# PRIVACY IMPACT ASSESSMENT

## Regional Security Office Local Vetting (RESOLVE)

### 1. Contact Information

| |
|---|
| **A/GIS Deputy Assistant Secretary**<br>Bureau of Administration<br>Global Information Services |

### 2. System Information

**(a) Name of system:** Regional Security Office Local Vetting (RESOLVE)
**(b) System acronym:** RESOLVE
**(c) Bureau**: Diplomatic Security
**(d) iMatrix Asset ID Number:** 273422
**(e) Child systems (if applicable) and iMatrix Asset ID Number:** N/A
**(f) Reason for performing PIA:**

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

**(g) Explanation of modification (if applicable):**

### 3. Purpose

**(a) Describe the purpose of the system.**

The Regional Security Office Local Vetting (RESOLVE), Version 01.02.00, iMatrix 273422 supports Bureau of Diplomatic Security mission requirements for DS Identity Assurance system (DSIAS) by supporting background checks at Department of State Posts worldwide. RESOLVE provides the Regional Security Officer (RSO) with the ability to track and manage background investigations for Foreign Service Nationals. The process for conducting background investigations at Outside Continental United States (OCONUS) locations varies from Post to Post. This is partially due to varying host-country laws, a broadly scoped background investigation policy, and the lack of a commonly utilized tool for managing background investigations. RESOLVE has an on-screen display of DS background investigation requirements which apply across DS postings. This display is to be used by the RSO to track and communicate the status of vetting and adjudication tasks. RESOLVE Applicant Status Display provides a means of quickly confirming where applicants of interest are in the RSO vetting and adjudication process and also provides automation as a means of increasing the speed and amount of information shared between overseas Posts, RSOs, and Desk Officers at the headquarters during the RSO vetting and adjudication process.

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

- Full Name
- Street address
- City
- County
- Precinct
- Zip codes/equivalent geocodes
- Telephone/fax numbers· Email addresses
- Full Social Security Numbers (SSNs)
- Birth dates
- Full face photographic images and comparable images
- Passport Numbers
- Driver's License Numbers
- Usernames
- Other - Local host country identification document.

The above information is collected from both non-U.S. persons (non-USP) and U.S. persons (USP)Locally Employed Staff (LE Staff). For the purposes of this PIA, the focus will be on the collection of PII from LE Staff who are U.S. persons.

**(c) How is the PII above collected?**

Applicants complete the Overseas Vetting Questionnaire (OVQ) form DS-7801 fillable PDF, which is then submitted to Post. Foreign Service National Investigators (FSNI) personnel from the RSO Office will manually import that form into RESOLVE. FSNI personnel will then start an investigation of the applicant and use that PII during the background checks.

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

The information maintained in the RESOLVE system is necessary for conducting background investigations of current and potential USP LE Staff to ascertain eligibility for a security certification.

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

☒Yes ☐No

**4. Authorities and Records**

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

Omnibus Diplomatic Security and Antiterrorism Act of 1986.

Executive Order 13467, Reforming Processes Related to Suitability for Government Employment, Fitness for Contractor Employees, and Eligibility for Access to Classified National Security Information, July 2, 2008, as amended.

Title 5 Code of Federal Regulations Part 731.104(c).

Federal Investigative Standards. Delegation of Authority No. 214, dated September 20, 1994, Delegation of Responsibilities Under the Foreign Relations Authorization Act, Fiscal Years 1994 and 1995, and Certain Related Acts.

Delegation of Authority No. 293-2, dated October 11, 2011,

Delegation of Authority by the Secretary of State to Officers of the Department of State and the Administrator of the U.S. Agency for International Development of Authorities under the Foreign Assistance Act of 1961 and Other Related Acts.

12 FAM 251.7, Polygraph Examinations For Locally Employed Staff (LE Staff); and12 FAM 420, Post Security Management.

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

The collection of SSNs is permissible in accordance with the Omnibus Diplomatic Security and Antiterrorism Act of 1986 and Executive Order 13467, as amended. The collection of SSNs is an operational necessity in that they are needed to conduct BI of persons seeking employment at post in foreign countries. Such activities depend on interoperation with outside entities without significant risk of misidentifying individuals.

**(c) In regular business practice, is the information routinely retrieved by a personal identifier (e.g., name, Social Security number, etc.)?** If yes, please indicate relevant System of Records Notice (SORN) below

☒Yes, provide:

- SORN Name and Number:
  STATE-36 Security Records 12/15/2015

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

**(d) Does the existing SORN need to be amended to reflect the inclusion of this new or significantly modified system?** ☐Yes ☒No

If yes, please notify the Privacy Office at Privacy@state.gov.

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

Disposition Authority Number(s):
- Schedule numbers. DAA-GRS-2017-0006-0024 b. DAA-GRS-2017-0006-0025c. DAA-GRS-2017-0006-0026 Disposition Authority Number: GRS 5.6, item 180b. GRS 5.6, item 181c. GRS 5.6, item 190

**5. Data Sources, Quality, and Integrity**

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

☒Members of the Public
☒ U.S. Government employees/Contractor employees
☒ Other (people who are not U.S. Citizens or LPRs)

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

☐Members of the Public
☐ U.S. Government employees/Contractor employees
☐ Other (people who are not U.S. Citizens or LPRs)
☒N/A

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

During the investigation, applicant provided data is validated against the supporting documentation provided by the applicant.

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

Locally employed staff are subject to reinvestigation at least every five years, or more frequently depending on Post requirements. Beyond the 5-year investigations, the information cannot be altered and remains static.

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

☒Yes ☐No

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

☐Yes ☒No

Please list the commercial sources.

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

☐Yes ☒No

Please list the publicly available sources.

**(h) Does the system analyze the PII stored in it?**

☐Yes ☒No

If yes:
(1) What types of methods are used to analyze the PII?
(2) Does the analysis result in new information?
(3) Will the new information be placed in the individual's record?
(4) With the new information, will the Department be able to make new determinations about the individual that would not have been possible without it?
☐Yes ☐No

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

☐Yes ☐No ☒N/A
Please provide additional details.

**6. Redress and Notification**

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

Yes, notice is provided in the form of a Privacy Act statement (PAS) on the Overseas Vetting Questionnaire (OVQ), DS-7801.

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

☒Yes ☐No

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

☐Yes ☒No

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

Individuals do not have access to their information in RESOLVE. However, the Department's Privacy Act practices allow for record subjects to gain access to their information by filing a Privacy Act request. Details on this process can be found in the System of Records Notice, STATE-36.

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

☒Yes ☐No

Explain procedures and how record subjects are notified.

To the extent that material contained in RESOLVE is subject to the Privacy Act (5 U.S.C. 552a), individuals can request amendment of material in the system under the procedures set forth in 22C.F.R. Part 171.Redress and notification for correcting inaccurate or erroneous information occurs during initial and/or follow-up interviews with the applicant.

## 7. Sharing of PII

Information in this section is intentionally omitted as it contains SBU/LES information.

## 8. Security

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

The RESOLVE system uses role-based access controls and limits users to specific roles at specific locations. The system employs the use of Secure Sockets Layer (SSL) for all application interactions.

**(b) Where is the information housed?**

☒ Department-owned equipment
☐ FEDRAMP-certified cloud
☐ Other Federal agency equipment or cloud
☐ Other

- If you did not select "Department-owned equipment," please specify.

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

# PRIVACY IMPACT ASSESSMENT

| ROLE | WHAT DOES THIS ROLE DO? | WHAT PII DOES THIS ROLE HAVE ACCESS TO? | WHAT RIGHTS TO THE PII DOES THE USER HAVE? (READ-ONLY, EDIT, ETC.) | HOW DOES THE ROLE INITIALLY OBTAIN ACCESS? | WHO APPROVES THE ROLE'S ACCESS? |
|---|---|---|---|---|---|
| Administrator | Gives access to the admin pages in RESOLVE. | All PII for subjects in the system. | Read-only | Users request an account in RESOLVE via Access DS application. Their access request is reviewed and approved by their supervisor and information security office. Once approved, the request is routed to Help Desk personnel who will create the RESOLVE account with the approved roles and access. | Access is approved by the Business Owner and the ISSO |
| Investigator/Intake/Adjudicator | Gives access to subjects and investigations at the assigned posts. | All PII for subjects at assigned posts. | Read and write | Users request an account in RESOLVE via Access DS application. Their access request is reviewed and approved by their supervisor and information security office. Once approved, the request is routed to Help Desk personnel who will create the RESOLVE account with the approved roles and access. | Access is approved by the Business Owner and the ISSO |

| | | | | | |
|---|---|---|---|---|---|
| Oversite | Gives access to all subjects and investigations worldwide, intended for desk officers to manage investigations in their region. | All PII for all subjects in RESOLVE. | Read-only | Users request an account in RESOLVE via Access DS application. Their access request is reviewed and approved by their supervisor and information security office. Once approved, the request is routed to Help Desk personnel who will create the RESOLVE account with the approved roles and access. | Access is approved by the Business Owner and the ISSO |

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

The system enforces role-based access that dictates the task level and geographic level of user access. These roles are physically assigned within RESOLVE by the User Administrator role. This means a user can only access areas needed for their work position. Approving supervisors approve the level of access users have at each individual posts. These requests for access are tracked in the AccessDS application. Once a user gains access to RESOLVE, access is maintained via regular use of the application. If a user does not access RESOLVE over a 60-day period, access is disabled due to non-activity. Otherwise, access is maintained until access is requested to be removed. The official process when a user no longer requires access to RESOLVE is for the user (or their supervisor) to submit an AccessDS request to remove the access. As a backup, the RESOLVE system will automatically disable access for users who have not accessed RESOLVE for 60 days after a set period of inactivity defined in the ATO. In the event a user no longer works for the Department, their OpenNet will be disabled, which removes access as RESOLVE is a Single Sign On application that requires a working OpenNet account for authentication. There are no external users to RESOLVE.

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

☒Yes ☐No

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

☒Yes ☐No

# PRIVACY IMPACT ASSESSMENT

**(g) Privacy Related Training Certification**

- Do all OpenNet users of this system take PA-318 Protecting Personally Identifiable Information biennially?

  ☒Yes ☐No

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

  ☒Yes ☐No

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

  ☐Yes ☒No

  Please list the related trainings here: