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: 23 April 2009

(b) Name of system: Identity Management System

(c) System acronym: IDMS

(d) IT Asset Baseline number: 1000

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

The Identity Management System (IDMS) is a database application that stores information collected from persons requiring Department of State (DoS) Personal ID Cards. The information collected facilitates the production (printing) and encoding (data elements required for physical/logical access and verification of the cardholder) of the DoS Personal ID Card ultimately issued to an approved cardholder.

(f) Reason for performing PIA:

☐ New system

☐ Significant modification to an existing system

☒ To update existing PIA to new format

(g) Explanation of modification (if applicable): A system update and review

(h) Date of previous PIA (if applicable): 21 September 2006

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?

The IDMS contains personnel information as required by HSPD-12; information collected includes:

- Name;
- I-9 Documentation;

- Social Security Number;
- Date and Place of Birth;
- Place of residence and telephone number;
- Citizenship;
- Armed Forces, or miscellaneous number;
- Biometrics;
- Gender;
- Race;
- Height, weight, eye color, hair color; and
- Emergency Contact Information (name and phone numbers only).

This source of information includes:

- Current and former Department Civil Service and Foreign Service employees;
- Civil Service employees, contractors, interns, and U.S. Military personnel from other U.S Government agencies on detail or performing work at Department locations;
- Foreign National government and military personnel/employees on detail to, or participating in foreign exchange programs;
- Organizations providing services to Department employees such as the State Department Federal Credit Union and American Foreign Service Association;
- Non-government entities residing in, or adjacent to Department facilities where access through Department access controls is required;
- Vendors supplying services to the Department such as food service employees, childcare providers, and vending machine providers;
- Foreign National diplomatic, consular, administrative, technical staff, and international organization employees;
- Domestic and household members (to include private servants), and other foreign government personnel and their dependents accredited to the United States; and
- Domestic and Foreign Press.

b. How is the information collected?

The information is collected interactively from or on forms filled out by the individual requiring the DoS Personal Identification Card. These forms include:

- DS-1838: Request for Building Pass Identification Card;
- SF85: Questionnaire for Non-sensitive Positions;
- SF85P(S): Questionnaire for Public Trust Positions;
- SF86: Questionnaire for National Security Positions; and
- DSP-97: US DoS Building Access Application.

c. Why is the information collected and maintained?

The information is collected to determine an applicant's suitability for access to Department facilities and information systems.

d. How will the information be checked for accuracy?

The information is verified by the individual applicant.

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

- 5 U.S.C. 301; Federal Information Security Management Act (FISMA);
- National Defense Authorization Act, Act (Pub. L. 104–106, sec. 5113);
- Homeland Security Presidential Directive (HSPD) 12, Policy for a Common Identification Standard for Federal Employees and Contractors, August 27, 2004;
- Federal Property and Administrative Act of 1949, as amended;
- Executive Order 10450 — Security Requirements for Government Employees;
- Executive Order 10865 — Safeguarding Classified Information Within Industry;
- Executive Order 12958 — Classified National Security Information;
- Executive Order 12968 — Access to Classified Information;
- Executive Order 12829 — National Industrial Security Program; and
- 5 CFR 731 — OPM part 731, Suitability.

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

The IDMS collects the absolute minimum amount of personally identifiable information (PII) required to satisfy its statutory purposes and the mission of the bureau. Access, authorizations and permissions are granted at a level commensurate with the user's "needs to know" and database management. The PII collected and maintained by the IDMS resulted in a security categorization of "Moderate," which requires specific privacy and security controls. The controls are subject to the rigorous testing, a formal certification and accreditation process, and authority to operate.

4. Uses of the Information

a. Describe all uses of the information.

The information is for issuance of DoS Personal Identification Cards for access to DOS owned or leased facilities and/or information systems. No non-production usage exists.

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

There is no "Analysis" of the PII and no new information will be produced.

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

No, the system does not use commercial information, publicly available information, or information from other Federal Agency Databases.

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

The IDMS is the property of the Bureau of Diplomatic Security and is owned by the DoS. However, contractors use and maintain the operations of the system within DoS facilities. All contractors undergo an annual computer cyber security briefings and Privacy Act briefings. All contracts contain approved Federal Acquisition Regulation Privacy Act clauses.

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.

Appropriate use is regulated by automated controls in the IDMS and by the System Rules of Behavior. Instruction for system use is periodically refreshed and re-issued. The IDMS does not provide flexibility of features that might initiate a functional vulnerability creep or threat.

5. Retention

a. How long is information retained?

The Department will delete the cardholder's record from the IDMS within five years of the cardholder's separation from the Department of State.

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

The utility of the information/data enclosed in the database about a particular individual will not extend over the allotted time defined in the Department's Disposition Schedule of Diplomatic Security Records, Chapter 11. When appropriate time limitations occur, the data is removed from the database. All backups of the database are protected in secured locations. Over time, the backup tapes are reused in a cycle shorter than the defined limitations allotted for retention. When the backup media is no longer usable, it is destroyed per DoS policies.

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?

The PII data elements listed below is shared with AlarmNet for the purpose of allowing an individual's authentication and access control to Department facilities.

- Name;
- Social Security Number;
- Birth date;
- Biometrics; and
- Gender.

Applicant information in the IDMS may also be shared internally with authorized DoS security personnel and DoS in the administration of their responsibilities.

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

The information is passed from IDMS via a single interface between Credential Management System (CMS) server with the IDMS enclave and the CMS Server on AlarmNet. Information between DoS security officials may occur via voice communications, DoS e-mail, or in paper form.

Only employees with a "need to know" are granted access to the records and all users are trained annually as to the use and misuse of Sensitive but Unclassified (SBU) data. DoS government and contractor employees who use/support the IDMS are subject to a rigorous background investigation by the Department or the Defense Security Service and are vetted for facts that may bear on the individual's loyalty and trustworthiness. All DoS government and contractor employees must pass an annual computer security briefing from the DoS.

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

The use of the information is in accordance with the stated authority and purpose. Risks to privacy are mitigated by granting access only to authorized persons. All employees of the Department of State have undergone a thorough personnel security background investigation. Access to Department of State facilities is controlled by security guards and admission is limited to those individuals possessing a valid identification card or individuals under proper escort. All records containing personal information are maintained in secured-file cabinets or in restricted areas, access to which is limited to authorized personnel. Access to computerized files is password-protected and under the direct supervision of the system manager. The system manager has the capability of printing audit trails of access from the computer media, thereby permitting regular ad hoc monitoring of computer usage.

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?

The information shared can include:

- Name;
- Social Security Number;
- Date and place of birth;
- Place of residence;
- Citizenship;
- Armed Forces, or miscellaneous number;
- Biometrics (fingerprints);
- Gender;
- Race; and
- Height, weight, eye color, hair color.

The information may be shared with:

- A Federal, State, or local agency, or other appropriate entities or individuals, or through established liaison channels to selected foreign governments, in order to enable an intelligence agency to carry out its responsibilities under the National Security Act of 1947 as amended, the CIA Act of 1949 as amended, Executive Order 12333 or any successor order, applicable national security directives, or classified implementing procedures approved by the Attorney General and promulgated pursuant to such statutes, orders or directives.
- Another federal agency to notify them when, or verify whether, a PIV card is no longer valid.
- The news media or the general public, factual information for which the disclosure of would be in the public interest and which would not constitute an unwarranted invasion of personal privacy, consistent with Freedom of Information Act (FOIA) standards.

b. How is the information shared outside the Department?

Information may be shared via voice communications, e-mail, or in paper form as necessitated by the need and or urgency.

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

Risks to privacy are mitigated by limited access to and release of personal information. Information may only be released on a “need-to-know” basis to other government agencies having statutory or other lawful authority to maintain such information. The information is used in accordance with the statutory authority and purpose.

8. Notice

The system:

☒ constitutes a system of records covered by the Privacy Act.
System of Records Notice Identify Management System State-72

☐ does not constitute a system of records covered by the Privacy Act.

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

A Privacy Act Statement is available for those individuals that provide this information by form and notice is also given through System of Record Notice 72.

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

The individual may decline to provide the required information; however, such actions may prevent him/her from gaining access to DoS facilities and/or information systems.

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?

Conditional consent is not applicable to the official purpose of the IDMS.

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.

A Privacy Act Statement is available on all forms. Furthermore; notification is provided to the Public via SORN State-72 (IDMS).

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?

Procedures for notification and redress are published in the system of records.

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

Procedures are available for individuals to access or amend records they believe are incorrect. The notice is reasonable and adequate in relationship to IDMS's purpose and use.

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?

All users maintain a least a public trust and SECRET security clearance level in order to gain access to the Department's unclassified computer network. To access records, the individual must first be an authorized user of the Department's unclassified computer network. Each prospective authorized user must first sign a user access agreement before being given a user account. The individual's supervisor must sign the agreement certifying that access is needed in order for the individual to perform his or her official duties. The user access agreement includes rules of behavior describing the individual's responsibility to safeguard information and prohibited activities (e.g. curiosity browsing). A username and password is created and a user's access is restricted depending upon their role and "need to know." Audit logs are maintained to record system and user activity including invalid logon attempts and access to data. An Information System Security Officer (ISSO) monitors audits logs monthly for unusual activity.

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 being given access to the system and must complete refresher training yearly in order to retain access. Users must also take a Departmental information system security briefing and quiz prior to receiving access to a DoS network. DS/SI/CS has a Departmental Cyber Security Awareness program in-place. DS/CTO identifies key personnel within DS/CTO/SMD/OPS and DS/CTO/SMD/SEC who needs to attend the Department's mandated Information Assurance training for system administrators.

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.

There is no expected residual risk associated with this system.

11. Technologies

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

There are no technologies used that involve privacy risk.

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

Not applicable.

12. Security

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

The IDMS Version 1.0 was Authorized-to-Operate on October 31, 2006, via the C&A Process; this Authorization expires on October 31, 2009.