Email the completed PIA to
PIAteam@state.gov

RPC-GSS PIA

1. Contact Information

A/GIS/IPS Director
Bureau of Administration
Global Information Services
Office of Information Programs and Services

2. System Information

(a) Name of system: Refugee Processing Center General Support System

(b) Bureau: PRM/A

(c) System acronym: RPC – GSS

(d) iMatrix Asset ID Number: 5880

(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 Security Categorization Form (SCF) has been modified to reflect that the GSS has two child systems (ITAB 671-WRAPS and ITAB 2580-WRAPSnet).

3. General Information

(a) Does the system have a completed and submitted Security Categorization Form (SCF)?
_X__ Yes ____ No

(b) What is the security Assessment and Authorization (A&A) status of the system?
The A&A for RPC-GSS is currently underway and has an estimated date of completion of September 2016.

(c) Describe the purpose of the system:

The RPC General Support System consists of the RPC computing and network infrastructure for the Worldwide Refugee Admissions Processing System (WRAPS) application, WRAPSnet.org website as well as the office support systems (like e-mail, phone, and fax). Most of the PII is collected via the WRAPS application, and a small percentage via WRAPSnet.org. The RPC-GSS

holds/maintains all the PII data collected by the WRAPS application and WRAPSnet.org in a secure database.

WRAPS is a Major Application composed of custom-written software, and is a child of the RPC-GSS. WRAPS is an electronic refugee resettlement case management system that links the Department of State Bureau of Population, Refugees and Migration (PRM) and its worldwide partners to facilitate the refugee resettlement process. WRAPS contains case information and tracks the processing of refugee applicants as they move through the required administrative steps up to arrival in the U.S.

WRAPSnet.org is also a child of the RPC-GSS, and is a public-facing website using commercial software as the content management system. WRAPSnet.org provides general information about the U.S. Refugee Admission program, updates on specific refugee programs for the U.S. Refugee Admission Program (USRAP) partners and statistical reports for refugee arrivals. This website provides a forum for authenticated users from PRM, DHS and other program partners to access dynamic reports and for RPC to electronically receive initial refugee application information from some United Nations High Commissioner for Refugees (UNHCR) offices via a secure link.

All three systems are managed as a single unit. All share the same system owner, physical location, management and operational staff, funding sources, and user base.

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

RPC-GSS maintains all PII. The WRAPS application collects, uses (processes) and disseminates PII, and WRAPSnet.org collects and disseminates PII.

RPC-GSS contains PII about refugee applicants in other countries and anchor relatives already located in the U.S.
WRAPS contains and maintains the following PII about refugee applicants:

- biographic information: name, gender, date of birth, place of birth, identification documents;
- nationality, ethnicity, and religion;
- family relationships;
- Alien Number;
- biometrics such as height, weight, color of eyes and hair, and facial marks;
- information about significant medical conditions;
- persecution claim and information about the situation in the country of first asylum; and
- results of DNA testing.

WRAPS may contain the following information from anchor relatives:

- 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 an anchor relative. Such family members may include parents, step parents, foster parents, spouses, children, brothers, and sisters. The PII of these other family members may include biographic information such as name, gender, date of birth, place of birth, marital status, place and date of marriage, and date of the termination of a marriage.

The WRAPSnet.org website serves as a transit point for initial application information for refugees provided by some UNHCR offices via a secure link and by Resettlement Agencies for family reunification programs. The PII included in the UNHCR electronic form and the DS-7699/7656 is a subset of the information included in WRAPS, which is detailed above. This information is imported into the RPC-GSS after quality checks. Once imported into RPC-GSS, this information is removed from the website.

(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 _X__ If 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 ___ If a SORN is not required, 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 __ X __

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 _X___ 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
- Length of time the information is retained in the system: Retain online for 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 a DNA test result is entered in RPC-GSS, and a copy of the DNA test result sheet with genetic marker (allele) information redacted is scanned into WRAPS, the actual laboratory test result sheet is shredded. According to the RPC-GSS retention schedule (A-25-003), the DNA information and all other records are kept online 5 years after the refugee arrives in the U.S. or until the case is closed. After 5 years, records are archived to an off-line system and kept another 10 years, then destroyed.

Active and non-active records are subject to the same security and privacy safeguards. The risk is mitigated by the fact that very few people at the RPC have access to DNA-related record fields. All other RPC-GSS users, overseas and domestic, have read only access. No genetic marker (allele) information is stored in RPC-GSS. Except in cases where DNA results are subsequently challenged, results are only used at the time of determination that the refugee applicant is eligible to apply to the Program and in the subsequent DHS adjudication. It is also conceivable that DHS could refer back to an individual's case file when adjudicating a future benefit for a family member in order to check if the file contains DNA testing results (negative or positive) between the individual and that family member.

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 _X___ 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

Refugee applicants are referred by UNHCR, NGOs, and U.S. embassies that receive applications for the Visa 93 program. In some cases, refugee applicants may apply directly to the program.

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. In addition, for cases under the Priority 2 Central American Minor (CAM) program, anchor parents in the U.S. can file the CAM AOR, Form DS- 7699, on behalf of their QFM minor child abroad. For both programs, 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.

On the AOR, the anchor relative is required to include information about him or herself and information about relatives in order to assist the Department in determining whether a prospective QFM is qualified to apply for access to the USRAP for family reunification purposes. Anchors also must sign an acknowledgment that they understand they and prospective QFMs may be requested to submit DNA evidence to verify the claimed biological relationships; that they will submit DNA evidence at the time it is requested; and that they will pay all necessary fees associated with that expense and the expenses associated with the submittal of DNA evidence of a prospective QFM. The voluntary agencies electronically submit the completed AORs to the Refugee Processing Center (RPC) for data entry, scanning, and case processing.

After the RPC creates a case in WRAPS, the Resettlement Support Center (RSC) responsible for the case commences pre-screening. Once pre-screening is completed, the RSC sends a letter to the anchor advising them that DNA testing is required, along with a fact sheet about DNA testing and a list of laboratories approved by the American Association of Blood Banks (AABB) in the U.S. where the testing must be done. Testing must be conducted in accordance with joint AMA-ABA Guidelines set forth by the AABB. Prior to conducting the DNA test, the RSC provides notice to prospective QFMs explaining that the DNA sample will only be used for the purpose of establishing a claimed biological relationship, that the DNA samples will be sent to the laboratory for analysis, and that the samples will not be kept by the U.S. Government. The prospective QFMs will sign the form acknowledging that the RSC has explained the purpose of the DNA testing.

DNA testing is done using cells from inside the mouth, which are collected with a cotton swab (buccal swab). DNA testing of anchor relatives is conducted in the U.S. at an approved lab. The testing of the QFM is conducted by an embassy-appointed panel physician or by the International Organization for Migration (IOM). A panel physician is a medically trained, licensed, and experienced doctor practicing overseas who is appointed by the local U.S. embassy or consulate. The IOM serves as the panel physician in many locations overseas.

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 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 Refugee Processing Center (RPC). Different laboratories may have different reporting formats, but DNA testing results are typically issued by the lab as a one-page summary that list 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 RPC-GSS electronic record to the effect that a biological relationship is confirmed or not confirmed, and enters the test number, report date, and the name of the lab. The report is scanned into the RPC-GSS 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 RPC-GSS.

The AOR and the results of the DNA test is sent to DHS USCIS for an initial review of claimed relationships by the Refugee Access Verification Unit (RAVU). Following completion of the RAVU review, RPC notifies the RSC that case processing can continue.

Electronic Forms

Since 2006, some UNHCR offices electronically submit refugee applicants' information to WRAPSnet.org website. The submissions are handled through a secure internet link between UNHCR and the RPC.

As part of the refugee adjudication, in relation to the security interests of the U.S., PRM obtains security check results for applicants from a number of security vetting partners and law enforcement agencies. These results are received via the Department's Consolidated Consular Database (CCD) or other conduit and then entered into RPC-GSS via WRAPS.

(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. Caseworkers in the U.S. work with anchor relatives to ensure that information supplied on the AOR is correct. Whenever possible, anchor family members in the U.S. and refugee applicants overseas are requested to provide documentation that corroborates the information they provide verbally. Form I-94, Arrival-Departure Records, green card or citizenship records, marriage certificates, birth certificates, passports, baptismal certificates, and similar documents are kinds that are reviewed both domestically and overseas. Each refugee applicant overseas has a face-to-face meeting with an RSC caseworker and DHS USCIS officers

to verify that the information on their record is correct. DNA test results will only be accepted from approved laboratories in the U.S. For traceability, information entered in RPC-GSS includes the result of the testing, the test number, the date of the report, and the name of the laboratory that conducted the test.

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

Yes, caseworkers update applicant information as necessary. In addition, the status of a case is updated automatically as a case moves through the approval cycle and security checks.

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

RPC-GSS does not use commercial or publicly available information.

(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 Section 222(f) of the Immigration and Nationality Act, which states that these records "shall be considered confidential and shall be used only for the formulation, amendment, administration, or enforcement of immigration, nationality, and other laws of the United States." 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 or CAM 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.

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 anchor relatives, refugee applicants, and, with their consent, by family members and other designated agents. Failure to provide the information may result in denial of refugee admission.

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?

RPC-GSS collects the minimum amount of PII from refugee applicants in order to successfully complete refugee processing. RPC-GSS needs to 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.

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 includes the status determination made by the Department of Homeland Security, United States Citizenship and Immigration Services (DHS/USCIS), records of the applicant's clearance for medical or security reasons, and 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?

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. 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 and partner agencies. New statistical reports may show numbers of refugee applicants 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:
Department of State Bureau of Consular Affairs
DHS/USCIS officers and other Intelligence Community vetting partners
Department of Health and Human Services (HHS), Office of Refugee Resettlement (ORR)
Center for Disease Control (CDC)
NGO and international organization partners
Department of the Treasury

(b) What information will be shared?

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

Biographic, educational and employment information is shared with security vetting partners including 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:

- Biographic information on all applicants is checked against the Bureau of Consular Affairs' Consular Lookout and Support System (CLASS) to determine whether there is a 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 stored in CLASS. No DNA information is exchanged with, or stored in, CA systems.
- 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 derogatory information in the security vetting partners' holding.
- Biographic and medical information for all applicants is also shared with HHS/ORR and CDC for any special medical needs.
- DHS/USCIS officers have access to RPC-GSS records for adjudication of refugee cases, for fraud prevention, 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 RPC-GSS 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.

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

Information is shared by secure transmission methods permitted by internal DoS 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 password-protected spreadsheets uploaded to a secure access controlled part of WRAPSnet.org website for security partners to access, as well as a secure FTP exchange.

DHS/USCIS partner offices and other USG security vetting partners have online inquiry access to RPC-GSS by means of a secure internet link. 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. 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, secure vetting partners have identified personnel who can access RPC-GSS information based on their official duties. 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. RPC-GSS 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, 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 verify information via forms that are printed from the system and signed. Record notice and amendment procedures 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 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 interview with PRM partners. Additionally, the STATE-59 SORN informs the anchor relative how they can access and amend their information.

8. Security Controls

(a) How is the information in the system secured?
Information in RPC-GSS 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 NGO 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.

Information in RPC-GSS is accessible to only authorized staff at the RPC who have undergone background security checks. The RPC implements role-based access controls to implement the principles of least privilege, separation of duties, and need to know.

The WRAPS application uses a SQL-compliant relational database solution to store and maintain electronic records of refugee applicants. WRAPS implements role-based access controls to implement the principles of least privilege, separation of duties, and need to know. Per DOS guidelines, the RPC is in the process of implementing Transparent Data Encryption (TDE) for data at rest.

Specialized reports for USG and other partners on WRAPSnet.org website are accessible only to authenticated users and they are compartmentalized by specific user groups.

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

User access controls and system audit trails are utilized to deter and detect any unauthorized activity.

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

All users must pass computer security and privacy awareness training prior to receiving access to the system and must complete annual refresher training 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 __X___ No ____
If yes, please explain.

The RPC-GSS infrastructure is secured via an enterprise level security appliance (firewall) with AES, DES, and Triple DES encryption to prevent any unauthorized access to the RPC information assets.

The data exchange between the RPC and its NGO 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 is in the process of implementing Transparent Data Encryption (TDE) for data at rest.

WRAPSNET.org is accessed by authorized users. Authorized users are authenticated by the website using their user ID and password. All communication between WRAPSNET.org and the authenticated external users' client browsers is encrypted using Transport Layer Security (TLS) 1.2.

Finally, the RPC is the process of implementing Multi-Factor Authentication (MFA) using SecurID protocol for access to the RPC work-stations as well as WRAPS application.

(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 RPC-GSS. These include U.S. Government employees, contractors, system administrators, and other authorized technical staff granted privileged access.

(b) Access to data in the system is determined by:

Access to RPC-GSS records is 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. Access to wrapsnet.org and WRAPS is governed by user roles and privileges to ensure that users only access information that they need to know.

All access requests must be approved by a senior manager at the RPC, or in some cases, other US Government agencies may request access for their staff. Those access requests are reviewed by WRAPS operations staff and approved by the RPC Director before access is granted.

(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.

RPC-GSS 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?

RPC-GSS 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.

Once the PII is in RPC-GSS, the system tracks changes made to a refugee record to ensure both accuracy and privacy protection. Managers periodically run audit reports to ensure that users are not performing unauthorized functions. RPC-GSS contains a warning banner that is compliant with Federal policy.