Privacy Impact Assessment
Of the
Office of Inspector General
Information Technology Infrastructure Systems

Program or application name:

Office of Inspector General Information Technology Infrastructure Systems

Contact Information:

System Owner:	Elizabeth Coleman, Inspector General
Organization:	Office of Inspector General
Address:	20th and C Streets, N.W. Washington, DC 20551
Telephone:	(202) 973-5005
IT Security Manager:	Sue Souvannavong, Information System Manager
Organization:	Office of Inspector General
Address:	20th and C Streets, N.W. Washington, D.C. 20551
Telephone:	(202) 528-3723

Summary description of the IT System:

The Office of Inspector General (OIG) operates and maintains an Information Technology (IT) Infrastructure (our general support system) that contains three databases (Magnum, AutoAudit, and IssueTrack, collectively referred to herein as the "ITI Systems").

Magnum is the case management system for the OIG Office of Investigations. This system is used by the Office of Investigations pursuant to its responsibilities under the Inspector General Act of 1978, as amended (IG Act), to manage, track and report on all aspects of complaints and investigations reported to or initiated by the Office of Investigations. Magnum contains files on individual investigations, including investigative reports and related documents generated during the course of or subsequent to an investigation. It includes electronic case tracking information, investigatory information, "Hotline" telephone logs, and investigator work papers, memoranda and letter referrals to management or others.

AutoAudit and IssueTrack are automated working paper, audit production, and audit recommendation tracking systems that support the OIG's audit and evaluation responsibilities set forth in the IG Act. These systems are maintained to increase the efficiency and productivity of the audit/evaluation processes by automating working paper preparation, internal review, and retention.

1. The information concerning individuals that is being collected and/or maintained:

Magnum includes personally identifiable information, such as names, addresses, and social security numbers contained in witness statements, concerning officers or employees of the Board and other persons from outside of the Board involved in activities related to the Board's programs and operations who are or have been under investigation by the Board's OIG in order to determine whether such officers, employees, or other persons have been or are engaging in fraud and abuse or other wrongdoing with respect to the Board's programs and operations. Magnum also includes personally identifiable information concerning complainants and witnesses where necessary for future retrieval.

AutoAudit and IssueTrack include information collected during the course of an audit or evaluation that, depending on the nature and scope of the objectives of the audit/evaluation, may or may not contain personally identifiable information, such as names, addresses, and salary information. Any personally identifiable information maintained in these systems may be used as part of the basis for developing the results of an audit/evaluation or related recommendations.

2. Source(s) of each category of information listed in item 1:

Personally identifiable information in the Magnum database is compiled from many sources including, but not limited to: the subject of an OIG investigation, employees of the Board and the Federal Reserve System, other government employees, witnesses and informants, and nongovernmental sources.

Personally identifiable information in the AutoAudit and IssueTrack databases is compiled from the examination of books and records, and through interviews of an auditee or other individuals regarding a particular audit or evaluation, and parties acting on behalf of such persons or entities.

3. Purposes for which the information is being collected.

The OIG maintains personally identifiable information in its ITI Systems for the purpose of conducting its mission under the IG Act. More specifically, the OIG maintains personally identifiable information in Magnum for the purpose of conducting its inquiries and investigations and issuing reports related to the administration of the Board's programs and operations and to manage the investigatory program. The OIG maintains personally identifiable information in AutoAudit and IssueTrack for the purpose of (1) conducting audits and evaluations and issuing reports related to the administration of the Board's programs and operations, (2) following up on outstanding recommendations, and (3) managing the audit and evaluation programs.

4. Who will have access to the information.

For the most part, access to personally identifiable information maintained in the ITI Systems by a user within the OIG is on a "need-to-know" basis by authorized employees who have a need for the information for official business purposes. Care is taken to ensure that only those employees who are authorized and have a need for the information for official business purposes have access to that information. For all the databases, the OIG IT staff have access to the databases in order to maintain them properly.

Information in Magnum is covered by a Privacy Act System of Records. For the most part, access to information is generally determined by the "need-to-know" requirements of the Privacy Act. In addition, the information maintained in Magnum may be released pursuant to either the Freedom of Information Act, the Privacy Act conditions of disclosure, or the routine uses published by the Board or in the OIG's Privacy Act System of Records Notice entitled, "Office of Inspector General Investigative Records" (BGFRS/OIG-1).

With respect AutoAudit and IssueTrack, all OIG staff have read access to these databases; however, edit capabilities to a particular project within the databases are limited to those individuals assigned to the project. Access to a particular project can be further restricted so that only individuals assigned to the project (and managers) can view information. Outside parties may temporarily be granted limited access to select work papers, with appropriate safeguards.

5. Whether the individual to whom the information pertains will have an opportunity to decline to provide the information or to consent to particular uses of the information (other than required or authorized uses).

Individuals to whom the information pertains will not have the opportunity to decline to provide the information or to consent to particular uses of the information.

6. Procedure(s) for ensuring that the information maintained is accurate, complete, and up-to-date.

OIG staff relies upon the individuals initiating a complaint, subjects of investigations, or witnesses for the accuracy, completeness, and timeliness of the personally identifiable information maintained in Magnum; however, additional information developed during the course of an investigation may corroborate or refute information provided by those individuals.

Portions of the personally identifiable information maintained in Magnum have been determined by the Board, pursuant to 5 USC 552a(j)(2), to be exempt from any part of the Privacy Act (5 USC 552a), except the provisions regarding disclosure, the requirement to keep an accounting, certain publication requirements, certain requirements regarding the proper maintenance of systems of records, and the criminal penalties for violation of the Privacy Act, respectively, 5 USC 552a(b), (c)(1), and (2), (e)(4)(A)

through (F), (e)(6), (e)(7), (e)(9), (e)(10), (e)(11) and (i). Magnum is a designated Privacy Act system of records maintained by the OIG, a Board component that performs as its principal function an activity pertaining to the enforcement of criminal laws. The exempt portions of the records consist of—(1) information compiled for the purpose of identifying individual criminal offenders and alleged offenders; (2) information compiled for the purpose of a criminal investigation, including reports of informants and investigators, and associated with an identifiable individual; and (3) reports identifiable to an individual compiled at any stage of the process of enforcement of the criminal laws from arrest or indictment through release from supervision.

To maintain the accuracy of data in AutoAudit and IssueTrack, edit access to each work paper is limited to OIG staff who created the work paper or to whom the work paper was sent for review, unless additional edit privileges are specifically granted by the creator of the work paper. OIG staff do not have delete privileges within the database, so work papers cannot accidentally be deleted. Edit history logs can be used to identify the date of the last edit update to a particular document. All work papers are subject to at least one level of supervisory review.

7. The length of time the data will be retained, and how it will be purged.

Information maintained in Magnum is cut off annually and destroyed 10 years after cutoff. Information maintained in AutoAudit and Issue Track is cut off annually and destroyed 8 years after cutoff.

8. The administrative and technological procedures used to secure the information against unauthorized access.

Personally identifiable information and other sensitive information maintained in the ITI Systems are stored on file servers protected by applicable security settings, such as a unique User IDs, complex passwords, and specific privileges for specific users. In addition, all three databases, as well as all user laptops, are encrypted.

9. Whether a new system of records under the Privacy Act will be created. (If the data is retrieved by name, unique number, or other identifier assigned to an individual, then a Privacy Act system of records may be created).

Magnum operates under Privacy Act System of Records Notice, BGFRS/OIG-1 entitled, "Office of Inspector General Investigative Records."

AutoAudit and IssueTrack do not require a system of records under the Privacy Act. To the extent that personally identifiable information about an individual is collected, maintained, or disseminated, it is not retrieved by reference to an individual's name or other personal identifier.

Reviewed:

(signed) Elaine Boutilier 11/28/2007

Chief Privacy Officer Date

Reviewed:

(signed) Maureen Hannan 11/30/2007

Chief Information Officer Date