Privacy Impact Assessment of the Office of Inspector General (OIG) Information Technology Infrastructure Systems (ITI)

System Owner:

The Office of Inspector General for the Board of Governors of the Federal Reserve System and the Bureau of Consumer Financial Protection

Contact information:

System Manager:	Peter Sheridan
Title:	Associate Inspector General for Information Technology
Division:	Office of Inspector General
Address:	1875 I Street NW, Washington, DC 20006
Telephone:	202-973-5009

IT System Manager:	Fred Gibson
Title:	Deputy Inspector General
Division:	Office of Inspector General
Address:	1875 I Street NW, Washington, DC 20006
Telephone:	202-973-5022

Description of the IT system:

The Office of Inspector General (OIG) operates and uses an Information Technology Infrastructure (ITI) provided by the Board of Governors of the Federal Reserve System's (Board) Division of Information Technology that consists of the OIG's Investigative Management System, the OIG's Audit Management Systems, 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 (including Board-

delegated functions performed by the Federal Reserve Banks) and the Bureau of Consumer Financial Protection (Bureau) 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 OIG's Office of Legal Services also has limited access to the Investigative Management System. 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, investigator workpapers, memoranda, and letter referrals to management or others. The Office of Investigations' Electronic Crimes Unit (ECU) houses a closed-network system that comprises equipment maintained and used by the ECU staff and Office of Investigations special agents. The ECU equipment is used exclusively for law enforcement activities. It stores evidence for investigative cases and is used to research casework and examine and analyze evidence.

The Audit Management Systems are automated workpaper, audit production, and audit report systems that support the OIG's audit and evaluation responsibilities under the IG Act. These systems increase the efficiency of audit and evaluation processes by automating the preparation, internal review, and retention of workpapers.

Each access-controlled network drive or folder is used to support the OIG's audit, evaluation, investigative, and other responsibilities under the IG Act. Additionally, information obtained through the OIG Hotline is maintained in an access-controlled network drive. These network drives are generally established as a repository for data and files relevant to the OIG's mission of conducting oversight of the programs and operations of the Board (including Board-delegated functions performed by the Reserve Banks) and the Bureau.

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

The Investigative Management System and the ECU closed-network system contain files that 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 and the ECU closed-network system may include, but is not limited to, names, employee identification numbers, addresses, social security numbers, financial information, personal contact information, and other information about individuals obtained during the course of the OIG's investigations. Such individuals include Board employees, Reserve Bank employees, Bureau employees, contractors, other OIG employees, and, in limited circumstances, former employees and other members of the public who may have information relevant to an OIG investigation.

The Audit Management Systems 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 or evaluation, may contain personally identifiable information. The personally identifiable information in the Audit Management Systems may include, but is not limited to, names, employee identification numbers, addresses, social security numbers, financial information, personal contact information, and other information about individuals associated with an OIG audit or evaluation. Such individuals include Board employees, Reserve Bank employees, Bureau employees, contractors, other OIG employees, and, in limited circumstances, former employees and other members of the public whose information was obtained during the course of an OIG audit or evaluation.

Access-controlled network drives and folders are used as a secure repository for personally identifiable information. The personally identifiable information in such access-controlled network drives and folders may include, but is not limited to, names, employee identification numbers, addresses, social security numbers, financial information, personal contact information, or other information about individuals collected in the course of an OIG audit, evaluation, investigation, other review, or Hotline complaint.

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

Personally identifiable information maintained in the Investigative Management System and the ECU closed-network system is compiled from many sources

including, but not limited to: the subject of an investigation; employees and contractors of the Board, the Reserve Banks and the Bureau; other federal government agencies and employees; witnesses and informants; non–federal government entities; and nongovernmental sources.

Personally identifiable information maintained in the Audit Management Systems applications is compiled from the examination of agency, Reserve Bank, and contractor 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 Reserve Banks, and the Bureau; other federal government employees; witnesses and informants; Hotline complainants; non–federal government and law enforcement sources; 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 and the ECU closed-network system for the purpose of conducting its inquiries and investigations, issuing reports related to the administration of the programs and operations of the Board (including Board-delegated functions performed by the Reserve Banks) and the Bureau, and managing the OIG investigatory program.

The OIG maintains personally identifiable information in its Audit Management Systems for the purpose of conducting audits and evaluations, issuing reports related to the administration of the programs and operations of the Board (including Board-delegated functions performed by the Reserve Banks) and the Bureau, following up on corrective action recommendations, and managing the audit and evaluation programs.

The OIG maintains personally identifiable information in access-controlled network drives and folders when it is relevant to an OIG audit, evaluation, investigation, other review, or OIG Hotline complaint.

4. Who will have access to the information:

Access to personally identifiable information maintained in the ITI is limited to authorized employees within the OIG on a need-to-know basis who use the information for official business purposes. In limited circumstances, a contractor within the OIG may have access on a need-to-know basis. To the extent the Investigative Management System, the ECU closed-network system, or OIG Hotline information is subject to the Privacy Act, 5 U.S.C. § 552a, such records 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. In addition, the OIG may disclose information in the Investigative Management System for the purposes set forth in the System of Records entitled BGFRS/OIG-1, "FRB—OIG Investigative Records." 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 the Audit Management Systems, all OIG employees performing audit and evaluation work may be provided with access to these applications. In limited circumstances, a contractor within OIG may have access to these applications on a need-to-know basis. Access to a particular project (e.g., an audit, evaluation, or other review) can be restricted so that only individuals (e.g., those assigned to the project and their managers) can view the information on a need-to-know basis. When the OIG restricts access to a particular project, OIG staff members who are not assigned to the project are unable to access any of the information it contains. Information technology network administrators are also provided with access to the Audit Management Systems to carry out their official duties. Because personally identifiable information stored on the Audit Management Systems is not retrieved by name or other personal identifier, the information is not subject to disclosure pursuant to the Privacy Act. Information maintained in the Audit Management Systems, however, may be released pursuant to the Freedom of Information Act with the exception of information that is subject to exemption, which may be withheld.

Access-controlled network drives and folders have been established by OIG staff to support the OIG Hotline and when needed during the course of an OIG audit, inspection, evaluation, investigation, or other review. Access to each drive or folder is limited to those OIG staff who work for the OIG's Hotline function and to those OIG staff who have been assigned to the particular project or activity for which the network drive or folder was established.

Information technology network administrators are also provided with access to access-controlled network drives and folders to carry out their official duties. Because personally identifiable information stored on network drives and folders is not retrieved by the OIG through the use of names or other personal identifiers, 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 of information that is subject to exemption, which may be withheld.

5. Whether the individuals to whom the information pertains 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 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. This is due to the OIG's access to records and subpoena authority under the IG Act.

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

OIG staff members rely on the individuals providing information to the OIG, the Board, the Bureau, or the Federal Reserve Banks for the accuracy, completeness, and timeliness of the personally identifiable information maintained in the ITI. The personally identifiable information provided by individuals may or may not be corroborated during the course of an audit, evaluation, investigation, or other review. Additionally, in order to maintain the accuracy of data in the Audit Management Systems, edit access to each workpaper is only provided to OIG staff who create or review workpapers, OIG audit management, and certain OIG

network administrators, unless additional edit privileges are specifically granted by the creator of the workpaper 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 workpapers within the Audit Management Systems are subject to at least one level of supervisory review.

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

The National Archives and Records Administration (NARA) has approved a detailed records retention schedule for various categories of OIG records. In general, OIG investigative records are cut off when the investigation is closed and are destroyed no sooner than 10 years after cutoff, unless the records relate to a significant investigation (e.g., cases resulting in substantive change in agency policy, cases with national or regional media attention, and cases that attract congressional attention). In such instances, the files are cut off when the investigation is closed and are transferred to NARA in 5-year blocks 30 years after cutoff.

In general, records concerning the OIG case files of audits, evaluations, and other reviews are cut off on the issuance of the final report and destroyed no sooner than 5 years after cutoff; final OIG reports are cut off when the case is closed and are transferred to NARA in 5-year blocks 30 years after cutoff, except for congressional reports, which are cut off annually and transferred to NARA in 5-year blocks 5 years after cutoff.

For files containing anonymous or vague allegations not warranting an investigation and support files providing general information that may prove useful in OIG investigations, the files are cut off annually and destroyed no sooner than 5 years after cutoff. Additionally, files in access-controlled network drives that contain personally identifiable information and do not fit in any of the above categories are disposed of when no longer needed, which is generally at the conclusion of the relevant audit, evaluation, investigation, or other review.

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 servers protected by applicable security settings, such as unique user IDs, complex passwords, and specific privileges for specific users. Database servers are encrypted. 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 are 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, the ECU closed-network system, and the OIG Hotline operate under the Privacy Act System of Records Notice, BGFRS/OIG-1 entitled "FRB—OIG Investigative Records."

The Audit Management Systems and the access-controlled network drives and folders (other than those related to OIG Hotline information) do not require a system of records under the Privacy Act because to the extent that personally identifiable information is maintained within the systems, or within 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:

/signed/ ***2/10/20***
Raymond Romero Date
Senior Agency Official for Privacy

/signed/ ***2/10/20***
Sharon Mowry Date
Chief Information Officer