



**Privacy Impact Assessment**  
***IDMS – ITAB 1000***  
***August 22, 2014***

## 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: August 22, 2014

(b) Name of system: Identity Management System

(c) System acronym: IDMS

(d) IT Asset Baseline (ITAB 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 for a triennial security reauthorization

(g) Explanation of modification (if applicable): Not Applicable

(h) Date of previous PIA (if applicable): 23 April 2009

## 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 (including Maiden Name) Social Security Number

- Date and Place of Birth
- Place of Residence and telephone number
- Citizenship
- Armed Forces, or miscellaneous number
- Biometrics (photographs and electronic fingerprints)
- Gender
- Emergency Contact Information (name and phone numbers only)

The 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 a Department location;
- Foreign National Locally Employed Staff (LES) in our overseas Embassies and Consulates;
- 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 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 U.S.;
- 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;
- DSP-97: US DoS Building Access Application
- I-9: Employment Eligibility Verification

#### **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 (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;
- 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.**

This system collects the absolute minimum amount of personally identifiable information required to satisfy the statutory purposes of this system and the mission of the bureau. By collecting only the minimum amount of information, this ensures that we mitigate unnecessary risk to our personnel who must use the system, and lower the profile of the data that we do collect and maintain – using only what is necessary to create a unique identifier.

**4. Uses of the Information**

**a. Describe all uses of the information.**

The information collected in IDMS 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 or publicly available information. Information from other Federal Agency IDMS Databases may be used to populate the DOS' IDMS for granting other agency personnel physical/logical access to DOS facilities/networks.

**d. Are contractors involved in the uses of the PII?**

The IDMS is the property of the Bureau of Diplomatic Security, and is ultimately owned by the DoS. However, contractors use and maintain the operations of the system within DoS facilities. All contractors undergo an annual computer security briefing. 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.

Access, authorizations and permissions are granted at a level commensurate with the user's needs to know and only at the level necessary for management of the data. The PII collected and maintained has resulted in a security categorization of "HIGH" for the IDMS which requires specific privacy and security controls. The controls are subject to rigorous testing, a formal assessment and authorization process, and an acceptance of risk prior to receiving authority to operate.

In an attempt to mitigate these risks, the Department of State has implemented numerous management, operational, and technical security controls 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.

## **5. Retention**

**a. How long is information retained?**

In accordance with A-11-014-16 a-16 g of the DOS, Diplomatic Security, Records Disposition Schedule, records are temporary. Delete/destroy 20 years after separation, or transfer of cardholder from the Department of State. PII is to be deleted/destroyed in accordance with DS approved records disposition schedule on retention of information/data on a particular individual

Note: those that are retirees of the Department are issued retiree badges. As long as they keep a retiree badge, their information is retained.

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

IDMS collects and maintains a significant amount of PII. Records within IDMS are only retained in accordance with the Diplomatic Security Records disposition schedule and are not used for purposes outside of employee ID verification. There are inherent risks associated with maintaining this type of information. Users are asked to update their information whenever they receive a new card, or execute a change in the pin associated with their badge.

## 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?

**AlarmNet (ITAB 885)** - The PII data elements listed below are shared with AlarmNet for the purpose of allowing for an individual's authentication and access control to Department facilities.

- Name
- Social Security Number
- Birth date
- Biometrics
- Gender

Applicant information in the IDMS may also be shared internally with authorized DoS security personnel in the administration of their responsibilities (i.e., employee verification).

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

**AlarmNet (ITAB 885)** - The information is passed from IDMS via a single encrypted interface between Credential Management System (CMS) server within 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 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

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.
- To the news media or the general public, factual information the disclosure of which would be in the public interest and which would not constitute an unwarranted invasion of personal privacy, consistent with the Privacy Act of 1974.

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

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:

contains information covered by the Privacy Act.

Provide number and name of each applicable system of records.

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

State-72, Identity Management System

does NOT contain information covered by the Privacy Act.

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

A Privacy Act Statement is provided on the form, which provides notice to the individuals prior to the collection. Additional notice is given through the publication of a System of Record Notice, State-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). By ensuring that all users of the system are provided the Privacy Act Statement when they register, provided they read what is provided, all users should be well informed as to their rights governed by the Privacy Act.

## 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?

IDMS 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.. The procedures inform the individual of 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.

**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 the system'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 must have, as a minimum, a successfully adjudicated FBI National Criminal History Check (fingerprint check) and be pending, or possessing at least a public trust or SECRET security clearance level in order to gain access to the Department's unclassified computer network. To access IDMS 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). Users are uniquely identified within the system, and a PIV card is used to support two factor authentication for end-user login access to IDMS. A username and password are created and users' 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. Information System Security Officer monitors audit 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. Operators of the IDMS system are trained upon deployment of the system, whether direct hire or third party contractor. Users must also take a Departmental information system security briefing and quiz prior to receiving access to a DoS network, as well as PA-459, Protecting Personally Identifiable Information. DS/SI/CS has a Departmental Security Awareness program in-place. DS/CTO identifies key personnel within DS/CTO/SMD/OPS and DS/CTO/SMD/SEC that need 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 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 01.03.00 is pending re-authorization. The assessment has been completed and the application is expected to obtain its new authority to operate in October 2014. This PIA update is to support the full reaccreditation process.