RPC START & AWS PIA

1. Contact Information

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

2. System Information

(a) Name of system: (i) Refugee Processing Center START (RPC START)

(ii) Refugee Processing Center Amazon Web Services Government Cloud (RPC AWS GovCloud)

(b) Bureau: Bureau of Population, Refugees, and Migration (PRM/A)

(c) System acronym (i) START

(ii) RPC AWS

(d) iMatrix Asset ID Number: (i) 301046 (START)

(ii) 308235 (RPC AWS)

(e) Reason for performing PIA:

☒ New system

☐ Significant modification to an existing system

☐ To update existing PIA for a triennial security reauthorization

(f) Explanation of modification (if applicable):

3. General Information

(a) Does the system have a completed and submitted Security Categorization Form (SCF)?

☒Yes

☐No - Contact IRM/IA at IASolutionCenter@state.gov for assistance.

The Security Categorization Form (SCF) for START has been completed in the Xacta assessment tool as part of the initial security assessment initiative.

The SCF will be completed in Xacta for the RPC AWS system once the security assessment commences.

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

The systems are currently in the process of an initial security assessment and accreditation. The A&A for START is currently scheduled for September 2020 and the A&A for RPC AWS is currently scheduled for August 2020.

(c) Describe the purpose of the system:

START and **RPC AWS** are the two component systems being developed as Next-generation case management system for the United States Refugee Admissions Program (USRAP) managed by the Bureau of Population, Refugees, and Migration (PRM). Both systems are on two separate platforms and function independent of each other, but are both covered in this PIA because START will be hosted within a ServiceNow cloud instance (as a SaaS) with automated testing support, reporting, and ancillary infrastructure services provided by RPC AWS. START's database (within the ServiceNow instance) will be automatically synced to a data lake hosted within RPC AWS.

START

The START application is a standardized electronic case management system that is the successor to the Worldwide Refugee Admissions Processing System (WRAPS) application. START is primarily used by case processors at the Refugee Processing Center (RPC) and overseas Resettlement Support Centers (RSC) to facilitate the tracking and processing of cases through the USRAP and resettlement processing. The general functions of START includes entry of biographic information, security check requests, and tracking of cases at the individual and aggregate level.

Other users include authorized individuals at PRM and other USG partners. The START application interfaces with key USG partner systems to facilitate security vetting and adjudication of refugee status, as well as key non-governmental organization (NGO) partners to receive refugee case referrals, process related applicant information, and facilitate tasks required for resettlement including medical, travel, and assurance. Application interface partners include DOS Bureau of Consular Affairs, DHS U.S. Citizenship and Immigration Services (USCIS), the United Nations High Commissioner for Refugees (UNHCR), the International Organization for Migration (IOM), and NGOs operating under grant/authority of PRM.

RPC AWS

The RPC AWS system provides additional support to the START application. START will require deployment of instances, supporting tools and development, management, security and production virtual private clouds (VPCs) in the RPC AWS GovCloud region. RPC AWS facilitates reporting and statistical analysis of refugee data as collected in the START application, and serves as a data sharing vehicle with several of the key partners named above. Access to the RPC AWS is provisioned on an as needed basis, and access to the START application does not guarantee access to the RPC AWS or vice-versa. Key users to the RPC AWS include users at the RPC, RSCs, USG partners and NGO partners.

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

START

START collects, uses and maintains PII for all refugee applicants who applied or were referred for resettlement to the United States including cases that were resettled to the United States, as well as cases that were denied, withdrawn, or closed while they were still in other countries overseas. START also contains PII about anchor relatives and/or U.S. ties already located in the U.S.

START contains and maintains the following PII about refugee applicants, who are non-U.S. persons:

- biographic information: name, gender, date of birth, place of birth, identification documents;
- nationality, ethnicity, and religion;
- family relationships: parents, spouses, siblings and children (including marriage, divorce, and foster and adoption information);
- Alien Number;
- biometric information such as height, weight, color of eyes and hair in addition to a photo of each applicant (Note: START will not store any fingerprint, iris, or facial recognition biometrics);
- information about significant medical conditions;
- persecution claim information from the applicant and information about the situation in the country of first asylum;
- Persecution claim information from the UN High Commissioner for Refugees (UNHCR);
- Results of DNA testing;
- Employment history;
- Education history;
- Contact information (telephone numbers, physical addresses, email addresses) for last ten years;
- Results of security checks on applicants; and
- Results of DHS/USCIS interviews on applicants.

START may contain the following information about relatives of the refugee applicant (parents, spouses, siblings and children), who are U.S. persons, and/or U.S. ties:

- biographic information: name, date of birth, gender, place of birth, marital status, identification documents;
- contact information: telephone numbers, physical address and email addresses;
- overseas case number;
- alien number;
- immigration or refugee processing numbers/documents;

- family relationships; and
- Results of DNA testing.

START may contain PII from other family members listed by a principal applicant or an anchor relative. Some of these individuals may be U.S. persons. Such family members may include parents, step parents, foster parents, spouses, children, brothers, sisters including adopted, foster, or step children. The PII of these other family members may include biographic information such as name, telephone numbers, physical addresses, email addresses, gender, and date of birth, place of birth, marital status, place and date of marriage, as well as date of the termination of a marriage.

RPC AWS

RPC AWS maintains refugee case and application information as collected by START to enable statistical analysis and reporting of refugee data. RPC AWS also provides the capability to collect the types of PII as described above from authorized partners such as the UNHCR and other NGOs to inform the creation and processing of refugee cases. This data is collected and entered into START, transferred to RPC AWS, and removed from RPC AWS when it is no longer needed.

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

- 8 U.S.C. 1157, Annual admission of refugees and admission of emergency situation refugees.
- 8 U.S.C. 1522(b), authorization for programs for initial domestic resettlement of and assistance to refugees.

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

☒Yes, provide:

- SORN Name and Number: State-59, Refugee Case Records
- SORN publication date (found under the Volume Number and above the Public Notice Number on the published SORN): Monday, February 6, 2012

☐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.

- The SORN requires update due to system moving to a cloud environment. It will be submitted to the Privacy Office to account for cloud storage and administrative changes.

(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)): (A-25-003)
- Type of information retained in the system: Biographic and DNA test results (see Question 3d for complete list)
- Length of time the information is retained in the system: All Records are currently retained and stored on premise at the RPC location: Retained online for at least five (5) years after the refugee's arrival in the United States or case was inactivated, and then transfer to offline storage. Retain offline for ten (10) years. Delete when fifteen (15) years old.

Once transition from legacy WRAPS system is completed; all records would be retained and stored on START and RPC AWS.

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

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

- If yes, under what authorization?

N/A, The system does not collect social security numbers

(c) How is the information collected?

START

All information is received in electronic format and either uploaded to START or entered into the system by a User. The information is submitted by various sources as outlined by the Report to Congress on Proposed Refugee Admissions for a given fiscal year. The

various sources of information outlined in the Report to Congress include UNHCR, NGOs, and National Visa Center for Follow-To-Join (FTJ) refugee applicants. Refugee applicants also provide the information directly to case workers at RSCs and the case workers enter it into the system.

Persons who are admitted to the United States as a refugee or granted asylum in the U.S. may submit the DS-7656 for their qualifying family members to gain access to the P-3 Family Reunification Category of the USRAP. Eligible P-3 nationalities are determined annually by the President and specified in the annual Report to Congress on Proposed Refugee Admissions. Once access is gained to the P-3 program, RSC caseworkers interview the applicant directly and enter applicant information into START.

Additional information is added to START by implementing partners of the USRAP in accordance with Cooperative Agreements, MOUs and/ or ISAs. The additional information can include security vetting results from Intelligence Community (IC) partners, medical information from the International Organization for Migration (IOM) and domestic, non-profit organizations related to placement locations in the US.

The START application will maintain the record of refugee applications and related documents in electronic form, even if those applications were first completed in physical form**.** The case workers enter the information into the system.

RPC AWS
RPC AWS does not receive, process or store any paper files on applicants. START's database (within the ServiceNow instance) will be automatically synced to a data lake hosted within RPC AWS.

(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.

START
START is hosted in the ServiceNow GovCommunityCloud (GCC) cloud hosted offering which is a FedRAMP High / Department of Defense (DoD) Impact Level 4 (IL-4) certified environment. ServiceNow implements NIST approved encryption modules to ensure protection of data at rest and in transit. ServiceNow's datacenters are included within the ServiceNow security authorization boundary.

RPC AWS is housed in Amazon Web Services (AWS) GovCloud, which is an isolated AWS data center region designed to host sensitive data and regulated workloads in the cloud and meet U.S. government compliance requirements. AWS GovCloud customers can run sensitive workloads in the region, which adheres to strict regulatory standards, including U.S. International Traffic in Arms Regulations (ITAR) regulations, Federal Risk and Authorization Management Program (FedRAMP) requirements and Department of Defense (DoD) Cloud Computing Security Requirements Guide (SRG) Levels 2 and 4.

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

Standard operating procedures are in place both overseas and domestically to ensure the accuracy of refugee applicants' records. Resettlement Support Centers (RSC) caseworkers conduct "pre-screening" interviews for all refugee applicants where the caseworker will go through each piece of information on the application and confirm its accuracy with the applicant, as well as solicit further information needed for resettlement processing.

RSC and RPC caseworkers also request refugee applicants overseas and anchor family members in the U.S. to provide documentation that corroborates the information they provided verbally.

Additionally, the START and RPC AWS applications will have built in validations to ensure data integrity is maintained for all data collected. Quality control measure and Standard Operating Procedures (SOPs) are used both at the Refugee Processing Center as well as Resettlement Support Centers to ensure the accuracy of information collected.

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

Yes, caseworkers will update applicant information in START as necessary throughout the resettlement process and the information will flow to RPC AWS during data replication. Refugee applicants are encouraged in all stages of resettlement processing to provide any new or updated information to the RSC, as it is available. This includes new births in the family, deaths, marriages, divorces, changes in addresses and phone numbers, and other changes to the refugees' biodata.

In addition, the status of a case is updated automatically as a case moves through the approval cycle and security checks. Security checks are required to be re-run for any changes to core bio-data and/or family information, at any point in the process.

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

START and RPC AWS does not use commercial or publicly available information. Refugee applicant PII is not available to the public at any stage of resettlement processing.

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

Each applicant to the USRAP who is fourteen years or older is asked to sign a notice of confidentiality, per current State Department Privacy guidance. This notice informs applicants of entities or persons with whom information will be shared and for what purposes.

Anchors who seek admission of family members under the USRAP P-3 Program file the Affidavit of Relationship (AOR), DS-7656, which includes a Privacy Act statement outlining the purposes of the information collected and with whom it may be shared. General notice to the public about the routine uses for these records under the Privacy Act is provided through publication of System of Records Notice State-59 in the Federal Register.

(i) Do individuals have the opportunity to decline to provide the information or to consent to particular uses of the information? Yes _X___ No ____

- If yes, how do individuals grant consent?

Information is voluntarily provided by refugee applicants, anchor relatives, and, with their consent, by family members and other designated agents. Failure to provide the information may result in the inability to move forward with, and eventual denial of, refugee admission to the United States.

All applicants 14 years and older sign a Notice of Consent which details how their information can be used.

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

(j) How did privacy concerns influence the determination of what information would be collected by the system?

RSC and RPC caseworkers collect the minimum amount of PII from refugee applicants in order to successfully complete refugee processing. START and RPC AWS store the information currently being collected in order to ensure DHS/USCIS has the requisite information to adjudicate a refugee claim and security vetting partners have the needed PII to run security checks. Further, the personal information provided for refugee

admission is used in a limited manner. Dissemination of refugee applicant data is highly restricted under Department and PRM regulations.

5. Use of information

(a) The intended use(s) for the information is/are:

The information gathered is used to determine the eligibility of individuals for admission to the U.S. under the USRAP and, if eligible, to provide initial resettlement services in the U.S. to the applicant. This information is used by the Department of Homeland Security, United States Citizenship and Immigration Services (DHS/USCIS) to make a status determination of the refugee applicant's eligibility for resettlement and includes pertinent biographical information necessary for placement and resettlement in the U.S.

(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 information is collected for the purposes of determining if an applicant should be admitted to the United States and for the provision of initial domestic resettlement of and assistance to refugees. The information provided may, in certain limited circumstances, be released to other government agencies (federal, state and/or local), when there has been a demonstrated need for disclosure, such as for purposes of investigation or legal action on criminal matters, or in connection with issues arising from the adjudication of benefits.

(c) Does the system analyze the information stored in it? Yes _X__ No ___

If yes:

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

Statistical methods are used by both applications to generate standard and ad hoc reports for U.S. Government purposes and partner agencies. New statistical reports may show numbers of refugee applicants at any stage in the resettlement "pipeline," as well as those recently resettled. Reports also include those with confirmed or non-confirmed relationships based on the DNA results; however, these will be aggregate results without PII that distinguish individuals.

(2) Does the analysis result in new information?

No.

(3) Will the new information be placed in the individual's record? Yes ___ No _X__

(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 _X___

6. Sharing of Information

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

The information in both applications will be shared with the following:

Internal
Department of State Bureau of Consular Affairs
State Department Office of the Legal Adviser (L)

External
DHS Officers
Department of Health and Human Services (HHS), Office of Refugee Resettlement (ORR)
Center for Disease Control (CDC)
NGO and international organization partners, including the International Organization for Migration (IOM) and the UN High Commissioner for Refugees (UNHCR)
Department of the Treasury
U.S. Census
Department of Justice and courts
U.S. Congress
Other intelligence and law enforcement community vetting partners

(b) What information will be shared?

Internal

Biographic information on all applicants is checked against the Bureau of Consular Affairs' Consular Lookout and Support System (CLASS). Information on denied applicants (i.e., name, date of birth, citizenship, country of birth, aliases, and reason for denial) is entered into CLASS. No DNA information is exchanged with, or stored in, CA systems.

All case information may be disclosed to the Office of the Legal Adviser (L) for the purpose of seeking legal advice.

External

Biographic, educational, employment, and medical information may be disclosed to USG agencies and non-governmental resettlement agencies to ensure appropriate placement and resettlement services in the U.S.

Biographic, educational and employment information is shared with security vetting partners including but not limited to the National Counterterrorism Center (NCTC) and DHS/USCIS, while medical information is shared with HHS/ORR and CDC. Statistical and demographic information from these records may be disclosed to state refugee coordinators, ORR, health officials, and interested community organizations.

Arrival and address information may be disclosed to consumer reporting agencies, debt collection contractors, and the Department of the Treasury to assist in the collection of indebtedness reassigned to the U.S. Government under the refugee travel loan program administered by IOM.

(c) The purpose for sharing the information is:

The most common reasons for sharing the information include the following:

Internal

- Biographic information on all applicants is checked against the Bureau of Consular Affairs' Consular Lookout and Support System (CLASS) to determine whether there is certain "hit" information associated with it. Information about a denied applicant (i.e., name, date of birth, citizenship, country of birth, aliases, and reason for denial) is entered into CLASS.

External

- Biographic information on all applicants is also shared with security vetting partners to determine whether there is a potential match between the biographic information provided by the refugee applicant and any derogatory information in the security vetting partners' holdings.
- Biographic and medical information for all applicants is also shared with CDC and HHS/ORR, to ensure the medical examination overseas is complete, that there are no medical ineligibilities for resettlement, and to address any special medical needs following arrival.

- All case and applicant information is made available to DHS/USCIS officers in order to adjudicate refugee applicant cases, for fraud prevention purposes, and to conduct relationship and family tree research related to granting "following-to-join" applications or adjudication of other immigration benefits.
- NGO and international organization partners working under cooperative agreements with the Department have access to refugee information to facilitate the arrival and resettlement of refugees. Pursuant to these cooperative agreements, NGOs must handle the information in accordance with applicable U.S. law and PRM policy.
- IOM has access to basic biographical information and limited medical information needed to arrange transportation to the U.S., including departure and transit formalities.
- For cases it has referred to USRAP, UNHCR is provided with adjudication results to coordinate resettlement and protection activities.

Records may occasionally be disclosed for the following reasons:

- Limited case status information may be provided to Members of Congress if requested in writing.
- Information from START is provided to other Federal, State, and local government agencies having statutory or other lawful authority as needed for the formulation, amendment, administration, or enforcement of immigration, nationality, and other laws.
- Litigation by applicants or other parties

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

START

If required and approved to share information externally, ServiceNow leverages existing Department of State personal identity and authentication services to authenticate external users and limit access to just those organizations and individuals approved for access to the system and information

START Information is shared by secure transmission methods permitted by internal Department of State policy for the handling and transmission of sensitive but unclassified (SBU) information. DHS/USCIS partner offices and other USG security vetting partners have online inquiry access to START via the public internet.

Other users include authorized individuals at PRM and other USG partners. The START application interfaces with key USG partner systems to facilitate security vetting and adjudication of refugee status, as well as key non-governmental organization (NGO) partners to receive refugee case referrals, process related applicant information, and facilitate tasks required for resettlement including medical, travel, and assurance. Application interface partners include DOS Bureau of Consular Affairs, DHS U.S.

Citizenship and Immigration Services (USCIS), the United Nations High Commissioner for Refugees (UNHCR), the International Organization for Migration (IOM), and NGOs operating under grant/authority of PRM.

RPC AWS

If required and approved to share information externally, RPC AWS leverages existing Department of State personal identity and authentication services to authenticate external users and limit access to just those organizations and individuals approved for access to the system and information. They can also access specific data produced for them in RPC AWS using their authorized and approved access credentials. Specialized reports for USG and other partners website are accessible only to authenticated users and they are compartmentalized by specific user groups.

Other partners receive, upon request and approval by the RPC Director, refugee information through an encrypted email.

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

PRM/START maintains control over permissions for all information on the ServiceNow START application to ensure that only authorized personnel with a "need to know" have access to the information. Once the user no longer needs access to the information, the user's access permissions are removed.

For information shared with external users, START relies on IRM ServiceNow SSL/TLS encryption of all transmissions combined with multi-factor authentication of external user access to the information.

For information shared with external users, RPC AWS relies on IRM AWS GovCloud SSL/TLS encryption of all transmissions combined with multi-factor authentication of external user access to the information.

Memoranda of Understanding (MOU), as well as Interconnection Security Agreements (ISA) govern required safeguards for internal and external sharing. The MOUs detail access control and safeguards in accordance with DOS policies for protection of DOS data. Safeguards include only sharing information via secure exchanges and/or encrypted messages and role based Identity and Access Management (IAM). If any information is requested beyond the agreed-upon exchange mechanisms, the PRM/RPC Director must review the request against the relevant sharing arrangement and approve the request in writing. If the request goes beyond the current sharing arrangement with the specified party, PRM will consult the Department of State's Office of the Legal Adviser to determine how to handle the request.

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

Privacy is always a concern in sharing PII since it can lead to exposure and misuse. However, PRM has signed cooperative agreements or MOUs with all of the NGO and international organizations operating RSCs, ensuring complete compliance with statutes, and PRM and Department regulations and policies regarding data privacy and the security of refugee data. In addition, Department-wide and PRM agreements with UNHCR ensure the privacy of refugee information, including data received and transmitted back to that agency. DHS/USCIS operates under USG laws and regulations governing privacy, including for refugee applicant data. Security vetting partners have identified personnel who need to be granted access to START's and RPC AWS's information to carry out their official duties, and who are subject to the same USG privacy laws, regulations, and policies. The information provided to security vetting partners is limited to information they require to complete security vetting of refugee applicants prior to admission being granted to the United States. START and RPC AWS information is purged from vetting partners' systems based on the time specified in the MOUs with each partner.

For information that is shared with CA, the risk is negligible because authorized users of CLASS are subject to administrative and physical controls commensurate with system security categorization. Refugee refusal information may be used by consular officers to adjudicate visa applications in accordance with the stated authority and purpose for the information.

7. Redress and Notification

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

Individual refugee applicants are able to request a printed version of their application from PRM's overseas partners to verify information from the system. Record notices and amendment procedures for U.S. persons are published in System of Record Notices published in the Federal Register and in agency rules published at 22 CFR 171. Individual refugee applicants are also able to request their information through the FOIA process.

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

If yes, explain the procedures.

Individual refugee applicants can inform PRM's overseas partners of the need to correct inaccurate information. Refugee applicants inform these overseas partners of the error either by phone in some circumstances, in person, or via email. PRM partners can then make the correction directly in START

If no, explain why not.

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

Individuals are notified of the procedures to correct their information during the initial pre-screening interview with an RSC caseworker. Additionally, an RPC caseworker domestically may inform the anchor relative how they can access and amend their information should the individual be unable to do so.

8. Security Controls

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

Information in START and RPC AWS is secured at multiple levels – (1) Access is restricted to approved users by secure multifactor login, (2) Role-based access control to limit the access to data on need to know basis, (3) Exchange of information between the START, RPC AWS, NGOs and USG Partners is only via secure connections as defined in respective MOUs or ISAs. (4) START and RPC AWS are both located on government approved FedRamp Cloud Services (ServiceNow Cloud and AWS Government Cloud).

(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.

Access to the START application data and RPC AWS is governed by least privilege, separation of duties, and need to know principles. Role based access controls are implemented to ensure that access is mapped to the user's role and function. Specialized reports for USG and other partners on File Cloud Server Enterprise in RPC AWS are accessible only to authenticated users and they are compartmentalized by specific user groups.

Access to START and RPC AWS requires a unique user account, supervisor's approval and signed user access agreement before access is granted. The user access agreement includes rules of behavior describing the individual's responsibility to safeguard information.

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

Role based user access controls and system audit trails will be utilized to detect any unauthorized activity; a subset of activities and events by START and RPC AWSs authorized users will be logged and, audited periodically for suspicious activities. There is a planned implementation of near real-time monitoring of the START and RPC AWS's logs leveraging the SPLUNK SIEM tool.

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

START and RPC AWS users at the Refugee Processing Center (RPC) are required to participate in cyber security awareness training by the Department of State which covers the procedures for handling Sensitive but Unclassified information, including personally identifiable information. Annual refresher training is mandatory for all employees. Additionally, all employees are required to take the online privacy course PA459 – Protecting Personally Identifiable Information.

RSC management provides oversight and support to maintain a trained and knowledgeable workforce. RSC staff are briefed on the confidentiality of refugee data and instructed regarding proper handling procedures. This is enforced through signed Cooperative Agreements which include adherence to Department of State and USG policies. PRM provides additional policy guidance to RSCs through the USRAP manual which provides guidance on sharing refugee, records, data and information, through the Treatment of Refugee Records (TRR).

(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 _X_ No __
If yes, please explain.

The START application and RPC AWS are both located in FedRamp approved environments which allows both systems to inherit the commensurate level of security controls for encryption, and strong authentication procedures. All data transfer/exchange is achieved through encrypted connections and secure APIs connections. In addition, the system implements role-based access controls to implement the principles of least privilege, separation of duties, and need to know.

The START log in authentication web page is encrypted using Transport Layer Security (TLS) to provide authentication, privacy, and data integrity for all log on transactions.

The RPC AWS log in authentication through the AWS GovCloud Console is encrypted using Transport Layer Security (TLS) to provide authentication, privacy, and data integrity for all log on transactions.

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

Due to the sensitive nature of the information collected by START and RPC AWS, the systems implements role-based access controls to implement the principles of least privilege, separation of duties, and need to know.

The System Categorization Form was completed in DoS Xacta, which identified the system as Moderate impact level. The Control Selection Tool (NIST-800-53 guidelines) then indicated which controls must be implemented. The security measures detailed above follow the recommended system controls.

9. Data Access

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

Only authorized users directly involved in refugee processing or in technical support roles have access to START Application and RPC AWS. These include U.S. Government employees, selected international organization staff operating RSCs under an MOU with the USG, selected Reception & Placement agency employees and system administrators. Non USG employees have access to only the systems components that is required by their roles.

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

Access to START records is governed by user roles and privileges to ensure that users only access information that they need to know. Access is also governed by the Department's data sharing policy, in which user access is determined and approved by the system owner only after careful evaluation of the user and the need to access START. Access to RPC AWS is governed by user roles and privileges to ensure that users only access commensurate to the access required for their role.

All access requests must be approved by a senior manager at the RPC, senior management at an RSC, or authorized individuals at other US Government agencies. For other USG agencies, PRM sets a quota for the number of overall users they can maintain.

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

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

START and RPC AWS implements role-based access controls to implement the principles of least privilege, separation of duties, and need to know.

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

START and RPC AWS implements role-based access controls to enforce the principles of least privilege, separation of duties, and need to know. Further, audit trails deter users from inappropriately accessing or misusing the information.

A subset of activities and events by START and RPC AWS's authorized users are logged and audited periodically for suspicious activities. There is a planned implementation of near real-time monitoring of both START application and RPC AWS using the SPLUNK SIEM tool.