1. Contact Information

Department of State Privacy Coordinator
Margaret P. Grafeld
Bureau of Administration
Global Information Services
Office of Information Programs and Services

2. System Information

(a) Date PIA was completed: October 8, 2009

(b) Name of system: Report Management System

(c) System acronym: RMS

(d) IT Asset Baseline (ITAB) number: 726

(e) System description (Briefly describe scope, purpose, and major functions):

RMS provides an efficient means for the Office of Personnel Security and Suitability (DS/SI/PSS) offices to conduct background investigations (BIs) on candidates for positions that require security and suitability determinations and clearance updates.

RMS allows the DoS personnel assigned to a case to compile investigative data electronically on the subject of the investigations. RMS reduces the amount of time that it takes to receive case assignments and return reports of the investigation therefore reducing the time it takes for individuals to be granted a clearance.

(f) Reason for performing PIA:

☐ New system

☐ Significant modification to an existing system

☒ To update existing PIA for a triennial security re-certification

(g) Explanation of modification (if applicable): Certification & Accreditation

(h) Date of previous PIA (if applicable): October 2, 2008

3. Characterization of the Information

The system:

☐ does NOT contain PII. If this is the case, you must only complete Section 13.

☒ does contain PII. If this is the case, you must complete the entire template.

a. What elements of PII are collected and maintained by the system? What are the sources of the information?

RMS collects and maintains the following information on the subject of the investigation and may list some of the following information on any individuals that the subject may list

as points of contact during the investigation. This includes but is not limited to the subject's immediate family, neighbors, co-workers, and/or classmates:

- Name
- Phone Number
- Address
- Date of Birth
- Place of Birth
- Social Security Number
- Medical History
- Employment History
- Criminal History
- Credit History
- Citizenship Status
- Ethnicity
- National Origin
- Educational History
- Mother's Maiden Name

b. How is the information collected?

The information collected by RMS is obtained from the individual being investigated and the investigating officer. The information collected from the individual being investigated is provided through the use of the Standard Form (SF) 86, Questionnaire for National Security Positions and Standard Form (SF) 85, Questionnaire for Non Sensitive Positions. The level of sensitivity of the unclassified information accessed, processed, stored and transmitted on RMS is sensitive but unclassified (SBU). RMS processes privacy data as defined by the Privacy Act of 1974.

Information is also obtained National Agency Checks performed through the Federal Bureau of Investigation and manually fed into the system.

Tri Credit Bureau information is obtained through an electronic interface that supports a secure two-way transmission mechanism for the request of a credit checks on the subject and the return of the results of a consolidated, merged credit history report.

c. Why is the information collected and maintained?

The information collected and maintained by RMS is for the purpose of providing DS/SI/PSS and authorized DS personnel a more efficient means of conducting background investigations on subjects referred for security clearance and suitability determinations.

RMS allows the DoS personnel assigned to a case to compile investigative data electronically on the subject of the investigations. RMS reduces the amount of time that it takes to receive case assignments and return reports of the investigation therefore reducing the time it takes for individuals to be granted a clearance.

d. How will the information be checked for accuracy?

The individual being investigated is responsible for submitting true and accurate information. In addition, any agency or external source providing the information is responsible for verifying accuracy. Specific methodologies for verification employed by Diplomatic Security (DS) include, among other things, maintaining the system as a live feed and allowing the information to be updated/edited at any time.

Completeness of data will be checked through investigations and/or through personal interviews with the subject and sources holding the information.

e. What specific legal authorities, arrangements, and/or agreements define the collection of information?

The legal authorities as documented in STATE-36, Diplomatic Security Records, specific to RMS, are as follows:

- Pub.L. 99-399 (Omnibus Diplomatic Security and Antiterrorism Act of 1986, as amended;
- Pub.L. 107-56 Stat.272, 10/26/2001 (USA PATRIOT Act); (Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism); and
- Executive Order 13356, 8/27/04 (Strengthening the sharing of Terrorism Information to Protect Americans).
- Executive Order 12968, 8/2/95 (Access to Classified Information).
- Executive Order 10450, 4/27/53 (Security Requirements for Government Employment).
- ICND 704

f. Privacy Impact Analysis: Given the amount and type of data collected, discuss the privacy risks identified and how they were mitigated.

RMS collects the minimum amount of personally identifiable information necessary to conduct background investigations (BIs) on candidates for positions that require security and suitability determinations and clearance updates.

There are numerous management, operational, and technical security controls in place to protect the data, in accordance with the Federal Information Security Management Act of 2002 and the information assurance standards published by the National Institute of Standards and Technology. These controls include regular security assessments, physical and environmental protection, encryption, access control, personnel security, identification and authentication, contingency planning, media handling, configuration management, boundary and information integrity protection (e.g., firewalls, intrusion detection systems, antivirus software), and audit reports.

4. Uses of the Information

a. Describe all uses of the information.

The information is used to coordinate and facilitate all DS/SI/PSS investigative case actions. Storage and retrieval of previously obtained information is for reference purposes in determining an individual's suitability for access.

b. What types of methods are used to analyze the data? What new information may be produced?

Reports are associated with Management Oversight (the number of cases currently being worked and assigned to a specific Investigation Officer).

Analysis of the information is limited to non-record date-based statistical information, such as the number of cases entered, subject matter or action taken on an aggregate cycle (i.e., Monthly, Quarterly, Yearly, etc.).

c. If the system uses commercial information, publicly available information, or information from other Federal agency databases, explain how it is used.

Tri Credit Bureau information is obtained through an electronic interface that supports a secure two-way transmission mechanism for the request of a credit checks on the subject and the return of the results of a consolidated, merged credit history report. Currently Choice Point is the contract provider for this information. This tri credit report information is used to make an adjudicative decision based on 13 adjudicative guidelines outlined in Executive Order 12968 and ICND 704.

d. Is the system a contractor used and owned system?

RMS is a Government owned system which was primarily designed and developed by contractors. All contractors have abided to regulatory guidelines and have signed and follow DS's Rules of Behavior.

e. Privacy Impact Analysis: Describe the types of controls that may be in place to ensure that information is handled in accordance with the above uses.

RMS performs basic internal analytical functions on the PII but does not create new information about the record subject. Thus, there are adequate safeguards in place to preserve data accuracy or integrity and avoid faulty determinations or false inferences about the record subject, thereby mitigating privacy risk. There is also no risk of "function creep," wherein with the passage of time PII is used for purposes for which the public was not given notice. Based on these specific uses that do not create additional information about the record subject, there is minimal privacy risk.

5. Retention

a. How long is information retained?

The retention period of data is consistent with established Department of State policies and guidelines as documented in the Department of State's Disposition Schedule of Diplomatic Security Records, Chapter 11.

b. Privacy Impact Analysis: Discuss the risks associated with the duration that data is retained and how those risks are mitigated.

RMS collects and maintains names, phone numbers addresses, dates of birth, medical, employment, criminal, educational, and credit history information, social security numbers, citizenship information, ethnicity information, and national origins information. There are inherent risks associated with these types of information. In an attempt to mitigate these risks the Department of State has implemented numerous management,

operational and technical security controls in order to protect the information in accordance with the Federal Information Security Management Act of 2002 and the information assurance standards published by the National Institute of Standards and Technology. These controls include regular security assessments, physical and environmental protection, encryption, access control, personnel security identification and authentication, contingency planning, media handling, configuration management, boundary and information integrity protection (e.g., firewalls, intrusion detection systems, antivirus software) and audit reports.

6. Internal Sharing and Disclosure

a. With which internal organizations is the information shared? What information is shared? For what purpose is the information shared?

RMS is utilized by all organizations within Diplomatic Security that conduct background investigations for DS/SI/PSS (i.e. Regional Security Offices, Assistant Regional Security Officers and Field Investigators.) Only enough information is shared in order for the Investigator to ensure that all leads are scoped and conduct to fulfill the Adjudicative Guidelines as outline in EO 12968.

b. How is the information transmitted or disclosed? What safeguards are in place for each sharing arrangement?

Information is sent via leads to the specified individual within RMS. All users have a DS Secure Sites Login, a RMS Account Login, and access control constraints are put on the system using account types to ensure that individuals using the system do not access more information than is needed to complete their function.

c. Privacy Impact Analysis: Describe risks to privacy from internal sharing and disclosure and describe how the risks are mitigated.

It is possible for an employee with authorized access working for the Department of State to use his or her access to this information to retrieve PII on an individual and use this information in an unauthorized manner. In order to mitigate this risk all Department employees are required to undergo computer security and privacy awareness training prior to accessing RMS, through which the information is shared, and must complete refresher training yearly in order to retain access.

7. External Sharing and Disclosure

a. With which external organizations is the information shared? What information is shared? For what purpose is the information shared?

DS/SI/PSS currently holds a contract with Choice Point/West Government Services to obtain a Tri Bureau credit report. In order to obtain the correct report on the subject the following information is shared with Choice Point: Full Name, Home Address, Length of Time at Home Address, Date of Birth, and Social Security Number. DS/SI/PSS obtains written release to request this Tri Bureau report from the subject.

b. How is the information shared outside the Department? What safeguards are in place for each sharing arrangement?

Tri Bureau credit information is obtained through an electronic interface that supports a secure two-way transmission mechanism for the request of credit checks on the subject and the return of the results is a consolidated, merged credit history report. The security requirements for this transmission meet Federal Information Processing Standard (FIPS) 140-2. The Department currently utilizes a VPN Connection with ftp. The requested and return reports are in the Extensible Mark-up Language (XML), MISMO 2.3 format.

c. Privacy Impact Analysis: Describe risks to privacy from external sharing and disclosure and describe how the risks are mitigated.

The appropriate safeguards have been put into place to ensure that FIPS 14-2 is met and that there is no information disclosure to outside entities.

The risks associated with sharing privacy information externally and the disclosure of privacy information is generally higher than internal sharing and disclosure. Intentional and unintentional disclosure of privacy information from personnel can result from social engineering, phishing, abuse of elevated privileges or general lack of training. Transmission of privacy data in an unencrypted form (plain text), and use not secure connections are also a serious threat to external sharing. Numerous management, operational and technical controls are in place to reduce and mitigate the risks associate with external sharing and disclosure including, but not limited to formal Memorandums of Agreement/Understandings (MOA/MOU), service level agreements (SLA) annual security training, separation of duties, least privilege and personnel screening.

8. Notice

The system:

☒ Contains information covered by the Privacy Act.

Provide number and name of each applicable systems of records.

(visit *www.state.gov/m/a/ips/c25533.htm* for list of all published systems):

STATE-36

☐ Does NOT contain information covered by the Privacy Act.

a. Is notice provided to the individual prior to collection of their information?

Notice of the purpose, use and authority for collection of information submitted are described in the System of Records Notices titled STATE-36.

b. Do individuals have the opportunity and/or right to decline to provide information?

The individual is informed of the Privacy Act statement; whereby, the acknowledgement of the Privacy Act notice signifies the individual's consent to the use of his or her information. Notice of the purpose, use and authority for collection of information submitted are also described in the System of Records Notice titled STATE-36.

c. Do individuals have the right to consent to limited, special, and/or specific uses of the information? If so, how does the individual exercise the right?

No. The utility of the information in the system about a particular individual will not extend over the allotted time in the Department of State's Disposition of Schedule, as defined in Diplomatic Security Records, Chapter 11. Moreover, there is negligible privacy risk as a result of degradation of its information quality over an extended period of time.

d. Privacy Impact Analysis: Describe how notice is provided to individuals and how the risks associated with individuals being unaware of the collection are mitigated.

The notice offered is reasonable and adequate in relation to the system's purposes and uses.

9. Notification and Redress

a. What are the procedures to allow individuals to gain access to their information and to amend information they believe to be incorrect?

RMS contains Privacy Act-covered records; therefore, notification and redress are rights of record subjects. Procedures for notification and redress are published in the system of records notice identified in paragraph 8 above, and in rules published at 22 CFR 171.31. The procedures inform the individual about how to inquire about the existence of records about them, how to request access to their records, and how to request amendment of their record. Certain exemptions to Privacy Act provisions for notification and redress may exist for certain portions of a passport records on grounds pertaining to law enforcement, in the interest of national defense and foreign policy if the records have been properly classified, and to carry out protective responsibilities under 18 U.S.C. 3056. These exemptions are published as agency rules at 22 CFR 171.32.

b. Privacy Impact Analysis: Discuss the privacy risks associated with notification and redress and how those risks are mitigated.

The notification and redress mechanisms offered to individuals are reasonable and adequate in relation to the system's purpose and uses.

10. Controls on Access

a. What procedures are in place to determine which users may access the system and the extent of their access? What monitoring, recording, and auditing safeguards are in place to prevent misuse of data?

The Business Owner DS/SI/PSS approves and authorizes use of the RMS system and DS/EX/CTO controls access. System accounts are maintained and reviewed on a regular basis. The following DoS policies establish the requirements for access enforcement.

- 5 FAM 731 SYSTEM SECURITY (Department computer security policies apply to Web servers)
- 12 FAM 622.1-2 System Access Control

- 12 FAM 623.2-1 Access Controls
- 12 FAM 629.2-1 System Access Control
- 12 FAM 629.3-3 Access Controls

The database enforces a limit of 3 consecutive invalid access attempts by a user during a 15 minute time frame. After 20 minutes of inactivity a session lock control is implemented at the network layer.

The information system restricts access to privileged functions (deployed in hardware, software, and firmware) and security-relevant information to explicitly authorized personnel. The level of access for the user restricts the data that may be seen and the degree to which data may be modified. A system use notification ("warning banner") is displayed before log-on is permitted, and recaps the restrictions on the use of the system. Activity by authorized users is monitored, logged, and audited.

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

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

b. What privacy orientation or training for the system is provided authorized users?

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

c. Privacy Impact Analysis: Given the sensitivity of PII in the system, manner of use, and established access safeguards, describe the expected residual risk related to access.

Several steps are taken to reduce residual risk related to system and information access. Access control lists, which define who can access the system, and at what privilege level, are regularly reviewed, and inactive accounts are promptly terminated. Additionally, the system audit trails that are automatically generated are regularly analyzed and reviewed to deter and detect unauthorized uses. (An audit trail provides a record of which particular functions a particular user performed, or attempted to perform on an information system.)

11. Technologies

a. What technologies are used in the system that involves privacy risk?

All hardware, software, middleware, and firmware are vulnerable to risk. There are numerous management, operational, and technical controls in place to mitigate these risks. Applying security patches and hot-fixes, continuous monitoring, checking the national vulnerability database (NVD), following and implementing sound federal, state, local, department and agency policies and procedures are only a few of the safeguards

implemented to mitigate the risk to any Information Technology. RMS has been designed to minimize risk to privacy data.

b. Privacy Impact Analysis: Describe how any technologies used may cause privacy risk, and describe the safeguards implemented to mitigate the risk.

All hardware, software, middleware and firmware are vulnerable to risk. There are numerous management, operational and technical controls in place to mitigate these risks. Applying security patches and hot-fixes, continuous monitoring, checking the national vulnerability database (NVD), following and implementing sound federal, state, local, department and agency policies and procedures are only a few of safeguards implemented to mitigate the risks to any Information Technology.

12. Security

What is the security certification and accreditation (C&A) status of the system?

RMS is scheduled for C&A October 2009.