PRIVACY IMPACT ASSESSMENT

myServices

1. Contact Information

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

2. System Information

(a) Name of system: myServices
(b) Bureau: Bureau of Administration (A/LM/PMP/SYS)
(c) System acronym: myServices
(d) iMatrix Asset ID Number: 161803
(e) Reason for performing PIA:

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

(f) Explanation of modification (if applicable):

3. General Information

(a) Does the system have a completed and submitted Security Categorization Form (SCF)? ☒Yes ☐No - Contact IRM/IA at IASolutionCenter@state.gov for assistance.

(b) What is the security Assessment and Authorization (A&A) status of the system?

myServices is currently undergoing its Assessment and Authorization (A&A) in order to receive an Authorization to Operate (ATO). myServices is expected to receive its ATO by June 2021.

(c) Describe the purpose of the system:

myServices uses ServiceNow as its Software as a Service (SAAS) platform. myServices provides end-users a centralized platform to submit service requests and have service providers fulfill those requests via an online interface. There are four types of myServices users: end-users, privileged users, standard users, and system administrators. myServices end-users include Department of State employees, eligible family members, and government agency employees. Once an end-user submits a request it gets routed to the appropriate privileged user (approver or fulfiller) that approves the request. Once the request is approved it gets routed to standard users that are the service providers that fulfill requests. System administrators maintain the system and implement system enhancements. The system contains an array of moderate to highly sensitive PII of all users for the purpose of submitting visitor access service requests, residential services requests, and travel related requests such as eCountryClearance and Permanent Change of Station.

The core myServices system consists of two User Interface (UI) portals, a Customer Portal and a Service Provider Portal. The Customer Portal is the designated interface for end-users to complete and submit service request forms. The Service Provider portal is an interface where standard and privileged users can view the information about service requests that need to be approved and/or fulfilled.

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

The system collects personally identifiable information (PII) from U.S. persons (Department employees, eligible family members, and visitor requestors) as listed below:
First Name
Last Name
Date of Birth
Business E-Mail
Alternate E-Mail
Business Address
Personal Address
Mobile Phone
Business Phone
Passport Type
Passport Number
Last 4 Digits of SSN
Scans of Government issued I.D.s (i.e., Driver's licenses or Passport)
UserID

The system collects personally identifiable information (PII) from non-U.S. persons (foreign nationals) as listed below:
National ID Number
First Name
Last Name
Date of Birth
Business E-Mail
Alternate E-Mail
Business Address
Personal Address
Mobile Phone
Business Phone
Passport Type
Passport Number
Scans of Government issued I.D.s (i.e., Driver's licenses or Passport)
UserID

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

- 22 U.S.C. Chapter 52 (Foreign Service)
- 31 U.S.C. 901—903 (Agency Chief Financial Officers)
- Federal Financial Management Improvement Act of 1996
- 22 U.S.C. 4081, Travel and Related Expenses
- 22 U.S.C. 5724, Travel and Transportation Expenses of Employees Transferred
- 5 U.S.C. 301, 302, Management of the Department of State
- 22 U.S.C. 2651a, Organization of the Department of State
- 28 CFR 16.5.3, Use and Collection of Social Security Numbers

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

☐Yes, provide:

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

☒No, explain how the information is retrieved without a personal identifier.

Information within myServices is searchable via a service request number which is viewable based on assignment group. End-users are only able to view their own requests. Every request form that is filled out in myServices will receive an auto-generated request number that can be used as a unique identifier for tracking the lifecycle of the request. Privileged and standard users can view requests which have been routed to them via the service request's workflow. If an end-user needs to contact a privileged or standard user about a request they provide the service request number which is the unique ID of the request. End-users can find their service request number within myServices on the landing page after logging in.

(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:

Disposition Authority Number: DAA-0059-2018-0003-0006

Length of time the information is retained in the system: Destroy/delete 3 years after cut-off but no later than 10 years if required for business use.

Type of information retained in the system: Program Support Records

Description: Records relating to the support of security and law enforcement programs and initiatives. Records include, but are not limited to, memoranda, memorandum of agreements (MOAs); memorandum of understandings (MOUs); correspondence; congressional request or inquiries; counterintelligence, countermeasures, cybersecurity, crisis management, contractors, courier services, emergencies covering U.S. citizens abroad, emanations, physical security, protective detail, security incidents, shielding, special events, travel schedules, employee work schedules and assignments, Law Enforcement Availability Pay (LEAP) and other law enforcement personnel related matters.

Disposition Authority Number: DAA-0059-2018-0003-0007

Length of time the information is retained in the system: Destroy/delete 5 years after cut-off but no later than 30 years if required for business use.

Type of information retained in the system encompassed by Disposition number: Security Projects and Special Program Records

Description: Records documenting technical and physical security upgrades/improvements of embassy, consulate, and U.S. occupied buildings, communications equipment, computers, defensive equipment, records of special programs, operations, and events relating to security threats, incidents, or actions taken against individuals or property. visits

Disposition Authority Number: DAA-GRS-2017-0007-0013 GRS 2.2, Item 090

Length of time the information is retained in the system: Temporary. Destroy when 3 years old or upon employee separation or transfer, whichever is sooner; but longer retention is authorized if required for business use.

Type of information retained in the system: Records related to official passports.

Description: Documents relating to the issuance of official passports, including requests for passports, transmittal letters, receipts, and copies of travel authorizations.

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 (for myServices purposes, EFMs are counted as employees as they only have access due to their relationship to a DoS employee)
☒ Other (people who are not U.S. Citizens or LPRs)

(b) If the system contains Social Security Numbers (SSNs), is the collection necessary?
☒Yes ☐No

Yes. myServices requires partial SSN (last 4 digits) to verify the identity of DOS travelers who are doing a permanent change of station (PCS), going on temporary duty (TDY) or submitting an eCountryClearance request.

- If yes, under what authorization?

- 22 U.S.C. 4081, Travel and Related Expenses
- 22 U.S.C. 5724, Travel and Transportation Expenses of Employees Transferred
- 28 CFR 16.5.3, Use and Collection of Social Security Numbers

(c) How is the information collected?

Date of birth, passport number, national ID number, last 4 digits of SSN, name, e-mail, and phone number of end-users, standard users, and privileged users are captured in three ways: (1) filled in by all users directly upon completing Visitor Access Request (VAR); (2) filled in by all users directly upon completing their traveler profile or within myServices when they schedule a Permanent Change of Station (PCS) or eCountryClearance(eCC) request (this is an account request); or (3) integrated directly from HR through the myServices/HR GEMS integration. System administrators input their name, email, and phone number during profile completion.

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.

myServices uses ServiceNow as their FEDRAMP certified cloud provider.

(d) What process is used to determine if the information is accurate?

myServices requires end-users, privileged users, and standard users to update their account information every six months to ensure accuracy of their information. System administrators are responsible for ensuring their information is accurate in the system on their user profile. For PII derived from HR GEMS, it is the responsibility of GTM, which owns HR GEMS, to ensure the information is accurate. The information is not checked against any other source of information before the information is used to make decisions about an individual.

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

myServices privileged users are responsible for maintaining accounts for end-users at their location and performing an annual account review to validate that the PII within the platform is current. End-users may also update certain PII types within their myServices profile, such as: name, business e-mail, alternate e-mail, mobile phone and business phone, to validate the information is current. myServices requires end-users, privileged users, and standard users to update/verify their account information is current every six months. For PII derived from HR GEMS, it is the responsibility of GTM, which owns HR GEMS, to ensure the information is current. The information is not checked against any other source of information before the information is used to make decisions about an individual.

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

No, the system doesn't use information from commercial sources, nor is it publicly available.

(g) Is notice provided to the individual prior to the collection of his or her information?

Yes. A Privacy Act statement is displayed and needs to be agreed to via an acceptance checkbox prior to initial log on and annually thereafter. By acknowledging the statement, the end-users, standard users, privileged users, and system administrators accept the system collecting their PII. The Privacy Act Statement is also accessible by clicking on the Privacy Act statement link within myServices and is displayed on all request forms capturing PII. The Privacy Act statement also provides the user with information pertaining to the System of Records Notice (SORN) Integrated Logistics Management System, STATE-70 where the user can learn more about how their PII will be utilized. myServices also obtains PII from HR GEMS (owned by GTM) and it is GTM's responsibility to provide notice prior to the collection of PII.

(h) Do individuals have the opportunity to decline to provide the information or to consent to particular uses of the information? ☒Yes ☐No

- If yes, how do individuals grant consent?

End-users, standard users, privileged users, and system administrators are informed that the system collects PII and how the system uses their information prior to log-in. End-users, standard users, privileged users, and system administrators grant their consent by checking a box that indicates they acknowledge and accept the collection of their PII, when they log into the system.

- If no, why are individuals not allowed to provide consent?

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

The minimum amount of personal information required to support service requests is included on the profile page of all myServices users:

a. First name
b. Last name
c. Business phone
d. Mobile phone
e. Business email
f. Alternate email

Additional personal information such as passport number, date of birth, clearance, citizenship and last 4 digits of SSN appear on applicable service requests which may require that information for completion of a service.

End-users, standard users, and privileged users' profile information such as name, e-mail, and phone number are tied to all requests as standard contact information and are required for general correspondence with an individual throughout the course of providing a service. Personal address and personal phone number are only collected on the specific requests which would require a service provider to complete a service at an individual's personal residence, such as to perform maintenance and repair tasks at department-owned housing. Passport number is collected on the myServices Visitor Access Form and a myServices traveler profile. It is used by standard and privileged users to verify end-users' identity when they arrive at post, by confirming the passport number they present matches the passport number recorded on the visitor access request.

5. Use of information

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

Information is used to support fulfillment of International Cooperative Administrative Support Services (ICASS) services at post. Fulfillment of services commonly requires name and contact information (name, e-mail address, and phone number) of the end user requesting the service so that the standard user may coordinate fulfillment of the request.

A service may need to be performed at a specific location which could be either a business address or a personal address. This information is provided as part of a service request to the standard user when necessary. Passport number is used by privileged and standard users' posts to verify an end-user's identity when they arrive at post. Date of birth and passport number are also used to identify end-users that are transferring between posts as part of permanent change of station (PCS) travel or as part of temporary duty (TDY) or other official Department of State travel.

System administrator's PII is collected as it is needed to create their unique user profile.

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

Yes. Information is used for requesting and fulfilling services.

(c) Does the system analyze the information stored in it? ☐Yes ☒No

If yes:

(1) What types of methods are used to analyze the information?

(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

6. Sharing of Information

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

Internal: myServices shares some of the PII referenced in 3 (d) with the Safety and Accountability for Everyone (SAFE) program, owned by The Bureau of Information Resource Management (IRM).

External: There is no external sharing of information in myServices.

(b) What information will be shared?

Internal: myServices shares end-user address, email, first and last name, itinerary number, post, and departure and arrival date with SAFE.

External: N/A

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

Internal: myServices shares information with SAFE so the program is aware of the planned itineraries of end-users to ensure safety and accountability for everyone.

External: N/A

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

Internal: myServices uses a management, instrumentation, and discovery (MID) server which is a Java application that runs on a server on your local network. MID servers facilitate communication and data movement to pass information from myServices to SAFE. The MID Server is a Java application that runs as a windows service on OpenNet to facilitate the information sharing. The traffic is encrypted during transmission.

External: N/A

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

Internal: Prior to myServices sharing any information with SAFE, a Memorandum of Understanding (MOU) and Information Security Agreement (ISA) that outlines how each party will utilize and safeguard the data is signed. The information is encrypted during transmission.

External: N/A

(f) What privacy concerns were identified regarding the sharing of the information? How were these concerns addressed?

To mitigate concerns regarding individuals without a need-to-know obtaining access to PII, a role-based security model was implemented to only allow access to personal information by individuals who must see it in order to provide a service, and to limit when possible the scope of that data that are visible.

7. Redress and Notification

(a) What procedures allow individuals to gain access to their information?

End-users, standard users, privileged users, and system administrators can view and update their profile information on their profile page as well as look up any service requests they have submitted in the system via searching by the service request number within myServices. For PII derived from HR GEMS, it is the responsibility of GTM, which owns HR GEMS, to allow individuals to gain access to information obtained via that integration.

(b) Are procedures in place to allow an individual to correct inaccurate or erroneous information? ☒Yes ☐No

If yes, explain the procedures.

End-users, standard users, privileged users, and system administrators are able to update their personal information via their user profile in myServices. Users are able to cancel and re-submit myServices requests that have inaccurate information. For PII derived from HR GEMS, it is the responsibility of GTM, which owns HR GEMS, to provide individuals with procedures to correct inaccurate or erroneous information.

If no, explain why not.

(c) By what means are individuals notified of the procedures to correct their information?

All users receive a reminder email every six months in addition to a warning banner on the myServices Customer Portal to update/verify their profile. The training materials for the respective application modules include processes and procedures to correct incorrect inputs/information. The reminder email will notify users to update their account information. All users are given the option to navigate to their myServices profile in OpenNet or the Internet via hyperlink (for users who do not have OpenNet access), to correct their information if needed. End users, privileged users, and standard users are suggested to contact their Post Administrator (Overseas users) or ILMS Support Desk (Domestic users) for those fields within the profile that they are unable to properly update. When all information is inputted correctly, the user will click the "Confirm User Information" button on their account settings on the myServices Customer Portal. System administrators can update their information as needed. For PII derived from HR GEMS, it is the responsibility of GTM, which owns HR GEMS, to provide individuals notice of the procedures to correct inaccurate or erroneous information.

8. Security Controls

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

Access to myServices requires a User ID and password and is accessed over a secure HTTPS connection. Users can submit service requests and view prior service requests that have been submitted.

Additional roles and groups are assigned to an account which allows an approver or fulfiller at post to only see the requests routed to their group at their post. In addition, myServices has implemented encryption for PII at rest and other sensitive data.

(b) Describe the procedures established to limit access to only those individuals who have an "official" need to access the information in their work capacity.

Post administrators perform annual review of accounts for their location to ensure the active accounts are valid users at post, and that only approved roles and groups are assigned to the account. Post administrators ensure that only those with a need-to-know have access to the PII in the system.

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

All users' (to include end-users, privileged users, standard users, and system administrators) actions executed within myServices are logged in a table and viewable/searchable by system administrators. System administrators are unable to edit these logs and can only view for the purposes of continuous monitoring. The system administrators monitor the logs and get email alerts for any attempts at gaining unauthorized access, unusual activity, and integration errors. There is an established baseline of normal system activities and the system uses Splunk to monitor and alert on activities outside of that baseline. Login and logout activities and the addition or removal of roles within the system are tracked and included in this alerting in myServices. The ISSO also has access to monitor system administrators' actions executed in the system.

(d) Explain the privacy training provided to authorized users of the system.

DoS end-users, privileged users, standard users, and system administrators are required to take the mandatory biennial privacy course, PA318 Protecting Personally Identifiable Information, delivered by the Foreign Service Institute. They are also required to take PS800 Cyber Security Awareness Training, which has a privacy component. End users are required to take and consent to the annual rules of behavior guidelines which includes a privacy policy component.

(e) Are any security controls, such as encryption, strong authentication procedures, or other controls, in place to make the information unusable to unauthorized users?
☒Yes ☐No

If yes, please explain.

As a cloud system, myServices must comply with applicable security measures that are outlined in FISMA, FedRAMP, OMB guidance, NIST Federal Information Processing Standards (FIPS) and Special Publications, and Department of State policy and standards. These privacy and security requirements are designed to keep end-user, privileged users, standard user, and system administrators' information safe and to make the information unusable to unauthorized users.

Specifically, data at rest and in transit are encrypted. ServiceNow's centralized key management platform (utilizing SafeNet), generates a key that encrypts these drives (FIPS 140-2 Level 2 validated hard drive model) and further encrypts the encryption keys using a FIPS 140-2 Level 2 validated encryption module. ServiceNow runs SafeNet in NIST Federal Information Processing Standards (FIPS) mode which only allows for FIPS-approved algorithms to be utilized by myServices. Backups, for ServiceNow, are encrypted utilizing FIPS approved ciphers. Additionally, myServices has also implemented tablespace encryption for data at rest to enhance the security posture of the system.

(f) How were the security measures above influenced by the type of information collected?

Given the type of PII collected and used by myServices, security measures were put in place specifically to meet FIMSA Moderate and FedRAMP Moderate requirements as well as OMB guidance, FIPS 140-2 requirements and Department of State policy and standards such as Foreign Affairs Manual/Foreign Affairs Handbook (FAM/FAH) policies.

9. Data Access

(a) Who has access to data in the system?

End-users only have access to their own PII: first name, last name, DOB, business e-mail, alternate e-mail, business address, personal address, mobile phone, business phone, passport type, passport number, last 4 SSN, scans of Government issued I.D.s (i.e., Driver's licenses or Passport), userID.

Standard and privileged users have access to the PII necessary to approve and/or fulfill the request that the end-user submitted. The requests include: first name, last name, DOB, business e-mail, alternate e-mail, business address, personal address, mobile phone, business phone, passport type, passport number, last 4 SSN, scans of Government issued I.D.s (i.e., Driver's licenses or Passport), userID. Each request that an end-user can submit in the system only includes the least amount of PII for that request to be fulfilled. Standard users and privileged users at post can only see the PII of the end-users at their respective posts.

System administrators can see the PII of all users: first name, last name, DOB, business e-mail, alternate e-mail, business address, personal address, mobile phone, business phone, passport type, passport number, last 4 SSN, scans of Government issued I.D.s (i.e. Driver's licenses or Passport), userID.

(b) How is access to data in the system determined?

Access to data is determined by the groups and roles assigned to an individual's myServices User ID. Department of State accounts are initially created by Active Directory then myServices groups and roles are assigned by Post Administrator or System Administrator. Non-Department of State users submit account requests that are routed to a Post Administrator for approval and for additional access.

(c) Are procedures, controls or responsibilities regarding access to data in the system documented? ☒Yes ☐No

(d) Will all users have access to all data in the system, or will user access be restricted? Please explain.

All users do not have access to all the data in the system. End-users only have access to their own PII. Privileged and standard users have access to the minimal amount of PII to approve and/or fulfill an end-user's request. System administrators have access to all data in the system Access to PII is restricted by the implementation of a role-based security model to only allow access to the minimal amount of PII for an end-user, privileged user, and standard user to fulfill a request.

(e) What controls are in place to prevent the misuse (e.g. unauthorized browsing) of data by users having access to the data?

The details in section 8 (b), 8 (c), 8 (e) and 9 (b) have been implemented to monitor and prevent the misuse of the PII that end-users, privileged, standard and system administrators have access to.