Commodity Futures Trading Commission
Privacy Impact Assessment

System Name: Office of Inspector General (OIG) System

Date: April 22, 2015

1. Overview

In accordance with the Inspector General Act of 1978 (Public Law 95–452; 5 U.S.C. Sections 6 and 8G(g)(1)) ("IG Act"), the CFTC's Office of the Inspector General (OIG) conducts and supervises audits and investigations of CFTC programs and operations and recommends policies to promote economy, efficiency and effectiveness. It also investigates reports of fraud, waste, and abuse received from CFTC employees, contractors and members of the public. Moreover, the OIG investigates reports from Federal contractors of Federal criminal law involving fraud, conflict of interest, bribery, or a gratuity violation, or a violation of the civil False Claims Act. See Federal Acquisition Regulations (FAR) (73 Fed. Reg. 67064).

As stated in the IG Act, to obtain the necessary information and evidence for its audits and investigations, the Inspector General and his or her designees have the right to:

- Access all records, reports, audits, reviews, documents, papers, recommendations, and other materials available to the CFTC and relating to the CFTC's programs and operations;
- Require by subpoena the production of information, documents, reports, answers, records, accounts, papers, and other data and documentary evidence;
- Administer oaths and affirmations or take affidavits; and
- Request information or assistance from any Federal, state, or local government agency or unit.

OIG staff collect and store many types of information to fulfill the Inspector General's mission, including as needed for specific audits and investigations personally identifiable information (PII) and sensitive personally identifiable information (SPII),[1] financial information, employee payroll, benefits or travel information, information related to trades in the markets that the CFTC oversees, and information related to CFTC programs and activities. When information is in electronic form, OIG staff maintains this information within the OIG System, which is part of the CFTC General Support System (GSS).

The OIG System consists of:

[1] Under the Commission's Safeguarding Personally Identifiable Information policy, "sensitive personally identifiable information" means "a subset of PII, which if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual."

- A local area network (LAN) which may include scanners, copiers, fax machines, printers and OIG staff desktop workstations with typical office support applications, such as e-mail, calendars and word processing applications.
- Hard drives, USB and other storage devices, back-up media and long-term storage media as may be needed by OIG staff.
- An Internet website that allows individuals to submit information to the OIG electronically, either anonymously or after identifying themselves.
- A TeamMate Electronic Work Papers ("TeamMate") application and database, which is a commercial off-the-shelf (COTS) audit management system enabling OIG staff to manage electronic information, including work papers, and collaborate during audits and investigations. TeamMate collects and stores information submitted by individuals; data accessed and collected from other CFTC databases for audit and investigation purposes (e.g., **the Integrated Surveillance System (ISS)**); notes, files, drafts and reports; and testimony, witness statements and other evidence. OIG staff also use TeamMate to organize documents and track the status of audits and investigations.

OIG staff manage, support, and store information for all audits, investigations, reports and related work materials in the OIG System.

2. Data Collected and Stored Within the System

2.1. What information will be collected, used, disseminated or maintained in the system?

The OIG System includes many types of data, for example, information from or regarding individuals who are part of an audit or investigation, internal staff memoranda, copies of subpoenas issued during the investigation, affidavits, witness statements, transcripts of testimony, accompanying exhibits, notes, files, drafts of reports, opening reports, closing reports, and an index of individuals investigated.

The nature and amount of PII and SPII collected and maintained depends on the objective and topic of the investigation or audit. For example, an investigation into an allegation of illegal trading by a CFTC employee might include interview notes with the subject employee; forensic images of the employee's computer; copies of relevant emails exchanged between the employee and other CFTC staff; and trading information. An investigation into employee pay, travel or benefits could include payroll, travel and benefits information, including data such as social security number, date of birth and personal contact information. On the other hand, an audit of a CFTC program may only include as PII selected employees' names, CFTC titles and work-related activities.

Information used by the OIG and contained in the OIG System could include any of the following depending on the nature of OIG audits and investigations:

Categories	Is collected, processed, disseminated, stored and/or accessed by this system or project.	CFTC Employees	Members of the Public	Other (e.g. contractors, other government employees)
Name (for purposes other than contacting federal employees)	X	X	X	X
Date of birth	X	X	X	X
Social Security Number (SSN, last 4 digits)	X	X	X	X
Tax Identification Number (TIN)	X	X	X	X
Photographic identifiers				
Driver's license				
Mother's maiden name				
Vehicle identifiers				
Personal mailing address	X	X	X	X
Personal e-mail address	X	X	X	X
Personal phone number	X	X	X	X
Medical records number				
Medical notes or some other health information	X	X	X	X
Financial account information	X	X	X	X
Certificates			X	
Legal documents	X	X	X	X
Device identifiers	X	X	X	X
Web uniform resource locator(s)				
Education records	X	X	X	X
Military status				
Employment status	X	X	X	
Employment performance ratings or other information	X	X	X	X
Applicant information	X	X	X	
Foreign activities	X	X	X	
Trader identities (please indicate whether firm/business or natural person)	X	X	X	
Trader positions (please indicate whether firm/business or natural person)	X	X	X	X
Reports from individuals of any instance of fraud, waste, and abuse at CFTC	X	X	X	X
Other complaint for handling by DOE			X	X
Banking data	X	X	X	
Procurement/contracting records	X	X	X	X

Categories	Is collected, processed, disseminated, stored and/or accessed by this system or project.	CFTC Employees	Members of the Public	Other (e.g. contractors, other government employees)
Data/information from foreign sources	**X**	**X**	**X**	
Data/information received through a memorandum of understanding or other sharing arrangement	**X**			**X**
Proprietary or business information	**X**	**X**	**X**	**X**
Other (please list the type of info and describe as completely as possible)				

2.2. What will be the sources of the information in the system?

The sources of the information in the OIG System can be members of the public, CFTC employees or contractors, or any other CFTC systems that OIG staff access for an audit or investigation. In addition, the OIG may receive information from public sources or other Federal, state, local or foreign government authorities, including other Inspectors General, for example, during a peer review process.

2.3. Why will the information be collected, used, disseminated or maintained?

As explained above, the OIG will collect, use, disseminate and maintain information in the OIG System to fulfill its responsibilities under the IG Act. These responsibilities include conducting and supervising audits and investigations of CFTC programs and operations, recommending policies to promote economy, efficiency and effectiveness, and investigating reports of waste, fraud and abuse.

2.4. How will the information be collected by the Commission?

The OIG collects information from CFTC employees, contractors, members of the public, public sources or other Federal, State, local or foreign government authorities, or other CFTC systems in the following ways:

- information submitted to the OIG electronically via the Internet;
- calls received through the OIG hotline;
- letters mailed to the OIG;
- facsimile and email to and from OIG staff;
- interviews and meetings with individuals;
- witness statements and testimony;
- notes, draft reports and analyses prepared by OIG staff;
- investigation activities conducted by OIG staff, which may include review of public sources of information, e.g., from the Internet, or information from other Federal, state, local or foreign government authorities;

- information received pursuant to subpoena or other legal process;
- information received or copied from other CFTC systems, e.g., forensic collection of employee email, instant messages, payroll systems, ISS or other systems;
- information hand delivered anonymously.

2.5. Is the system using technologies in ways that the Commission has not previously employed (e.g., monitoring software)?

No. All software and technologies used are common to the Commission's current infrastructure.

2.6. What specific legal authorities authorize the collection of the information?

The Inspector General Act (5 U.S.C. Sections 6 and 8G(g)(1)) authorizes the collection of information by the OIG. 13 CFR 101.302 identifies the scope of the Inspector General's authority. Additionally, the OIG investigates any reports from Federal contractors of any violation of Federal criminal law involving fraud, conflict of interest, bribery, or a gratuity violation, or a violation of the civil False Claims Act. See Federal Acquisition Regulations (FAR) (73 Fed. Reg. 67064).

To obtain the necessary evidence, the Inspector General and his or her designees have the right to:

- Access all records, reports, audits, reviews, documents, papers, recommendations, and other materials available to CFTC and relating to CFTC's programs and operations;
- Require by subpoena the production of all information, documents, reports, answers, records, accounts, papers, and other data and documentary evidence;
- Administer oaths and affirmations or take affidavits; and
- Request information or assistance from any Federal, state, or local government agency or unit.

3. Data and Records Retention

3.1. For what period of time will data collected by this system be maintained and in what form will the data be retained?

Information collected and stored in the OIG System is maintained in electronic form, primarily within accessible systems, but possibly on secure back-up or long-term storage media. Paper records are retained in file folders, loose-leaf binders and similar paper filing methods in secure offices and lockable cabinets. OIG records are maintained according to **CFTC's records disposition schedule**, beginning at record code 200.

3.2. What are the plans for destruction and/or disposition of the information?

Paper files that have been scanned into the OIG System or are eligible for destruction will be placed in shredding bins immediately after scanning. Electronic records will be deleted once they have exceeded the retention period.

4. Access to and Sharing of the Data

4.1. Who will have access to the information in the system (internal and external parties), and with whom will the data be shared? If contractors, are the Federal Acquisition Regulations clauses included in the contract (24.104 Contract clauses; 52.224-1 Privacy Act Notification; and 52.224-2 Privacy Act)?

The OIG generally grants access to the information it collects and uses in the OIG System to its employees and contractors, including independent auditors or other private firms, to carry out specific audit functions or perform analyses or other support tasks.

The TeamMate database contains security features, such as file and project-level restrictions, that provide authorized individuals access to only the specific files or project-level information they need to perform their responsibilities. TeamMate links to CFTC's Windows Active Directory (AD) to ensure that authorized personnel can only access the specific project information or documents to which they are assigned. For example, auditors working on a pending report in TeamMate will only be granted access to the audit projects for which they are responsible. Furthermore, a partition in TeamMate prevents auditors from accessing investigation materials, and prevents investigators from accessing audit information, unless either has demonstrated a business need-to-know the information.

Only individuals designated by the OIG and Office of Data and Technology (ODT) will be allowed access to information on the OIG System. These individuals will include OIG employees and contractors, ODT system administrators, and possibly selected others with a legitimate and confirmed need to know the information to perform their Commission responsibilities.

OIG and CFTC contractors with access to the OIG System are required to comply with the Privacy Act contractually through either FAR terms or other terms and conditions. The Office of the Executive Director's Financial Management Branch (FMB) ensures that the contract between the Commission and contractors contains the provisions necessary to protect and secure information to which the contractors have access.

The information also may be shared in accordance with the applicable Privacy Act System of Records Notice, **CFTC-32, Office of the Inspector General Investigative Files (exempted)**, 76 FR 5993 (February 2, 2011).

4.2. If the data will be shared outside the Commission's network, how will the data be transferred or shared?

Confidential information, including SPII, stored in the OIG System will not be shared outside of the Commission's network, except in accordance with the Inspector General Act or in accordance with the CFTC-32 System of Records Notice, as described above. If transferred or shared outside the Commission's network, confidential information will be protected in a manner designed to prevent unauthorized access and disclosure, for example, by redacting confidential information such as SPII, by clearly marking any unredacted information as "confidential," by transferring electronic confidential information in encrypted form, and by restricting dissemination to only those individuals who are legally authorized to receive the information.

The OIG publishes many of its reports to **its webpage on the Commission's public website**. Before publishing a report, OIG staff allows the CFTC Privacy Office and OGC to redact CFTC confidential information, including SPII, financial position or trading information. The Privacy Office and OGC follow the principles under the Privacy Act of 1974 and the Freedom of Information Act in determining redactions, for example, typically redacting the names and if needed, the titles or other identifying information about individuals who are not CFTC decision-makers. Any redacted reports are marked with the following or similar language on the cover page: "This CFTC OIG Report is subject to the provisions of the Privacy Act of 1974, 5 USC § 552a, and has been redacted as determined by the Commodity Futures Trading Commission. The redactions are not determined by the CFTC OIG."

4.3. If the data will be released to the public, consultants, researchers or other third parties, will it be aggregated or otherwise de-identified (i.e. anonymized)? If yes, please also explain the steps that the Commission will take to aggregate or de-identify the data.

Before releasing a report publicly, OIG staff allows the CFTC Privacy Office and OGC to redact CFTC confidential information. As to PII and SPII, the Privacy Office and OGC use their best efforts to anonymize information related to individuals who are not CFTC decision-makers, as explained above (Section 4.2). For example, if a report refers to an individual who has a unique title and that individual is not a decision-maker, they would change his or her title to a more generic title to avoid re-identification of the individual.

The OIG uses contractors to support OIG functions as needed, including outside auditors. Based on TeamMate security features, individuals working for these contractors will only have access to the information they need to perform their responsibilities. See Section 4.1

4.4. Do the recipients of the aggregated or de-identified information have another dataset, or is there a publicly available dataset that could be used to re-identify Commission information?

When the OIG plans to publish a report on its website, OIG staff allows the CFTC Privacy Office and OGC to redact the report to protect the identities of individuals named in the report, other than CFTC decision-makers. Because the titles of CFTC employees are publicly available, when needed to avoid re-identification, the Privacy Office and OGC use their best efforts to make employee titles more generic.

4.5. Describe how the CFTC will track disclosures of information that will be shared with outside entities. The Privacy Act requires that the CFTC record the date, nature, and purpose of each disclosure of a record to any person or to another agency.

OIG staff track disclosures of information to outside entities through the TeamMate application and database, and through other means, e.g., Excel spreadsheets or SharePoint sites. They track what information was disclosed, to whom it was disclosed (the organization and individual who receives the information) and the date of disclosure, among other things.

4.6. Do other systems share the information or have access to the information in this system? If yes, explain who will be responsible for protecting the privacy rights of the individuals affected by the interface (e.g., System Administrators, System Developers, System Managers)?

The OIG uses the CFTC GSS. Each time an individual logs into the CFTC network, he or she views a Privacy Notice that discusses the importance of maintaining the confidentiality and integrity of the CFTC network and its contents. Various OIG staff, including OIG database administrators and the TeamMate subject matter expert, and the ODT system administrators are responsible for protecting the privacy rights of individuals whose information may be accessible through these interfaces.

OIG staff monitor at least monthly the audit trails of information travelling to, accessed by and stored in the OIG System. They are responsible for detecting unusual system behavior, unusual access or handling of information, and raising any privacy concerns with the CFTC Privacy Office.

5. Notice, Consent and Access for Individuals

5.1. What notice will be provided to individuals about the collection, use, sharing and other processing of their personal data?

The following sub-headers of the **CFTC Privacy Policy** are relevant to the OIG System: "If You Choose To Send Us Personal Information" and "Sharing of Your Information."

This PIA also will appear on **the Privacy Office's CFTC website,** and as noted below, the CFTC maintains a System of Records Notice for the OIG systems of records.

5.2. What opportunities will exist for an individual to decline to provide information or to consent to particular uses of the information? If opportunities exist, how will this notice be given to the individual and how will an individual grant consent?

An individual may decline to provide a report or complaint to the OIG and may choose to submit such information anonymously. For example, the instructions on the online portal instruct users that they may submit anonymously.

However, under the IG Act, the Inspector General may conduct forensic analyses, may subpoena documents or witnesses and engage in other activities to fulfill his or her responsibilities. Depending on the nature of an audit or investigation, individuals may not be able to decline to provide information to OIG staff.

5.3. What procedures will exist to allow individuals to gain access to their information and request amendment/correction, and how will individuals be notified of these procedures?

The OIG system of records is exempt from certain sections of the Privacy Act of 1974 under 5 U.S.C. § 552a(j)(2) and (k)(2).

Under 5 U.S.C. 552a(j)(2), to the extent the OIG system of records relate to the enforcement of criminal laws, such records are exempted from certain sections of the Privacy Act.[2] Under 5 U.S.C. 552(k)(2), other records within the OIG system of records are exempted from 5 U.S.C. 552a(c)(3), (d), (e)(1), (e)(4)(G), (H), and (I) and (f). These records are exempt from the notification procedures, records access procedures, and record contest procedures set forth in the system notices of other systems of records, and from the requirement that the sources of records in the system be described.

6. Maintenance of Controls

6.1. What controls will be in place to prevent the misuse of the information by those having authorized access and to prevent unauthorized access, use or disclosure of the information?

Commission staff are trained to keep OIG confidential information secure and confidential. Records are protected from unauthorized access and improper use through administrative, technical and physical security measures. Technical security measures within the OIG System and the GSS include restrictions on computer access to authorized individuals, unique usernames, strong passwords that are frequently changed, use of encryption for certain data types and transfers, and regular review of security procedures and best practices to enhance security.

Remote access to the OIG System is available only via CFTC-issued laptops through the CFTC's virtual private network (VPN). Further, as described above, access to records is limited to those individuals whose official duties require access by security features built into TeamMate. Physical measures include restrictions on building and OIG office access to authorized individuals and maintenance of records in lockable offices and safes.

6.2. While the information is retained in the system, what will the requirements be for determining if the information is still sufficiently accurate, relevant, timely, and complete to ensure fairness in making determinations?

Audit and investigatory information is analyzed, compared to and reconciled with other information available to the OIG. Government Auditing Standards require that audit information be reviewed by supervisory personnel as part of an audit or review and that it be timely and reflect current CFTC operations.[3]

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

No. The information provided does not allow the OIG to monitor an individual's movement or actions.

---

[2] Specifically, as stated in SORN CFTC 32, OIG records within its system of records are exempt from 5 U.S.C. 552a, except subsections (b), (c)(1), and (2), (e)(4)(A) through (F), (e)(6), (7), (9), (10), and (11), and (i), to the extent the system of records pertains to the enforcement of criminal laws. Under 5 U.S.C. 552(k)(2), such OIG records are exempted from 5 U.S.C. 552a(c)(3), (d), (e)(1), (e)(4)(G), (H), and (I) and (f) to the extent the system of records consists of investigatory material compiled for law enforcement purposes and otherwise as stated in 5 U.S.C. 552a(k)(2).

[3] See Government Auditing Standards 2011 Revision, **GAO-12-331G**.

6.4. Are all IT security requirements and procedures required by Federal law being followed to ensure that information is appropriately secured?

Yes. The CFTC follows the National Institute of Standards and Technology (NIST) Special Publication 800-53, 'Recommended Security Controls for Federal Information Systems' to secure its systems as required by the Federal Information Security Management Act (FISMA).

6.5. Describe the privacy training provided to users either generally or specifically relevant to the program or system.

Commission personnel are subject to agency-wide procedures for safeguarding PII and receive annual privacy and security training. ODT database and system administrators receive special role-based training that will be enhanced and will specifically discuss the sensitivity of the information contained in the OIG System.

7. Privacy Act

7.1. Will the data in the system be retrieved by a personal identifier in the normal course of business? If yes, explain. If not, can it be retrieved by a personal identifier?

Yes. Certain information on the OIG System is generally retrieved by information in identifiable form. However, information stored within TeamMate is labeled so as not to identify an individual who may be the subject of an investigation.

7.2. Is the system covered by an existing Privacy Act System of Records Notice ("SORN")? Provide the name of the system and its SORN number, if applicable.

Yes, **CFTC – 32 Office of the Inspector General Investigative Files (exempted)**.

8. Privacy Policy

8.1. Confirm that the collection, use and disclosure of the information in this system have been reviewed to ensure consistency with the Commission's Privacy Policy on **www.cftc.gov**.

Yes, the following sub-headers of **the CFTC privacy policy** are relevant to the OIG System:

- If You Choose to Send Us Personal Information
- Sharing of Your Information

9. Privacy Risks and Mitigation

9.1. What privacy risks are associated with the collection, use, dissemination and maintenance of the data? How have those risks been mitigated?

The CFTC has adopted the following protections, in addition to those stated above in Section 6 and others, to appropriately safeguard OIG information:

- OIG System is confidential; the CFTC and OIG have limited access strictly to those with a need-to-know based upon an individual's role and responsibility. ODT has vetted its system administrators who have access to TeamMate and provided them with rules of behavior that govern their use of administrator privileges; these system administrators will receive enhanced training that discusses the sensitivity of OIG System information. Unauthorized access and disclosure will be investigated by the OIG.
- When the OIG has access to other CFTC internal systems (e.g., ISS), custodianship is governed in accordance with CFTC information systems security policies.
- Information in the OIG System is secured by, among other controls, complex, frequently-changed passwords; sound security practices that are integrated into the daily routines of OIG staff; audits of events that are significant and relevant to the security of the OIG System and the environment in which it operates; only qualified and authorized individuals may make changes to the OIG System; and the OIG System uniquely identifies and authenticates users. All of the above controls are implemented according to FISMA standards.