PRIVACY IMPACT ASSESSMENT

RSO Tools PIA

1. Contact Information

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

2. System Information

(a) Date of completion of this PIA: 10/2022
(b) Name of system: Regional Security Officer (RSO) Tools
(c) System acronym: RSO Tools
(d) Bureau: Bureau of Diplomatic Security (DS)
(e) iMatrix Asset ID Number: 335104
(f) Child systems (if applicable) iMatrix Asset ID Number:
(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): The RSO Tools system is being re-assessed for FISMA High authorization.

3. General Information

(a) Does the system have a completed and submitted data type 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 :
RSO Tools is a suite of modules, used by Department of State (State) employees, contractors, and locally employed staff (LES) at overseas posts, that provides a single place to track and manage Diplomatic Security initiatives, such as local guard programs,

contracts, reports, finance, travel, staffing, scheduling, training, and requests related to the execution of the Diplomatic Security initiatives. The RSO Tools modules facilitate tracking contract and post budget information, maintaining post profile information, maintaining travel information, and tracking communications between Washington D.C. and post. To fulfill these initiatives, RSO Tools utilizes the minimum amount of PII from six types of record subjects, described in section 3(d) below.

RSO Tools utilizes ServiceNow, the Cloud Services Provider (CSP), which is FedRAMP authorized. The Bureau of Diplomatic Security, International Programs, Overseas Protective Operations (DS/IP/OPO) is the business owner.

The following modules make up the RSO Tools suite:

1. **myRD (including SETL):** The myRD module allows Regional Directors (RD), Desk Officers, and RSOs the ability to manage and access oversight events, resource requests and security directives. The portal provides regional security offices, the Offices of Regional Directors (DS/IP/RD and DS/HTP/RD), and the Office of Overseas Protective Operations (DS/IP/OPO) with a consolidated view to manage and access key post security programs and processes. The Security Environment Threat Level (SETL) Requirements dashboard provides a tracking system for the RSOs to ensure compliance and view all applicable policy requirements for mobile patrol, bodyguards, facilities and residential guards.

2. **OPO Enterprise:** The OPO Enterprise module provides overseas post management capabilities for Overseas Protective Operations (DS/IP/OPO), including visibility and oversight of Exhibit As, cables, travel, communications, requests, contracts, events, finances and reports.

3. **myLGP** (Local Guard Program): The myLGP module provides the on-site Regional Security Office (RSO) team at each overseas post with daily management of local guard activities including vetting, training, scheduling, and invoicing. myLGP provides visibility into those operations and program performance for the Diplomatic Security Headquarters (DS HQ)

4. **myWPS** (Worldwide Protective Services): The myWPS module provides Diplomatic Security's High Threat Post Overseas Protective Operations (DS/HTP/OPO) program office and on-site Regional Security Officer (RSO) teams at high threat posts (HTP) the ability to manage task orders while also providing contractors with daily management of guard and canine activities including training, scheduling, invoicing, and contract deliverables.

5. **myMSG** (Marine Security Guard): The myMSG module provides RSOs and the Office of Special Programs and Coordination the ability to submit Marine Guard requests, reports, and manage detachment information such as staffing, scheduling, requests, and reporting processes.

6. **AccessDS** (Access Diplomatic Security): The AccessDS module centralizes the submission and tracking of system access requests for applications managed by DS's Chief Technology Office (DS/CTO) from initial user access request submission to approval and fulfillment.

7. **myST** (Security Technology): The myST module streamlines tasks and actions across multiple contributors involved when scheduling and assigning ST personnel globally, managing service requests, global tasks and surveys, and tracking the operational status of security technology equipment.

8. **CAP Tools** (Contracting and Procurement): The CAP Tools module provides access to key information and required actions for multiple contributors involved when preparing requirements packages for Personal Service Contractors and Acquisition Planning. The module allows users to prepare to solicit Personal Service Contract (PSC) positions, complete contract actions for awarded PSC's, and plan for acquisitions through custom task assignment, milestone tracking, and contract actions.

9. **myPPD** (Program Planning Division): The myPPD module provides a central location for DS program offices and PPD to collaborate, track and complete DS policy and planning requirements by incorporating annual program plans, quarterly performance reports, and organizing policy information for bureau's tracking.

10. **myDSIR (**Diplomatic Security Information Reporting): The myDSIR module streamlines processes for submitting, distributing, and centralizing DS information reports such as significant post observed threats (SPOT), significant activities, surveillance incidents, and other reports at domestic and overseas posts.

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

RSO Tools uses, manages, disseminates, or maintains PII on six types of record subjects:

1. State employees (U.S. Citizens, and in some cases dual-citizens)
2. Candidates for Personal Service Contracts (U.S. Citizens) - members of the public who have applied to and are being considered for PSC positions in the Bureau of Diplomatic Security. These record subjects may become State employees.
3. Contract Guards at High Threat Posts (U.S. Citizens) – guards are hired through third-party contractors supplying guard services at High Threat Posts.
4. Contract Guards (non-U.S. Citizen foreign nationals, except some cases of dual-citizens) are hired through third-party contractors supplying Local Guard services at non-High Threat Posts.

5. Personal Service Agreement (PSA) Guards (non-U.S. Citizen foreign nationals, except rare cases of dual-citizens) - these are direct-hires to the embassy supplying local guard services and are treated as U.S. government employees.
6. Person, Subject, or Victim (typically non-U.S. person except in rare cases) described in the narrative of a Suspicious Activity report in the myDSIR module. Although such reports may include anonymous references to a U.S. person victim, the myDSIR module is not intended to collect or disseminate PII about U.S. person victims in Suspicious Activity reports. Report authors are instructed to maintain anonymity of U.S. person victims.

   Each module in RSO Tools uses, manages, disseminates, or maintains minimum PII from the record subjects listed above to fulfill the module initiatives, as described below. The remainder of this PIA will address the PII of U.S. persons only: State employees, Candidates for PSCs and Contract Guards at High Threat Posts.

   1. State employees: myRD (including SETL), the OPO Enterprise, myLGP, myWPS, myMSG, AccessDS, myST, myCAP, myPPD, and myDSIR collect and use the following information on State employees:

      a. First Name
      b. Last Name
      c. Middle Initial
      d. Business Phone
      e. Business Email
      f. Business Title
      g. Personal Phone
      h. Work Address

   In addition to items a-h, AccessDS collects and uses the following information on State employees to determine the State employee's eligibility to access applications:

      i. Social Security Number (SSN)
      j. Date of Birth (DOB)
      k. Clearance and/or Certification Information

   In addition to items a-h, myWPS and myST collect and use the following information from State employees to prepare travel documents:

      l. Passport Number
      m. Passport Expiration
      n. Visa Number
      o. Visa Expiration

   In addition to items a-h and i-o, myST collects and uses the following information from State employees.

      p. Photograph of individual

In addition to items a-h, CAP Tools collects and uses the following information from State employees and Candidates for PSCs to determine a candidate's eligibility for a PSC award, or contract modifications.

q. Personal Email
r. Clearance Status
s. Gender/Sex
t. Personal Address
u. SSN
v. Date of Birth

2. Candidates for Personal Service Contracts: The CAP Tools module collects the following information from candidates for PSCs:

    a. First Name
    b. Last Name
    c. Middle Initial
    d. Business Phone
    e. Business Email
    f. Personal Email
    g. Clearance Status
    h. Gender/Sex
    i. Address
    j. SSN
    k. Date of Birth

    CAP Tools uses this information on candidates for PSCs to determine a candidate's eligibility for a PSC award, and for State employees to determine eligibility for a PSC Contract Modifications. Since candidates for PSCs are U.S. citizens, for the purposes of this document they are considered as members of the public because they are not State employees until their PSC contract is awarded. Once their PSC contract is awarded, they are considered State employees per 3 FAM 9000. All candidates for PSCs provide the same information listed above in the candidate application.

3. Contract Guards at High Threat Posts: myWPS and OPO Enterprise collect and use the following PII on Contract Guards at High Threat Posts to determine an instructor's eligibility to provide training, or a guard's eligibility for assignments and travel:

    a. First Name
    b. Last Name
    c. Middle Initial
    d. Date of Birth
    e. Place of Birth
    f. Foreign National ID
    g. Gender/Sex
    h. Business Phone

i. Citizenship (if a dual citizen)
j. Business Email
k. SSN
l. Clearance and/or certification information
m. Passport Number
n. Passport Expiration
o. Visa Number
p. Visa Expiration
q. Employee Number (series of numbers, can be used in lieu of SSN)
r. Employee ID (series of letters and potentially numbers)

Note: Employee ID and Employee Number may be any kind of employer-provided unique identifier, such as a string of numbers or letters, used by the employer to uniquely identify their personnel when managing a contract in RSO Tools. Employee ID may be specific to their employee such as Firstname.Lastname@employee.com or an Employee Number such as 11223344. Employee ID and Employee Number fields are optional and dependent upon the employer.

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

- 5 U.S.C. 301, Departmental Regulations
- 5 U.S.C. 302, Delegation of Authority (Management of the Department of State)
- 22 U.S.C. 2581, General Authority
- 22 U.S.C. 2669(c) (contracting for services abroad)
- 22 U.S.C. 3921, Management of the Foreign Service
- Omnibus Diplomatic Security and Antiterrorism Act of 1986, 22 U.S.C. 4802(a) (Secretary of State security responsibility)
- Omnibus Diplomatic Security and Antiterrorism Act of 1986, 22 U.S.C. 4824 (Contracting Authority)
- 22 U.S.C. 3927, Responsibility of Chief of Mission
- 26 U.S.C. § 6109 Identifying Numbers

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

☒Yes, provide:
- SORN Name and Number: Security Records, STATE-36
- SORN publication date (found under the Volume Number and above the Public Notice Number on the published SORN): June 15, 2018

☐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):

- Disposition Authority Number:
  a. **Security Projects and Special Program Records,** DAA-0059-2018-0003-0007
  b. **Program Support Records,** DAA-0059-2018-0003-0006

- Length of time the information is retained in the system:
  a. Temporary. Cut-off at end of calendar year of final action. Destroy/delete 5 years after cut-off but no later than 30 years if required for business use.
  b. Temporary. Cut-off at end of calendar year of final action. 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:
  a. Security Projects and Special Program Records
  b. Program Support Records

- Description:
  a. Records documenting technical and physical security upgrades/improvements of embassy, consulate, and U.S. occupied buildings, communications equipment, computers, defensive equipment, armored vehicles, and security countermeasures. This schedule also covers actions taken against individuals or property. Records include, but are not limited to, specifications for the test and evaluation of vendor products, design drawings, floor plans, inspections, standards, certification/non-certification letter, tracking and control information on statistical data and other related subjects.
  b. 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); requirements and investigations covering accreditation, anti-terrorism, assessments, asset forfeiture, building construction, computer security, counterintelligence, countermeasures, cybersecurity, crisis management, contractors, courier services, government-owned and commercially leased motor vehicles, electronic security, emergencies covering U.S. citizens abroad, emanations, engineering, inspections, inventories, penetration, physical security, product certification, product evaluation, program reviews, protective detail, security incidents, shielding, special events, surveillance detection, systems development, training, travel schedules, zones of control, victim resource advocacy, employee work schedules and assignments, Law Enforcement

Availability Pay (LEAP) and other law enforcement personnel related matters, and other related subjects.

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?

- 28 CFR § 16.53 - Use and collection of social security numbers.

(d) How is the PII collected?

For each record subject type and module described in section 3(d), PII is collected as follows:

1. State employees: The information listed below on State employees in RSO Tools is collected in real time by an integration with State's Active Directory:
    a. First Name
    b. Last Name
    c. Middle Initial
    d. Business Phone
    e. Business Email

Additional PII on State employees is collected as follows:

    f. SSN and Date of Birth is populated by the State employee themselves when submitting a request in AccessDS.
    g. Clearance and/or certification information is populated in AccessDS by an integration with State's Clearance Check. The SSN and DOB is provided

by the State employee when requesting a State Clearance Check and/or certification information.

h. Passport expiration, visa number, and visa expiration is populated by the State employee themselves or government supervisor when preparing a travel itinerary in the myST module, or when completing a GTM profile in myWPS module.
i. For State employees who are Personal Service Contractors in the DS Bureau: Personal email, clearance and/or certification information, gender/sex, address, SSN, and date of birth is collected from the record subject when initially completing an application for a Personal Service Contract, as described in #2 below.

2. Candidates for Personal Service Contracts (PSCs): The following PII is provided by the candidate when completing an application for a PSC position within Diplomatic Security. The application process occurs outside of the RSO Tools system. Then, the PII is entered manually into the CAP Tools module by a Department HR analyst to create a candidate's profile:

    a. First Name
    b. Last Name
    c. Middle Initial
    d. Business Phone
    e. Business Email
    f. Personal Email
    g. Clearance and/or Certification Information
    h. Gender / Sex
    i. Address
    j. SSN
    k. Date of Birth

3. Contract guards at High Threat Posts: The following PII on contract guards at high threat posts is collected by the contractor program manager (PM), and manually entered into the HITS application (a DS application separate from RSO Tools), and then it is automatically shared through an integration between HITS and myWPS and the OPO Enterprise modules in RSO Tools.

    a. First Name
    b. Last Name
    c. Middle Initial
    d. Date of Birth
    e. Gender / Sex
    f. Business Phone
    g. Citizenship (if a dual citizen)
    h. Business Email
    i. SSN
    j. Clearance and/or Certification Information
    k. Passport Number

l. Passport Expiration
m. Visa Number
n. Visa Expiration
o. Employee Number
p. Employee ID

(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.

RSO Tools is housed in the ServiceNow Federal Environment for the Government Community Cloud (GCC) and includes several ServiceNow management, instrumentation, and discovery (MID) servers provisioned by IRM that reside on a virtual machine on a Department of State server. The MID servers are used to facilitate data sharing between RSO Tools and on-prem Department systems.

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

1. State employees: State's Active Directory is the source from which RSO Tools obtains items a-e on State employees. The accuracy of the PII is the responsibility of the State employee who enters it into the myProfile application before it is shared to State's Active Directory.

    a. First Name
    b. Last Name
    c. Middle Initial
    d. Business Phone
    e. Work Email

Additional PII on State employees is checked for accuracy as follows:

f. SSN and Date of Birth is populated by the State employee when submitting a request in DS AccessDS. It is the responsibility of the State employee to ensure it is accurate.
g. Clearance/certification information is checked for accuracy against the State Clearance Check database. It is the responsibility of the State Clearance Check database to ensure it is accurate.
h. Passport number, passport expiration, visa number, and visa expiration is populated by the State employee themselves or government supervisor when preparing a travel itinerary in myST module, or when completing a Government Technical Monitor (GTM) profile in the myWPS module. It is

the responsibility of the State employee or government supervisor to ensure accuracy when populating this information.

i. For State employees who were formerly candidates for PSCs: Personal email, gender/sex, address, SSN, date of birth, and clearance and/or certification information is populated on a State employee's profile from their candidate profile, as described in #2 below.

2. Candidates for Personal Service Contracts: The candidate is responsible for ensuring the accuracy of their own PII entered on their application to any PSC job postings on Jobs.MonsterGovt.com or USAJobs.gov. Once the candidate profile is manually created by an HR Analyst in the CAP Tools module in RSO Tools, the candidate for a PSC is granted access to their PII and can update it or amend any inaccurate information to ensure accuracy. This PII is not checked against any other system.

3. Contract Guards at High Threat Posts: The accuracy of the PII is the responsibility of the contract guard providing their PII to the contractor PM before it is entered in the HITS application, which occurs before it is shared to the myLGP module of RSO Tools. This PII is not checked against any other system because it comes into RSO Tools from HITS.

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

1. State employees: The items a-f remain current through a daily integration with State's Active Directory, which receives the PII from myProfile. It is the responsibility of the State employee to ensure the PII remains current in myProfile.

    a. First Name
    b. Last Name
    c. Middle Initial
    d. Business Phone
    e. Work Email

Additional PII on State employees is kept current as follows:

    f. SSN and Date of Birth is populated by the State employee when submitting a request in AccessDS. It is the responsibility of the State employee to ensure it is current.
    g. Clearance/certification information is checked for currency against the State Clearance Check database. It is the responsibility of the State Clearance Check to ensure it is current.
    h. Passport number, passport expiration, visa number, and visa expiration is populated by the State employee themselves or government supervisor when preparing travel itinerary in the myST module, or when completing a GTM profile in the myWPS module. It is the responsibility of the State employee or government supervisor to ensure this information remains current.

i. For State employees who are Personal Service Contractors in the DS Bureau: It is the responsibility of the State employee hired to a PSC position to ensure personal email, clearance and/or certification information, gender/sex, address, SSN, and date of birth remains current on their user profile.

2. Candidates for Personal Service Contracts: It is the responsibility of the candidate to ensure their PII remains current.

3. Contract Guards at High Threat Posts: The PII is kept current through a daily integration with the HITS application. As the source of the PII, it is the responsibility of the Contractor PM to ensure the PII is kept current in the HITS application before it is shared to the myWPS and OPO Enterprise modules of RSO Tools.

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

No, RSO Tools does not use information from commercial sources nor is the information publicly available.

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

Privacy concerns were at the forefront of the system's design and enhancements are continuously made to limit the amount of PII maintained to only that which is required to support the purpose of the system. For example, SSNs are only collected for record subjects who will need to have their clearance validated through the secure integration with the State Clearance Check. The clearance status of those record subjects is required to determine their eligibility for training, scheduling, and contract actions in the system. These record subjects include guards at high threat posts, and PSC's. For most other record subjects in the system, SSN is not required and therefore is not collected.

5. Use of information

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

The PII is used to assist in the management of staff at post, including vetting, training, staffing and scheduling, contract management, current and upcoming assignments, travel documents and itineraries, certifications, leave, and vendor employment history. The PII is also used to generate the PSC's contract file from candidacy to State employment, including the tasks and actions required for contract modifications and additional contract actions such as signing and uploading required documents.

(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 PII is relevant to the purpose the system, which was designed for State employees and contractors domestically and at overseas posts to track and manage Diplomatic Security initiatives. The PII is necessary to perform the functions to fulfill

these initiatives in the RSO Tools modules, such as: personnel management, post contracts and budgets, travel, staffing, eligibility for assignment and training, communications between Washington D.C. and posts, and requests related to the execution of these Diplomatic Security initiatives. RSO Tools utilizes only the minimum amount of PII necessary to perform these functions as designed. 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: Diplomatic Security, Chief Technology Officer (DS/CTO): PII on State employees is shared with DS/CTO, which owns the State Clearance Check system, when the clearance or certification information of the record subject is required for actions or tasks within the relevant RSO Tools modules.

External: There is no external sharing of PII.

(b) What information will be shared?

Internal: DS/CTO: SSN, DOB, first name, and last name.

External: N/A

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

Internal: DS/CTO: The PII is shared to query the State Clearance Check database to return a clearance or certification information back to RSO Tools. The clearance status is used within the relevant RSO Tools modules to determine the record subject's eligibility

to request access to other State applications, as well as eligibility for future assignments and training in the myWPS module. No other PII is shared with DS/CTO.

External: N/A

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

Internal: The information is transmitted to DS/CTO by Transport Layer Security/Hypertexttransfer protocol secure (TLS/HTTPS), which is encrypted to increase security of all information transmitted.

External: N/A

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

Internal: Data is encrypted while in transit between systems.

External: N/A

7. Redress and Notification

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

Yes, notice is provided to each record subject listed in section 3(d) prior to the collection of their information.

1. State employees: For PII integrated from State's Active Directory, State employees are provided notice during onboarding, in the form of a Privacy Act statement (PAS), when their PII is entered into the myProfile application, which occurs before it is shared with the modules in RSO Tools.

State employees are provided notice for the following PII items as follows:

a. A PAS is presented on the user access request form in AccessDS to provide notice to the State employee prior to the collection of SSN, DOB, and clearance/certification information.
b. A PAS is presented on the user profile and travel itinerary forms in myST and myWPS to provide notice to the State employee prior to the collection of their passport number, passport expiration, visa number, and visa expiration. When the PII is manually entered on behalf of a State employee by their government supervisor, then the government supervisor will inform them verbally or by email. If the information is being entered solely by a third party, and the record subject is not actively providing the info to the third party as they enter it, a PAS is not required.
c. State employees who are awarded a Personal Service Contract in the DS Bureau: State employees who are hired to a PSC position are provided notice

in the PSC job posting prior to the collection of personal email, gender/sex, address, SSN, date of birth, and clearance and/or certification information and saved in CAP Tools. A PAS is presented on the State Employee's user profile to provide notice when the State employee updates or amends this information.

2. Candidates for Personal Service Contracts: are provided a PAS is provided on the PSC job postings on Jobs.MonsterGovt.com or USAJobs.com, before the PII is manually entered into the CAP Tools module in RSO Tools to create the candidate's profile. A PAS is also presented on the candidate's profile to provide notice when the candidate updates or amends this information.

3. Contract Guards at High Threat Posts: are provided notice by Contract PMs verbally or in a PAS prior to entering their PII into the HITS system, which occurs before it is shared to the OPO Enterprise and myWPS modules in RSO Tools.

(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?

1. State employees have the opportunity to grant consent for providing the following PII items:

    a. SSN, date of birth, and clearance/certification information when submitting a user access request in AccessDS.
    b. Passport number, passport expiration, visa number, and visa expiration when completing a Government Technical Monitor (GTM) profile in the myWPS module or completing a travel itinerary in the myST module, or by providing the PII to their government supervisor to enter it into myST or myWPS module on their behalf.
    c. Personal email, gender/sex, address, SSN, date of birth, and clearance and/or certification information in CAP Tools when the State employee was a candidate for a PSC job posting. When amending or updating the PII on their profile, the State employee grants consent by submitting the changes.

2. Candidates for Personal Service Contracts have the opportunity to provide or decline consent for the use of their PII when completing and submitting an application to a PSC job posting. The record subject cannot apply to the PSC position without providing the necessary information, including PII.

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

State employees: Since the items listed below in RSO Tools are obtained directly from State's Active Directory without the involvement of the records subject, State employees do not have the opportunity to decline or consent.

a. First Name

b. Last Name
c. Middle Initial
d. Business Phone
e. Work Email

Contract guards at High Threat Posts generally do not have the opportunity to provide or decline consent to the use of their PII (stated in their contract) when Contract program managers (PMs) enter it in HITS, which occurs before it is shared to the OPO Enterprise and myWPS modules in RSO Tools.

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

1. All State employees are granted access to the AccessDS module in RSO Tools to view their PII. From the DS AccessDS module, State employees can request further access to other RSO Tools modules or submit a request to the RSO Tools administrative support team to request access to their information. Instructions are available to all State employees in the DS AccessDS Knowledge Base.
2. All Candidates for PSCs are granted access to their own candidate profile in the CAP Tools module to view their PII.
3. Contract Guards at High Threat Posts who are granted access to the OPO Enterprise or myWPS modules receive training and materials with instructions on how to access their PII. Contract Guards at High Threat Posts who do not have access to these modules can contact their contractor PM or government supervisor to obtain their PII contained in these modules.

Additionally, State's Privacy Act practices allow for all record subjects to gain access to their information by contacting the Department's Freedom of Information Act (FOIA) office for copies of the records retained. Details on this process can be found in the System of Records Notice, Security Records, STATE-36. Notice of these procedures is provided to the record subject in the Privacy Act statement associated with the form utilized for data collection.

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

☒Yes ☐ No

If yes, explain the procedures.

For PII that is manually obtained and kept current directly in RSO Tools, the following procedures are in place to allow a record subject to correct inaccurate or erroneous information:

1. State employees can update the PII themselves or submit a request to the RSO Tools administrative support team to make any corrections.
2. All candidates for PSCs are granted access to their own candidate profile in the CAP Tools module to view and correct their information or submit a request to the RSO Tools administrative support team to make any corrections.

3. Contract Guards at High Threat Posts who are granted access to the OPO Enterprise or myWPS module can correct their own PII or submit a request to the RSO Tools administrative support team to make corrections. Contract Guards at High Threat Posts who do not have access to these modules can contact their contractor PM or government supervisor to make corrections to their PII on their behalf.

If no, explain why not.

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

For PII in RSO Tools that is obtained and kept current from other sources such as State's Active Directory, State Clearance Check, and HITS, it is the responsibility of those sources to notify record subjects of the procedures to correct inaccurate or erroneous information.

For PII that is manually obtained and kept current directly in RSO Tools, the following procedures are in place to allow a record subject to correct inaccurate or erroneous information:

1. State employees are granted access to the knowledge base with information on the procedures to update their PII themselves or submit a request to the RSO Tools administrative support team to make any corrections.
2. All Candidates for PSCs in the CAP Tools module have access to the knowledge base with resources on the procedures to update their PII themselves or submit a request to the RSO Tools administrative support team to make any corrections.
3. Contract Guards at High Threat Posts who are granted access to the OPO Enterprise or myWPS modules are trained on the procedures to correct their own PII during their initial onboarding. These users also have access to the knowledge base to update their PII themselves or submit a request to an RSO Tools administrative support team to make corrections. Contract Guards at High Threat Posts who are not granted access to the OPO Enterprise or myWPS modules are trained by their Contractor PM on the process to access and correct their information.

Additionally, the Department's Privacy Act practices allow for record subjects to gain access to their information by contacting the Department's Freedom of Information Act (FOIA) and/or Privacy office for copies of the records retained. Details on this process can be found in the System of Records Notice, Security Records, STATE-36.

8. Security Controls

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

The system relies on inherent security controls native to the FedRAMP-approved GCC on which it resides, as well as the inherent security controls from the cloud-service provider ServiceNow, in addition to the implementation of all State security mandates, applicable NIST 800-53 controls and by conducting annual security assessments. Furthermore, the transfer of this data is encrypted following standard State encryption protocols. In addition, RSO Tools has implemented the concepts of least privileged,

separation of duties and role-based access control (RBAC) so, users are only granted the minimum amount of access to complete their duties.

(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).

Basic Users - Basic users have access to the minimum amount of PII required to perform assigned tasks within their assigned module and post or domestic location. This PII may be limited to their own PII and in other cases include that of others. These users include State employees, candidates for PSCs, and Contract Guards at High Threat Posts. Basic users cannot edit or remove PII elements that integrate from other sources such as State's Active Directory, HITS, or State Clearance Check.

Module Administrator - Module administrators include the module product owners, and the module support teams. These users have access to their specific module programs, libraries, test data files, etc. These administrators are able to view all PII within their assigned module, utilizing the least-privileged access framework. These administrators are able to edit or remove PII that is entered or generated directly in their module but cannot edit or remove PII that integrates from other sources such as State Active Directory, HITS, or State Clearance Check.

Limited Administrators - Limited administrators are assigned the appropriate permissions to common features across modules to which they are granted access based on their job responsibilities, such as managing user access, managing system notifications, or importing and exporting system data. Limited administrators do not have access to all PII in all modules. Limited administrators include Tier 1-3 end user support and the RSO Tools training and re-engagement teams. Limited administrators are able to view some PII across all modules, consistent with their assigned privileges and duties, utilizing role-based and least-privileged access framework. For example, a Notification Administrator is a type of Limited Administrator with access to manage notifications for all users. A Notification Administrator can view and edit a user's email and phone as it pertains to managing notification devices but does not have access to edit a user's SSN or Clearance Status because those elements are outside of their responsibilities. In contrast, a Configuration Admin is another type of Limited Admin with access to manage system configurations but does not have access to edit a user's PII because it is not required for their assigned responsibilities. Additionally, Limited Administrators cannot edit or remove PII that integrates from other sources such as State Active Directory, HITS, or State Clearance Check.

System Administrators - System administrators are the only users with full access across all modules. This small group of users has access to all data, including all PII in the system. System administrators require this access to conduct maintenance such as applying relevant patches and fixing issues that arise. However, System Administrators cannot edit or remove PII that integrates from other sources such as State Active Directory, HITS, or State Clearance Check.

(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.

RSO Tools implemented role-based user access (RBAC) and the concepts of least-privileged user access and separation of duties framework to allow the minimum amount of access to PII required to perform their job function. In addition, access is only granted after the user's FTE government supervisor's review and approval.

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

For Basic User Access - All basic users require government supervisor approval. Some users will require additional approvals based on considerations such as a user's assigned post, mission, region, or duties.

For Limited Administrator and Module Administrator access - This role requires approval from the relevant module product owner, in addition to the requester's government supervisor. All module product owners are State employees in management positions authorized to oversee the development, implementation, user access, and maintenance associated with a module in RSO Tools.

For System Administrators access - This role requires approval from all module product owners and the business owner, in addition to the requester's government supervisor. The business owner is a State employee assigned to oversee and govern the activities of all module product owners.

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

RSO Tools retains system audit logs to prevent misuse of the system. Access to the audit logs is limited to system administrators should they need to be reviewed by third party assessors or auditors. The execution of privileged functions (e.g., administrator activities) is included in the audit log of events that are sent to the ISSO daily for monitoring. The purpose of the audit logs is to document unintended modification or unauthorized access to the system and to dynamically audit any access made to designated critical data. Information in the audit log that is sent to the ISSO for monitoring contains: system property changes, access control list changes, committed update sets, deleted user accounts, added user accounts, after-hours access, and changes to access privileges.

(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.

All users are required to take the biennial privacy course, PA318 Protecting Personally Identifiable Information, and the annual cyber security course, PS800, Cyber Security Awareness, delivered by the Foreign Service Institute.