

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: Mark Bialek, Inspector General
Organization: Office of Inspector General
Address: 20th and C Streets, N.W.
Washington, DC 20551
Telephone: (202) 973-5000

IT Security Manager: Sue Bowman, Senior Information Systems 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 Infrastructure (ITI) that consists of the OIG's Investigative Management System, Auto-Audit, and TeamMate, and a variety of access-controlled network drives and folders. These applications, network drives, and folders support the OIG's audits, evaluations, investigations, and other reviews of the programs and operations of the Board of Governors of the Federal Reserve System (Board) and the Consumer Financial Protection Bureau (CFPB) pursuant to the OIG's responsibilities under the Inspector General Act of 1978, as amended (IG Act).

The Investigative Management System is the case management system for the OIG's Office of Investigations. This system is used by the Office of Investigations to manage, track, and report on all aspects of complaints and investigations reported to and initiated by the Office of Investigations. The Investigative Management System 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, "OIG Hotline" telephone logs, and investigator work papers, memoranda, and letter referrals to management or others.

Auto-Audit and TeamMate are automated work paper, audit production, and audit report systems that support the OIG's audit and evaluation responsibilities under the IG Act.

These systems are maintained to increase the efficiency of the audit/evaluation processes by automating the preparation, internal review, and retention of work papers.

Each access-controlled network drive or folder within the OIG's ITI is used to support the OIG's audit, evaluation, investigative, and other responsibilities under the IG Act. These network drives are generally established as a temporary repository for data and files relevant to the OIG's mission of conducting oversight of the programs and operations of the Board and CFPB.

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

The Investigative Management System contains files that may include personally identifiable information concerning persons under investigation by the OIG, as well as individual complainants and witnesses relevant to the OIG's investigations. The personally identifiable information in the Investigative Management System may include, but is not limited to, names, addresses, social security numbers, financial information, personal contact information, and other information about individuals obtained during the course of the OIG's investigations.

Auto-Audit and TeamMate include information collected during the course of an OIG audit or evaluation that, depending on the nature and scope of the objectives of the audit/evaluation, may contain personally identifiable information concerning employees, contractors, complainants, and other individuals whose information may have been obtained during the course of an OIG audit or evaluation. The personally identifiable information in Auto-Audit and TeamMate may include, but is not limited to, names, addresses, social security numbers, financial information, personal contact information, and other information about individuals associated with an OIG audit or evaluation.

Each access-controlled network drive and folder within the OIG's ITI may be used as a temporary repository of personally identifiable information. The personally identifiable information in such access-controlled network drives and folders may include, but is not limited to, names, addresses, social security numbers, financial information, personal contact information, or other information about individuals collected in the course of an OIG audit, evaluation, investigation, or other review.

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

Personally identifiable information maintained in the Investigative Management System is compiled from many sources including, but not limited to: the subject of an investigation; employees of the Board, the Federal Reserve Banks, and the CFPB; other federal government employees; witnesses and informants; and nongovernmental sources.

Personally identifiable information maintained in the Auto-Audit and TeamMate applications is compiled from the examination of books and records, and through interviews of an auditee or other individuals regarding a particular audit or evaluation.

Personally identifiable information stored on an access-controlled network drive or folder is compiled from many sources, including, but not limited to, the subject of an investigation; employees of the Board, the Federal Reserve Banks, and the CFPB; other federal government employees; witnesses and informants; and nongovernmental sources.

3. Purposes for which the information is being collected:

The personally identifiable information collected and maintained in the ITI by the OIG is used to further the OIG's mission under the IG Act. More specifically, the OIG maintains personally identifiable information in the Investigative Management System for the purpose of conducting its inquiries and investigations, issuing reports related to the administration of the programs and operations of the Board and the CFPB, and managing the OIG investigatory program.

The OIG maintains personally identifiable information in Auto-Audit and TeamMate for the purpose of conducting audits and evaluations, issuing reports related to the administration of the programs and operations of the Board and the CFPB, following up on corrective action recommendations, and managing the audit and evaluation programs.

The OIG temporarily maintains personally identifiable information in access-controlled network drives and folders if it is relevant and necessary to the OIG's oversight responsibilities.

4. Who will have access to the information:

Access to personally identifiable information maintained in the ITI is limited to authorized employees and contractors within OIG with a need to know the information for official business purposes. To the extent the Investigative Management System is subject to the Privacy Act, 5 U.S.C. § 552a, an Investigative Management System record may be disclosed without the written consent of the individual to whom the record pertains if the disclosure falls within one or more of the categories enumerated in subsections 552a(b)(1) through (11) of Title 5 of the United States Code. With respect to § 552a(b)(3)'s "routine use" exception and pursuant to the applicable System of Records Notice ("FRB-OIG Investigative Records"), the following disclosures of Investigative Management System records are authorized:

- i. *Disclosure for enforcement, statutory, and regulatory purposes.* Information may be disclosed to the appropriate federal, state, local, foreign, or self-regulatory organization or agency responsible for investigating, prosecuting, enforcing, implementing, issuing, or carrying out a statute, rule, regulation, order, policy, or license if the information may be relevant to a potential violation of civil or criminal law, rule, regulation, order, policy, or license.
- ii. *Disclosure to another agency or a Federal Reserve Bank.* Information may be disclosed to a federal agency in the executive, legislative, or judicial branch of government, or to a Federal Reserve Bank, in connection with the hiring,

retaining, or assigning of an employee, the issuance of a security clearance, the conducting of a security or suitability investigation of an individual, the classifying of jobs, the letting of a contract, the issuance of a license, grant, or other benefits by the receiving entity, or the lawful statutory, administrative, or investigative purpose of the receiving entity to the extent that the information is relevant and necessary to the receiving entity's decision on the matter.

- iii. *Disclosure to a member of Congress.* Information may be disclosed to a congressional office in response to an inquiry from the congressional office made at the request of the individual to whom the record pertains.
- iv. *Disclosure to the Department of Justice, a court, an adjudicative body or administrative tribunal, or a party in litigation.* Information may be disclosed to the Department of Justice, a court, an adjudicative body or administrative tribunal, a party in litigation, or a witness if the Board (or in the case of an OIG system, the OIG) determines, in its sole discretion, that the information is relevant and necessary to the matter.
- v. *Disclosure to federal, state, local, and professional licensing boards.* Information may be disclosed to federal, state, local, foreign, and professional licensing boards, including a bar association, a Board of Medical Examiners, a state board of accountancy, or a similar governmental or nongovernment entity that maintains records concerning the issuance, retention, or revocation of licenses, certifications, or registrations relevant to practicing an occupation, profession, or specialty.
- vi. *Disclosure to the EEOC, MSPB, OGE and OSC.* Information may be disclosed to the Equal Employment Opportunity Commission, the Merit Systems Protection Board, the Office of Government Ethics, or the Office of Special Counsel to the extent determined to be relevant and necessary to carrying out their authorized functions.
- vii. *Disclosure to contractors, agents, and others.* Information may be disclosed to contractors, agents, or others performing work on a contract, service, cooperative agreement, job, or other activity for the Board and who have a need to access the information in the performance of their duties or activities for the Board.
- viii. *Disclosure where security or confidentiality has been compromised.* Information may be disclosed when (1) it is suspected or confirmed that the security or confidentiality of information in the system of records has been compromised; (2) the Board has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, identity theft or fraud, or harm to the security or integrity of this system or other systems or programs (whether maintained by the Board or

another agency or entity) that rely upon the compromised information; and (3) the disclosure is made to such agencies, entities, and persons who are reasonably necessary to assist in connection with the Board's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.

- ix. *Disclosure to other federal entities and certain private contractors.* Information may be disclosed to other federal entities, such as other federal Offices of Inspector General or the Government Accountability Office, or to a private party with which the OIG or the Board has contracted for the purpose of auditing or reviewing the performance or internal management of the OIG's investigatory program, provided the record will not be transferred in a form that is individually identifiable, and provided further that the entity acknowledges in writing that it is required to maintain Privacy Act safeguards for the information.
- x. *Disclosure to the Executive Council on Integrity and Efficiency, the President's Council on Integrity and Efficiency, and related others.* Information may be disclosed to officials charged with the responsibility to conduct qualitative assessment reviews of internal safeguards and management procedures employed in investigative operations. This disclosure category consists of members of the Executive Council on Integrity and Efficiency (ECIE), the President's Council on Integrity and Efficiency (PCIE), and officials and administrative staff within their investigative chain of command authorized by the ECIE or PCIE to conduct or participate in such qualitative assessment reviews.
- xi. *Disclosure to sources maintaining civil, criminal, or other relevant enforcement information or other pertinent information.* Information may be disclosed to any source, including a federal, state, or local agency maintaining civil, criminal, or other relevant enforcement information or other pertinent information, but only to the extent necessary for the OIG to obtain information relevant to an OIG investigation.

Information maintained in the Investigative Management System may additionally be subject to disclosure under the Freedom of Information Act, 5 U.S.C. § 552.

With respect to Auto-Audit and TeamMate, all OIG staff performing audit and evaluation work may be provided with access to these applications. Access to a particular project, however, can be restricted so that only individuals assigned to the project (and managers) can view the information. When the OIG restricts access to a particular project, OIG staff who are not assigned to the project may temporarily be granted limited access to select work papers on a "need-to-know" basis. Network administrators on the OIG's information technology staff are also provided with access to Auto-Audit and TeamMate to carry out their official duties. Because personally identifiable information stored on Auto-Audit and TeamMate is not retrieved by name or other personal identifier, the

information is not subject to disclosure pursuant to the Privacy Act. Information maintained in Auto-Audit and TeamMate, however, may be released pursuant to the Freedom of Information Act with the exception that information that is subject to exemption may be withheld.

Access-controlled network drives and folders are established by OIG staff when needed during the course of an OIG audit, inspection, evaluation, or investigation, and access to each drive or folder is generally limited to those OIG staff who have been assigned to the particular project or activity for which the network drive or folder was established. Network administrators on the OIG's information technology staff are also provided with access to network drives and folders to carry out their official duties. Because personally identifiable information stored on network drives and folders is not retrieved by name or other personal identifier, the information is not subject to disclosure pursuant to the Privacy Act. Information stored on network drives and folders, however, may be released pursuant to the Freedom of Information Act, with the exception that information that is subject to exemption may be withheld.

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):

As a general matter, due to the OIG's access to records and subpoena authority under the IG Act, individuals to whom the information pertains do not often have the opportunity to decline to provide the information or to consent to particular uses of the information, unless otherwise provided by law.

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

OIG staff relies upon the individuals providing information to the OIG, the Board, the CFPB, or the Federal Reserve System for the accuracy, completeness, and timeliness of the personally identifiable information maintained in the OIG's ITI. The personally identifiable information provided by individuals may or may not be corroborated during the course of an audit, inspection, evaluation, or investigation. Additionally, in order to maintain the accuracy of data in Auto-Audit and TeamMate, edit access to each work paper is provided to OIG staff who create or review work papers, OIG audit management, and certain OIG network administrators, unless additional edit privileges are specifically granted by the creator of the work paper or audit management for official business purposes. Edit history logs can be used to identify the date of the last edit to a particular document. All work papers within Auto-Audit and TeamMate 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:

Pursuant to the Board's records retention schedule, information maintained in the Investigative Management System is cut off annually and destroyed 10 years after cut-

off. Information in Auto-Audit and TeamMate is cut off annually and destroyed 8 years after cut-off. Generally, data held on an access-controlled network drive or folder is held until the completion of the associated audit, inspection, evaluation, or investigation, at which point the data is destroyed, deleted, or returned to its original provider. Alternatively, data held on an access-controlled network drive or folder may be transferred to Auto-Audit, TeamMate, or the Investigative Management System, in which case it follows the cut off and destruction timeframes for these applications, as provided above.

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 is stored on file servers protected by applicable security settings, such as unique user IDs, complex passwords, and specific privileges for specific users. In addition, all approved OIG mobile devices, including 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).

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

Auto-Audit, TeamMate, and the access-controlled network drives and folders do not require a system of records under the Privacy Act, because to the extent that personally identifiable information is maintained within Auto-Audit, TeamMate, or OIG network drives and folders, it is not the practice of the OIG to retrieve such information by reference to an individual's name or other personal identifier.

Reviewed:

Raymond Romero / *signed* /

08/29/2014

Chief Privacy Officer

Date

Reviewed:

Sharon Mowry / *signed* /

09/02/2014

Chief Information Officer

Date