RESOLVE
(Regional Security Office Local Vetting)
PIA

1. Contact Information

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

2. System Information

(a) Name of system: RESOLVE (Regional Security Office Local Vetting)

(b) Bureau: Diplomatic Security

(c) System acronym: RESOLVE

(d) iMatrix Asset ID Number: 273422

(e) Reason for performing PIA: RESOLVE is a System of Record for security certifications. RESOLVE will collect, track, and manage all information related to background investigations for locally employed staff. RESOLVE is not intended to collect PII on US persons; however, RESOLVE may collect some PII on US persons provided by applicants such as references and spouses. It is also possible that an individual may become a U.S. person at some time in the future and their information would still be stored in the system.

- ☒ 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?
RESOLVE RMF Step 4 Assessment began Thursday, February 8, 2018. The trigger for this action was the completion of Steps 1-3. The system is expected to complete the A&A April 2018.

(c) Describe the purpose of the system:

The purpose of RESOLVE is to provide automated functionality required by Regional Security Officers (RSOs) to complete background investigations on foreign nationals applying for employment at Department of State posts (work locations) around the globe.

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

- Full name, legal name
- Personal Address
- Business Address(es)
- Phone number(s), home, mobile, business
- Current, and prior job title and/or employment positions held
- SSN or equivalent for foreign nationals
- Date of Birth
- Passport Number
- Substantive individual financial information,
  e.g. bankruptcy, gambling, failure to file or failure to pay taxes, owning or planning to own foreign property, compensation for providing services or consulting to foreign governments or foreign intelligence services. Financial difficulties such as, but not limited to, counseled, warned, or disciplined for violating the terms of agreement for a travel or credit card provided by your employer, currently utilizing, or seeking assistance from, a credit counseling service or other similar resource to resolve your financial difficulties, lien placed against your property for failing to pay taxes or other debts, possessions or property voluntarily or involuntarily repossessed or foreclosed, financial support for any foreign national, you, your spouse or legally recognized civil union/domestic partner, cohabitant, or dependent children, having any foreign financial interests (such as stocks, property, investments, bank accounts, ownership of corporate entities, ownership of corporate entities, corporate interests or exchange traded funds (ETFs) held in specific geographical or economic sectors) in which you or they have direct control or direct ownership
- Substantive individual legal information,
  e.g. charged with, convicted of, or sentenced for a crime in any court (including all qualifying charges, convictions or sentences in any Federal, state, local, military, or non-U.S. court), party to any public record civil court action, been a member of an organization dedicated to terrorism, advocated any acts of terrorism or activities designed to overthrow the U.S. Government by force, currently a domestic violence protective order or restraining order issued, been charged with an offense involving firearms or explosives, alcohol or drugs
- Substantive individual personnel information
  e.g. held political office in a foreign country, sponsored any foreign national to come to the U.S. as a student, for work, or for permanent residence, you or any

member of your immediate family had any contact with a foreign government, its establishment (such as embassy, consulate, agency, military service, intelligence or security service, etc.) or its representatives, whether inside or outside the U.S.

- Substantive individual family information
  e.g., you, your spouse or legally recognized civil union/domestic partner, cohabitant, or dependent children received, or are eligible to receive in the future, any educational, medical, retirement, social welfare, or other such benefit from a foreign country.

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

- Pub.L. 99-399 Omnibus Diplomatic Security and Antiterrorism Act of 1986, as amended)

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

☒Yes, provide:

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

  - STATE-31, Human Resources Records, July 19, 2013
  - STATE-36, Security Records, December 15, 2015

☐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 Division 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:

- Schedule number (e.g., (XX-587-XX-XXX)): See below
- Length of time the information is retained in the system: See below
- Type of information retained in the system: See below

Schedule Number	Length of Time	Type of Information

B-08-002-01a(2) Local Personnel Investigative Files	Disposition: Destroy three years after termination of employment.	Description: This covers both Department of State Non-American employees and other U.S. Government agency Non-American employees - when post security office conducts investigation. a. Locals who were certified for employment. (2) Regional Security Office copy.
B-08-002-01b(2) Local Personnel Investigative Files	Disposition: Note card and destroy.	Description: b. Locals who were refused certification for employment on the basis of information of record. (2) Regional Security Office copy.
B-08-002-01c(2)(a) Local Personnel Investigative Files	Disposition: Destroy when 5 years old.	Description: c. Locals who were investigated, but who abandoned their application. (2) Regional Security Office copy. (a) File containing derogatory information.
B-08-002-01c(2)(b) Local Personnel Investigative Files	Disposition: Destroy when 1 year old.	Description: c. Locals who were investigated, but who abandoned their application. (2) Regional Security Office copy.
B-08-002-01d(2) Local Personnel Investigative Files	Disposition: Destroy 5 years after termination, except for certain reporting required by security regulations	Description: d. Locals and local applicants who were terminated for cause. (2) Regional Security Office copy.
B-08-002-05b Security Investigation Card Files	Disposition: Destroy 20 years after transfer to the inactive file	Description: Regional Security Office - Card files on security investigations conducted at post. Cards record basic data on cases of: Foreign Service Nationals certified for employment, including initial and subsequent investigations; Foreign Nationals refused employment; Foreign Nationals who abandoned an employment application after the security investigation was conducted; U.S. Government employees for whom overseas investigation is required; Non-American citizens being investigated for employment elsewhere, for a visa or other assistance, or for participation in an exchange program; Individuals involved in incidents such as attempted penetration, fraud, or loss of diplomatic pouches.

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) If the system contains Social Security Numbers (SSNs), is the collection necessary?

☒Yes ☐No

- If yes, under what authorization?

Authorization for collecting SSNs for passport operations is 26 USC 6093E, and 8 USC 1182 for Visa operations.

(c) How is the information collected?

Information is imported from an Adobe (.pdf) form completed by the applicant (applicants are either foreign nationals desiring employment or locally employed staff initiating the re-certification process) and updated as required by Department personnel at Post assigned the responsibility of updating RESOLVE. Data entry/import into the RESOLVE software portal (front-end) automatically results in population of the exact same information into the RESOLVE database (back-end). Information is also obtained by Foreign Service National Investigators and Regional Security Officers from public and government sources.

(d) 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.

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

The investigative process includes review of existing documentation and the use of questionnaires and interviews (person-to-person and/or telephonic) which employ variations of the same line of questions to ensure referential integrity. This is supported by experienced personnel who provide their perspectives and flag specific areas of interest/concern.

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

All personnel are required to accomplish re-certification at a pre-determined interval per authoritative guidance. This ensures that information remains current.

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

Yes, information may be obtained from commercial sources. Yes, some information may be publically available.

(h) Is notice provided to the individual prior to the collection of his or her information?
Yes. A notice similar to the writable Adobe (.pdf) form currently titled Overseas Vetting Questionnaire (OVQ) is provided in the opening pages of the SF-86 each applicant is asked to complete to begin the vetting process. The opening pages of the OVQ explain who should complete the OVQ, the types of information being gathered, and why and what happens if the OVQ is determined to be incomplete or incorrect during the background investigation.

(i) 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?
By completing the Adobe (.pdf) form or providing answers during the interview process, applicants provide consent.
- If no, why are individuals not allowed to provide consent?
Not applicable

(j) How did privacy concerns influence the determination of what information would be collected by the system?
Information captured in RESOLVE is the absolute minimum amount and types of information allowable for the purpose of issuing a security certification.

5. Use of information

(a) What is/are the intended use(s) for the information?
The information maintained in RESOLVE system consists of information necessary for vetting and adjudication of foreign national applicants to include performing background checks of applicants.

(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. The system is designed to facilitate the adjudication and vetting of foreign national applicants for each post globally. The use of contact information is consistent with the need to perform the adjudication process for applicants. The information available is relevant to the purpose of RESOLVE. The personal information collected is used by the system for vetting and adjudication of foreign national applicants.

(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.

RESOLVE does not share any information with any other systems. Background investigations are conducted on each foreign national applying for U.S. employment. Background investigations are also conducted for locally employed staff members on a regular recurring basis. Background investigations include a local law enforcement check to determine the applicant's local or international criminal history. To accomplish the law enforcement check a DS worker personally contacts a local law enforcement office to determine the applicant's local or international criminal history. To ensure the person being checked by local law enforcement is the same person as our applicant the DS worker presents a limited amount of information (based on information contained in the OVQ) (example: name and date of birth) to the local law enforcement representative.

Internal information sharing is conducted between workers at different posts when it is more efficient/cost effective to ask a local worker to complete a task rather than dispatch a worker to a distant location to perform the task. In these instances all of the workers involved already have access to RESOLVE.

(b) What information will be shared?

A limited amount of information is accessible to other postings (work locations) around the globe. More specifically, Name, Address, Phone, criminal background responses received from local and international law enforcement to determine local or international law criminal history.

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

The purpose is to increase the situational awareness between and among the organizations who comprise the community of interest to include local Post law enforcement to determine local or international law criminal history.

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

Information collected and stored by RESOLVE is not shared with any other automated system. As part of each applicant's background investigation a DS employee personally contacts a local law enforcement office to determine the applicant's local or international criminal history. To ensure the person being checked by local law enforcement is the same person as our applicant, the DS employee provides a limited amount of information (based on information contained in the OVQ) (example: name and date of birth) to the local law enforcement representative. No other information is shared. The process is not a formal one. Information is collected from the OVQ form and provided to local law

enforcement verbally or by informal means such as Name and ID number written on paper. No formal form or report is generated from the RESOLVE system and provided to local law enforcement.

(e) What safeguards are in place for each internal or external sharing arrangement?
External information sharing safeguards: RESOLVE does not share information with any external systems. Local law enforcement checks are limited in scope such that as much as possible the same workers provide and receive the information needed to complete the checks and only the absolute minimum amount of information is provided such as Name and ID number. Internal information sharing safeguards: Internal information sharing is conducted between workers at different posts when it is more efficient/cost effective to ask a local worker to complete a task rather than dispatch a worker to a distant location to perform the task. In these instances all of the workers involved already have access to RESOLVE. Internal information sharing is accomplished with the following safeguards. A number of management, operational and technical controls are in place to reduce and mitigate the risks associated with information sharing and disclosure including, but not limited to, annual security training, separation of duties, least privilege and personnel screening.

(f) What privacy concerns were identified regarding the sharing of the information? How were these concerns addressed?
It is possible for a Department employee to use his or her access to this information to retrieve contact information on an individual and use the information in an unauthorized manner. In order to mitigate this risk, all Department employees are required to undergo computer security and privacy awareness training prior to accessing OpenNet (through which information is shared) and must complete refresher training yearly in order to retain access. In an effort to protect the privacy of an applicant, only the minimum amount of PII is provided to local law enforcement consisting of Name and equivalent SSN. Information provided informally by means of written information on paper are maintained and destroyed by DS employees conducting background checks. Formal documents consisting of extensive PII data are not provided.

7. Redress and Notification

(a) What procedures allow individuals to gain access to their information?
Individuals do not have access to their information after they submit their OVQ. There are no procedures in place for individuals to access their information after the initial interview and submission in OVQ.

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

If yes, explain the procedures.

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 22 C.F.R. Part 171.

Redress and notification for correcting inaccurate or erroneous information occurs during initial and/or follow-up interviews with the applicant. RESOLVE authors collect references and contact information for adjudication of applicants.

If no, explain why not.

(c) By what means are individuals notified of the procedures to correct their information?
There are no procedures for individuals to be notified to correct their information.

Notice is provided at time of collection but individuals are entitled to avail themselves of the procedures outlined in 22 C.F.R. Part 171 in order to seek redress of their own information.

8. Security Controls

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

RESOLVE users must first authenticate to the OpenNet. The RESOLVE system uses role based access controls and limits users to specific roles at specific locations. The system employs the use of SSL for all application interactions.

The following Department of State policies establish the requirements for access enforcement.

- 5 FAM 731 System Security (Department computer security policies apply to Web servers)
- 12 FAM 622.1-2 System Access Control
- 12 FAM 623.2-1 Access Controls
- 12 FAM 629.2-1 System Access Control
- 12 FAM 629.3-3 Access Controls

(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.

RESOLVE users must first authenticate to the OpenNet. RESOLVE also requires an official approved user account to gain system access.

Additionally, a system use notification ("warning banner") is displayed before log-on to the network is permitted that encompasses the restrictions on the use of the system. Activity by authorized users is monitored, logged, and audited.

Non-production uses (e.g., testing, training) of production data are limited by administrative controls.

Only authorized users with post supervisor approval are permitted access to the application.

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

The Bureau of Diplomatic Security (DS) uses an array of configuration auditing and vulnerability scanning tools and techniques to periodically monitor the OpenNet-connected systems that host DS's major and minor applications, including the RESOLVE components, for changes to the Department mandated security controls.

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

All users are required to undergo computer security and privacy awareness training prior to accessing the system, and must complete refresher training yearly in order to retain access.

(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.

RESOLVE is protected from unauthorized access by an application specific access control list (ACL) that only allows approved users to add and change data.

As an OpenNet application, RESOLVE is protected by the general and inherited security controls already in place in addition to the ACL. There are numerous management, operational, and technical security controls in place to protect the data, in accordance with the Federal Information Security Management Act (FISMA) of 2002 and the information assurance standards published by the National Institute of Standards and Technology (NIST).

These controls include regular security assessments, physical and environmental protection, encryption, access control, personnel security, identification and authentication, contingency planning, media handling, configuration management, boundary and information integrity protection (e.g., firewalls, intrusion detection systems, antivirus software), and audit reports.

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

The inherited security measures above are standard for all Bureau of Diplomatic Security (DS) systems installed on the unclassified network. RESOLVE is installed on the unclassified network, and therefore inherits the aforementioned security measures by default.

The specific use of an ACL for RESOLVE on top of the standard security measures was influenced by the need to limit access only to authorized personnel. Only necessary personnel on the DS unclassified network requires access and has access to RESOLVE. Limiting user access limits damage that may result from unauthorized changes and use of system data.

9. Data Access

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

Embassy/Consulate workers posted to the different locations around the globe will have access to data in RESOLVE if their work (functional role) requires them to have access to that data. This role-based approach to limiting access is enforced by the RESOLVE software. In addition to this the RESOLVE software avoids a potential insider threat by blocking any user's access to data associated with their own background investigation. Examples of the Embassy/Consulate workers involved include: the RSO (Regional Security Officer), Assistant RSO, and Foreign Service National Investigators (FSNI).

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

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. Separation of duties is implemented within RESOLVE where personnel with the User Administrator role cannot edit information contained in the system and can only modify the permissions of RESOLVE users at their post.

(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.

Users will have specific access rights based on the work their assigned role must perform within the system. These roles as physically assigned within RESOLVE by User Administrators. Personnel with the User Administrator's role cannot edit information contained in the system and can only modify the permissions of RESOLVE Users at their post.

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

The system enforces role based access that dictates the task level and geographic level of system access. For example, Authors for London cannot misuse their access to update the applicants of Tokyo.