PRIVACY IMPACT ASSESSMENT

MyApps ServiceNow (MyApps)

1. Contact Information

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

2. System Information

(a) Date of completion of this PIA: April 2022
(b) Name of system: MyApps ServiceNow
(c) System acronym: MyApps
(d) Bureau: Bureau of Administration (A/EX/ITS)
(e) iMatrix Asset ID Number: 251565
(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:

MyApps is a platform-as-a-service, provided by ServiceNow, that hosts 48 separate and distinct applications. The applications within myApps fall into two categories, DS Forms and Requests. There are 24 automated DS forms, 5 of which collect PII, and 24 Requests, 6 of which collect PII. For the remainder of the document, these will be referred to as "forms and requests".

MyApps does not collect any PII directly, rather it supports/houses applications that collect or use PII for specific purposes.

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

MyApps forms and requests collect the following information from government employees, contractors, and potential employees. The following information is collected on U.S. persons.

- Full Name
- Citizenship
- Father's Full name
- Mother's Full name
- Passport Number
- Personal phone number
- Personal Email Address
- Personal Address
- Date of Birth
- Place of Birth
- Partial Social Security Number
- Full Social Security Number
- Business Phone Number
- Business Email Address
- Business Title
- Work Location
- Company Name
- Employee Identification Number (EIN)

The following PII is collected on non-U.S. persons:

- Full Name
- Citizenship
- Father's Full name
- Mother's Full name
- Personal phone number
- Personal Email Address
- Personal Address
- Date of Birth
- Place of Birth

- Business Phone Number
- Business Email Address
- Business Title
- Work Location
- Company Name
- National ID

The remainder of this PIA will focus only on the PII collected from U.S. persons.

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

- 5 U.S.C. 301 - Management of the Department of State
- 22 U.S.C. 2651a - Organization of the Department of State
- 22 U.S.C. § 3921 – Administration by Secretary of State
- 22 U.S.C. § 3943 – Appointments by the Secretary
- 22. U.S.C. § 3949 – Limited Appointments
- 22. U.S.C. § 3951 – United States citizens hired abroad
- Executive Order (EO) 12353 (March 23, 1982)
- 5 CFR 950 (January 1, 2017), Solicitation of Federal Civilian and Uniformed Service Personnel for Contributions to Private Voluntary Organizations
- 26 U.S.C. 2714a(f) (Revocation or denial of passport in case of certain unpaid taxes)
- 22 C.F.R. part 50 (October 20, 1966) Nationality Procedures
- 22 C.F.R. part 51 (November 19, 2007) Passports
- Executive Order 12968 (August 2, 1995)
- Executive Order 13467 (June 30, 2008)
- Executive Order 13764 (January 17, 2017)
- Foreign Service Act of 1980 (22 U.S.C. §4802et. seq.), Sections 201, 303, 309, and 311
- 5 CFR 731 (April 15, 2008) Suitability

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

☒Yes, provide:
Though myApps does not collect PII directly from record subjects, the myApps system allows for users to perform contextual searching. A user of the myApps forms and requests identified in 3c can search for information based on the level of access they have.

- SORN Name and Number:

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

State-36, Security Records, June 15, 2018
State-04, Confidential Statement of Employment and Financial Interest Records, September 27, 1997
State-44, Congressional Travel Records, July 9, 1997
State-40, Employee Contact Records, November 2, 2010
State-73, Global Financial Management System, July 15, 2008
State-31, Human Resources Records, July 19, 2013
State-70, Integrated Logistics Management System Records (ILMS), January 25, 2022
State-56, Network User Account Records, October 14, 2010
State-67, Office of Inspector General (OIG) Timesheet System, September 25, 2002
State-26, Passport Records, March 24, 2015
State-30, Personnel Payroll Records, February 11, 1998
State-38, Vendor Records, September 27, 1977

☐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	**Disposition Authority Number**	**Length of Time Retained**	**Type of Information**
A-03-003-02	DAA-GRS-2013-0005-0007 (GRS 3.1, item 011)	Temporary. Destroy 5 years after system is superseded by a new iteration, or is terminated, defunded, or no longer needed for agency/IT administrative purposes, but longer retention is authorized if required for business use.	Change management requests, approvals, enhancement request, and development stories.
A-06-025-113-005-34	DAA-GRS-2017-0001-0001 (GRS 5.8, item 010)	Temporary. Destroy 1 year after resolved, or when no longer needed for business use, whichever is appropriate.	Help desk incidents, problem tickets and access requests.

A-03-005-05	DAA-GRS-2017-0003-0002 (GRS 5.2, item 020)	Temporary. Destroy upon verification of successful creation of the final document or file, or when no longer needed for business use, whichever is later.	Records of an intermediary nature, meaning that they are created or used in the process of creating a subsequent record.

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?

- 5 C.F.R 950 (January 1, 2017) Solicitation of Federal Civilian and Uniformed Service Personnel for Contributions to Private Voluntary Organizations.
- 26 U.S.C. 2714a(f), Section 236 of the Admiral James W. Nance and Meg Donovan Foreign Relations Authorization Act, Fiscal Years 2000 and 2001;
- Executive Order 12968 (August 2, 1995)
- Executive Order 13467 (June 30, 2008)
- Executive Order 13764 (January 17, 2017)
- 5 C.F.R 731 (April 15, 2008) Suitability

(d) How is the PII collected?

The information collected by this system is obtained directly from the applicant via the following automated DS forms:

- DS-5137 (FSFRC Membership)
- DS-1833 (Debit Voucher and Returned Check Report)
- DS-1887 (Foreign Contact Report)

- DS-3064 (Foreign Service Emergency Locator Information)
- DS-1654 (CFC Enrollment)

The information collected by this system is obtained directly from the applicant via the following requests:

- Restored Annual Leave Request
- DS (Diplomatic Security) Security Clearance Request
- Travel Support Request
- Employee Departures Request
- Administration-Information Resource Management (A-IRM) Employee Relations Request.
- LSMX (Language Services Order Request)

The information from these myApps forms and requests are automatically recorded in the system once the applicant submits the form or request, except for DS Security Clearance request.

Potential employees provide their PII to an HR Specialist. Then the HR Specialist enters the PII into the DS Security Clearance request within myApps. The DS Clearance Coordinator team will verify the PII with the candidate.

Social Security number is collected on the following: The DS Security Clearance request, Restored Annual Leave request, and DS-1654 (CFC Enrollment) and DS-1833 (Debit Voucher and Returned Check Report) forms.

(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.

MyApps is housed on the ServiceNow GCC FedRamp-Certified cloud.

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

Information is collected directly from the individual when they submit the myApps forms or requests listed in 4d.

Potential employees' PII is provided by HR team members in the DS Security Clearance request and verified with the candidate by the Clearance Coordinator team. The Clearance Coordinator team verifies information by meeting with the potential employee via phone or video conference.

Employee PII is provided by Employee Relations team members in the A-IRM Employee Relations application, and they are responsible for verifying the information with the employee.

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

PII is current at time of entry and during the processing of the relevant myApps form or request lifecycle. After a myApps form or request has been fully processed, the data will not be changed in order to keep the information current. Any changes to PII that are relevant to the initiated myApps form or request require the submission of a new copy of that form or request. This is true for the below :

- DS (Diplomatic Security) Security Clearance Request
- Travel Support Request
- DS-3064 (Foreign Service Emergency Locator Information)
- DS-1654 (CFC Enrollment)
- Restored Annual Leave Request
- Employee Departures Request
- LSMX (Language Services Order Request)

Below, are the forms the record subject is able to access via myApps and change information as long as they have an account in the system:

- DS-5137 (FSFRC Membership)
- DS-1833 (Debit Voucher and Returned Check Report)
- DS-1887 (Foreign Contact Report)

Only the Employee Relations Specialists have access to the data types below and are able to update this information. Employee Relations Specialists ensure that the information in these records remains current.

- Administration-Information Resource Management (A-IRM) Employee Relations request

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

Information is not collected from commercial sources. The information is not publicly available.

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

During the requirements gathering phase, it was determined that the PII collected by the myApps forms and requests is relevant and necessary in order to fully process and complete the forms and requests submitted by the system users. Forms and requests in myApps collect the minimum amount of PII needed to fulfill the requests and only collect data that are direcly relevant to the fulfillment process.

5. Use of information

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

The PII collected by myApps forms and requests consists of information that is necessary in order to confirm individual identity, ensuring accurate information,and minimizing fraud. The PII collected is used for purposes such as collecting personal information needed for payroll processing, supporting travel requests, and issuing security clearances.

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

Yes, the purpose of this system is to process forms and requests (listed in 4d) submitted by an individual to the Department of State. All of the foms and requests listed in 4d are completed and submitted by users directly in myApps. As such, all of the PII in the application is stored within myApps for processing purposes. The PII collected is necessary and only kept so that the system can perform the functions that it was designed to carry out. 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:
PII is shared from Restored Annual Leave and LSMX with the Bureau of the Comptroller and Global Finanance.

External:
No information is shared externally.

(b) What information will be shared?

Internal:
The PII that is shared with CGFS includes:

- Restored Annual Leave shares: Employee Identification Number (EIN)
- LSMX shares Name and Business/personal email address

External:
No information is shared externally.

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

Internal:

CGFS uses the provided PII for the purpose of processing payroll and contractor invoicing.

External:
No information is shared externally.

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

Internal:
CGFS will receive information from Restored Annual Leave via a electronic file posted to a location that only CGFS and a POC from A/EX/ITS can access. For LSMX, the file is sent via email to Global Financial Management System (GFMS), a CGFS processing system.

External:
No information is shared externally.

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

Internal:

The Restored Annual Leave file is compiled by a user with application administrator access to the system and is then transmitted via the Department of State's email to the A/EX/ITS POC who will post it to CGFS's file storage. Limiting the role which has the ability to create and transmit the file is a safeguard.

The LSMX file is compiled by the system, and sent through encrypted email to GFMS' State Department intake email address. Having the system generate and send the file reduces the number of individuals who access and view the PII.

External:
No information is shared externally.

7. Redress and Notification

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

Yes, it is the responsibility of the myApps form/request owner to include a Privacy Act statement on any collection of PII. This is an A/EX/ITS requirement. The user is provided with the Privacy Act statement to review prior to submission of all requests and forms that collect PII.

(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?
By submitting the myApps form or request in question the user grants their consent to the collection of PII. Record subjects may decline to provide the PII, but doing so may result in their form/request not being processed or approved.

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

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

Below are the forms/requests where the records subject gains read only access to their submission for as long as it is retained in the system. If changes to a completed submission need to be made, the user is required to submit a new copy of the form/request.

- DS (Diplomatic Security) Security Clearance Request
- Travel Support Request
- DS-3064 (Foreign Service Emergency Locator Information)
- DS-1654 (CFC Enrollment)
- Restored Annual Leave Request

- Employee Departures Request

Below, are the forms/requests where the record subject is able to access their information via myApps and change information as long as they have an account in the system:

- DS-5137 (FSFRC Membership)
- DS-1833 (Debit Voucher and Returned Check Report)
- DS-1887 (Foreign Contact Report)
- LSMX (Language Services Order Request)

Due to the sensitive information in the Administration-Information Resource Management (A-IRM) Employee Relations Request, record subjects do not have access to this information.

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

☒Yes ☐No

If yes, explain the procedures.

If a user submits a form/request that has incorrect or erroneous data then they have two options to correct this data. 1) The user can cancel their form/request and submit a corrected version. 2) The user can request that their submission be sent back for them to make a correction to their record.

Specifically on the DS-1833 (Debit Voucher and Returned Check Report), DS-1887 (Foreign Contact Report), and DS-5137 (FSFRC Membership), the user will be able to reenter their data without the need for cancelling their form or having it sent back by the approver.

For LSMX, the user submits a request via the myApps incident request which is routed to the System Administrator. The System Administrator will update the information to their account profile.

If no, explain why not.

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

Forms and requests in myApps have accompanying user guides, knowledge articles, and community forums where users can seek out information, including how to correct their data. If users have trouble locating the procedure or have any questions they can reach out to the support desk which will provide guidance on the procedure or can contact a support team by submitting an incident ticket in the system for assistance.

8. Security Controls

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

All data in myApps are stored within the ServiceNow environment, and maintained on their cloud servers. Security for the instance is managed by ServiceNow as a platform and the controls are inherited from the Customer Responsibility Matrix. Users are able to access the system via single sign on using their state account through Azure, or through multi-factor authentication using Okta.

(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).

Requesters: A requester is a user that submits a form or request. Requesters will have access to their own form and request submissions, and will retain access to their submissions for as long as they have access to the environment, and as long as the data is retained. A requester can provide access to their records by adding a user to the 'watchlist', providing them access where they would not otherwise have it.

Approvers: Retain access to submissions that they are listed as an approver on for as long as they have access to the environment, and as long as the data are retained. Approvers will be able to view all of the PII on the submissions they are assigned. Approvers are unable to edit PII, with the exception of the DS Security Clearance application, where the approver is able to edit PII since the subject of that information does not have access to the system.

Application Administrators: Have access to form and request data including PII with the exception of social security numbers. These users are given access in order to provide support for the application or to manage the use of the application.

System Administrators: Have the ability to access all records in the system that do not contain PII.

(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.

Access to the system and its information is limited according to role-based restrictions.

Requesters: Have access only to the records they create, or are specifically granted access by the user who created the record.

Approvers: Receive access to all PII for records that require their approval, and they will maintain access to records that they were listed as an approver for as long as they are maintained in the system.

Application Administrators: Given access to application data, including all PII (with the exception of social security numbers), once they have been added to a group in the system. Group membership for application administrator groups is self-managed and can otherwise only be modified by system administrators.

System Administors: This role generally does not have access to PII in the system. However, system administrators are only provided access to records with PII if they are added to the application administrator group for the application in question and will only do so when requested to provide support. If they are added to the application administrator group they will have access to all PII for that application for as long as they are in the group. A system admininstrator is added to the application administrator groups when they are performing support to a user, and will remove themselves from the group after providing their assistance

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

Requesters: Submit forms/requests and view records of their submissions. They can initiate forms and requests and view their past submissions that they need to access. All requesters are given access to form submissions (forms with a DS-XXXX number) and the Restored Annual Leave Request upon account creation. Access to other myApps requests are granted directly by application administrators, or by submitting a request for access which needs approval by a user with at least the level of permission in the application that is being requested.

Approvers: Approve forms/requests and view records of their previous approvals. For some myApps forms and requests, approvers will be given viewership of a record once they are selected as an approver by the submitter, while for other myApps forms and requests they will be given a role to view and approve all records that are relevant to their position. Approvers are given access if they are the designated approver on a form or request (e.g. the form requires supervisor approval and they are the submitter’s supervisor) or if they belong to a group with approver roles for the form or request. Group membership can be granted directly by an application administrator, or by submitting a request for access which needs approval by a user with at least the level of permission in the application that is being requested.

Application Administrators: View all records for a form or request to provide support, but are prevented from seeing sensitive data such as social security numbers. Application administrators consist of the support team for a specific application. Application Administrators are given access to data by the System Administrator and existing Application Administrator.

System Administrators: Provide support across the platform, and have access to most forms and requests. If an form or request contains sensitive data, then access will be restricted, and the system administrator will be unable to access records for the application without an additional role such as application administrator. System administrators can only be added by other system administrators and require the approval of the platform owner and/or ISSO.

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

Access to data and the ability to modify data in the system is restricted using roles and group membership. Changes to data in the system are audited and tracked for each record, and a history of changes can be viewed by users with access to the record. In addition, admistrative activity, such as the deletion of records is audited. The date, object change, and user who made the change are included in this audit information.

In addition, SSN fields have additional protections so that a system or application administrator can provide support while still being unable to view the data in the SSN field without the approver role for the application.

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

☒Yes ☐No

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

There is no role-based specific training. All users who have access to the myApps platform are required to complete mandatory security (PS800 Cyber Security Awareness) and privacy (PA318 Protecting Personally Identifiable Information) training to ensure they understand the proper protocols for protecting the PII they can access. In order to retain access, users must complete annual security and biennial privacy training as mandated by the Department of State.