DEPARTMENT OF STATE

PRIVACY IMPACT ASSESSMENT

Integrated Document Management and Analysis System (IDMAS)
(Updated April 2008)

Conducted by:
Bureau of Administration
Information Sharing Services
Office of Information Programs and Services
Privacy Office
Email: pia@state.gov

The Department of the State
Privacy Impact Assessment for IT Projects

A. SYSTEM APPLICATION/GENERAL INFORMATION:

1) Does this system contain any personal information about individuals or *personally identifiable information? If answer is no, please reply via e-mail to the following e-mail addresses: pia@state.gov. If answer is yes, please complete the survey in its entirety.

YES _X__ NO__ __

*****The following are examples of personally identifiable information:

- Name of an individual
- Date and place of birth
- Address
- Telephone number
- Social security, Passport, Driver's license or other identifying number(s)
- Education
- Financial transactions
- Employment, Medical or Criminal history
- Finger print, voice print or photograph
- Any other identifying attribute assigned to the individual

2) What is the purpose of the system/application?

The Integrated Document Management and Analysis System (IDMAS) is a document management application specifically developed by Abacus Technology Corporation to support L/CID within the Office of the Legal Advisor (L) at the Department of State (DOS). L/CID represents the United States in a multi-billion dollar claim filed by the Government of Iran against the United States (Case B/1) before the Iran-U.S. Claims Tribunal in the Hague. The case involves Iran's purchase of defense articles and services under 1126 separate contracts as part of its Foreign Military Sales (FMS) program from the mid-1950's through the 1970's. IDMAS is a tool that enables L/CID to analyze the nearly two million lines of billing data ($7.5 billion in total) that form the basis of Iran's challenges to these contracts and to match up millions of pages of FMS documents as potential evidence to refute Iran's challenges. IDMAS is critical to all aspects of the litigation support of the United States' defense in this case, including the identification, inventory, organization, analysis and preparation of evidence and data in support of the U.S. position. IDMAS supports the work of a large and varied team of users at multiple worksites throughout the country – attorneys, paralegals, DOD auditors, military service technical personnel, analysts, and DOD contractors. The system is constantly undergoing systems development and enhancements, using the latest hardware and software available, in order to meet L/CID's ever-growing needs in defending the United States.

3) What legal authority authorizes the purchase or development of this system/application?

L/CID has sole source statutory authority to purchase and develop this system.

C. DATA IN THE SYSTEM:

1) Does a Privacy Act system of records already exist?

YES __X___ NO___

If yes, please provide the following:
System Name & Number _State-54

If no, a Privacy system of records description will need to be created for this data.

2) What categories of individuals are covered in the system?

All witnesses or potential witnesses in the Iranian litigation are covered in this system. A witness database stores the names, phone numbers, and addresses for these individuals, often for both their home and work. Also stored in the system are the home addresses and telephone numbers of L/CID employees and contractors.

3) What are the sources of the information in the system?

Witness interviews, investigations, data gleaned from document reviews, etc.

a. Is the source of the information from the individual or is it taken from another source? If not directly from the individual, then what other source?

Both. Witnesses often provide not only their own personal information, but also provide the names of other contacts and personnel relevant to the program. Information is also often found in document reviews and investigations, trip reports, and so on.

b. Why is the information not being obtained directly from the individual?

It is. (See above)

c. What Federal agencies are providing data for use in the system?

The United States Navy, Army, Air Force all provides relevant personnel information to identify/locate potential witnesses. Records stored in the Federal Records Centers (FRCs) and through the National Archives Record Administration (NARA) are also utilized. Other government agencies that may provide relevant records are General Services Administration, U.S. Customs Service, and the Defense Contract Audit Agency.

d. What State and/or local agencies are providing data for use in the system?

N/A

e. From what other third party sources will data be collected?

Data is also collected from FMS corporate contractor files and interviews, as well as from archived federal records.

f. What information will be collected from a State Department employee and the public?

DOS employees that may have files or records regarding the FMS program will be contacted as potential witnesses and their information collected should they need to be contacted again regarding the case. Relevant files and records will be provided.

3) Accuracy, Timeliness, and Reliability

a. How will data collected from sources other than DOS records be verified for accuracy?

Data, records, files and information retrieved from prospective witnesses, from other government agencies and from government contractors are all reviewed and analyzed by U.S. government attorneys, contractors and analysts. Specific witness information is verified throughout the investigation including contact in further interviews or depositions. Other information gathered through the course of the litigation would be verified when briefs are filed and/or affidavits are signed.

b. How will data be checked for completeness?

Only basic personal witness information is collected, and would be verified at the time of testimony or affidavit**.**

c. Is the data current? What steps or procedures are taken to ensure the data is current and not out-of-date? Name the document (e.g., data models).

Witness information and data is kept current on an as-needed basis to fulfill the requirements of this on-going, 25 year litigation.

d. Are the data elements described in detail and documented? If yes, what is the name of the document?

Yes, in the IDMAS Data Dictionary.

D. <u>DATA CHARACTERISTICS:</u>

1) Is the use of the data both relevant and necessary to the purpose for which the system is being designed?

Yes.

2) Will the system derive new data or create previously unavailable data about an individual through aggregation from the information collected, and how will this be maintained and filed?

No.

3) Will the new data be placed in the individual's record?

N/A

4) Can the system make determinations about employees/public that would not be possible without the new data?

N/A

5) How will the new data be verified for relevance and accuracy?

N/A

6) If the data is being consolidated, what controls are in place to protect the data from unauthorized access or use?

Access to the data depends heavily on security protocols established and enforced via the IDMAS software. Those with access are within the closed system and can only access with passwords. All users must have security clearances. Abacus has written standard rules of behavior and procedures for L/CID and has placed them on the system. The system is certified. Within the closed system, passwords are required and specific permissions are set for users.

7) **If processes are being consolidated, are the proper controls remaining in place to protect the data and prevent unauthorized access? Explain.**

N/A

8) **How will the data be retrieved? Does a personal identifier retrieve the data? If yes, explain and list the identifiers that will be used to retrieve information on the individual.**

We do not have social security numbers in the system. We generally retrieve data by searching on name, state, or contract number. Results are displayed by matching the search criteria, with user access restricted to the rights they have to particular documents.

9) **What kinds of reports can be produced on individuals? What will be the use of these reports? Who will have access to them?**

Reports are issued only on the fields of information collected. Those are name, rank (if applicable), address (work and home), phone (work and home), and dates of previous interviews or affidavits. Also, work history regarding the specific aspect of their experiences regarding the FMS program.

Uses would be to perform additional research, to obtain additional evidence, to obtain signed affidavits, and to prove specific lines in the B/1 case.

E. MAINTENANCE AND ADMINISTRATIVE CONTROLS:

1) **If the system is operated in more than one site, how will consistent use of the system and data be maintained in all sites?**

Even though the system can be accessed from various locations, the same controls are in effect to retrieve and review data. (See D.6)

2) **What are the retention periods of data in this system?**

The retention period is for the life of the litigation.

3) **What are the procedures for disposition of the data at the end of the retention period? How long will the reports produced be kept? Where are the procedures documented?**

The retention period is a function of the investigation and litigation itself. Active litigation is currently on-going and the disposition of the case is unknown. Data, information and reports would be kept for the life of the litigation.

4) Is the system using technologies in ways that the DOS has not previously employed (e.g., monitoring software, Smart Cards, Caller-ID)?

No, they are not using technologies not previously employed.

5) How does the use of this technology affect public/employee privacy?

It makes the information more secure. This system provides that data and personal information are secure. Security measures are in place at all levels of IDMAS, but specifically at the folder and document level.

6) Will this system provide the capability to identify, locate, and monitor individuals? If yes, explain.

It can do nothing more than provide contact information for already-identified witnesses, and provide documents for review that may include additional relevant names.

7) What kinds of information are collected as a function of the monitoring of individuals?

Individuals are not monitored in the system. It only lists name, rank and military affiliation (if applicable), address (work and home), phone (work and home), and dates of previous interviews or affidavits. Also, work history regarding the specific aspect of their experiences as it pertains to the FMS program.

8) What controls will be used to prevent unauthorized monitoring?

See D6.

10) If the system is being modified, will the Privacy Act system of records notice require amendment or revision? Explain.

N/A.

11) Are there forms associated with the system? YES ___ NO _X__ If yes, do the forms include Privacy Act statements that include required information (e.g. – legal authorities allowing for the collection of the information being requested, whether provision of the information is mandatory or voluntary, the routine uses of the data,

with whom the data will be shared, the effects on the individual if the data is not provided)?

F. ACCESS TO DATA:

1) **Who will have access to the data in the system (e.g., contractors, users, managers, system administrators, developers, other)?**

All of the above; anyone within and approved to be on the secure, closed system.

2) **How is access to the data by a user determined? Are criteria, procedures, controls, and responsibilities regarding access documented?**

Users are given access to the system once all previously mentioned criteria are met. Network rules, procedures and protocols are documented in the system. Password restrictions are utilized. Users are trained in these areas, as well as in setting specific document and folder permissions, thereby securing access even on those levels. See D6.

3) **Will users have access to all data on the system or will the user's access be restricted? Explain.**

No, users do not have access to all data or documents on the system. Access within the shared system is limited by group level access (i.e., certain service-specific users may only see documents that pertain to their own service area), as well as user level access where permissions may be set at both the folder and document levels.

4) **What controls are in place to prevent the misuse (e.g., unauthorized browsing) of data by those having access? (Please list processes and training materials.**

   In addition to the scenarios mentioned above, every user is required to be familiar with all security policies and practices concerning the LCID LAN environment as will with IDMAS operations. All system users are required to complete annual IT Security Awareness training at the DOS level. The contractor, Abacus, has annual corporate security briefings to cover security as well. At the L/CID level, training takes place for all new users on all security set-ups within the closed system and mentioned above - the New User Procedures, Rules of Behavior, and Departing Employees Procedures. L/CID staff and contractors must certify that they understand these rules and practice responsible behavior in accordance with policy. Current security policies and procedures are readily available to all staff within IDMAS and on the State intranet.

   Additionally, users of IDMAS receive training on permissions as well as access to the IDMAS User Manual which describes folder and document permissions. IDMAS has received Certification and Accreditation from the State IRM and follows the security procedures and policies outlined within their System Security Plan and related documentation

5) **Are contractors involved with the design and development of the system and will they be involved with the maintenance of the system? If yes, were Privacy Act contract clauses inserted in their contracts and other regulatory measures addressed? Have rules of conduct been established and training regarding the handling of such information under the Privacy Act of 1974, as amended?**

Yes. All DOS security procedures have been and are currently being followed. Privacy Act clauses can be found in the Abacus contract at Part I, Section H10.

6) **Do other systems share data or have access to the data in the system? If yes, explain.**

No, it is a closed system.

7) **Who will be responsible for protecting the privacy rights of the public and employees affected by the interface?**

N/A.

8) **Will other agencies share data or have access to the data in this system (Federal, State, Local, Other)?**

No, it is a closed system.

9) **If so, how will the data be used by the other agency?**

N/A.

10) **Who is responsible for assuring proper use of the data?**
L/CID Lead Attorneys and the System Manager. This is achieved via document review cycles as well as system controls on data access.