Commodity Futures Trading Commission (CFTC)
Privacy Impact Assessment

System Name: Trade Surveillance System (TSS)

Office: Office of Data and Technology

Date: September 30, 2014

1. Overview

CFTC staff in the Division of Market Oversight (DMO), Division of Enforcement (DOE), Office of the Chief Economist (OCE), and the Division of Clearing and Risk (DCR) use the Trade Surveillance System (TSS) to perform various mission-critical futures and options market analyses. TSS receives transactional data on a daily basis directly from "Reporting Markets," as defined in Commission Regulation 15.00(q), that are required, under Part 16 to report data. The transactional data includes the time that the trade was executed, the parties involved, and the amount traded. TSS enables CFTC staff to conduct surveillance of electronic trading by allowing for both intra- and inter-exchange analysis as well as comparisons across side-by-side platforms.

In order to perform effective surveillance, the Commission must receive data sets that contain a sufficient number of reference points for the Commission to uncover relationships between related accounts and analyze information based on surveillance criteria that are frequently evolving in response to market events. The collection of information regarding trading accounts and traders enables the Commission to perform efficient and effective surveillance. Prior to TSS, these trades handled through the Reporting Markets were monitored manually.

2. Data Collected and Stored Within the System

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

The following data is collected by TSS:

- Cleared Trades – Cleared and allocated trades (Source: Trade Capture Report)
- Time and Sales - Best Bid/Ask and Trade quotes
- Market Data Summary - End-of-day summary such as daily volume and high/low/open/close/settlement price
- Trade Types - All possible trade types
- Executing Firms – All executing firms
- Listed Products – All Products listed by the Reporting Markets
- Traded Contracts – All contracts
- Exchange – All Exchanges/Reporting Markets

- Regular Trading Time – Settlement periods
- Early Close Event – Settlement periods on early close events
- Market Close Event – Dates when markets are closed

As noted in the chart below, the personally identifiable information (PII) stored in TSS is limited to names and account numbers so that trades may be associated with individuals, if necessary.

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				
Personal E-Mail Address				
Personal Phone Number				
Medical Records Number				
Medical Notes				
Financial Account Information, specifically includes:				
Order Entry Operator ID*	X		X	
Trader ID**	X		X	
Options Account Number	X		X	
Futures Account Number	X		X	
Special Account Reporting Number	X		X	
Certificates				
Legal Documents				
Device Identifiers				
Web Uniform Resource Locator(s)				
Education Records				
Military Status				
Employment Status (e.g., job title)				

Foreign Activities				

* Order Entry Operator ID is the identifier of a person responsible for a trade on an electronic venue.
** Trader ID is the identifier of the person responsible for a trade on an open outcry venue.

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

TSS receives transactional data on a daily basis directly from Reporting Markets, including, for example at the time of the publication of this document, the Chicago Mercantile Exchange (CME). **A current list of Reporting Markets** is available on the CFTC's website.

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

The data is collected, used, and maintained to allow CFTC staff to monitor and detect trade practice violations within financial exchanges that operate markets overseen by the CFTC. By law, the CFTC must protect market participants and the public from fraud, manipulation, abusive practices and systemic risk related to derivatives – both futures and swaps – and to foster transparent, open, competitive and financially sound markets.

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

The information will be collected by receiving feeds of the data listed in Section 2.1 from the Reporting Markets. The PII may be used to identify individuals associated with trading accounts.

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

No. TSS utilizes automated monitoring of trade data to flag potential violations, which are then reviewed and investigated by appropriate CFTC staff. TSS uses software and technologies that are common to the CFTC's infrastructure.

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

The Commodity Exchange Act, 7 U.S.C. 2, 6a, 6c, 6g, 6i, 7, and 7b-3 and the rules and regulations promulgated thereunder authorize the collection of this information.

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?

CFTC is revising the records disposition schedules that apply to records covered by this PIA.

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

CFTC is revising the records disposition schedules that apply to records covered by this PIA. When it is determined that records are to be destroyed, paper records will be shredded and electronic records will be purged from systems.

4. Access to and Sharing of the Data

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

Through security features built into TSS, access to information in this system is limited to those individuals whose official duties require access. At the CFTC, only individuals designated by DMO, OCE, DOE, DCR and ODT will be regularly allowed access to the information. These individuals will include employees of the CFTC, developers and administrators, and possibly others with a legitimate and confirmed need to know the information to perform their CFTC responsibilities. CFTC contractors with access to TSS are required to comply with the Privacy Act contractually through either FAR terms or other terms and conditions. CFTC's Office of Financial Management (OFM) ensures that the contract between the CFTC and contractors contains the provisions necessary to protect and secure information to which they have access. Direct TSS access is not granted to external parties.

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?

Data from TSS is not shared outside of the CFTC's network, except in accordance with the CFTC-15 System of Records Notice, as described above. Such sharing may include, but is not limited to, other Federal or state law enforcement or regulatory agencies for use in meeting their statutory and regulatory requirements or with foreign law enforcement, investigatory, or administrative authorities in order to comply with requirements set forth in international arrangements, such as memoranda of understanding. If transferred or shared outside the CFTC's network, the data will be 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.

The CFTC has assigned confidential reporting numbers to reporting firms and traders to help ensure privacy of the information they provide. The Commission is prohibited under Section 8 of the CEA, **7 USC 12**, from publicly disclosing any person's positions, transactions, or trade secrets, except under limited circumstances.

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

Other than contractors working within TSS to fulfill their job responsibilities, e.g., contactors responsible for managing the database or consultants providing requested data analyses, TSS system data generally will not be released to the public or third parties.

However, as described in Section 4.2, in the event that the CFTC receives lawful requests for the data from Congress or others, ODT shall consult the Office of General Counsel (OGC) and/or the Privacy Office, as appropriate, with the goal of minimizing any release of identifiable information, and whenever possible, providing aggregated, anonymous data using strategies designed to prevent re-identification through other available information.

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

As explained above, the CFTC does not expect to release TSS system data to the public or third parties. In the event such data needs to be released through a lawful request and may be released in aggregated form, the CFTC to the greatest extent possible will use aggregation or de-identification strategies designed to prevent re-identification of such information through other available information.

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

Any disclosure in PII-form outside the CFTC is unlikely. In such case, CFTC staff would confirm the legal authority to release such information, track such disclosures to outside entities by documenting, among other things, which person or party/organization made the request, the date and nature of the request, the decision made to disclose or not disclose the data and by whom, and any restrictions on further dissemination of the requested information.

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

The TSS integrates with the Integrated Surveillance System (ISS) through the Trader Linking System. Both TSS and the Trader Linking System include a Privacy Notice immediately following the log in screen that requires users to agree to protect the secrecy of confidential information contained within the system. End users and the TSS System Administrators are responsible for protecting the privacy rights of the individuals whose information may be accessible through the interface. In addition, privacy training is administered on an annual basis to all CFTC employees.

ODT staff regularly monitor the information travelling to and stored by the CFTC. They are responsible for detecting unusual system behavior and raising any privacy concerns with the CFTC Privacy Office.

5. Notice, Consent and Access for Individuals

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

This PIA and SORN **CFTC-15, Enterprise Surveillance, Oversight & Risk Monitoring System** shall appear on **the Privacy Office's CFTC website.**

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?

Individuals are given an opportunity to consent to providing personal information, however, market participants are required by law to provide this information in order to trade in these markets. Each Reporting Market is responsible for providing notice at the point of PII collection. The associated consent processes are unique to the Reporting Markets.

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?

Market participants are required by law to provide this information in order to trade in these markets. Individuals seeking access to records about themselves, or seeking amendment of records about themselves should **address a written inquiry** to the Office of General Counsel, Paralegal Specialist, Commodity Futures Trading Commission, Three Lafayette Centre, 1155 21st Street, NW, Washington, DC 20581.

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?

Access to TSS requires an individual user's unique username and password. Users can query only the datasets to which they have been granted access. CFTC staff are trained to recognize the sensitive nature of TSS information. Records are protected from unauthorized access and improper use through administrative, technical and physical security measures. Technical security measures within CFTC include restrictions on computer access to authorized individuals, unique usernames, strong passwords that are frequently changed, use of encryption for certain data types and transfers, and regular review of security procedures and best practices to enhance security.

Access to records is limited by security features built into TSS to those individuals whose official duties require access. Physical measures include restrictions on building access to authorized individuals and maintenance of records in lockable offices and filing cabinets.

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?

The information comes in to the CFTC on a constant basis and is automatically historical once it enters TSS. The information is time stamped and the CFTC uses appropriate technical safeguards to help ensure that the information transmitted into TSS is not changed. Under CFTC rules, reporting firms and individual traders are responsible for ensuring that information provided to the CFTC is accurate and, therefore, for updating information as needed. If CFTC staff determine that options records or other data submitted by the reporting firms is missing or incorrect, they contact the source to have the data re-submitted.

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?

Yes. The CFTC follows the National Institute of Standards and Technology (NIST) Special Publication 800-53, 'Recommended Security Controls for Federal Information Systems' to secure its systems as required by the Federal Information Security Management Act (FISMA). A security assessment of TSS was conducted by the CFTC ODT Security Team in accordance with the Office of Management and Budget Circular A-130, Appendix III, Security of Federal Automated Information Resources and NIST Special Publication 800-37, Guide for the Security Certification and Accreditation of Federal Information Systems. TSS received its most recent certification and accreditation (C&A) on June 27, 2013.

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

CFTC personnel are subject to agency-wide procedures for safeguarding PII and receive annual privacy and security training. Many staff receive additional training focused on their specific job duties, for example, Division of Enforcement staff regularly receive training concerning privacy rights of individuals and the importance of safeguarding information, and system administrators receive role-based training.

7. Privacy Act

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

Yes, records can be retrieved by name and unique account information.

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**.

Yes, the following sub-header of the CFTC privacy policy includes language that is relevant to the TSS:

- **Sharing of Your Information**

9. Privacy Risks and Mitigation

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

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

- All transmissions of transactional data from the Reporting Markets to the TSS system are secured through the use of Secure File Transfer Protocol (SFTP).
- TSS provides access to authorized users only. Access is based upon an individual's role and responsibility. There are 3 general types of user roles:
    - Read Only users: These users can read data within certain portions of TSS but cannot make changes.
    - System Administrators – These users are CFTC staff on the Data Engineering and Processing (DEAP) team who have login/read/write permission to the data.
    - Developers – These users are contractors and CFTC staff who have limited permissions to view data.

TSS data is confidential; therefore, the CFTC has limited access to TSS information strictly to those with a need-to-know. Access to any TSS data provided to other systems (e.g., ISS) is role-based and the administrators of the connected systems have been vetted by ODT.