1. Contact Information

DoS 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: April 15, 2010

(b) Name of system: Integrated Document Management and Analysis System

(c) System acronym: IDMAS

(d) IT Asset Baseline (ITAB) number: 647

(e) System description:

IDMAS is a document management application developed by Abacus Technology Corporation to support the Office of International Claims and Investment Disputes (L/CID) within the Department of State (DoS) Office of the Legal Advisor (L) for the primary purpose of providing litigation support for the defense of a claim (Case B/1) filed by the Government of Iran against the U.S. before the Iran-U.S. Claims Tribunal in The Hague, The Netherlands (the "Tribunal"). The case involves Iran's purchase of defense articles and services through the 1970's under numerous contracts as part of the Foreign Military Sales (FMS) program.

IDMAS enables analysis of voluminous billing records that form the basis of Iran's claims and the matching of voluminous documents as potential evidence to rebut those claims. IDMAS is critical to litigation support, providing identification, inventory, organization, analysis, and preparation of evidence and data. IDMAS supports the work of teams, comprised of attorneys, paralegals, analysts, and Department of Defense (DoD) auditors, contractors, and military service technical personnel, at multiple locations throughout the U.S..

(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: Not applicable

(h) Date of previous PIA: March 2008

3. Characterization of the Information

The system:

- ☐ does NOT contain PII.

☒ does contain PII.

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

The PII of witnesses or potential witnesses in the case is maintained. The PII includes the names, military rank (as may be applicable), phone numbers, and addresses of these individuals. Both home and work contact information is often, but not always, included. The home addresses and telephone numbers of L/CID employees and contractors involved in the case are also maintained, as is contact information for Members of the Tribunal.

Sources of the PII include witness interview transcripts, investigations, trip reports, and information gleaned from document reviews. Information about individuals may also be collected from FMS corporate contractor files and interviews. The DoD branches of service provide information about DoD personnel to identify and locate potential witnesses. Other Government agencies that may provide relevant information are the General Services Administration, the U.S. Customs and Border Patrol, and the Defense Contract Audit Agency. Records stored in Federal Records Centers and records from the National Archives and Record Administration (NARA) may also be sources. Witnesses often provide not only their own personal information, but also provide the names of other individuals who may be relevant to the case. Information about an L/CID employee or contractor is provided by that individual, while information concerning Members of the Tribunal is provided regularly by the Tribunal itself.

b. How is the information collected?

PII is gleaned from the kinds of source documents described in 3.a. above and is subsequently key-entered or scanned into IDMAS by L/CID staff.

c. Why is the information collected and maintained?

The PII is used solely for the purpose of contacting relevant witnesses as may be required to provide effective representation of the U.S. Government in the case and for other reasons directly related to the activities of the U.S. Government before the Tribunal.

d. How will the information be checked for accuracy?

PII compiled from all sources is reviewed and analyzed by U.S. Government attorneys, contractors, and analysts. PII is also checked for accuracy through direct contact with the individual in subsequent interviews or depositions, when briefs are filed, or when affidavits are signed.

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

- 28 U.S.C. 1346, United States as defendant
- 28 U.S.C. Chapter 171, Tort Claims Procedure

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

IDMAS does not maintain especially sensitive PII information elements such as the Social Security number or other similar identifiers that uniquely distinguish an individual to the degree he or she may be at risk to threats such as identity theft. No adverse determination by the Government about an individual may arise from the PII about the individual that is collected.

4. Uses of the Information

a. Describe all uses of the information.

The PII is used to guide further research, obtain additional evidence, secure signed affidavits, to prove specific lines, and to engage with the Tribunal, as may be required to effectively represent the U.S. Government in the case.

Individual records are most commonly retrieved by the person's name, by a contract number or by subject matter specific to the B1 cases.

Computer-generated reports are organized in various ways, including by name, rank (if applicable), address (work and home), phone number (work and home), and dates of interviews or affidavits. Work history regarding the specific aspect of a witness' experiences with the FMS program may also be a means of organizing generated reports.

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

No special methods (e.g., pattern matching, record scoring) are used to analyze the PII; and no new information about an individual is generated from any computer-based IDMAS process.

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

Some publicly available information such as telephone directories may be used to correct or corroborate contact information. The PII compiled in IDMAS about an individual is not otherwise correlated or cross-referenced with records from commercial sources, publicly available sources, or other Federal agency databases for the purpose of assembling a dossier on the individual.

d. Are contractors involved in the use of PII?

Contractors regularly work with the PII maintained in IDMAS. The contracts that cover these contractors include required Federal Acquisition Regulation clauses applicable to Privacy Act-covered records. Privacy Act provisions are enforced the same as they would be for Federal employees who use the information.

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.

Employees and contractors who have access to IDMAS have been determined to be authorized by virtue of their security clearance level and to have a need to know to access the information. They are subject to security policies and rules of behavior for protecting PII issued by DoS in the form of periodic workforce notices and computer security awareness training.

5. Retention

a. How long is information retained?

The retention period is required to be for the life of Case B/1, which was filed by Iran in 1981 and is likely to continue for many more years, although it is impossible to determine with any precision an exact timeframe.

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

Privacy risk related to retention is considered negligible because the PII is not used for the purpose of providing a right, benefit, or privilege due the individual by the Government or to otherwise derive an adverse determination about the individual. The only risk from information becoming outdated over the course of time is that the Government may have difficulty establishing subsequent contact with the individual because the individual's location or telephone number may have changed.

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?

PII compiled into IDMAS is not shared with any DoS organizations outside the Office of the Legal Advisor.

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

Not applicable.

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

Not applicable.

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?

PII compiled into IDMAS is not shared with any organizations outside DoS.

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

Not applicable.

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

Not applicable.

8. Notice

The system:

☒ contains information covered by the Privacy Act.

System of Records Notice STATE-54, "Records of the Office of the Assistant Legal Adviser for International Claims and Investment Disputes"

☐ does NOT contain information covered by the Privacy Act.

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

The System of Records Notice STATE-54, "Records of the Office of the Assistant Legal Adviser for International Claims and Investment Disputes," serves as a general notice to the public that DoS collects PII as a part of representing the U.S. Government in claims brought against it. For Case B/1, an individual may be made specifically aware of the collection of PII when, for example, they are interviewed or deposed as a witness.

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

Where information is requested of individuals (during interviews, for example), they are free to decline to provide information. Otherwise, the limited contact information compiled in IDMAS about a witness is necessary to effectively represent the U.S. Government in the claim, and is not of the kind that offers the U.S. Government and the individual any opportunities to jointly negotiate partial provision of the contact information.

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?

As a practical matter, options for the limited, special, or specific uses of contact information about witnesses does not apply because of the nature of the PII.

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.

Because the PII collected about witnesses is limited to just their contact information, privacy risk that may arise in relation to notice and consent does not exist.

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?

The PII compiled in IDMAS is covered by Privacy Act System of Records STATE-54, "Records of the Office of the Assistant Legal Adviser for International Claims and Investment Disputes." The record notification and record access procedures are described in STATE-54. As a practical matter, all records covered by STATE-54 are exempt from the access and amendment provision of the Act based on rules published in the Federal Register at 22 CFR 171.36.

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

Because the PII collected about witnesses is limited to just their contact information, privacy risk that may arise from obstacles to record access and amendment does not exist.

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?

Access to IDMAS is password-protected. To access the system, the employee or contractor must first be an authorized user of the LCID private network. This network is a closed network which does not provide access to any other network or the internet. The user is presented with a system use notification ("warning banner") when they log on ; and the user must acknowledge they will abide by DoS standard rules of behavior.

IDMAS access privileges are assigned by a system administrator using a privileged computer account based on the principles of separation of duties, least privilege, and need-to-know. Authorized users maintain a security clearance level commensurate to the classification level of records in IDMAS.

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

All authorized system users of IDMAS are subject to an annual Computer Security Awareness Training requirement that covers practices aimed at protecting the confidentiality of PII. In addition, the contractor administers annual corporate security briefings. IDMAS-specific training is provided to all new users. All users are familiarized with the security policy for IDMAS, folder and document permissions, and security of the L/CID local area network environment within which IDMAS operates. All users must certify that they understand the policy and will practice responsible behavior in accordance with policy. Current security policies and procedures are posted within IDMAS and on the DoS intranet for later review by all staff.

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.

Safeguards for access are commensurate with the security categorization assigned the system using Federal Information Process Standard 199. The safeguards reduce privacy risk related to access by authorized users to a negligible level.

11. Technologies

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

The system does not incorporate technologies that elevate privacy risk. The computer environment within which the system operates is configured to enable only essential capabilities, to specifically prohibit or restrict the use of unnecessary functions or services, and to otherwise comply with the principle of least functionality to effectively isolate the environment from any functions or services not essential to the system. No remote access to IDMAS is permitted.

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

Privacy risk resulting from the use of specific technologies is negligible.

12. Security

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

IDMAS was last granted approval to operate on May 30, 2008 for a three-year period.