their official mobile numbers.

4. **ISC Feedback**: The ISC collects PII to get feedback on the other applications inside the system. PII is optional, and the user is not required to submit their PII to use the application.

5. **RSO FSNI Cases**: After RSO FSNI investigations, the PII is used by the application in generating reports and paperwork for certification.

6. **Telephone Directory**: Receptionists collects the PII in order to perform everyday business functions, such as finding employees when needed.

7. **Software License Manager**: The Information Systems Center (ISC) collects PII in order to keep record of software license assignment to each user per their request.

8. **ISC Assets**: PII is used for ICASS accounts and subsequent equipment monitoring.

9. **Log Incident Application (LIA)**: The Security Receptionist Unit (SRU) collects PII to inform the RSO and the security dispatchers in order to take further action on security incidents related to the Embassy and the officer's homes.

10. **Voucher Manager**: The FMC collects PII in order to keep a track of generated vouchers records for different vendors.

11. **Representational Expenses Form**: The FMC collects PII in order to take authorization from the Deputy Chief of Mission (DCM) in case expenses exceed the limits per event.

12. **Cellphone Manager**: PII is used to assign work phone numbers, SIM cards, and devices to employees.

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

☒Yes ☐ No

If no, please explain:

4. Authorities and Records

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

- 22 U.S.C. 4084 (Health Care program)
- 5 U.S.C. 7361-7362 (Drug abuse, Alcohol Abuse and Alcoholism)
- 5 CFR part 792 (Federal Employees' Health, Counseling and Work/Life Programs)
- 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. 3901 et seq. (Foreign Service Act of 1980)
- 22 U.S.C. 3921 (Management of the Foreign Service)
- 22 U.S.C. 4041 (Administration of the Foreign Service)
- 5 U.S.C. 301-302 (Management of Executive Departments)
- Executive Order 9397, as amended (Numbering System for Federal Accounts Relating to Individual Persons)
- Executive Order 9830 (Amending the Civil Service Rules and Providing for Federal Personnel Administration)
- Federal Managers' Financial Integrity Act of 1982
- Federal Financial Management Improvement Act of 1996
- Debt Collection Act of 1982 and 1996

(b) If the system contains Social Security numbers (SSNs), list the specific legal authorities that permit the collection of Social Security numbers.

N/A

(c) In regular business practice, is the information routinely retrieved by a personal identifier (e.g., name, Social Security number, etc.)?

☒ Yes, please indicate relevant System of Records Notice (SORN) below.

- SORN Name and Number:

  OPM/GOVT-01 General Personnel Records
  STATE-35 Information Access Programs Records 08/13/2012
  STATE-36 Security Records 12/15/2015
  STATE-40 Employee Contact Records 11/02/2010
  STATE-73 Global Financial Management System 7/15/2008

If no, explain how the information is retrieved without a personal identifier.

(d) 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.

(e) List the Disposition Authority Number(s) of the records retention schedule(s) submitted to or approved by the National Archives and Records Administration (NARA) for this system?

Disposition Authority: DAA-GRS-2017-0010-0011 (GRS 2.7, item 062)
Disposition Authority: N1-059-89-37, item 1b
Disposition Authority: DAA-GRS-2013-0002-0016 (GRS 4.1, Item 010)
Disposition Authority: DAA-GRS-2016-0012-0001 (GRS 5.5, item 010)
Disposition Authority: DAA-GRS-2013-0003-0001 (GRS 1.1, item 010)
Disposition Authority: DAA-GRS-2017-0006-0001 (GRS 5.6, item 010)
Disposition Authority: DAA-GRS-2013-0005-0004 (GRS 3.1, item 020)

5. Data Sources, Quality, and Integrity

(a) What categories of individuals below originally provide the PII in the system? Please check all that apply.

☐ Members of the public (U.S. persons which includes U.S. citizens or LPRs)
☒ U.S. government employees/contractor employees
☐ Other (people who are not U.S. citizens or LPRs)

(b) Do the individuals listed in 5(a) provide PII on individuals other than themselves? Please check all that apply.

☒ Members of the public
☒ U.S. government employees/contractor employees
☒ Other
☐ N/A

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

In RMO Lab Records, ISC Feedback, and RSO FSNI Cases, PII is collected directly from the record subjects and the system relies on the record subjects to provide accurate and timely information. In the case of Log Incident Application, when PII is obtained via witnesses or public sources, there is no validation of accuracy during the initial submission, and any further validation occurs during the investigative process. In the case of ELSA, the information is automatically uploaded via SHIFTS, and ABAS relies on the source system for accuracy. For other systems in ABAS, the information is collected from other sources, such as vendor transaction data or service providers, and therefore relies on them for accurate information.

(d) What steps or procedures are taken to ensure the PII remains current?

In RMO Lab Records, ISC Feedback and RSO FSNI Cases, PII is collected directly from the record subjects and the system relies on the record subjects to provide accurate and timely information. In the case of Log Incident Applications, when PII is obtained via live or public sources, there is no validation of currency other than what is being discovered, and any further validation occurs during the investigative process. In the case of ELSA, the information is automatically uploaded via SHIFTS, and ABAS relies on the source system for currency. For other systems in ABAS, the information is collected from other sources, such as vendor transaction data or service providers, and therefore relies on them for current information.

(e) Was the minimization of PII in the system considered?

☒ Yes ☐ No

If no, please explain.

(f) Does the system use information, including PII, from commercial sources?

☐ Yes ☒ No

If yes, please list the commercial sources.

(g) Is the information, including PII, collected from publicly available sources?

☒ Yes ☐ No

If yes, please list the publicly available sources.

Information is collected from web searches (primarily Google), local authorities, and social media (mainly Facebook, Twitter and Linkedin). The information includes anything that might be helpful for investigators during the background check. This may include education, nicknames, emails, posts with specific comment etc.

(h) 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?

(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

(i) If the system will use test data, will it include real PII?

☐ Yes ☒ No ☐N/A - this system does not use test data

If yes, please provide additional details.

6. Redress and Notification

(a) Explain whether a notice is provided to the record subject at the point of collection of their information.

RMO Lab Records: Notice is provided verbally by MED staff or within appointment paperwork prior to collection of PII by MED staff.

ELSA: Notice is not provided to record subjects, as the information is being pulled from SHIFTS.

Phone Billing Application: Notice is not provided to record subjects as the information is being pulled from local service providers.

ISC Feedback: PII is not required, but record subjects are notified that they can provide their information if they would like a response.

RSO FSNI Cases: Notice is provided to record subjects within required release forms, the Authority to Release Information, Drug Certification, and Overseas Vetting Questionnaire forms, which allow investigators to collect and maintain PII and other data.

Telephone Directory: Notice is not given when business contact information is collected for Telephone Directory, but the Security Reception Unit (SRU) notifies individuals that their information will be used in the Mission's telephone directory.

Software License Manager: PII gathered for ISC services is not filled out by the individual and is used to provide the requested service, therefore no further uses or notification is provided.

Information Systems Center Assets: PII gathered for ISC services is not filled out by

the individual and is used to provide the requested service, therefore no further uses or notification is provided.

LIA: Notice is not provided to record subjects who's information is entered into LIA, as they are not the ones providing the information. This is for security reasons and unfeasibility of contact.

Voucher Manager: Notice is not provided to record subjects as the information is collected from vendors' transactions data, not from the individuals themselves.

Representational Expenses Form: Notice is not provided to record subjects when they submit the business contact information required for the representational claims form.

Cellphone Manager: Notice is not provided to record subjects as the initial information (phone number) is retrieved from the service provider and assigned to employees later.

(b) Are opportunities available for record subjects to decline to provide the PII?

☒ Yes ☐ No

If no, please explain why not.

(c) Are opportunities available for record subjects to consent to particular uses (other than authorized uses) of PII?

☐ Yes ☒ No

If yes, please explain.

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

Record subjects do not have access to their information in Telephone Directory, Lab Records, Software License Manager, ISC Assets, LIA, ISC Feedback, Voucher Manager, or RSO FSNI Cases.

For the following three applications, users log in using their OpenNet credentials and standard Windows authentication software:

ELSA: Each record subject has access to their own data in ELSA.

Phone billing application: Each record subject has access to their own data in Phone Billing Application.

Representational claims: FMC can see everything; record subjects can see their own data, and the data for the ones they submitted on behalf of.

(e) Are procedures in place to allow a record subject to correct or amend their information?

☒ Yes ☐ No

If yes, explain procedures and how record subjects are notified.

If information provided by a record subject needs to be corrected/amended, the record subject needs to reach out to the section handling the related ABAS component and then provide with the correct information and justification for the correction/amendment. These procedures are laid out during the first appointment or interaction. For example, investigators let you know that if you remember something else, or if you change your number/address, please send an email.

If no, explain why record subjects are not able to correct their information.

7. Sharing of PII

(a) To what entities (outside of the owning office) will the PII be transmitted? Please identify the recipients of the information.

Internal (Within the Department)	External (Outside of the Department)
N/A	Police and local ministries including Financial Ministry and Teiresias (a public service that informs on debts).

(b) For each of the entities in 7(a), list the PII from 3(b) that will be transmitted.

Internal (Within the Department)	External (Outside of the Department)
N/A	Full Name, Home Address, Business And Personal Telephone Number, Business and Personal Email, DOB, Nationality, National Identification Number

(c) For each of the entities in 7(a), what is the purpose for transmitting the information?

Internal (Within the Department)	External (Outside of the Department)
N/A	Local Police, Financial Ministry, Teiresias - PII is sent to provide additional information about the record subject to support Security Background Checks

(d) For each of the entities in 7(a), list the methods by which the information will be transmitted.

Internal (Within the Department)	External (Outside of the Department)
N/A	OpenNet Department secured email

(e) For each of the entities in 7(a), what safeguards are in place for each method of internal or external transmission?

Internal (Within the Department)	External (Outside of the Department)
N/A	Each email is marked as Sensitive but Unclassified (SBU) and identifies the specific SBU type. In addition to following all other Department procedures for sending SBU information via email.

8. Security Controls

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

Athens Business Application Suite's authentication is restricting access to Athens-OU users and Thessaloniki-OU users. Additionally, each component authorizes specific users/groups to gain access to specific data within the application using role based access restrictions. Both the Athens and Thessaloniki servers are virtual and provided by Enterprise Service Operations Center (ESOC). These servers reside on OpenNet which means they are secured by the OpenNet router firewall and then they use all the protocols and certificates provided by ESOC. At the same time, in both servers Windows Defender and Symantec Endpoint protection run at all times. ESOC also provides audit controls on each server, Embassy firewall, antivirus software, least-privilege access controls, and account level restrictions, in additional to following all security policies that are established and being used on OpenNet.

Internally, only specific roles have access to this data and data cannot be transmitted/reviewed by employees with no role in the specified component. Employees with roles into the system can transmit data within the application and/or via email using the appropriate sensitivity markings.

(b) 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.

(c) In the table below, list the general roles that access the system (e.g., users, managers, developers, administrators, contractors, other). Include what PII is accessed, the procedure for each role to access the data in the system, and how access to the data in the system is determined for each role.

Role	What does this role do?	What PII does this role have access to?	What rights to the PII does this user have (read-only, edits, etc.)	How does the role initially obtain access?	Who approves the role's access?
Users	Access data in which they have been granted permissions.	All PII and call record logs	Read-only and/or edit	Granted by the Administrator	American Supervisor
Managers	maintain data of employees	All PII and call record logs, medical data	Full control	Granted by the Administrator	American Supervisor
Administrators	has full access to an application, manages and delegates responsibilities within an application, but cannot assign roles. They also have access to specialized reports and can add/remove permissions, depending on the application.	All PII and call record logs, medical data, criminal records	Full control	Granted by American Supervisor	American Supervisor
American Supervisors	has full access to an application and Manages access to ABAS; manages delegates	All PII and call record logs, medical data	Full control	Granted by American Supervisor	American Supervisor

	responsibility within application, is able to take all actions a user can take within application. They also have access to specialized reports and can add/remove permissions, depending on the application.				
Developers	Responsible for applying patches, updates, upgrades, and bug fixes	All PII	Full control	Granted by ISO/ISSO	Permission requested of Information Security Officer (ISO)/Information System Security Officer (ISSO)

(d) After receiving initial access, describe the steps that are taken for the roles defined above to maintain access.

Access is maintained as long as the person keeps the same position or until the American Supervisor rescinds access. This access might be rescinded due to role rotations within a unit or if someone is not performing at an appropriate level and is put into a different role. An existing administrator accesses a web form inside the application and removes/assigns roles depending on the scope of work or a job reassignment. If there is no existing administrator, a myServices ticket is submitted that requires American Supervisor approval so ISC can grant specific roles.

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

☒ Yes ☐ No

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

☒ Yes ☐ No

(g) Privacy Related Training Certification

- Do all OpenNet users of this system take the course PA318 Protecting Personally Identifiable Information biennially?

  ☒ Yes ☐ No

- Do all OpenNet users of this system take the course PS800 Cybersecurity Awareness Training annually?

  ☒ Yes ☐ No

- Are there any additional privacy related trainings taken by any of the roles identified in 8(c) that has access to PII other than their own for this system?

  ☒ Yes ☐ No

  If yes, please list the related trainings here:

  Information Assurance 210 and Information Assurance 610