Privacy Impact Assessment
for the

Office of Inspector General Investigative Records

January 18, 2008

Contact Point
Thomas Frost
Assistant Inspector General for Investigations
Office of Inspector General
U.S. Department of Homeland Security
(202) 254-4042

Reviewing Official
Hugo Teufel III
Chief Privacy Officer
Department of Homeland Security
(703) 235-0780

Abstract

The Department of Homeland Security (DHS) Office of Inspector General (OIG) Investigative Records System includes both paper investigative files and the "Investigations Data Management System" (IDMS) -- an electronic case management and tracking information system, which also generates reports. OIG uses IDMS to manage information relating to DHS OIG investigations of alleged criminal, civil, or administrative violations relating to DHS employees, contractors and other individuals and entities associated with the DHS. This PIA is being conducted to assess the privacy impact of the OIG Investigative Records system that includes both paper investigative files and the IDMS.

Introduction

DHS OIG Investigative Records System collects information in order to meet its investigative and reporting responsibilities under the IG Act (5 U.S.C. App. 3, §§ 4-5). OIG uses its paper investigative files to document DHS OIG investigations of alleged criminal, civil, or administrative violations relating to DHS employees, contractors and other individuals and entities associated with the DHS. OIG uses IDMS to manage information relating to these investigations in order to record disposition of allegations; track actions taken by DHS management regarding misconduct; track legal actions taken after referrals to DOJ for prosecution; provide a system for creating reporting statistical information; and to track OIG investigators' firearms qualification records and government property records.

The IDMS and related paper investigative files are used for various purposes. For example, a typical transaction would involve reference to the IDMS to determine whether the subject of an investigation has been named in any other case currently being worked, or that has been closed, by OIG. Another typical transaction involves reviewing the IDMS for cases under a specific person's name in response to a FOIA/Privacy Act request filed with OIG by that person.

IDMS is shared with other law enforcement agencies on a need to know basis in order to obtain and verify information required to conduct investigations. IDMS is not connected to any other system, either outside or inside DHS OIG.

DHS OIG's predecessor agencies included the OIG for the U.S. Department of Treasury (Treasury); the OIG for the Federal Emergency Management Agency (FEMA); and the OIG for the Department of Justice. The FEMA and Treasury OIG offices had investigative data management systems that were incorporated into the IDMS. Specifically, the FEMA OIG maintained the "FEMA/IG–1, General Investigative Files" system of records, and the Treasury OIG maintained the "Treasury/DO.190, Investigation Data Management System." *See also* 5 U.S.C. app. 3, § 8I (special provisions concerning the DHS OIG); 6 U.S.C. § 555 (continuity of DHS Inspector General oversight). Thus, the IDMS contains records from 2002 to the present, and historical data is included from OIGs for three legacy DHS agencies, Treasury, Justice, and FEMA.

On October 6, 2005, DHS OIG published a revised System of Records Notice (SORN) for the this system of records which updated and revised its predecessor data management system, paper records, routine uses, and records maintenance information in the SORN. *See* 70 F.R. 58448-58451 (Oct. 6, 2005). On November 9, 2005, DHS OIG published notice that it was proposing to exempt this system of records from certain Privacy Act Provisions, 70 F.R. 67931-67933 (Nov. 6, 2005). This PIA was conducted in order to highlight changes in routine uses made in the revised

SORN published on October 6, 2005.

Section 1.0 Information collected and maintained

1.1 What information is to be collected?

Information entered into the IDMS includes: (1) information relating to a complaint or allegation submitted to OIG's Hotline office, information that includes various information depending on the type of complaint received, whether the complainant requests confidentiality, the nature of the allegation made; (2) tracking information regarding the status of a specific pending OIG investigation; (3) OIG Reports of Investigation and related documentation which may be subsequently reviewed as part of a criminal, administrative, or civil action or related matter; background investigation; security clearance; and (4) information relating to agents' firearms qualification and property management.

The IDMS has searchable data fields associated with complainants, witnesses, and subjects. The fields include:

- Name
- Date of birth
- Mailing address
- Telephone number
- Social Security Number
- E-mail address
- Zip code
- Facsimile number
- Commercial data, for investigative purposes such as identifying potential witnesses, verifying addresses, tracing proceeds from illegal activities, and for other investigative purposes
- Work related information such as status of investigations, agencies involved, date opened and closed, type of investigation, allegations, ultimate disposition of case, etc.

The IDMS case record is linked to electronic copies of part or all of the OIG paper investigative files, which are scanned and stored.

The contents of OIG paper investigative files vary depending on the particular investigation, but may include:

- letters, memoranda, and other documents alleging criminal or administrative misconduct;
- Reports of Investigation resulting from allegations of misconduct or violations of law with related exhibits, statements, affidavits, records or other pertinent documents (including those obtained from other sources, such as Federal, State, local, or foreign investigative or law enforcement agencies and other government agencies) obtained during investigations;
- transcripts and documentation concerning requests and approval for consensual (telephone and non-telephone) monitoring;
- reports from or to other law enforcement bodies;
- prior criminal or non-criminal records of individuals as they relate to investigations;

- subpoenas issued pursuant to OIG investigations and legal opinions, advice, and other legal documents provided by agency counsel;
- reports of actions taken by management personnel regarding misconduct allegations and reports of legal actions, including actions resulting from violations of statutes referred to the Justice Department for prosecution;
- records involving the disposition of investigations and resulting agency actions (e.g., criminal prosecutions, civil proceedings, administrative action);
- medical record numbers; bank account numbers; health plan beneficiary numbers; certificate/license numbers; vehicle identifiers including license plates; marriage records;
- civil or criminal history information; device identifiers and serial numbers;
- uniform resource locators (URLs);
- education records; biometric identifiers; photographs;
- other unique identifying numbers or characteristics, and;
- property records and Firearms and Training qualification records for all OIG Office of Investigations employees. This includes records showing date of firearms qualification, training course titles and sources of training, and subject area of training.

The IDMS is used to generate reports relating to OIG investigations, such as OIG special agents' firearms qualification records and property tracking records and investigative statistics and narratives that Congress requires OIG to submit under the IG Act through the OIG "Semi-Annual Report to Congress."

1.2 What are the sources of the information in the system?

Information is collected from individuals filing complaints of criminal, civil, or administrative violations, including, but not limited to individuals alleged to have been involved in such violations; individuals identified as having been adversely affected by matters investigated by the OIG; and individuals who have been identified as possibly relevant to, or who are contacted as part of an OIG investigation.

Information is also collected from DHS OIG Office of Investigations employees who are required to qualify for firearms and who receive government property.

Information is collected from sources other than the individual, because investigations require verification and confirmation of information through third parties. Such sources may include eyewitnesses, third parties with financial or other information relating to the subject of the investigation, or the matters under investigation; other law enforcement agency personnel; and any other persons or entities with information pertinent to the matter under review.

1.3 Why is the information being collected?

DHS OIG collects information in order to meet its responsibilities under the IG Act to conduct investigations relating to DHS programs and operations. OIG collects information only where OIG has specific legal authority to do so and the information is required to meet OIG's responsibilities, including those expressly established under the Inspector General Act. OIG collects SSNs to verify the identity of subjects, complainants, witnesses, and third parties; to use as a search term in searching public and non-public databases for information relating to the case; and for other investigative purposes.

Commercial data is sometimes collected as background information; to verify addresses, identities, and

contact information; to trace proceeds from illegal activities; to identify possible witnesses; and for other investigative purposes.

1.4 How is the information collected?

OIG investigators collect and analyze evidence through a number of techniques, including interviews of complainants, witnesses, victims, and subjects; reviews of records (e.g., personnel files, contract or grant files, financial records, etc.); collection of forensic evidence; surveillance and consensual monitoring; and use of computer technology (e.g., link analysis, databases, spreadsheets, cyber forensics, data mining, etc.). The decision-making process with respect to what information is required for a specific investigation and how that information should be obtained, varies considerably depending on type of investigation underway.

1.5 What specific legal authorities, arrangements, and/or agreements defined the collection of information?

OIG is authorized to conduct investigations under the Inspector General Act, 5 U.S.C. App. 3, § 6(a)(1)-(3) which expressly authorizes OIG:

(1) to have access to all records, reports, audits, reviews, documents, papers, recommendations, or other material available to [DHS] … which relate to [DHS] programs and operations;
(2) to make such investigations and reports relating to the administration of [DHS] programs and operations of the applicable establishment as are, in the judgment of the Inspector General, necessary or desirable; and
(3) to request such information or assistance as may be necessary for carrying out the duties and responsibilities provided by this Act from any Federal, State, or local governmental agency or unit thereof.

DHS OIG also compiles information through formal and informal task force operations involving other Federal, State, and local law enforcement agencies. OIG's participates in such task forces and similar interagency functions under task force agreements, memoranda of understanding, and other formal and informal agreements. OIG's involvement in such coordinated activities varies depending on the cases under investigation at any given time.

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

Privacy risks associated with information maintained in IDMS include: that the information may not be accurate or timely because it is not always collected directly from the individual involved; information could be used in a manner inconsistent with established OIG privacy policies; and the individual may not be aware that information relating to him/her is being compiled by OIG.

To mitigate these privacy risks, OIG conducts its investigations with due professional care, as follows:

- Investigations are conducted in a diligent and complete manner, taking reasonable steps to ensure sufficient relevant evidence is collected; pertinent issues resolved; and appropriate administrative, civil, and criminal remedies are considered.

- Investigations are conducted in accordance with applicable laws and regulations, prosecutorial guidelines; OIG policy and procedures; and with due respect for rights and privacy of those involved.

- Evidence is gathered and reported in an unbiased manner.

- Investigations are conducted in a timely manner based on the variables and complexities involved in each case, and are supported with appropriate documentation.

- Appropriate investigative techniques are employed to ensure data gathered is sufficiently reliable for making judgments regarding the matters being investigated.

- Sources of investigative information are documented in sufficient detail to provide a basis for assessing its reliability.

- Data gathered and analyzed as part of the investigation is accurately interpreted, logically presented, and maintained in the investigative case file.

In addition, and as stated above, OIG has already published a SORN (*see* 71 FR 64543) On October 6, 2005, DHS OIG published a revised SORN for the DHS OIG IDMS (*see* 70 F.R. 58448-58451 (Oct. 6, 2005)), along with an exemption notice (*see* 70 F.R. 67931-67933 (Nov. 6, 2005)) which, along with this PIA, provides additional information to inform persons individuals about the contents and purposes of IDMS.

Section 2.0 Uses of the system and the information

2.1 Describe all uses of the information.

DHS OIG uses information maintained in this system of records in order to conduct investigations relating to DHS programs and operations. OIG's most common use of such information, including Social Security Numbers (SSN), and other PII in order to confirm the identity of individuals.

DHS OIG uses SSN to confirm identities; to trace people, assets, and transactions; etc. The specific use depends on the allegation under investigation.

OIG collects information only where OIG has specific legal authority to do so and the information is required to meet OIG's responsibilities, including those expressly established under the Inspector General Act. OIG collects SSNs to verify the identity of subjects, complainants, witnesses, and third parties; to use as a search term in searching public and non-public databases for information relating to the case; and for other investigative purposes.

2.2 Does the system analyze data to assist users in identifying previously unknown areas of note, concern, or pattern?

DHS OIG conducts data mining primarily for statistical and case management purposes. For example, OIG may review data to track trends in terms of pending and completed investigations, types of complaints received, geographical locations, and various other factors in order to analyze office and personnel needs for the OIG Office of Investigations. OIG also compiles information relating to

investigative statistics for various reporting requirements, including but not limited to, the Semi-Annual Report to Congress required under the Inspector General Act, 5 U.S.C. App. 3, § 5. OIG also reviews data to evaluate incoming complaints and to respond to various Congressional, law enforcement and litigation requests, and information requests by other Federal agencies and U.S. attorneys' offices during the course of a criminal prosecution or civil enforcement action.

The IDMS can be used to cross-check various terms, such as name, case number, subject of investigation, alleged statutory or regulation violation, employing DHS component, results, status, special agent assigned, and date of complaint and of closing, in order to verify information, generate reports, and ascertain relationships between complaints, complainants, assignments, and other investigative matters.

2.3 How will the information collected from individuals or derived from the system be checked for accuracy?

DHS OIG's Office of Investigations has an intense editing and review process for all OIG Reports of Investigations. Agents are instructed to ensure accuracy and thoroughness through the investigative process; to consider confidentiality and security issues; to include disclosure caveats where appropriate; and to use electronic and other verification services to verify information as appropriate. The particular methods used to verify information compiled during the course of an investigation vary considerably depending on the type of investigation. Methods may include reference to commercial databases to: obtain background information; verify addresses, identities, and contact information; trace proceeds from illegal activities; identify possible witnesses; and for other investigative purposes. In addition, each record has a unique file number to prevent duplication. OIG verifies records by checking every incoming complaint to ensure that OIG has not received the same complaint previously. If so, OIG cross-references the two complaints; if not, the complaint is processed as a new entry. Information contained in the complaint is verified through the investigative process, which varies depending on the allegation and information at issue. OIG also updates the IDMS with timely information on referrals, administrative actions, prosecutions, civil enforcements, and other information addressing the status of, or results of, an investigation or complaint review.

2.4 Privacy Impact Analysis: Given the amount and type of information collected, describe any types of controls that may be in place to ensure that information is used in accordance with the above described uses.

Privacy risks involve the potential for misuse of data or unauthorized access to data. However, IDMS information and OIG investigative paper files are closely safeguarded in accordance with applicable laws, rules and policies, including DHS 4300a - Sensitive Systems Policy and Federal Regulations. The IDMS file server and Investigations paper records are located in a controlled secure zone to provide a layer of physical security to the server, backup tapes, and paper records. Access is strictly limited to authorized staff that require access to perform their official duties. File areas are locked at all times or kept in otherwise secure areas, and facilities are protected from the outside by security personnel.

IDMS records are also protected from unauthorized access through appropriate technical safeguards, including multi-layer firewall architectures, access codes, and passwords. Each user has an account established within IDMS and gains access to the system using a logon name and password on a secure network. Each authorized user is provided with a limited permission level based upon their position

and need to know. In addition, all OIG employees are notified of the sensitivity of IDMS and OIG investigative records and information, as well as restrictions on disclosure through the Privacy Act, Inspector General Act with respect to confidential informants, and other statutory and regulatory safeguards.

The IDMS data is secure in accordance with FISMA requirements; has had the required Certification and Accreditation completed; and the ATO (authorization to operate) was signed by Inspector General Skinner on June 24, 2005. The DHS Chief Information Officer (CIO) tracks the Certification and Accreditation information for the IDMS. The Trusted Agent FISMA (TAF) system identification number for the IDMS is OIG-0363.

Section 3.0 Retention

3.1 What is the retention period for the data in the system?

OIG is in the process of developing a records retention schedule in conjunction with the DHS Records Office and the National Archives and Records Administration (NARA). NARA has not yet approved the proposed schedule that is currently under review by the DHS Records Office. The retention schedule currently under consideration involved temporary retention of Investigative paper case files, with destruction 20 years after cutoff unless the case file involves significant matters. Electronic IDMS entries are retained until superceded or no longer needed for operational purposes. IDMS data relating to complaints is deleted 20 years after cut-off, or when no longer needed for operational purposes.

Paper case files relating to significant cases that involve senior DHS officials, or attract significant Congressional, judicial, or media attention are permanently retained for historical purposes.

3.2 Has the retention schedule been approved by the National Archives and Records Administration (NARA)?

No, the proposed schedule is currently under review by the DHS Records Office.

3.3 Privacy Impact Analysis: Given the purpose of retaining the information, explain why the information is needed for the indicated period.

Paper case files relating to significant cases that involve senior DHS officials, or attract significant Congressional, judicial, or media attention are permanently retained for historical purposes. All other case files are retained for 20 years to ensure records are available for any subsequent action, including but not limited to judicial appeals and related civil, criminal, or administrative actions. In addition, records may be needed in order to respond to inquiries from other law enforcement agencies relating to law enforcement matters, and for background or clearance investigations.

Electronic IDMS entries are maintained for the same reasons stated above with respect to paper case files, except the longer retention period is required in order to have a record on misconduct and any violation of law or regulation in order to respond to inquiries from other law enforcement agencies relating to law enforcement matters, and for background or clearance investigations.

Section 4.0 Internal sharing and disclosure

4.1 With which internal organizations is the information shared?

DHS OIG shares information in IDMS and related paper files with other DHS agencies, including but not limited to Transportation Security Administration, Customs and Border Protection, Citizenship and Immigration Services, Coast Guard, Federal Emergency Management (FEMA), and Secret Service. Such information is shared on an as needed basis, depending on the particular persons and programs under investigation, and on whether a particular complaint, case, or allegation is referred for further action or for information, to obtain information pertaining to the OIG investigation, etc.

4.2 For each organization, what information is shared and for what purpose?

OIG is authorized to conduct investigations pertaining to all DHS programs and operations. *See* 5 U.S.C. App. 3, § 2(1). Again, the information shared and the purpose for which it is shared, depends on the nature of the matters under investigation. OIG is statutorily authorized to keep the head of the agency "fully and currently informed" regarding problems and deficiencies relating to the administration of DHS programs and operations and the necessity for, and progress of, corrective action. *Id.* at § 2(3). In addition, reviews existing and proposed legislation and regulations in order to make recommendations concerning "the impact of such legislation or regulations on the economy and efficiency in the administration of [DHS] programs and operations . . . or the prevention and detection of fraud and abuse in such programs and operations." *Id.* at § 4(a)(2). To fulfill these statutory responsibilities, OIG shares information on an as needed basis with DHS agencies and components, including but not limited to Transportation Security Administration, Customs and Border Protection, Citizenship and Immigration Services, Coast Guard, Federal Emergency Management (FEMA), and Secret Service.

4.3 How is the information transmitted or disclosed?

OIG transmits information in a variety of ways, including electronically, in oral briefings and interviews, in writing, by telephone, etc. The method of transmission depends on the nature of the information, including its classification, privacy interests, status of the investigation, confidentiality, etc. No direct access is given to IDMS on paper investigative files. Electronic transmissions of information follows required technical controls such as encryption and media safeguarding.

4.4 Privacy Impact Analysis: Given the internal sharing, discuss what privacy risks were identified and how they were mitigated.

Privacy risks involved in internal sharing are similar to those addressed above in section 2.0 with respect to uses of information. Privacy risks involve the potential for misuse of data or unauthorized access to data. Again, OIG paper investigative files and IDMS information is closely safeguarded in accordance with applicable laws, rules and policies, including the DHS 4300a. All OIG employees are notified of the sensitivity of investigative records and information, as well as restrictions on disclosure through the Privacy Act, Inspector General Act with respect to confidential informants, and other statutory and regulatory safeguards. Any information transmitted internally within DHS agencies is marked accordingly as sensitive,

investigative information; as "For Official Use Only;" and with other warnings as appropriate.

Section 5.0 External Sharing and Disclosure

5.1 With which external organizations is the information shared?

The specific external organizations with which DHS OIG shares IDMS information and OIG investigative paper files externally, depend on the nature, subject, status, and other factors unique to each investigation. Such agencies include other Federal and/or State OIGs; State and local police departments; and other Federal agencies, including but not limited to the Federal Bureau of Investigation, Drug Enforcement Agency, Federal Protective Service, Postal Inspection Service, National Security Agency, and Bureau of Alcohol, Tobacco, and Firearms. If an investigation involves persons employed by other Federal, State, or local agencies, information may be shared with those other agencies. If a case is referred for prosecution, information will be shared with the Federal, State, or local prosecutors and/or law enforcement agencies. Information may also be shared with Congressional Committees with jurisdiction over matters under investigation.

DHS OIG participates on a regular basis, in interagency task forces involving Federal, State, and local law enforcement agencies and shares information in such cases, under the confines of the Privacy Act, 5 U.S.C. § 552a and the Freedom of Information Act, 5 U.S.C. § 552. Information sharing during the course of task force operations and other joint investigations is authorized under the Inspector General Act, 5 U.S.C. App. 3, § 4(a)(4) which authorizes OIG to "or coordinate relationships between such establishment and other Federal agencies, State and local governmental agencies, and nongovernmental entities with respect to . . . the identification and prosecution of participants in such fraud or abuse." *Id.*

In addition, the revised SORN published in October of 2005, included changes to routine uses for the IDMS. These included routine uses that expressly authorize release to Federal intelligence community agencies and other Federal agencies to further the mission of those agencies relating to persons who may pose a risk to homeland security; and release for purposes of peer reviews and inspections, including release to the President's Council on Integrity and Efficiency (PCIE) and Federal agencies in response to an audit, investigation or review.

5.2 What information is shared and for what purpose?

Specific information shared during the course of investigative activities depends on the particular investigation. It can include all information contained in the IDMS and Investigative paper files, including complaints, Reports of Investigation with related exhibits, statements, affidavits, records and other documents, transcripts, reports from or to other law enforcement entities, records involving the disposition of investigations and resulting agency actions (e.g., criminal prosecutions, civil proceedings, administrative action); and property records and Firearms and Training qualification records for OIG Office of Investigations employees.

In addition, the revised SORN published in October of 2005, included changes to routine uses for the IDMS. These included routine uses that expressly authorize release to Federal intelligence community agencies and other Federal agencies to further the mission of those agencies relating to persons who may pose a risk to homeland security; and release for purposes of peer reviews and inspections, including release to the President's Council on Integrity and Efficiency (PCIE) and Federal agencies in response to an audit, investigation or review.

5.3 How is the information transmitted or disclosed?

OIG transmits information in a variety of ways, including electronically, in oral briefings and interviews, in writing, by telephone, etc. The method of transmission depends on the nature of the information, including its classification, privacy interests, status of the investigation, confidentiality, etc. Personnel who maintain the IDMS do not have direct access to OIG investigative paper files.

5.4 Is a Memorandum of Understanding (MOU), contract, or any agreement in place with any external organizations with whom information is shared, and does the agreement reflect the scope of the information currently shared?

DHS OIG participates in a regular basis on interagency task forces involving Federal, State, and local law enforcement agencies. Some of these arrangements are made pursuant to Memoranda of Understanding (MOUs) and other informal and formal agreements. The scope of information shared in any particular case, under a particular MOU, depends on the nature of the investigation, allegations under review, status of the agencies involved, and status of the investigation.

5.5 How is the shared information secured by the recipient?

Information is shared primarily with other law enforcement agencies and government agencies with personnel who are already familiar with the Privacy Act and other restrictions on release of information. OIG notifies recipients of the confidential nature and disclosure restrictions through verbal statements, written markings on documents, and agency policies recognizing the confidential nature of such materials. DHS OIG closely follows and is attuned to Privacy Act requirements and other confidentiality concerns in sharing information with other Federal and State agencies. Access is strictly limited to authorized persons with a need to know, who require access to perform their official duties.

5.6 What type of training is required for users from agencies outside DHS prior to receiving access to the information?

Information is shared primarily with other law enforcement agencies and government agencies familiar with Privacy Act and other restrictions on release of information. These other agencies conduct training for their personnel on disclosure restrictions and Privacy Act requirements. In addition, any information transmitted internally within DHS agencies is marked accordingly as sensitive, investigative information; as "For Official Use Only;" and with other warnings as appropriate.

5.7 Privacy Impact Analysis: Given the external sharing, what privacy risks were identified and describe how they were mitigated.

The types of privacy risks at issue very depending on the nature of the investigation and parties/entities involved. Risks are mitigated by proper markings on documents; requirements for secure access; and appropriate transmittal mechanisms that vary depending on the nature of the information contained therein, and the vehicle by which it is transmitted.

Section 6.0 Notice

6.1 Was notice provided to the individual prior to collection of information? If yes, please provide a copy of the notice as an appendix. (A notice may include a posted privacy policy, a Privacy Act notice on forms, or a system of records notice published in the Federal Register Notice.) If notice was not provided, why not?

The publication of this PIA, the System of Records Notice SORN DHS/OIG 002, Investigations Data Management System (70 FR 58449, October 6, 2005), the Notice of Proposed Rule Making (70 FR 61931, November 9, 2005), and the final rule provide public notice of the collection, use, and maintenance of this information. Affirmative Privacy Act (e)(3) notice to individuals at the point of collection may not be feasible in some instances. Notice provided to individuals could interfere with OIG's ability to obtain, serve, and issue subpoenas, warrants and other law enforcement mechanisms that may be filed under seal, and could result in disclosure of investigative techniques, procedures, and evidence. In addition, providing notice to subjects of investigations would impede law enforcement in that it could compromise the existence of a confidential investigation or reveal the identity of witnesses or confidential informants. The final rule for the system of records officially exempts the system from portions if the Privacy Act

6.2 Do individuals have an opportunity and/or right to decline to provide information?

Individuals have the opportunity and/or right to decline to provide information depending on the nature of the investigation. OIG investigators undergo extensive training on interviewees' rights and obligations in the context of responding to OIG investigative inquiries, and OIG has policies and procedures in place addressing interviewees' rights and obligations that vary depending on the type of investigation and on whether the interviewee is a Federal employee.

6.3 Do individuals have the right to consent to particular uses of the information, and if so, how does the individual exercise the right?

Again, depending on the nature of the investigation, OIG investigators may ask persons if they wish to consent to particular use of the information they provide – for example, whomever requests confidentiality will be advised of the extent to which confidentiality can be provided under applicable laws and regulations.

6.4 Privacy Impact Analysis: Given the notice provided to individuals above, describe what privacy risks were identified and how you mitigated them.

The publication of this PIA, the System of Records Notice SORN DHS/OIG 002, Investigations Data Management System (70 FR 58449, October 6, 2005), the Notice of Proposed Rule Making (70 FR 61931,

November 9, 2005), and the final rule provide public notice of the collection, use, and maintenance of this information. Affirmative Privacy Act (e)(3) notice to individuals at the point of collection may not be feasible in some instances. See answer to 6.1.

Section 7.0 Individual Access, Redress and Correction

The following questions are directed at an individual's ability to ensure the accuracy of the information collected about them.

7.1 What are the procedures which allow individuals to gain access to their own information?

Individuals' privacy rights, including notice and rights to request amendment, are set forth in the Privacy Act, 5 U.S.C. §§ 552a. In accordance with 5 U.S.C. § 522a, OIG has exempted the IDMS system of records (*see* 70 F.R. 67931-67933 (Nov. 9, 2005)) (j)(2) and (k)(2) because access to the records contained in this system of records could inform the subject of an investigation of an actual or potential criminal, civil, or regulatory violation, to the existence of the investigation, and reveal investigative interest on the part of DHS or another agency. Access to the records could permit the individual who is the subject of a record to impede the investigation, tamper with witnesses or evidence, and avoid detection or apprehension. Amendment of the records could interfere with ongoing investigations and law enforcement activities and would impose an impossible administrative burden by requiring investigations to be continuously reinvestigated. In addition, permitting access and amendment to such information could disclose security-sensitive information that could be detrimental to homeland security.

Requests for information will be evaluated by DHS on a case-by-case basis to ensure that exemptions are only taken where the request meeting the specific standards set forth in 5 U.S.C. § 552a(j)(2) and (k)(2).

7.2 What are the procedures for correcting erroneous information?

As stated above, OIG has exempted the IDMS system from subsection 552a(e)(1) of the Privacy Act requiring correction of erroneous information. Again, during the course of investigations into potential violations of federal law, the accuracy of information obtained or introduced may be unclear or the relevance of the information may not be immediately apparent. In the interest of effective law enforcement, it is appropriate to retain all possibly relevant information that may aid in establishing patterns of unlawful activity.

7.3 How are individuals notified of the procedures for correcting their information?

See answer to section 7.2, above.

7.4 If no redress is provided, are alternatives available?

See answer to section 7.2, above.

7.5 Privacy Impact Analysis: Given the access and other procedural rights provided for in the Privacy Act of 1974, explain the procedural rights that are provided and, if access, correction and redress rights are not provided please explain why not.

See answer to section 7.2, above.

Section 8.0 Technical Access and Security

The following questions are intended to describe technical safeguards and security measures.

8.1 Which user group(s) will have access to the system?

User groups with access to the system are DHS-OIG Investigations and DHS-OIG IT Division. Each employee with access to IDMS must first have a valid OIG network account and then an individually identifiable IDMS account.

Access to OIG investigative paper files are restricted to OIG Investigations personnel assigned to the case, the OIG office that is handling the investigations, OIG management, and other OIG personnel as required.

8.2 Will contractors to DHS have access to the system? If so, please submit a copy of the contract describing their role to the Privacy Office with this PIA.

OIG IT Division has contractors providing programming support for IDMS, and IT Division's contractors provide general IT and programming support to OIG as an organization. However, outside contractors and non-OIG employees do not have access to IDMS and IT Division contractors do not have access to OIG paper investigative files.

8.3 Does the system use "roles" to assign privileges to users of the system?

Each OIG employee who is given an IDMS account is assigned privileges to the user in order to restrict access to specific case files including the ability to write and read each case record.

8.4 What procedures are in place to determine which users may access the system and are they documented?

OIG has established procedures for requesting access to IDMS. Each OIG employee assigned to the Office of Investigation is given OIG network account after the employee's clearance has been validated. Each new employee's name is submitted to the IDMS administrator, who validates the employee's assigned office, division, location, and need to access IDMS. This individual approves the creation of the employee's IDMS account and the associated security controls.

Access to OIG investigative paper files are restricted and premised on a need to know basis, with access validated by OIG management.

8.5 How are the actual assignments of roles and rules verified according to established security and auditing procedures?

As part of the procedures for creating an IDMS account, the IDMS administrator validates the employee's assigned office, division, location, and need to access IDMS. This individual approves the creation of the employee's IDMS account and the associated security controls. The internal technical controls within IDMS restrict case files to the owner of the file and by office location.

8.6 What auditing measures and technical safeguards are in place to prevent misuse of data?

As part of the internal technical controls within IDMS, case files are restricted to those persons with a need to know. Each record has an audit trail to track the modification and who made the changes (by person and date/time stamp). The Administrator of the IDMS reviews the audit trail of all activities on the system on an as needed basis and where there is a change in the system, to determine who made the change and whether the change was authorized and appropriate.

8.7 Describe what privacy training is provided to users either generally or specifically relevant to the functionality of the program or system?

All authorized users are notified during their orientation of the confidential nature of the data and prohibitions against misuse and improper disclosure of IDMS data and paper investigative files. OIG conducts an annual Security Awareness Session that addresses privacy issues, nondisclosure, methods of protecting data and outputs, and confidentiality and security concerns generally. In addition, the professionalism of OIG employees and in particular, of OIG investigators trained in and authorized to access IDMS information and paper investigative files, provides a further barrier to misuse and protection of individual privacy rights. All OIG special agents also receive specific direction through OIG directives and manuals that address the unique privacy interests in investigative materials.

8.8 Is the data secured in accordance with FISMA requirements? If yes, when was Certification & Accreditation last completed?

IDMS data is secure in accordance with FISMA requirements; has had the required Certification and Accreditation completed; and the ATO (authorization to operate) was signed by Inspector General Skinner on June 24, 2005. The Trusted Agent FISMA (TAF) system identification number for the IDMS is OIG-0363.

8.9 Privacy Impact Analysis: Given access and security controls, what privacy risks were identified and describe how they were mitigated.

Privacy risks involve the potential for misuse of data or unauthorized access to data. However, IDMS information is closely safeguarded in accordance with applicable laws, rules and policies, including

the DHS 4300a - Sensitive Systems Policy and Federal Regulations. All OIG employees are notified of the sensitivity of IDMS records and information, as well as restrictions on disclosure through the Privacy Act, Inspector General Act with respect to confidential informants, and other statutory and regulatory safeguards.

In addition, IDMS file server is located in a controlled secure zone to provide a layer of physical security to the server and backup tapes. All records are also protected from unauthorized access through appropriate technical safeguards, including multi-layer firewall architectures, access codes, and passwords. Finally, the IDMS data is secure in accordance with FISMA requirements; has had the required Certification and Accreditation completed; and the ATO (authorization to operate) was signed by Inspector General Skinner on June 24, 2005.

DHS OIG also maintains its investigative paper records in a restricted area that is accessed only by authorized DHS OIG personnel. Access is strictly limited to authorized staff that require access to perform their official duties. File areas are locked at all times or kept in otherwise secure areas, and facilities are protected from the outside by security personnel.

Section 9.0 Technology

The following questions are directed at critically analyzing the selection process for any technologies utilized by the system, including system hardware, RFID, biometrics and other technology.

9.1 Was the system built from the ground up or purchased and installed?

DHS OIG did not create a new system of records, but revised and re-named the two existing systems of records previously maintained by the former FEMA OIG (FEMA/IG–1, General Investigative Files); Treasury OIG (Treasury/DO .190, Investigation Data Management System); and the DOJ OIG Investigative Data Management System. Therefore, OIG did not create or purchase a new system for the IDMS.

9.2 Describe how data integrity, privacy, and security were analyzed as part of the decisions made for your system.

See answer to section 9.1, above.

9.3 What design choices were made to enhance privacy?

See answer to section 9.1, above.

Responsible Official

Thomas Frost
Assistant Inspector General for Investigations
Office of Inspector General
U.S. Department of Homeland Security
Counsel to the Inspector General
Office of Inspector General
Department of Homeland Security

Approval Signature Page

Original signed and on file with the DHS Privacy Office.

Hugo Teufel III
Chief Privacy Officer
Department of Homeland Security
(703) 235-0780