Privacy Impact Assessment
for
Ownership and Control Reporting (OCR)

June 9, 2025

Point of Contact
Howard Rosen
Information Security Officer
CFTC Market Financial System (MFS) - Data Engineering & Processing (DEAP)(MFS-DEAP) Program

Reviewing Official
Kellie Cosgrove Riley
Chief Privacy Officer

OVERVIEW

On November 18, 2013, the Commodity Futures Trading Commission ("Commission" or "CFTC") published the ownership and control rules and related forms (the "OCR final rule") to better identify futures and swap market participants. The OCR final rule, 78 Fed. Reg. 69187 (Nov. 18, 2013) (17 CFR Parts 15, 17, 18, and 20,) leverages the Commission's current position and transaction reporting programs by requiring the electronic submission of trader identification and market participant data on the following electronic forms: CFTC Form 102A Identification of Special Accounts, CFTC Form 102S Identification of Consolidated Accounts, CFTC Form 102B Identification of Volume Threshold Accounts, and CFTC Form 40 Statement of Reporting Trader Form.

The Commission receives end-of-day position reports electronically from exchange clearing members, Futures Commission Merchants (FCMs), Designated Contract Markets (DCMs), foreign brokers, and other reporting firms. The OCR forms require the reporting of certain trading accounts active on designated contract markets or swap execution facilities (SEFs).

CFTC Form 102A collects information on all industry participants (who may be individual participants or may be firms) that own or control position-based special accounts and the trading accounts associated with that special account. CFTC Form 102B collects information on all participants that own or control trading accounts that meet specified volume-based reporting levels. CFTC Form 102S collects information on all participants that own or control consolidated accounts associated with the Physical Commodity Swaps (from Part 20 data). CFTC Form 40 collects information on all participants to include how the participants identify themselves to the Commission, the type of participants that they are (e.g., individual, corporation), their registration type (e.g., broker, trader, FCM), and their trading and related business activities.

The information collected on these forms allows the Commission to more efficiently link special accounts holding reportable positions to the transactions and associated trading accounts identified on daily trade capture reports received by the Commission. By illustrating the connections between end-of-day position reporting and daily trade capture reports, the OCR final rule enables the Commission to perform a more accurate and timely accounting of market position at the level of individual trading accounts. Furthermore, the addition of volume-based reporting on CFTC Form 102B provides the Commission with an efficient means to collect the information required to aggregate positions, detect intra-day position limit violations, and calculate market share. The CFTC designed the Ownership and Control Reporting System (OCR) to:

- receive and store ownership and control information concerning each large trader and reportable account related to futures, options, physical commodity swaps, and swaptions positions;

- automate the forms 40 and 102A/B/S receipt process, moving from the legacy process of receiving these files via postal mail and email/PDF to better secure those forms during transmission;
- enhance forms 40 and 102A/B/S to get better and more accurate data about market participants;
- link transaction-level data to position-based data in the futures and options market;
- email participants to request their Form 40 submissions;
- email a notification to the reporting firm carrying the account if a trader misses the Form 40 filing deadline;
- collect ownership and control information for market participants' special accounts (and associated trade accounts), consolidated accounts, and volume accounts;
- correlate trade data with end-of-day position data so that CFTC staff can more-easily conduct analysis and monitor intraday position limits; and
- aggregate and anonymize OCR data for use in the Commission's public reports, such as the Commitment of Traders report and the Cotton-On-Call report.

OCR also enables the CFTC to load the data into powerful analytical tools that perform a variety of functions across the oversight program. CFTC staff in the mission facing divisions of the CFTC rely on OCR to understand the ownership and control structures of organizations or individuals who hold positions in the markets that the CFTC oversees.

OCR data may be shared with other agencies outside of the CFTC to include the Federal Energy Regulatory Commission (FERC) and the Federal Agency Members of the Inter-Agency Working Group for Market Surveillance. This sharing with other agencies is documented within Memorandums of Understanding (MOUs) and details the purpose that the information is shared to identify industry market participants.

OCR data is confidential; the CFTC has limited access strictly to those with a need-to-know based upon an individual’s role and responsibility. The Division of Data (DOD) has vetted the administrators of the connected systems.

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 information in OCR is primarily collected by the Commission pursuant to the authority of sections 4a, 4c(b), 4g, 4i, 4t, and 8 of the Commodity Exchange Act

(CEA). Collectively, these CEA provisions warrant the maintenance of an effective and rigorous system of market and financial surveillance and authorize the collection of related information. For example, CEA Section 4i requires the filing of reports as the Commission may require when positions taken or obtained on a designated contract market equal or exceed Commission set-levels; Section 4g requires, among other things, the filing of such reports as the Commission may require regarding proprietary and customer transactions and positions in commodities for future delivery on any board of trade in the United States or elsewhere; and 4c(b) gives the Commission plenary authority to regulate transactions that involve commodity options.

Pursuant to the CEA, the Commission promulgated final rules codified at 17 CFR parts 15, 17, 18 and 20 that collectively require certain reporting firms and parties, as well as persons owning or controlling reportable positions, to report information contained in CFTC Forms 40, 71, and 102, as applicable. The information requested on these forms, which are appendices to parts 17 and 18, are the primary sources of the OCR System data.

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. The CFTC-15, Enterprise Surveillance, Oversight & Risk Monitoring System SORN covers any Privacy Act records in OCR.

1.3 Please identify the applicable accreditation boundary evaluated during the Authorization to Operate (ATO) process. If the system, or involved project or program, 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.

OCR is a system within the CFTC Market Financial System (MFS) - Data Engineering & Processing (DEAP) (MFS-DEAP) Program. The MFS-DEAP Program is comprised of 26 applications which provide systems implementation, operations and maintenance, and support for its user community. OCR is not a CSP but is self-hosted in the Commission's instance of the Microsoft Azure cloud environment. The MFS-DEAP boundary was authorized on March 27, 2023. Much of the data within OCR is received through the CFTC Portal, which is included in the CFTC Portal boundary, which was authorized on July 18, 2023. All the data is processed and stored within the MFS-DEAP boundary.

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 OCR are governed by the following CFTC Mission Records Schedules:

- 602, *Market, Financial, and Other Data Submissions*, DAA-0180-2022-0003-0001
- 603, *Noteworthy Market Events*, DAA-0180-2022-0003-0002
  604, *Summary of Data Submissions*, DAA-0180-2022-0003-0003

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.

Form Name and Form Number	**OMB Control No.** *(If applicable)*
CFTC Form 102A: Identification of "Special Accounts"	3038-0103
CFTC Form 102S: Identification of Consolidated Accounts"	3038-0103
CFTC Form 102B: Identification of Volume Threshold Accounts	3038-0103
CFTC Form 40: Statement of Reporting Trader	3038-0103

2. INFORMATION

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

The data that is received from forms listed below contains information about industry participants, special accounts, trade accounts, consolidated accounts, and volume accounts. The detail of the data on these forms include names, addresses, and firm information of the associated owners and controllers of the accounts.

- CFTC Form 102A - This is an updated version of the legacy 102 form, the "Identification of Special Accounts" form, described in the Commission's regulations at 17 C.F.R. § 17.01. Form 102A captures data about the Special Account, including more owner and controller information as well as data about the trade accounts that comprise the Special Account, including ownership and control data associated with those trade accounts. The

information collected from this form includes Name, Legal Entity Identifier (LEI), National Futures Association (NFA) ID, Business Phone Number or Fax Number, Business E-mail Address, Business Mailing Address, and Business Mobile Number.

- CFTC Form 102S - This is an updated version of the legacy Form 102S form, the "Identification of Consolidated Accounts" form, described in the Commission's regulations at 17 C.F.R. §§ 20.4, 20.5. This enhanced version of the previous Form 102S captures more data about the Consolidated Account, including more information about the owners and controllers of the account. The information collected from this form includes Name, LEI, NFA ID, Business Phone Number or Fax number, Business E-mail Address, Business Mailing Address, and Business Mobile Number.

- CFTC Form 102B - This form, the "Identification of Volume Threshold Accounts," is described in the Commission's regulations at 17 C.F.R. § 17.01(b). Form 102B is used to identify trade accounts that meet a volume threshold set forth in the OCR final rule within a single trading day, regardless of whether positions continue to be held at the end of the day. This form captures owners and controllers of the trade account. The information collected from this form includes Name, LEI, NFA ID, Business Phone Number or Fax number, Business E-mail Address, Business Mailing Address, and Business Mobile Number.

- CFTC Form 40 – This form, the "Statement of Reporting Trader," requires traders to identify themselves to the Commission, describing the type of traders that they are (e.g., individual, corporations), their registration type (e.g., broker, trader, FCM), and their trading and related business activities, as well as more detailed information about the owners and controllers of the trader. The Commission sends Form 40 (described in the Commission's regulations at 17 C.F.R. § 18.04) to the trader via a special call which requires entities to detail the actual values of commodity-index investment related to each US futures market. The information collected from this form includes Name, Business Phone Number or Fax number, Business Mailing Address, and Business Mobile Number.

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?

The information on the forms described above is collected directly from industry participants who complete the electronic forms and submit them through the CFTC Portal or using a secure file transfer protocol (SFTP).

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

The Commission's regulations authorize it to request reporting information from industry participants with large futures and the Commission has designed its forms to collect only the information authorized by the regulation. Therefore, only the information necessary to identify ownership and control information concerning each large trader and reportable accounts, market participants' special accounts (and associated trade accounts), consolidated accounts, and volume accounts is requested. The Commission provides specific instructions to the industry participants on forms 102A/B/S and 40 regarding what information to submit. The DOD and DMO reviews the forms to ensure accurate data is provided. If any information pertaining to individuals were to be provided within the forms where numerical data should be, the DMO would request resubmission of the form. None of the individual data is included in the Commission's public reporting.

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

By regulation, all submitters are responsible for making sure their data are complete and correct; given the regulatory requirement, it is generally presumed that the industry participants have an interest in submitting accurate data and, therefore, it is generally presumed to be accurate and of good quality and integrity. If inaccuracies are discovered, submitters have the ability to update their data through submission of updated forms. The OCR Technical Guidance Document states the requirement and procedures for submitting corrected data to the CFTC.

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

There is a risk that more information is collected than necessary to meet the business needs of processing. OCR has mitigated this risk by providing specific instructions regarding what information submitters must provide, in accordance with the applicable regulations, to avoid unnecessary collection of information; and by redacting any information that is collected inadvertently.

3. USE OF THE INFORMATION

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

The information in OCR is used to identify industry participants in futures, options, and commodity-based swaps markets. The information is also used to do analysis of the end-of-day futures and options position data (Part 17), transaction data for futures and options (Part 16.02), and end-of-day commodity-based swaps and swaptions data (Part 20).

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.

Approximately 300 individuals in the CFTC mission divisions have access to the information in OCR in order to fulfill their mission duties as designated by the commission. They use the information for the purposes described above in Section 2.

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

There is a risk that an unauthorized individual may access the information or that an authorized individual may access the information for an unauthorized purpose resulting in information within OCR being used in a manner that is inconsistent with the purpose for which it is being collected and maintained in OCR.

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. Individuals within the division must show a need to access the OCR data for their work within their division. OCR further secures information through audits of events that are significant and relevant to the security of OCR and the environment in which it operates. These audit logs are reviewed by the CFTC security team and the CFTC applications team on an as-needed basis. 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.

Information is shared with other agencies via Memorandums of Understanding (MOU) in place with those agencies. The decision to share this information with other agencies is made on a case-by-case basis.

Currently, there are two MOUs in place that might include data from OCR: the Memorandum of Understanding Between the Commodity Futures Trading Commission and the Federal Energy Regulatory Commission (FERC), and the Memorandum of Understanding Regarding the Treatment of Non-Public Information Shared Among the Federal Agency Members (the Department of Treasury, the

Board of Governors of the Federal Reserve System, and the Securities and Exchange Commission) of the Inter-Agency Working Group for Market Surveillance.

OCR data may be shared with FERC for the purpose of market surveillance or an investigation into potential manipulation, fraud, or market power abuse in markets subject to FERC's regulation or oversight. FERC's oversight ensures that information requests to markets within the respective jurisdiction of each agency are properly coordinated to minimize duplicative information requests and to address the treatment of confidential information. All data shared with FERC is transferred securely through the Secure File Transfer Protocol (SFTP).

OCR data may be shared with the Inter-Agency Working Group for Market Surveillance for the purpose of assisting parties in the surveillance of U.S. Treasury securities related derivatives markets. All data shared with Inter-Agency Working Group for Market Surveillance is transferred securely through SFTP.

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?

The information sharing described above is done for market surveillance and investigatory purposes and is permissible pursuant to general routine use 8 and is compatible with the purpose for which the information was collected as described in thein the CFTC-15, Enterprise Surveillance, Oversight & Risk Monitoring System SORN:

"The records in this system are used to support market oversight, and market, risk and financial surveillance activities, specifically, monitoring the commodity futures and swaps markets, performing various mission-critical commodity futures, and swaps market analyses, reviewing activities of registered entities for compliance with the Commodity Exchange Act and Commission regulations, and conducting surveillance on both intra and inter-exchange and across side-by-side electronic trading platforms. Records are also used to support firm and registrant oversight, including compliance with the Commission's financial and regulatory requirements."

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

The information sharing is documented in MOUs: the Memorandum of Understanding Between the Commodity Futures Trading Commission and the Federal Energy Regulatory Commission (FERC), and the Memorandum of Understanding Regarding the Treatment of Non-Public Information Shared Among the Federal Agency Members of the Inter-Agency Working Group for Market Surveillance.

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 limitations on re-dissemination of the information by the third party in place. The MOUs clearly state that the agencies may not disclose any information provided by the CFTC to any third party (including any governmental party) without the prior written consent of the CFTC.

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

When information is shared with an external agency or entity outside of the CFTC, OCR accounts for and maintains a record of those disclosures. The record of disclosures includes an application log that contains all transmissions of data to include date, nature, and purpose for the sharing, and the name and address of the external agency of which there is an MOU in place.

4.6 Privacy Impact Analysis: Related to Information Sharing

There is a risk that information from OCR may be inappropriately disclosed outside of the CFTC. This risk is mitigated by only sharing information about individuals as permitted by the applicable SORN, CFTC-15, Enterprise Surveillance, Oversight & Risk Monitoring System, and, where appropriate, documenting that information sharing in an MOU or other information sharing agreement.

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 where the sharing is subject to written agreements as described in sections 4.3 above, which define the purposes for which the information is shared, prohibits additional uses, and appropriately limits any onward sharing with third parties.

5. DATA RETENTION

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

The records in OCR are maintained and then disposed of in accordance with the CFTC Mission Schedules described in Section 1. Records subject to CFTC Mission Schedule 602, Market, Financial, and Other Data Submissions, are retained under Disposition Authority DAA-0180-2022-0003-0001, which requires that the records be destroyed between 20 years and 40 years after they are submitted to the CFTC. Records subject to CFTC Mission Schedule603, Noteworthy Market Events, are retained under Disposition Authority DAA-0180-2022-0003-0002, which requires that the records be destroyed 50 years after an identified event. Lastly, records

subject to CFTC Mission Schedule 604, Summary of Data Submissions, are retained under Disposition Authority DAA-0180-2022-0003-0003, which requires that the records be destroyed 75 years after submission.

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

Records are kept in accordance with their applicable retention schedules. Information will be deleted as part of the manual archive/deletion process that runs on a monthly basis, based on the data retention processes. At the time of this PIA, data within OCR has not reached the applicable cutoff and disposition dates.

5.3 Privacy Impact Analysis: Related to Retention

There is risk that information in OCR 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 schedules, which address the business need to retain the information. When records are scheduled for destruction based on the retention schedule, the information is deleted as part of the manual OCR archive/deletion process that runs on a monthly basis.

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.

Industry participants are provided notice about the collection of information through the Privacy Act Statements on forms 102A/B/S and 40 located within CFTC Portal, at the point of collection. Notice is also provided via this PIA and the CFTC-15, Enterprise Surveillance, Oversight & Risk Monitoring System SORN published in the Federal Register and posted online.

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

Industry participants are required by the CEA to submit their data to the Commission. Traders can decline to provide their information by not participating in U.S markets. Consent is implied when industry participants fill out and submit forms 102A/B/S and 40. The following notice is provided within forms 102A/B/S and 40 which explains the consequences of industry participants not providing their information:

"NOTICE: Failure to file a report required by the Commodity Exchange Act ('CEA' or the 'Act') and the regulations thereunder, or the filing of a report with the Commodity Futures Trading Commission ('CFTC' or 'Commission') that includes a false, misleading or fraudulent statement or omits material facts that are required

to be reported therein or are necessary to make the report not misleading, may (a) constitute a violation of section 6(c)(2) of the Act (7 U.S.C. 9), section 9(a)(3) of the Act (7 U.S.C. 13(a)(3)), and/or section 1001 of Title 18, Crimes and Criminal Procedure (18 U.S.C. 1001) and (b) result in punishment by fine or imprisonment, or both."

The Privacy Act Statement on form 40 further provides notice regarding the effect of traders declining to provide information:

"The collection of this information is required, and failure to comply may result in the imposition of criminal or administrative sanctions (see, e.g.,7 U.S.C. §§ 9 and 13a-1, and/or 18 U.S.C. § 1001)."

6.3 Privacy Impact Analysis: Related to Notice

There is a risk that individuals will not receive notice about how OCR collects and uses their information. This risk is mitigated for industry participants using the CFTC Portal to submit electronic forms 102A/B/S and 40 via the Privacy Act statement presented to them at the point of collection. The risk is also mitigated through the publication of this PIA and the CFTC-15, Enterprise Surveillance, Oversight & Risk Monitoring System SORN.

7. REDRESS

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

Individuals do not have direct access to OCR to view or obtain data that they previously submitted to the Commission. Industry participants may retain a copy of the Extensible Markup Language (XML) version of the information they submit to the Commission via the SFTP submission process. Those Industry participants who submit through the CFTC Portal, can receive copies of the XML being created by the CFTC Portal forms. Individuals may also request access to records about themselves that are included in the CFTC-15, Enterprise Surveillance, Oversight & Risk Monitoring System SORN by following the procedures outlined in that SORN and in the Commission's regulations at 17 C.F.R. Part 146.

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

Industry participants are required by the CEA to submit corrected or amended versions of their OCR data whenever the data changes. Amended data can be sent to the Commission through SFTP submissions or through the CFTC Portal.

Individuals may also request amendment of Privacy Act covered records about themselves by following the procedures outlined in the CFTC-15, Enterprise Surveillance, Oversight & Risk Monitoring System SORN by following the procedures outlined in that SORN and in the Commission's regulations at 17 C.F.R. Part 146.

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

Industry participants are required by regulation to submit corrected or amended versions of their data whenever the data changes. The ownership and control rules and the OCR Technical Guidance Document clearly state the requirement and procedures for submitting corrected data to the CFTC. The OCR Technical Guidance Document may be found within the Ownership & Control Reporting page on cftc.gov.

The procedures for submitting a request to correct Privacy Act covered information are also outlined in the applicable SORN, CFTC-15, Enterprise Surveillance, Oversight & Risk Monitoring System, and in the Commission's regulations at 17 C.F.R. Part 146.

7.4 Privacy Impact Analysis: Related to Redress

There is a risk that individuals may not be able to access information about them that is contained within OCR nor be afforded adequate opportunity to correct that information. This risk is mitigated by providing individuals with an appropriate opportunity to request access to and amendment of their records as outlined in the applicable CFTC-15, Enterprise Surveillance, Oversight & Risk Monitoring System SORN. This risk is further mitigated because traders are required by regulation to submit corrected or amended versions of their OCR data whenever the data changes; the processes for keeping OCR data current and submitting corrected data are clearly described in the OCR regulation and the OCR Technical Guidance Document.

8. AUDITING AND ACCOUNTABILITY

8.1 How is the information in the system secured?

OCR data submissions are submitted through the CFTC's SFTP process and through the CFTC Portal, which are both secure means of transmission. Commission users who access the data access it through the secured processes set up by the CFTC, managed through the CFTC Active Directory environment.

The CFTC has limited access strictly to OCR to those with a need-to-know based upon an individual's role and responsibility. Whenever OCR information is made accessible through other CFTC systems (e.g. Integrated Surveillance System

(ISS)), access to that information continues to be role-based. The Division of Data has vetted the administrators of the connected systems. The data sent to OCR through the CFTC Portal or through SFTP are secured in transit according to Federal Information Processing Standards (FIPS) Publication 140-3 requirements. Once within the CFTC network, the information is secured by, among other controls: complex, frequently-changed passwords; sound security practices that are integrated into the daily routines of CFTC staff; audits of events that are significant and relevant to the security of OCR and the environment in which it operates; permitting only qualified and authorized individuals to make changes to the OCR System; and through uniquely identifying and authenticating users. All of the above controls are implemented according to Federal Information Security Modernization Act (FISMA) standards.

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.

Audit logs are generated for all submissions received through the CFTC Portal. Audit logs are generated for all loading of data into the Structured Query Language (SQL) Server databases. All SQL Server databases that contain data generate an audit log for all data accessed in the database. Audit logs contain the username of the individual who accessed data within the database.

The audit logs are reviewed by the CFTC security team and the CFTC applications team on an as-needed basis such as concern for unauthorized access to the data.

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

CFTC Staff that have access to OCR and all systems that have access to the data within OCR are certified on an annual basis. Each year, the Information System Security Officer (ISSO) confirms who has access to these databases and systems and confirms whether they have used the system within the last year. The list of users from each Division who have previously had access and who have used the data/systems within the year is sent to Divisional leadership for their recertification.

For new users who request access to the data and the systems, the ISSO confirms that the user has a legitimate need for the data with the user's manager.

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

All CFTC employees and contractors are required to complete Cybersecurity and Privacy Awareness Training prior to being granted access to the CFTC network and systems, including OCR, and annually thereafter. Any user who fails to complete the required annual training will have their access removed.

8.5 Privacy Impact Analysis: Related to Auditing and Accountability

There is a risk that audit logs are inconsistent or unreliable and also that CFTC staff are unaware of their responsibilities respective to handling personally identifiable information and Records Management.

This risk is mitigated through the logs being carefully designed and controlled in their use. The auditing of OCR is managed by staff in the Cyber and Physical Security Branch and by the Application and Database owners within the DOD. The auditing and review of audit data is done in a consistent manner on an as-needed basis. CFTC staff receive annual Cybersecurity and Privacy Awareness Training (CPAT) and Records Management training required to maintain access to CFTC information systems. CFTC staff are aware of how and when to report potential and actual incidents and breaches and are bound by the CFTC Rules of Behavior.