Privacy Impact Assessment
for
Office of the Inspector General (OIG) Case Management System

April 2025

Point of Contact
Dennis Phillips
System Owner

Reviewing Official
Kellie Cosgrove Riley
Chief Privacy Officer

OVERVIEW

The Commodity Futures Trading Commission (CFTC) Office of Inspector General (OIG) is implementing a commercial, off-the-shelf case management system operated by OPEXUS known as the OIG Case Management System. It is a cloud-based, FedRAMP certified case management system (CMS), with capabilities to store, manage, and maintain a repository for all CFTC OIG investigations and streamline the current management of those investigations.

The OIG Case Management System will be managed and operated by the CFTC OIG Office of Investigations (OIGI). CFTC OIG is authorized by the Inspector General Act of 1978, as amended, to "conduct and supervise audits and investigations relating to the programs and operations" of the CFTC. 5 USC §§ 402(b) and 415(a)(1)(A). The system will be used only for OIG investigations and not for audits or evaluations.

The Office of the Inspector General page at cftc.gov links individuals (complainants) looking to submit complaints of misconduct by a CFTC Employee or Contractor to the OIG hotline portal. Though uncommon, a complainant may also submit a complaint via FAX, telephone, or physical mail. Lastly, OIG investigators may receive complaints directly from the Chairman, a Commissioner, or a CFTC executive or other employee.

Information that is maintained, disseminated, and used by the system will include information provided by individual complainants via the electronic hotline portal, email, fax, or by phone as well as information and evidence gathered by OIGI personnel during the course of investigations. Information may relate to CFTC employees, contractors, and market participants.

The data within the OIG Case Management System is confidential. Use of the system will be limited strictly to CFTC OIG personnel. Information disseminated will be limited to that necessary to resolve hotline complaints and investigations, typically in investigative reports issued to the Commission by the IG.

1. AUTHORITIES AND OTHER REQUIREMENTS

1.1 What legal authority(ies) permit or require the CFTC to collect, use, maintain, or disseminate the information in the system, project, or program?

The Inspector General Act of 1978 as amended (codified at 5 U.S.C. § 401, et seq.) establishes Offices of Inspector General across the federal government and provides that such offices shall "conduct and supervise audits and investigations relating to the programs and operations" of their respective agencies. 5 U.S.C. § 402(b). The Act further specifically establishes an Office of Inspector General for the Commodity Futures Trading Commission. 5 U.S.C. § 415(a)(1)(A).

In addition, the Act provides that each OIG "may receive and investigate complaints or information from an employee of the establishment concerning the possible existence of an activity constituting a violation of law, rules, or regulations, or mismanagement, gross waste of funds, abuse of authority, or a substantial and specific danger to the public health and safety." 5 U.S.C. § 407(a). It further provides that each OIG "shall not, after receipt of a complaint or information from an employee, disclose the identity of the employee without the consent of the employee, unless the Inspector General determines the disclosure is unavoidable during the course of the investigation." 5 U.S.C. § 407(b).

1.2 Is there a Privacy Act System of Records Notice(s) (SORN(s)) that applies to the information in the system, project, or program? If yes, please identify it. If no, please explain why not.

Yes. CFTC-32, Office of the Inspector General Investigative Files (Exempted) 88 Fed. Reg. 20141, applies to the records in this system.

1.3 Please identify the applicable accreditation boundary evaluated during the Authority to Operate (ATO) process. If the system is hosted by a Cloud Service Provider (CSP), please identify the CSP and state whether the system has Federal Risk and Authorization Management Program (FedRAMP) authorization.

The OIG Case Management System is hosted by OPEXUS which is a FedRAMP® certified cloud environment. At the time of this PIA, the system is currently undergoing the CFTC's ATO process.

1.4 Is there a records retention schedule(s) approved by the National Archives and Records Administration (NARA) that governs the retention of the records maintained in the system, project, or program? If yes, please identify the schedule. If not, please explain.

Yes. The records in the OIG Case Management System are subject to CFTC-specific Records Schedule 312, *OIG Audit, Investigation, and Inspection Case Files,* DAA-0180-2018-0006-0004.

1.5 Please list all forms or other information collection instruments that are used to collect the information in the system. If the information collected is subject to the Paperwork Reduction Act, provide the name of the form or information collection and the applicable OMB control number.

Information may be collected with the OIG Intake Form through the electronic hotline portal. Though uncommon, information may also be collected in the form of an email, fax, or phone call through the OIG Hotline. Complaints may also come directly from

the Chairman, a Commissioner, or a CFTC executive or other employee to OIG investigators. The information collected is not subject to the Paperwork Reduction Act.

2. INFORMATION

2.1 Identify the information that the system, project, or program collects, maintains, uses, or disseminates.

The system will collect, maintain, and use information from individuals (complainants) about themselves and the subjects of complaints. The hotline portal will specifically request name(s), contact information (including personal/business email addresses and telephone numbers), employment information, and the substance of the complaint. In the course of providing the requested information, complainants may also choose to provide other information potentially relevant to their complaints that is not specifically requested. Once the complaint is submitted through the hotline portal, all the information within the form is then automatically populated within the system. For complaints submitted through other media such as FAX, physical mail, or phone, complainants may provide any information they believe to be potentially relevant and not limited to that which is requested at the hotline portal. These complaints are then manually input into the system by OIG Investigators.

CFTC Entra ID information will be collected for the purpose of allowing CFTC OIG Investigators to sign into the system via Single Sign On (SSO). During the course of evaluating complaints and conducting investigations, OIG investigators may gather additional information that is relevant to the complaint and enter it into the system.

2.2 Is the information collected directly from the individual and, if not, what are the sources of information collected. How is the information obtained?

Information may be provided by individuals (complainants) who submit complaints in web form via the hotline portal, email, fax, phone call through the OIG Hotline, or directly to a CFTC OIG investigator. Complaints that are received other than via the hotline portal are entered into the system by OIG Investigators, who access the system via SSO, enabled by credentials from Entra ID. CFTC OIG Investigators also collect information from sources other than the individual complainant in the course of their investigations. This information will be collected in paper form, email, secure file transfer protocol, and other collection mechanisms that depend largely on the way in which the information sought is stored by custodians. That information will then be uploaded, scanned, or manually input into the system by CFTC OIG investigative personnel.

2.3 What steps are taken to minimize the collection of information in the system, project, or program?

In the course of an investigation, it is not always immediately clear what information is necessary to fully investigate and resolve a complaint. While the hotline portal questionnaire is designed to obtain only relevant information pertaining to a complaint and the OIG Investigators seek out additional relevant information in the process of completing their investigation, the nature of investigations generally is such that the OIG Investigators may collect more information than is ultimately necessary for or relevant to their investigation. This is permissible here and consistent with the Privacy Act exemption the CFTC has taken with respect to the relevant system of records from 5 U.S.C. 552a(e)(1), See 17 C.F.R. 146.12(e)(4).

2.4 Discuss how the accuracy, integrity, and/or quality of the information identified above are determined.

The accuracy, integrity, and quality of information collected is determined on a case-by-case basis. Many hotline complaints do not require such determinations prior to resolution. In those cases in which hotline matters are formally investigated, a formal review of the information is conducted by OIG investigators, where the accuracy, integrity, and quality will be determined in accordance with the Quality Standards for Investigations promulgated by the Council of Inspectors General on Integrity and Efficiency, the CFTC OIG Investigations Manual, Department of Justice guidance, and statutes and regulations that govern the substance of the matter under investigation.

2.5 Privacy Impact Analysis: Related to the Collection and Characterization of the Information

There is a risk that more information will be collected than is necessary to meet the business needs addressed by the OIG Case Management System. Given the nature of OIG investigations, OIG Investigators may collect more information than is ultimately necessary for or relevant to their investigation as they analyze information and determine its relevance and veracity. This risk is mitigated in part by establishing effective procedures to identify and collect relevant and necessary information and, where additional information is collected, trained investigators determining what is to be included within the investigation file within the system, by mitigating any risk to individuals by securely storing the information within the system.

There is also a risk that the information collected may not be accurate. This risk is minimized by collecting relevant information directly from the individual who has an interest in providing accurate information and by the Privacy Act Statement on the hotline form that provides notice to the individual that that knowingly and willfully making false or fraudulent statements to the Commission is subject to the criminal penalties set forth in 18 U.S.C. § 1001, which include imprisonment of not more than five years, imposition of a substantial fine under the Federal Sentencing Guidelines, or both. This risk is further mitigated by employing trained OIG Investigators who

follow OIG standards for accuracy, integrity, and quality set forth in the Quality Standards for Investigations promulgated by the Council of Inspectors General on Integrity and Efficiency, the CFTC OIG Investigations Manual, Department of Justice guidance, and statutes and regulations that govern the substance of the matter under investigation.

3. USE OF THE INFORMATION

3.1 Describe how the information is used internally at the CFTC to support a business purpose.

The information collected from individuals via the hotline portal and from other sources by the OIG investigators will be used for purposes of resolving hotline complaints and conducting investigations under the authority of the Inspector General Act of 1978, as amended.

3.2 Identify all programs or offices, and an approximate number of individuals, within the CFTC that have assigned roles and responsibilities with respect to the system, project, or program or with whom information is shared. Explain how each uses the information.

Access to the information in the system will be limited strictly to CFTC OIG personnel (approximately 5 users). CFTC personnel outside the OIG (including IT staff) will not have access to the information.

3.3 Privacy Impact Analysis: Related to the Internal Access and Use

There is a risk that the information in the system will be accessed by an unauthorized user or accessed by an authorized user for a purpose that is not authorized or is inconsistent with the purpose for which it is being collected and maintained in the OIG Case Management System.

This risk is mitigated through the use of Role Based Access Controls (RBAC) comprised of user provisioning, permissions management, and access controls. User access is also mapped to organizational duties performed to ensure that users are only processing data specific to their authorized functions. Additionally, all users must agree to Rules of Behavior prior to being granted access to the system.

4. INFORMATION SHARING

4.1 Is the information shared outside of the CFTC as part of usual agency operations? If so, identify the organizations or individuals with whom the information is shared, how and *why* it is shared, and how it is to be used.

No outside agencies or entities have direct access to the OIG Case Management System. Information may be shared with other agencies only when it pertains to their mission (e.g., prosecution referrals to the Department of Justice). In circumstances where case information is shared with other agencies, the information is downloaded by OIG Investigators then sent via encrypted email to the respective agency.

4.2 How is the information sharing described in 4.1 compatible with the purpose for which it was originally collected described in 3.1?

As noted in section 3.1 and as set forth in the purpose section of the CFTC-32, Office of the Inspector General Investigative Files, SORN, the records in this system are collected to enable the OIG to effectively and efficiently conduct investigations relating to programs and operations at the CFTC. Disclosure of investigative records to the Department of Justice or to other agencies consistent with their missions is compatible with this purpose as such disclosures are intended to further the investigation and/or to act on the results of the investigation. Such disclosures are permitted pursuant to the routine uses set out in CFTC-32.

4.3 Is the information sharing documented in a Memorandum of Understanding, other information sharing agreement, or a contract?

Generally, the information sharing described above is not subject to an MOU, other information sharing agreement, or contract. Rather, it is dictated by statute. For example, 5 U.S.C. § 404(d) provides: "In carrying out the duties and responsibilities established under this chapter, each Inspector General shall report expeditiously to the Attorney General whenever the Inspector General has reasonable grounds to believe there has been a violation of Federal criminal law." With regard to coordination with other Inspectors General, 5 U.S.C. § 406(a)(3) provides that Inspectors General are authorized "to request such information or assistance as may be necessary for carrying out the duties and responsibilities provided by this chapter from any Federal, State, or local governmental agency or unit thereof[.]"

4.4 Are there limitations on re-dissemination of the information by the third party in place, either in the documents identified in 4.2 or otherwise?

There are no specific limitations on re-dissemination of the information disclosed to the Department of Justice or to other agency OIGs. The receiving agency is subject to the Privacy Act and the Inspector General Act and handles the disclosed information accordingly.

4.5 Describe how the system, project, or program accounts for and maintains a record of disclosures outside of the CFTC.

The OIG Case Management System includes a database to track external correspondence. In addition, the CFTC OIG maintains a correspondence log for information that is disclosed outside of the CFTC. The correspondence log tracks who the correspondence is addressed to, the date of correspondence, the subject, signed by, transmitted by, file type, and any comments pertaining to the correspondence. The correspondence logs are maintained within each respective case file within the OIG Case Management System. As such, they are retained the same amount of time as the case file itself.

4.6 Privacy Impact Analysis: Related to Information Sharing

There is a risk that information from the OIG Case Management System may be inappropriately disclosed outside of the CFTC. This risk is mitigated by sharing information about individuals only as permitted by the CFTC-32, Office of the Inspector General Investigative Files* (Exempted), SORN.

There is also a related risk that information, once shared appropriately, will be further shared or used in a manner that is inconsistent with the original purpose for which it was collected and shared. This risk is mitigated by sharing the information only pursuant to the relevant routine uses with entities that are also subject to the requirements of the Privacy Act and/or the Inspector General Act.

5. DATA RETENTION

5.1 Explain how long and for what reason the information is retained.

Records are kept in accordance with their applicable retention schedules as identified above. The records are retained under Disposition Authority DAA-0180-2018-0006-0004, which requires that the records within the OIG Case Management System destroyed 10 years after the case is completed.

5.2 Describe how the information is disposed of at the end of its retention period.

Once information with the OIG Case Management System has reached the end of its record retention schedule, it is manually deleted from the system. All records are destroyed using the proper destruction method outlined in the CFTC Records Management Manual and using the Records Destruction Approval Form.

5.3 Privacy Impact Analysis: Related to Retention

There is risk that information within the OIG Case Management System may be retained longer than is necessary to meet the business need for which it was collected. This risk is mitigated by adhering to the applicable records schedule, and

by adhering to the investigations manual, that has been amended by the system owner to include reference to the agency's records retention/deletion policy.

6. NOTICE

6.1 How are individuals provided notice prior to the collection of their information? If they are not provided notice, please explain why.

General notice regarding the collection and use of an individual's information within the OIG Case Management System is provided via publication of this PIA. Additional information regarding the collection and use of certain records about individuals that may ultimately be collected and used within the OIG Case Management System is provided via publication of the applicable Privacy Act system of records notice.

More direct notice is provided by the Privacy Act Statement within the hotline portal (OIG Intake Form) used by individuals to submit complaints.

6.2 Do individuals have the opportunity to consent to the use of their information or decline to provide their information? Please explain.

Hotline portal submissions are voluntary. Once an individual provides information via the hotline or other media, they do not have the opportunity to consent to the inclusion of their information in the OIG Case Management system. Other individuals from whom the OIG Investigators may request information must provide the requested information pursuant to 5 U.S.C. § 406(a)(1) or they may be subject to administrative or disciplinary action.

An individual is provided the opportunity to consent to the type of disclosure of their identity prior to submitting the intake form through the hotline portal. The individual is provided a drop-down menu within the form for them to choose if they wish to remain anonymous, to have their submission be confidential to only those inside the OIG, or to consent to full disclosure of their identify. This option is provided prior to submission of the form.

Individuals who are the subject of a complaint or investigation are not afforded the opportunity to consent to the collection or use of their information.

6.3 Privacy Impact Analysis: Related to Notice

There is a risk that individuals are not aware that the OIG Case Management System collects and uses their information. This risk is mitigated through the publication of this PIA and, for those individuals who submit complaints via the hotline portal, by providing notice via a Privacy Act statement, at the point of collection. The subject of a complaint is not notified unless the complaint leads to an investigation; the

subject of the investigation is notified after an investigation is opened no later than at their interview.

7. REDRESS

7.1 What procedures are in place that allow individuals to access their information?

Individuals who submit complaints do not have access to the OIG Case Management System. If the individual submitted a complaint through the hotline portal form that contained inaccurate or incorrect information, that individual would need to resubmit the form containing the correct information. Moreover, complaints received via the hotline portal are confidential, as provided at 5 U.S.C. § 407. As such, complaints that are dismissed or otherwise resolved without investigation are not publicly disclosed.

The records contained in the CFTC-32, Office of the Inspector General Investigative Files, system of records have been exempted by the Commission from the access and amendment provisions of the Privacy Act of 1974. Individuals may request access to any non-exempted records by following the procedures outlined in the relevant SORN.

7.2 What procedures are in place to allow individuals to correct inaccurate or irrelevant information about themselves?

Individuals who submit complaints do not have access to the OIG Case Management System. If the individual submitted a complaint through the hotline portal form that contained inaccurate or incorrect information, that individual would need to resubmit the form containing the correct information.

The records contained in the CFTC-32, Office of the Inspector General Investigative Files, system of records have been exempted by the Commission from the access and amendment provisions of the Privacy Act of 1974. Individuals may request access to non-exempted records by following the procedures outlined in CFTC-32. However, individual subjects of investigations are provided opportunities to rebut or otherwise correct adverse information in accordance with the Council of Inspectors General Quality Standards for Investigations and, should an investigation lead to agency corrective actions See 5 U.S.C. Chapter 75.

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

The procedures for submitting a request to correct information are outlined in the applicable SORN.

7.4 Privacy Impact Analysis: Related to Redress

There is a risk that individuals may not be able to access information about themselves that is contained within the OIG Case Management system nor be afforded adequate opportunity to correct that information. This risk is mitigated by providing individuals, where required and appropriate, with an opportunity to obtain access to and request amendment of their records.

8. AUDITING AND ACCOUNTABILITY

8.1 How is the information in the system secured?

CFTC employs a variety of physical, technical, and administrative controls to secure the OIG Case Management System. Access is limited by user role and "need to know." The data within the OIG Case Management System is confidential. Use of the system will be limited strictly to CFTC OIG personnel. The information within the system is only accessible within the CFTC environment using CFTC issued equipment.

8.2 Are audit logs generated reflecting access and use of the information in the system? If not, please explain. If so, please describe how often they are reviewed and for what purpose.

Access audit logs are generated continuously for the OIG Case Management System for the purpose of monitoring for suspicious or unusual activity. The audit logs contain limited personally identifiable information, such as username and case/matter ID. The system owner and OIG staff will have direct access to the logs and will review them as needed. Any information that is collected or amended by OIG Investigators is tracked by the system through the Chron log, which details what information was added or amended, along with what documents (if any) were uploaded. The Chron log also captures the date and time those amendments were made and by whom.

8.3. What procedures are in place to determine who has access to the system, and are they documented?

Access to the information will be limited strictly to CFTC OIG personnel. The system owner (the Assistant Inspector General for Investigations (AIGI)) is responsible for determining whether an individual may have access to the system. For new users who request access to the system, the AIGI confirms that the CFTC OIG personnel requesting access has a legitimate need for the use of the system before granting that individual access.

8.4 Describe what privacy training is provided to users, either general or specific to this system or project.

All users are required to complete Cybersecurity and Privacy Awareness Training prior to obtaining access to the Commission's network and systems and annually thereafter. A user's failure to complete the annual training requirement will result in their network access being terminated.

8.5 Privacy Impact Analysis: Related to Auditing and Accountability

There is a risk that the audit logs and access control lists will not be used effectively to maintain the security of the OIG Case Management System. This risk is mitigated through the creation of audit logs and Cron logs. The access control list is reviewed in a consistent manner on an as-needed basis and any time a change is made to the system to ensure that only the individuals who need access are granted access. There is also a more general risk that those with access to the OIG Case Management System will not understand their obligations with respect to the privacy and security requirements pertaining to the information in the system. This risk is mitigated through users receiving annual training and signing rules of behavior in order to access the system.