Commodity Futures Trading Commission
Privacy Impact Assessment

System Name: CFTC Portal OPERA (Updated April 16, 2015)

1. Overview

The Commodity Futures Trading Commission's ("Commission" or "CFTC") Portal is an Internet accessible system that enables communication between the CFTC and individuals authorized to submit information on behalf of CFTC registrants and applicants for CFTC registration ("users"). The Portal simplifies the process of submitting data, receiving and responding to user queries, and processing certain requests for registration with the CFTC.[1] The Portal streamlines information sharing with CFTC's regulated community and offers a means of exchanging accurate electronic data through a secure interface.

Users access the Portal by providing a valid username, password and secondary form of authentication to register for the site, i.e., to set up an account. Their credentials determine which parts of the Portal they may view or access. Once securely logged in to their accounts, users have access to information related to their registrants and a targeted menu of available actions. The content and menu options provide users with information related to the types of information they have submitted.

The Portal is hosted within CFTC's Amazon Web Services (AWS) GovCloud environment and managed day-to-day by CFTC contractor personnel. AWS is a Federal Risk and Authorization Management Program (FedRAMP) certified hosting provider, meaning it has been authorized for use under a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services. AWS GovCloud (US) is an isolated AWS region designed to allow U.S. government agencies and customers to move sensitive workloads into the cloud by addressing their specific regulatory and compliance requirements. The information submitted through the Portal passes through the AWS GovCloud environment to CFTC systems in encrypted form, and is deleted from the AWS GovCloud environment once its receipt has been confirmed in CFTC systems. The Portal Organizations, Products, Events, Rules and Actions (hereinafter "Portal OPERA") is used for submission, review and approval of reports of product data, organization registration data and organization rules, in order to meet CFTC's reporting requirements. Portal OPERA supports submission, receipt, review, communication and publication activities for:

- Registrations, designations, determinations and transfers of organizations such as Designated Contract Markets (DCMs), Derivatives Clearing Organizations

[1] The Portal also allows whistleblowers to complete and submit Form TCR (Tip, Complaint or Referral) (OMB Number 3038-0082) over the Internet. See **Whistleblower Electronic Submission Portal PIA** for more information.

(DCOs), Swap Execution Facilities (SEFs), Swap Data Repositories (SDRs) and Foreign Boards of Trade (FBOTs);
- Rule and product approvals and certifications; and
- Requests for Commission actions or interpretations.

This Privacy Impact Assessment addresses the Portal OPERA's use in supporting submission, receipt, review, communication and publication activities.

2. Data Collected and Stored Within the System

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

Portal OPERA collects information related to organizations, products, events, rules and actions. It also requires some information to register with the Portal, i.e., set up an account to submit information, such as the user's name, user's email address and phone number. Where marked below, the table includes the categories of personally identifiable information (PII) that may be requested through Portal OPERA.

PII Categories	**Collected, Generated or Maintained within the system**	**CFTC Employees**	**Members of the Public**	**Other (e.g. Contractors, Other government employees)**
Name (for purposes other than contacting federal employees)	X		X	
Date of Birth				
Social Security Number (SSN)				
Tax Identification Number (TIN)				
Photographic Identifiers				
Driver's License				
Mother's Maiden Name				
Vehicle Identifiers				
Personal Mailing Address				
E-Mail Addresses	X		X	
Phone Numbers	X		X	
Medical Records Number				
Medical Notes or other Health Information				
Financial Account Information	X		X	
Certificates				
Device Identifiers	X		X	
Web Uniform Resource Locator(s)	X		X	
Education Records				
Military Status				

PII Categories	Collected, Generated or Maintained within the system	CFTC Employees	Members of the Public	Other (e.g. Contractors, Other government employees)
Employment Status	X		X	
Foreign Activities				
Other: rule and product approvals and certifications	X		X	
Other: requests for Commission actions or interpretations	X		X	
Other: organization registration	X		X	

A user's phone number is required to enable dual authentication.

Portal OPERA also allows users to complete free text fields and upload documents, which allows submission of additional information, including possibly PII.

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

Portal OPERA collects information directly from the individuals authorized to submit information on behalf of DCMs, DCOs, SEFs, SDRs and FBOTs. The users submit information through multiple automated forms on **https://portal.cftc.gov**.

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

The CFTC collects, uses, and maintains information received to monitor compliance with the CEA and Commission regulations. Some user contact information, such as phone numbers, is collected to allow for dual authentication during log-on and password resets.

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

Users set up accounts in the Portal to submit information on behalf of their DCM, DCO, SEF, SDR or FBOT. Once logged into the Portal, they complete web forms and upload information. Once submitted, the information is transmitted to systems hosted within CFTC's AWS GovCloud environment for the Portal. The information passes through CFTC's system in the AWS GovCloud Portal environment to the Commission's enterprise database environment, where the information resides in accordance with Commission security procedures. CFTC's AWS GovCloud Portal environment stores a copy of the information only until its receipt by CFTC backend systems has been confirmed. CFTC's AWS GovCloud Portal environment keeps a log of dates of submissions, submission types and subtypes for verification purposes.

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?

- For DCM, DCO, SEF, SDR and FBOT registrations and designations, the legislative authority includes but is not limited to Commodity Exchange Act (CEA) §§ 37, 38, 39, 48 and 49;
- For submissions related to products, CEA §§ 30, 39, 40 and 41;
- For organization rules, CEA § 40;
- For product terms and conditions (rules), §§ 40 and 41; and
- For actions, orders and letters, CEA §§ 1a, 4, 13, 30, 140 and 718.

For specific CEA subsections and rules, please see the table in Section 10 below or in the menu of Portal OPERA, which is available after logging into the system.

3. Data and Records Retention

3.1. How will the information in this system be managed throughout its lifecycle? For what period of time will data collected by this system be maintained and in what form will the data be retained?

The Portal offers the CFTC and users a means of exchanging electronic data through a secure interface. To achieve that goal, a user's credentials are stored in the Commission's Portal's user database in encrypted form for as long as that user has an account. That account information is managed by CFTC staff administering the Portal. The data and documents that comprise information processed through Portal OPERA are stored in one or more Commission databases. That information, related to a user's DCM, DCO, SEF, SDR or FBOT, is retained in accordance with **CFTC's records disposition schedule**.

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

Depending on volume, the CFTC may move files to secure offline storage after the files are closed to conserve online storage space. Records are destroyed in accordance with CFTC's records disposition schedule for the specific types of records that are processed by Portal OPERA.

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 (FAR) clauses included in the contract (24.104 Contract clauses; 52.224-1 Privacy Act Notification; and 52.224-2 Privacy Act)?

At the Commission, only individuals designated by the Division of Market Oversight (DMO), Division of Clearing and Risk (DCR), Division of Swap Dealer and Intermediary Oversight (DSIO) or Office of Data and Technology (ODT) are regularly allowed access

to the information. These individuals include employees of the Commission, developers and administrators, including contractors, and possibly others with a legitimate and confirmed need to know the information to perform their Commission responsibilities.

Certain individuals who are specifically assigned access to CFTC's AWS Portal environment have access to the encrypted information transmitted through the Portal for information technology administrative purposes only. For example, the Portal in the AWS GovCloud environment keeps a log of dates of submissions, submission types and subtypes for verification purposes. As determined by the CFTC Office of Financial Management, the contract between the Commission and the hosting provider contains the FAR provisions necessary to protect and secure information to which it has access. The information also may be shared in accordance with the applicable Privacy Act System of Records Notice, **CFTC-15, Enterprise Surveillance, Oversight & Risk Monitoring System**, 77 Fed. Reg. 58814 (September 24, 2012).

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

Portal OPERA data is not shared outside of the Commission's network, except in accordance with the CFTC-15 System of Records Notice, as described above. If transferred or shared outside the Commission's network, the data is transferred in a manner designed to prevent the unnecessary and/or unauthorized disclosure of sensitive information. Such methods may include encryption of electronic information or hand delivery of documentation.

4.3. 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)?

No. The Portal is hosted in CFTC's AWS GovCloud. However, AWS personnel have no access to CFTC's AWS GovCloud environment for the Portal beyond the physical infrastructure within their data centers; they cannot access the CFTC data and information contained within the AWS GovCloud. The data centers are located in the United States and operated by US persons. CFTC's AWS GovCloud Portal environment stores a copy of the encrypted information only until its receipt by CFTC backend systems has been confirmed, at which point it is deleted from the AWS GovCloud Portal systems. CFTC's AWS GovCloud Portal keeps a log of dates of submissions, submission types and subtypes for verification purposes.

CFTC's Office of Data Technology staff, including specifically permitted employees and contractors, regularly monitor the information travelling through and/or stored for short-periods of time at CFTC's AWS GovCloud Portal environment. Together, they are responsible for detecting unusual system behavior and CFTC's Office of Data Technology staff are responsible for 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?

Portal OPERA users are required to agree to the Portal's Privacy Policy before registering for the site and submitting information. The Portal Privacy Policy describes, among other things, what information is collected and stored automatically; that users may choose to submit personal information about themselves to the CFTC; how submitted information may be shared; security; and the purposes of the information collection. Users may access the Portal Privacy Policy on any web page of the site and are reminded about the policy just before they submit information through the Portal.

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?

Users are given an opportunity to consent to providing personal information. However, for a user to submit information through the Portal, certain information is required, e.g., a telephone number to allow for dual authentication during log-on and password resets.

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?

A user may change or reset limited account information at any time. Portal OPERA allows a user to access the DCM, DCO, SEF, SDR or FBOT's history of submissions and make amendments by re-posting the entire submission. Directions on how to accomplish both of these tasks are available within Portal OPERA.

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 recognize the sensitive nature of Portal OPERA information. Records are protected from unauthorized access and improper use through administrative, technical and physical security measures. Technical security measures include restrictions on computer access to authorized individuals, required use of 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. The system also has a time-out function that requires users to re-authenticate after a specified period of inactivity.

AWS personnel have no access to CFTC's AWS GovCloud environment for the Portal beyond the physical infrastructure within their data centers. The data centers are physically located in the United States and operated by US persons. The AWS GovCloud meets US Government FedRAMP security requirements, and the CFTC contractor operating the CFTC AWS GovCloud is under strict contract terms concerning confidentiality.

When a user submits information through the Portal, the information is transferred via Transport Layer Security (TLS) encryption over the Internet into CFTC's AWS GovCloud Portal systems. The connection and transmissions between CFTC's AWS GovCloud Portal environment and the Commission are secured via an encrypted virtual private network (VPN) tunnel.

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?

Portal OPERA allows a user to update limited account information. It also allows a user to view the DCM, DCO, SEF, SDR or FBOT's history of submissions and make amendments by re-posting the entire submission. Under CFTC rules, users are responsible for ensuring that information provided to the CFTC is accurate and, therefore, for updating information as needed.

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 CFTC to monitor an individual's movement or actions.

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

The Commission follows all applicable FISMA requirements to ensure that information is appropriately secured. Portal OPERA resides on the AWS GovCloud. The AWS GovCloud is a FedRAMP certified hosting provider, meaning it has been authorized for use under a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services.

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

Commission staff are subject to agency-wide policies and procedures for safeguarding PII and receive annual privacy and security training. Many staff receive additional training focused on their specific job duties.

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, is it capable of being retrieved by a personal identifier?

Yes. Users are assigned a username.

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-15, Enterprise Surveillance, Oversight & Risk Monitoring System.

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**.

The collection, use and disclosure of the information has been reviewed. The Portal Privacy Policy was specifically created for users of the Portal. In addition, Portal users must agree to the following "opt-in" language before submitting data:

> I hereby certify that the information contained in this submission is accurate and complete to the best of my knowledge and belief.
>
> I also agree to abide by the Terms of Use Agreement, and to the collection, processing, disclosure and use of my personal information and other information submitted through this Portal as stated in the Portal Privacy Policy.

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 Commission has adopted the following protections, among others, to safeguard information and help ensure that privacy is appropriately maintained on Portal OPERA:

- Dual authentication is required to create an account on the Portal OPERA and to log into it. After entering a user name and password, the phone number associated with the account receives a call that requests confirmation of the CFTC Portal login attempt before granting access. After five failed password attempts, the account is locked.

- Portal OPERA provides access to authorized users only. Access is based upon an individual's role and responsibility. Three general types of users have been identified:

    - Industry Users – Complete and submit reports to the CFTC via the Portal.

    - CFTC Users – Access via CFTC Intranet to receive and respond to user queries and process certain requests for registration with the CFTC.

    - Portal Administrators – Access via CFTC Intranet to configure and maintain workflows, usergroups, and user roles.

- All Industry and CFTC users are defined in the Commission's Portal encrypted database prior to accessing Portal OPERA. Portal Administrator accounts'

account security and all password requirements are managed at the Active Directory level.

Additional risks relate to the use of a third-party contractor to host Portal OPERA. Such risks have been minimized by ensuring that AWS employees cannot access the data and information contained in the CFTC AWS environment. Risks also have been minimized by strong security requirements carried from AWS GovCloud FedRAMP certification, flushing of data from the CFTC AWS GovCloud Portal environment once data receipt has been confirmed by the Commission, regular audits of contained systems, the use of firewalls, intrusion detection applications and other security features, and establishing secure VPN connections between the CFTC AWS GovCloud Portal environment and Commission systems.

10. Provisions of the Commodity Exchange Act (CEA) Authorizing Portal OPERA

As of the publication date of this privacy impact assessment, the legislative authority for Portal OPERA submissions includes but is not limited to the following sections of the CEA:

OPERA Portal Submissions
CEA Section Organization
37.3 Swap Execution Facility (SEF) Registration
38.3 Designated Contract Market (DCM) Designation
39.3 Derivatives Clearing Organization (DCO) Registration
48.5 Foreign Board of Trade (FBOT) Registration
49.3 Swap Data Repository (SDR) Registration
CEA Section Product Type
30.13 Product Certification Foreign Security Index
39.5(a) Swap Clearing Eligibility Determination
39.5(b) Swap Clearing Requirement Determination
40.2(a) Product Certification
40.2(d) Product Certification Swaps Class
40.3(a) Product Approval
41.23(a) Product Certification Security Future
CEA Section Organization Rules
40.5(a) Rule Approval
40.5(g) Expedited Rule Approval
40.6(a) Rule Certification
40.6(a)(6) Emergency Rule Certification
40.6(d) Notification of Rule Amendments
40.10(a) SIDCO Advance Notice of Rule Certification
40.10(h) SIDCO Emergency Rule Certification
CEA Section Product Terms and Conditions (Rules)
40.4(b)(5) Amendments to Enumerated Agricultural Products - Non-Material

40.5(a) Rule Approval

40.5(g) Expedited Rule Approval

40.6(a) Rule Certification

40.6(a)(6) Emergency Rule Certification

40.6(d) Notification of Rule Amendments

41.24(a) Rule Certification Security Futures Product

Actions, Orders, Letters - CEA Section

Request for Determination - 1a(12)(C) Eligible Contract Participant

Request for Exemption - 4(c) DCM Transaction Execution

Petition for Exemption - 4a(a)(7) Position Limits

Request for Order - 4d Customer Funds and Property

Request for Determination - 718(a)(2)(B) Novel Derivative Product

Request for Exemption - 718(a)(2)(D)(ii) Novel Derivative Product

Petition for Issuance, Amendment or Repeal of a Rule under 13.2

Petition for Exemption - 30.10 Foreign

Request for Exemptive Letter - 140.99 (a)(1)

Request for No-action Letter - 140.99(a)(2)

Request for Interpretative Letter - 140.99(a)(3)

This list is also available to Portal OPERA users after they log into the system.