WRAPS PIA

1. Contact Information

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

2. System Information

(a) Name of system: Worldwide Refugee Admissions Processing System

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

(c) System acronym: WRAPS

(d) iMatrix Asset ID Number: 671

(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):

The WRAPS PIA was previously addressed under Refugee Processing Center General Support System (RPC-GSS); however, this PIA is limited to the WRAPS major application (MA) at the direction of PRM/IA, AODR.

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) has been completed in the Xacta assessment tool.

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

The system is operating under a triennial ATO, with an estimated A&A completion date of February 2020.

(c) Describe the purpose of the system:

The Worldwide Refugee Admissions Processing System (WRAPS) is the case management system for the United States Refugee Admissions Program (USRAP) managed by the Bureau of Population, Refugees, and Migration (PRM).

WRAPS was designed to create a standardized, globally linked case tracking system to more efficiently and effectively process the admission of refugees to the U.S. WRAPS has interfaces with governmental and non-governmental stakeholders including U.S. government (USG) vetting partners, U.S. Citizenship and Immigration Services (USCIS), United Nations (UN) organizations and Non-governmental Organizations (NGOs).

The general functions of WRAPS include entry of biographic information, security check requests, and tracking of cases at the individual and aggregate level. All data from the Refugee Processing Center (RPC) and external partners is entered directly into Resettlement Support Center (RSC) instances at the RPC using secure access and IPSec VPN tunnels or imported via the WRAPS Rsharenet portal. WRAPS also provides statistical analysis, and reporting to PRM via reports written in Tableau Report Writer.

The WRAPS application is a MA or Major System in ITAB that consists of custom-written software. It is used by refugee processing staff in Rosslyn, VA and at nine overseas sites.

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

WRAPS collects, uses and maintains PII of all applicants including those denied, withdrawn, whose applications have been closed, and those referred for resettlement to the United States and have been resettled.

WRAPS contains PII about refugee applicants in other countries and anchor relatives and/or U.S. ties already located in the U.S.

WRAPS 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, and facial marks in addition to a photo of each applicant (Note: WRAPS does 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;
- Social Security number;
- Contact information (telephone numbers, physical addresses, email addresses);
- Results of security checks on applicants; and
- Results of DHS/USCIS interviews on applicants;

WRAPS may contain the following information about anchor relatives, 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 and email address;
- Citizenship and immigration status;
- Overseas case number;
- Alien number;
- Social security number;
- Immigration or refugee processing numbers/documents;
- Family relationships; and
- Results of DNA testing.

WRAPS may contain PII from other family members listed by a principal applicant or an anchor relative. 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, phone number, email, gender, date of birth, place of birth, marital status, place and date of marriage, and date of the termination of a marriage.

The RshareNet.org website (a component of WRAPS) serves as a transit point for initial application information for refugees provided by UN High Commissioner for Refugees (UNHCR) offices via a secure link and by domestic resettlement agencies through family reunification programs. Active and non-active records are subject to the same security and privacy safeguards. All Records are retained and stored on premise at the RPC location.

(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 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:

- Schedule number (e.g., (XX-587-XX-XXX)): A-25-003
- Type of information retained in the system: Biographic and DNA test results
- Length of time the information is retained in the system: All Records are retained and stored on premise at the RPC location. Retain 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.

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 (SSNs), is the collection necessary?
☒Yes ☐No

- If yes, under what authorization?

- 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.

(c) How is the information collected?

Paper Forms

Priority 1 (P-1) refugees are referred by the UNHCR and/or selected NGOs, using the UNHCR Resettlement Registration Form (RRF). Priority 2 applicants can be referred by UNHCR or, for certain Iraqis and nationals in the former states of the Soviet Union, may apply directly for resettlement via an I-130 petition. Iranian religious minority applicants may also apply via their U.S. relatives for Priority 2 processing. U.S. embassies receive applications approved by USCIS for resettlement through the Follow-to-Join Refugee (FTJ-R) program. Afghan and Iraqi Special Immigrant Visa holders are eligible to apply directly for resettlement benefits.

Open Access Priority 2 (P-2) group referrals (in Iraq, the former Soviet States, and for Iranian religious minorities) allow individuals to seek access to the program on the basis of meeting designated criteria. Once the designation is in place, applicants may approach the program at any of the processing locations specified as available for the group to begin the application process. Applicants must demonstrate that they meet the specified criteria to establish eligibility for access to the USRAP, via application forms specific to the Priority 2 group.

Open Access Priority 2 (P-2) predefined group designation is a second kind of open access designation and is normally based on a UNHCR recommendation that lays out eligibility criteria that should apply to individuals in a specific location. Once PRM, in consultation with DHS/USCIS, has established the access eligibility criteria for the group, the referring entity (usually UNHCR) provides the biographical data of eligible refugee applicants for processing, using a shorter form referral application. Once an individual gains access to processing via a P-2 designation, all other processing steps are the same as for those referred under a P-1 designation, including individual pre-screening and USCIS interviews, and all security and medical checks.

For cases under the Priority 3 family reunification program (P-3 Program) of the U.S. Refugee Admission Program (USRAP), anchor relatives in the U.S. file the Affidavit of

Relationship (AOR), Form DS-7656, on behalf of their prospective Qualifying Family Members (QFMs) abroad to initiate their application to the USRAP for refugee resettlement to the U.S. AOR information is collected in person by resettlement agencies in the U.S., which work under cooperative agreements with the Department to assist persons in applying for their prospective QFMs to join them in the U.S.

Medical Information and DNA Results

Panel physicians receive U.S. immigration-focused training in order to provide examinations as required by the Centers for Disease Control and Prevention (CDC) and the Department of Homeland Security (DHS) U.S. Customs and Immigration Service (USCIS). An approved laboratory will provide tubes, packing materials, and instructions, which are forwarded to the RSC responsible for the case. The RSC works with the panel physician or International Organization for Migration (IOM) to arrange for the testing of the QFM, in accordance with laboratory instructions, and for shipment of the samples to the laboratory.

Persons who undergo DNA testing direct the laboratory conducting the test to send a paper report directly to the RPC. Different laboratories may have different reporting formats, but DNA testing results are typically issued by the lab as a one-page summary that lists the names of the persons tested, their dates of birth, test numbers, a comparison of "alleles" (genetic markers represented as a series of numbers), and a conclusion as to the probability that the anchor and applicant are biologically related. No other information about the applicant or anchor DNA is typically reported, and the DNA sample itself is not sent to the RPC.

An RPC staff member reviews the result, checks the appropriate box in the WRAPS electronic record to indicate whether or not a biological relationship is confirmed, and enters the test number, report date, and the name of the lab. The report is scanned into the WRAPS record, with the genetic marker (allele) information redacted, and is then destroyed. DNA samples taken overseas are in the possession of a designated RSC staff member in accordance with the chain-of-custody requirements of the laboratory until they are mailed to the U.S. by the RSC. No DNA samples are in the possession of PRM or the RPC. No genetic information about applicants is compiled or maintained in WRAPS.

Electronic Forms

Priority 1 (P-1) referrals from UNHCR and NGOs are submitted to the appropriate Regional Refugee Coordinator and Resettlement Support Center (RSC) for case processing and scheduling of the DHS/USCIS interview. UNHCR offices also electronically submit refugee applicants' information to RshareNet.org website. The

submissions are handled through a secure internet link between UNHCR and the RPC. RSCs are responsible for accepting the electronic submission from UNHCR or an NGO and confirming the data's entry into the WRAPS application. PRM's Office of Admissions reviews referrals from U.S. Embassies for completeness before they are transmitted to RSCs for continued processing.

For Priority 3 applicants, most application forms from anchor relatives and/or U.S. ties may be completed and signed and then scanned for transmission to the RPC for further processing.

Other Sources

As part of the refugee adjudication and to maintain the security of the program and the United States, PRM obtains security check results for every applicant from a number of security vetting partners and law enforcement agencies. These results are received via the Department's Consolidated Consular Database (CCD), the Department of Homeland Security's Enterprise Service Bus or other conduits and then entered into WRAPS.

The WRAPS application and database maintain the definitive record of refugee applications and related documents in electronic form, even if those applications were first completed in physical form**.** The RPC does not receive or process any paper files on applicants. The RSCs receive and process only those documents required for the purpose of USCIS adjudications and review, as well as for the final travel packet.

(d) 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. RSC caseworkers conduct "pre-screening" interviews for all refugee applicants, which seek to confirm all of the information contained in the initial application form, whether that application is a UNHCR resettlement referral, NGO resettlement referral, or an application made by the refugee under a Priority 2 access program. For Priority 3 cases, DNA test results will only be accepted from approved laboratories in the U.S. For traceability, information entered in WRAPS includes the result of the testing, the test number, the date of the report, and the name of the laboratory that conducted the test. In a pre-screening interview, the RSC 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. Domestically, caseworkers at the RPC work with resettlement agencies to ensure that any discrepant information supplied on the AOR is clarified. Both RSC and RPC caseworkers request refugee applicants overseas and anchor family members in the U.S. to provide documentation that corroborates the information they provide verbally. Both RSC and RPC Caseworkers review marriage certificates, birth certificates,

passports, baptismal certificates, and similar documents, and RPC caseworkers domestically also examine I-94 forms, arrival-departure records, and green card or citizenship records. Following the completion of a pre-screening interview, DHS USCIS officers interview every refugee applicant. USCIS officers review the information that the RSC has collected and the results of security screening processes and conduct an in-person interview with each refugee applicant before deciding whether to approve him or her for classification as a refugee.

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

Yes, caseworkers update applicant information in WRAPS as necessary throughout the resettlement process. 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.

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

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

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

Each applicant to the USRAP 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 AOR, 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 is provided through publication of System of Records Notice State-59 in the Federal Register.

Priority 3 anchors also must sign an acknowledgment that they understand that they and QFMs may be requested to submit DNA evidence to verify claimed biological relationships; that they will submit DNA evidence at such time it is requested; and that

they will pay all necessary fees associated with that expense and the expenses associated with the submission of DNA evidence of QFMs.

Prior to collecting a DNA sample, the RSC will provide notice to QFMs explaining that DNA will only be used for the purpose of establishing a claimed biological relationship, and that DNA will be sent to the laboratory for analysis and not kept by the U.S. Government. The QFMs sign the form acknowledging that the RSC has explained the purpose of DNA testing.

(h) 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.

If individuals provide information, they have no right to consent to limits on its use.

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

(i) 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. WRAPS stores 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. It is not used for any other purposes and is not provided to organizations not involved with making an admission determination or providing initial resettlement services. Therefore, the use is consistent with the purpose for which the system was designed.

(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 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 will be shared with the following:

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

External
DHS/USCIS Officers
Department of Health and Human Services (HHS), Office of Refugee Resettlement (ORR)
Center for Disease Control (CDC)
NGO and international organization partners, primarily the International Organization for Migration (IOM) and the UN High Commissioner for Refugees (UNHCR)
Department of the Treasury
Member of Congress
Federal, State, and local government agencies
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.

Biographic, education, employment, and medical 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. No DNA information is exchanged with, or stored in, CA systems.

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.
- DHS/USCIS officers have access to WRAPS records 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 WRAPS 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?

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. CLASS information is uploaded directly into CA systems through Telecommunications Manager (TCM). Biographic information on applicants is shared with security vetting partners via a secure FTP exchange.

DHS/USCIS partner offices and other USG security vetting partners have online inquiry access to WRAPS by means of a secure internet link. They can also access specific data produced for them via RshareNet. Specialized reports for USG and other partners on RshareNet.org 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?

Several Memoranda of Understanding (MOU) 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 Advisor 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 regarding data privacy and the security of refugee data. In addition, Department-wide and PRM agreements with UNHCR ensure the privacy of refugee 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 WRAPS information to carry out their official duties, and who are subject to the same USG privacy laws and regulations. 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. WRAPS' 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 request a printed version of their application to verify information from the system. Record notice and amendment procedures for U.S. persons are published in Privacy Act notices published in the Federal Register and in agency rules published at 22 CFR 171.

(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 WRAPS.

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 (the STATE-59 SORN).

8. Security Controls

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

Information in WRAPS is secured at multiple levels – (1) Access is restricted to approved users by secure log in and password, (2) Role-based access control to limit the access to data on need to know basis, (3) Exchange of encrypted information between the RPC and RSC partner systems through Virtual Private Network using IPSec protocol, (4) Production databases located in secure data center accessible only to authorized personnel.

(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 WRAPS application data is governed by least privilege, separation of duties, and need to know principles. Role based access controls are implemented to ensure access to the WRAPS application is mapped to the user's role and function. Specialized reports for USG and other partners on RshareNet.org website are accessible only to authenticated users and they are compartmentalized by specific user groups.

Access to WRAPS application and database requires a unique user account, superior's approval and each authorized user must sign a 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 are utilized to detect any unauthorized activity; a subset of activities and events by WRAPS' authorized users are logged on the WRAPS Database and, audited periodically for suspicious activities. There is near real-time monitoring of the WRAPS server and Database using SPLUNK SIEM tool.

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

WRAPS 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 and Department of State policies such as, The RSC Program announcement 2018-09; Guidance on sharing refugee, records, data and information and Treatment of Refugee Records (TRR) documents.

(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 WRAPS infrastructure is secured via an enterprise level security appliance (firewall) and all communications is encrypted with Transport Layer Security (TLS) to prevent any unauthorized access to the RPC information assets.

The data exchange between the RPC and its RSC partners is accomplished via secure VPN links. The data in transit is encrypted through an IPSec protocol.

In addition, the system implements role-based access controls to implement the principles of least privilege, separation of duties, and need to know. Per DOS guidelines, RPC implements Transparent Data Encryption (TDE) for all data at rest.

RshareNet.org is accessed by authorized users. Authorized users are authenticated by the website using their user ID and password. All communication between RshareNet.org and the authenticated external users' client browsers is encrypted using Transport Layer Security (TLS).

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

The WRAPS application uses a SQL-compliant relational database solution to store and maintain electronic records of refugee applicants. Due to the sensitive nature of the information collected by WRAPS, the system 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, 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 WRAPS Application. These include U.S. Government employees, selected international organization staff operating RSCs under an MOU with the USG, selected reception and placement agency employees and system administrators.

Non-USG employees have access to only the systems such as WRAPS, Tableau Report Writer and Rsharenet as required by their roles. They do not have access to other components of RPC such as email.

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

Access to WRAPS 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 WRAPS.

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.

No. WRAPS 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?

WRAPS implements role-based access controls to implement 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 WRAPS authorized users are logged on the WRAPS Database and, audited periodically for suspicious activities. There is near real-time monitoring of the WRAPS server and Database using SPLUNK SIEM tool.