Commodity Futures Trading Commission
Privacy Impact Assessment

System Name: Whistleblower Electronic Submission Portal (Updated April 16, 2015)

1. Overview

The Commodity Futures Trading Commission's (Commission or CFTC) whistleblower program is designed to pay awards to eligible individuals who voluntarily provide the Commission with original information about violations of the Commodity Exchange Act (CEA) that lead to the successful enforcement of covered judicial or administrative actions, or related actions. As part of its administration of the whistleblower program, the Commission's Whistleblower Office (WBO) maintains records of whistleblower tips, complaints, award claims and related records and correspondence.

In support of the whistleblower program, an electronic submission portal (Portal) is being launched to allow members of the public to complete and submit Form TCR (Tip, Complaint or Referral) (OMB Number 3038-0082) over the Internet. The data captured in the Form TCR, along with other inputs for the whistleblower program (emails, scans of letters and facsimiles, data from other whistleblower related forms, etc.), is stored in the Commission's Practice Manager database, which is part of the Commission's **eLaw Automated Law Office Software Suite**.[1]

The Portal is hosted within CFTC's Amazon Web Services (AWS) GovCloud environment for the Portal 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.

2. Data Collected and Stored Within the System

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

[1] Other forms associated with the Whistleblower program are not being automated on the web at this time, such as the Form WB-APP Application for Award for Original Information Submitted Pursuant to Section 23 of the Commodity Exchange Act (OMB Number 3038-0082).

The table below includes the categories of personally identifiable information (PII) requested in the Form TCR through the Portal, although all such data is not required for a whistleblower submission, as an individual may submit the Form TCR anonymously.

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	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	X		X	X
Personal E-Mail Address	X		X	X
Personal Phone Number	X		X	X
Medical Records Number				
Medical Notes or other Health Information				
Financial Account Information				
Certificates				
Legal Documents				
Device Identifiers				
Web Uniform Resource Locator(s)				
Education Records				
Military Status				
Employment Status				
Foreign Activities				
Other (e.g. Tip, Complaint or Referral/TCR number)	X		X	X

The Form TCR contains free text fields, which allows members of the public to provide additional information, including possibly PII.

The Form TCR data is stored in the Practice Manager database. As an investigation proceeds, given the nature of investigations, other types of PII may be collected and stored in Practice Manager. The Practice Manager database may hold: records, data and correspondence submitted by and sent to whistleblowers and/or their representatives (e.g., financial accounts/records, employment history, legal documents); correspondence with other law enforcement and regulatory agencies regarding referral of whistleblower information and related actions brought by such agencies based on

whistleblower information; interviews, memoranda and other work products prepared by Commission staff; information submitted on other whistleblower program related forms, such as the Form WB-APP Application for Award for Original Information Submitted Pursuant to Section 23 of the Commodity Exchange Act (OMB Number 3038-0082); affidavits, statements by witnesses, contracts and agreements with whistleblowers, including confidentiality agreements; and information available on the Internet or other electronic sources accessed for purposes of the whistleblower program. Practice Manager may also contain internal memoranda and declarations of Commission staff, correspondence and other miscellaneous investigatory matters.

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

The Portal collects information from the general public through an automated Form TCR on the www.cftc.gov**.** The database that holds the Form TCR information, Practice Manager, may contain information from other sources, such as the Whistleblower Award Determination Panel and information from CFTC or other agency investigations.

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

The CFTC collects, uses, disseminates and maintains information as part of its administration of the whistleblower program. The program is designed to pay awards to eligible individuals who voluntarily provide the Commission with original information about violations of the CEA that lead to the successful enforcement of covered judicial or administrative actions, or related actions. To meet this end, the WBO maintains records of whistleblower tips, complaints, award claims and related records and correspondence.

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

The information will be collected through a web form on the Portal, which is hosted within CFTC's AWS GovCloud environment. The information passes through CFTC's system in the AWS GovCloud Portal environment to the Commission's Practice Manager database. 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. The Practice Manager database also has the functionality to store information that is scanned, faxed or emailed that pertains to an investigation. The information will be used to discover violations of the CEA and to evaluate whistleblower award claims.

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?

Commodity Exchange Act Section 23, 7 U.S.C. § 26, and the Whistleblower Rules, 17 C.F.R. § 165.

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 information received through the Portal is stored electronically in the Practice Manager database, part of the eLaw Automated Law Office Software Suite, with a copy stored in CFTC's AWS environment for the Portal until the submission has been processed by the Commission.

The records collected by the Form TCR are closed after the last action on the relevant Division of Enforcement matter, after the final appeal of the decision of the Whistleblower Award Determination Panel is exhausted, or after the award payment to the whistleblower has been made, whichever is applicable and whichever is latest (the cut-off date). Such files are destroyed 15 years after the end of the fiscal year on which the latest cut-off date occurs.

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

Hard copy and electronic records will be deleted once they have exceeded their retention period and the WBO has approved their deletion. Depending on volume, it is possible that the CFTC may move whistleblower files to secure offline storage at some point after the files are closed to conserve online storage space.

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 specifically assigned access in Practice Manager will be allowed access to the information. These individuals will include employees of the WBO, employees and contractors of the Division of Enforcement (DOE), and developers and administrators of the eLaw Suite, 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 will have access to the encrypted information for information technology administrative purposes only. For example, the Portal in the AWS GovCloud environment will 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. These individuals will include employees and contractors of the Office of Data and Technology (ODT). The CFTC Office of Financial Management is charged with the execution and oversight of all CFTC procurement activities in accordance with the FAR.

The information also may be shared in accordance with the applicable Privacy Act System of Record Notice, **CFTC-49, Whistleblower Records (Exempted)**, 77 Fed. Reg. 41378 (July 13, 2012).

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

Staff of the Division of Enforcement and/or the WBO must approve all releases of data outside of the Commission's network. Pending approval, data will be shared outside the Commission's network in a manner designed to prevent the unnecessary and/or unauthorized disclosure of a whistleblower's identity. Such methods may include encrypted e-mail 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?

Users of the portal will be required to agree to the following Opt-In language before submitting their Form TCR electronically:

> I agree to the collection, processing, use and disclosure of my personal information as stated in the Privacy Act Statement and the Privacy Policy for www.cftc.gov.

The Commission's Privacy Policy also provides a specific example on the whistleblower program and its use of PII.

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?

Opt-In language is provided along with the requirement that users accept the Commission's Privacy Policy. Individuals may decline to provide certain information in the Form TCR, and may choose to submit the form anonymously. If an individual chooses to provide information anonymously they are responsible for maintaining their anonymity when interacting with the WBO. For example, they should not provide their name to the WBO and then request anonymity.

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 whistleblower system of records is exempt from certain sections of the Privacy Act of 1974 under 5 U.S.C. § 552a(k)(2), and the Commission's rules promulgated thereunder, 17 C.F.R § 146.12. 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.

Despite the system's exempt status, an individual may contact the WBO and request to have his/her records amended. At the discretion of the WBO and if the individual can provide verifiable proof that he/she submitted the information at issue – particularly the submission number that is provided to submitting parties – then the WBO may allow the individual to amend his/her submission.

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 whistleblower 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, a "defense-in-depth" approach to network security, regular review of security and access logs to determine anomalous activity, and regular review of security procedures and best practices to enhance security.

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 whistleblower 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?

Appropriate Commission personnel will routinely maintain and update the information in the system with any new information provided by the whistleblower or Commission staff.

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

The information provided does not allow the CFTC to monitor an individual's movement or actions. The system provides the capability to identify an individual and in some instances determine his/her address. An individual may voluntarily elect to provide his/her name, organization and/or mailing address.

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 Federal Information Security Management Act requirements to ensure that information is appropriately secured. The Portal 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 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. The WBO is considering developing role based training to specifically address the privacy and security needs of the whistleblower information.

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, records can be retrieved through several personally-identifiable attributes such as name, contact information and submission number.

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. Name of the System: Whistleblower Records (Exempted), SORN CFTC-49.

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 CFTC privacy policy includes the following language that is directly relevant to the whistleblower system:

> If you choose to provide personal information, you are consenting to the CFTC's use of that information and permitting that it be shared with CFTC employees and contractors to conduct official business. Such employees and contractors are subject to confidentiality restrictions to protect your personal information. The information may also be shared by the CFTC with third parties to advance the purpose for which you provide the information, including law enforcement and other federal or state government agencies. Your information will only be used to perform official business for which it was collected. For example:
>
> 1) If you report suspicious activity that suggests a violation of the Commodity Exchange Act, the information you have provided may be shared with law enforcement and other federal or state agencies. In this situation, the primary use of your PII would be to enable the government to contact you in the event we have questions regarding the information you have reported.
>
> 2) If you populate a Tip, Complaint or Referral (TCR) form to be considered as a whistleblower under the Dodd-Frank Act, the information you have provided may be disclosed to the Whistleblower Award Determination Panel, law enforcement, and other federal or state agencies. In this situation, the primary use of your PII would be to:
>
> a. Evaluate the merit of an award;
>
> b. Allow for the payment of monetary awards to eligible whistleblowers; and/or
>
> c. Provide anti-retaliation protections for whistleblowers that share information with or assist the CFTC, as limited by the Commodity Exchange Act (CEA)**.**
>
> Under certain circumstances, the CFTC may be required by law to disclose information you submit to other authorities for official purposes, for example, to respond to a Congressional inquiry or subpoena.
>
> When you choose to send e-mail to the CFTC, you are consenting to the CFTC using the information provided therein, including PII, in accordance with this notice, unless you expressly state in the email your objection to any use.
>
> Your personal information will be protected from misuse while in the possession of the CFTC. Management, operational and technical controls are in place with the goal of ensuring the confidentiality, availability, and integrity of the PII. If an incident or breach is suspected or confirmed involving sensitive personal information, contact will be made with all affected parties in a timely manner. The

CFTC will then work with individuals to ensure swift and appropriate action is taken to mitigate risks.

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 primary risk associated with whistleblower data is the risk of inadvertently disclosing whistleblower-identifying information outside of the circumstances called for by Commodity Exchange Act Section 23(h)(2), 7 U.S.C. § 26(h)(2), and Whistleblower Rule 165.4, 17 C.F.R. § 165.4. Such risks are mitigated by requiring outside disclosure of whistleblower-identifying information to be authorized by the WBO, logging each authorized disclosure, and the dissemination of policies to DOE staff regarding the handling of whistleblower-identifying information.

Additional risks relate to the use of a third-party contractor to host the whistleblower electronic submission portal. 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, a “defense-in-depth” approach to network security, and establishing secure VPN connections between the CFTC AWS GovCloud Portal environment and Commission systems.