Commodity Futures Trading Commission
Adapted Privacy Impact Assessment for Use of Third-Party Websites or Applications

System Name: Internet and Social Media Use

Office(s): Office of Public Affairs and Privacy Office (in the Office of the Executive Director)

Date: July 15, 2011

1. Overview and Purpose

Congress created the Commodity Futures Trading Commission ("CFTC" or "Commission") in 1974 as an independent agency with the mandate to regulate commodity futures and option markets in the United States. The agency's mandate has been renewed and expanded several times since then, most recently by the Dodd-Frank Wall Street Reform Act of 2010. In 1974 the majority of futures trading took place in the agricultural sector and trading occurred primarily on paper with individuals trading on the floor of an exchange. Over the past 30 years, the futures industry has become increasingly varied and today encompasses a vast array of highly complex financial futures contracts. Trading now most often occurs electronically and traders now solicit and communicate with clients through the Internet and World Wide Web,[1] including social media sites ("SMS").[2]

Despite the growth in the futures markets, increased complexity and technological changes, the CFTC's mission remains constant: to protect market users and the public from fraud, manipulation, abusive practices and systemic risk related to derivatives that are subject to the Commodity Exchange Act, and to foster open, competitive, and financially sound markets. The CFTC assures the economic utility of the futures markets by encouraging their competitiveness and efficiency, protecting market participants against fraud, manipulation, and abusive trading practices, and by ensuring the financial integrity of the clearing process. Through effective oversight, the CFTC enables the futures markets to serve the important function of providing a means for price discovery and offsetting price risk.

The CFTC brings civil, criminal and administrative enforcement actions to enforce its laws and provides education to enable the public to avoid common harms. The Commission's enforcement activities include complaint collection and analysis; individual, company and industry-wide investigations; administrative and federal court litigation; and outreach and education. Increasingly, these activities require access to information and services available on the Internet.

To fulfill its mission of protecting market participants and the marketplace in the Web 2.0 world, the Commission's specifically designated employees and contractors (collectively CFTC or Commission "staff") will use the Internet, including Facebook, **www.facebook.com**, LinkedIn, **www.linkedin.com**, and other third-party SMS, for the following purposes.

---

[1] This Privacy Impact Assessment ("PIA") will refer to the "Internet" to encompass both the "Internet" and "World Wide Web," and includes but is not limited to all websites on the Internet whether or not a user must register on the site to access it, e.g., social media and social networking sites. This PIA does not cover the website managed by the Commission, **www.cftc.gov**, or any information collected through that site.

[2] As used in this PIA, "social media" means any form "of electronic communication (as Web sites for social networking and microblogging) through which users create online communities to share information, ideas, personal messages, and other content (as videos)." Merriam-Webster, accessed 6/17/2011, **http://www.merriam-webster.com/dictionary/social%2Bmedia**. It includes "social networking sites," i.e., sites that provide "a virtual community for people to share their daily activities with family and friends, or to share their interest in a particular topic, or to increase their circle of acquaintances." PC Magazine, accessed 6/17/2011, **http://www.pcmag.com/encyclopedia_term/0,2542,t=social%2Bnetworking&i=55316,00.asp**.

(1) Public Affairs: CFTC will use the Internet to disseminate information to and interact with the public for outreach, education and similar purposes, and to review publicly-available posts about the CFTC by other Internet and SMS users. The CFTC SMS pages will provide an additional means for the CFTC to notify and hear from the public about CFTC upcoming events, press releases, newsworthy stories, CFTC reports, enforcement actions or comments on Commission related issues. CFTC SMS posts will be content that exists on **www.cftc.gov**, responses to other SMS users' posts, or non-substantive content that is time-sensitive. Commission staff will promote CFTC activities to SMS users, particularly those who indicate that they are "fans" of, "like" or "follow" the CFTC. In turn, these individuals may share the CFTC information with their SMS network of friends, providing a viral marketing component to the Commission's outreach and education efforts. CFTC staff may include newsworthy SMS posts in its internal news clipping service. For these purposes, SMS will be used by the Commission's Office of Public Affairs and other senior managers.

(2) Enforcement: CFTC will use the Internet to observe publicly-available information[3] or other information offered to the CFTC with consent for investigations and enforcement proceedings, and, when other investigative avenues are limited, to act as a member of the public by using a username and profile not affiliated with the CFTC, simulating the day-to-day customer experience. In these limited enforcement investigations, CFTC staff will seek information about business opportunities that may suggest a violation of the Commodity Exchange Act or harm to individuals or the market on matters within the Commission's jurisdiction. For this purpose, the Internet will be used primarily by law enforcers (e.g. attorneys, investigators, paralegals) in the Division of Enforcement and by litigation and computer forensics support staff in the Office of Information and Technology Services.

In the process of using the Internet for these purposes, the Commission will collect certain personally identifiable information ("PII") as stated in this Privacy Impact Assessment ("PIA"). As explained further below, the PII includes publicly-available information on the Internet, such as the authors of Internet stories that the CFTC circulates with internal news clips, and names of individuals who may be violating the Commodity Exchange Act through the Internet. Also, for security, administrative and management purposes, the CFTC will collect limited PII of CFTC staff related to their use of certain CFTC computers that are logically and physically isolated from the CFTC production network ("Off-Network Computers").[4]

2. Data Collected and Stored

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

Information collected from the Internet and used, disseminated or maintained in the system may include content freely available or offered through paid/premium services on the Internet. It may include website content or posts on SMS pages, and may include usage data and statistics, IP addresses, domain registration and ownership information. It also may include PII.

The CFTC will only collect, use, maintain, or disseminate PII from individuals through the Internet in two situations. For Public Affairs purposes, comments about the CFTC on SMS pages may be reviewed internally, and for newsworthy posts, included in internally-circulated daily news clips with the author's name and affiliated organization if publicly-available. For Enforcement purposes, information obtained from the Internet may be collected and preserved for use in investigations and enforcement proceedings.[5] The CFTC will not solicit personal information directly from customers, as the information collected will be from publicly-available sources on the Internet or will be offered to the CFTC with consent, except as noted above in certain limited

[3] In this PIA, "publicly-available information" refers to information that is open to anyone who wishes to access it, for example, when a Facebook user has made information available to "everyone" on Facebook through his or her privacy settings. In contrast, information that is meaningfully restricted -- i.e., when an Internet user applies privacy settings or other restrictions reflecting an intention to keep the information private -- is not "publicly-available information."

[4] This PIA only addresses this type of computer usage, administrative information collected for use of the Off-Network Computers. It does not cover CFTC users' use of the CFTC production network.

[5] Nothing herein shall be construed to limit the CFTC's ability to use all applicable legal authorities and powers to investigate and prosecute violations of the Commodity Exchange Act.

Enforcement investigations. Information collected for investigative purposes and to which the Privacy Act of 1974 would apply will be maintained in the Commission's investigatory system of records.[6]

Specific PII collected may include names, addresses, phone numbers, email addresses, and other PII otherwise publicly available on the Internet. Most PII collected will be information which an individual has chosen to give to the CFTC or make publicly-available, and which relates to commodities, futures and other matters regulated by the CFTC.

Administrative information about a CFTC user's use of the Internet and SMS, including event and usage logs, the user's name, CFTC phone number, division, time and date of entry and exit from website ("Internal Administrative Information") may be collected for management, security and review purposes as needed.

2.2. What will be the sources of the information in any new or modified use of third-party websites or applications?

For Enforcement purposes, the Commission collects and preserves information that is available to the public on the Internet or that is offered to the Commission with consent, and includes content freely available to market participants or content that is only offered through paid subscriptions or services or that may require some form of registration of a member of the public. For Enforcement purposes, in an enforcement investigation, a CFTC user may act as a member of the public and seek information from an individual or entity regarding a business opportunity that would be available to the public.

The sources of information posted by the CFTC will be the CFTC staff members specifically authorized to use the Internet, for example, Office of Public Affairs staff.

Internal Administrative Information may be collected directly from the computers being used by CFTC staff at or after the time of use.

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

The CFTC will only collect, use, maintain, or disseminate PII from individuals through the Internet for the two purposes stated above. One, for Public Affairs, comments about the CFTC on SMS pages may be reviewed internally, and for newsworthy posts for the purpose of attributing the post to the author, included in internally-circulated daily news clips with the author's name and affiliated organization if publicly-available. Two, for Enforcement, information obtained from the Internet may be collected and preserved for use in investigations and enforcement proceedings. The information collected will be offered to the CFTC with consent or will be from publicly-available sources on the Internet, except in certain limited enforcement investigations. For example, the Commission may collect and preserve web pages containing fraudulent information provided by targets of a CFTC investigation. Targets frequently change the content of their websites, and collection and preservation of this information is, therefore, critical to proving that a fraudulent statement appeared on a particular web page on a particular day.

Internal Administrative Information may be collected for administrative, management and security purposes. Event and usage logs may track which CFTC staff are using the Off-Network Computers to, among other things, ensure that such use is appropriate.

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

For Public Affairs purposes, the information will be collected using standard tools that facilitate copying of Internet content, e.g., "snipping tools," copy/paste and similar tools.

[6] See CFTC System of Record Notice ("SORN") CFTC-10, Investigatory Records (Exempted); such records are exempted by the Commission from certain provisions of the Privacy Act of 1974 pursuant to the terms of the Privacy Act, 5 U.S.C. 552a(k)(2), and the Commission's rules promulgated thereunder, 17 CFR 146.12.

For Enforcement purposes, the Commission provides CFTC staff with the hardware and software they need to perform investigations and capture, organize and present content available on the Internet in hardcopy, static and dynamic digital images and recordings (such as screen shots), and raw digital content (e.g., audio/video content, web pages and entire web sites). Tools also may be available to analyze Internet protocol and website registration information. In addition, when other investigative avenues are limited as explained above, the Commission will provide specifically-designated staff the ability to create email addresses and SMS profiles not affiliated with the CFTC so they may simulate the customer experience.

Information collection is performed by CFTC staff, and is not part of an automated collection mechanism. Information is generally stored in electronic and paper form.

Regarding use for Public Affairs, the names and organizations of authors of newsworthy Internet posts will be used by the CFTC in an electronic news clip service by posting the author's name and organization along with his or her post. This information is posted on the CFTC intra-net, printed for record-keeping purposes, and emailed to CFTC staff.

The records collected for Enforcement purposes could lead to enforcement action by the CFTC or other governmental authorities, including possible civil, criminal or administrative penalties. The records will become part of SORN CFTC-10, Investigatory Records (Exempted), used as stated in CFTC-10, and exempted by the Commission from certain provisions of the Privacy Act of 1974 pursuant to the terms of the Privacy Act, 5 U.S.C. 552a(k)(2), and the Commission's rules promulgated thereunder, 17 CFR 146.12. Such 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. Records also could become part of CFTC-16, Enforcement Case Files, and may be used in enforcement proceedings brought by the Commission in administrative tribunals or courts.

Internal Administrative Information may be collected through system event and usage logs. Such information may be used by CFTC management for administrative, security and management purposes, e.g., to track Internet usage and identify potential system misuse.

2.5. Is the third-party website or application being used in ways that the CFTC has not previously employed (e.g., monitoring software)?

Creation of CFTC SMS accounts will require the CFTC to use the websites and applications available to any Internet user and tools that enable the capture and preservation of content. The use of the sites and applications does not raise privacy concerns not otherwise discussed in this PIA.

Administrators of the CFTC SMS accounts will access third-party sites or applications by visiting them using a standard Web browser and, when needed, logging in with an email address and a password.

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

Information is collected pursuant to the CFTC's general law enforcement and investigatory authority, which is set forth in the Commodity Exchange Act, 7 U.S.C. 1 et seq., and the rules and regulations promulgated thereunder.

3. Data and Records Retention

3.1. How will the information maintained through this new or modified use be managed throughout its lifecycle? For what period of time will data collected be maintained and in what form will it be retained? What are the plans for destruction and/or disposition of the information?

The name and organization of an author of a post used for CFTC internal news clips will be maintained in electronic and paper form as part of daily files of news clips, which are retained for five (5) years or longer if needed for research purposes. When the news clips are no longer needed, electronic and paper copies will be destroyed.

Information collected for Enforcement purposes will be handled and retained in accordance with SORN CFTC-10, Investigatory Records (Exempted). PII will be collected from SMS in electronic form through tools that enable the capturing of Internet pages. PII will be maintained in electronic and paper form. Paper records will be stored in file folders, binders, and in scanned form in computer files (such as the Commission's "eLaw" system) and on computer disks. Electronic records, including computer files, will be stored on the Commission's network and on various other electronic media as needed, such as encrypted hard drives.

As explained in SORN CFTC-10, if an investigatory matter is closed without institution of a case, the files are maintained in off site storage for five (5) years, and then destroyed. When the Commission moves forward from an investigation to litigation:

(a) investigatory records that are disclosed by the Commission in the administrative, court or other proceedings become part of non-exempt SORN CFTC-16, Enforcement Case Files and/or SORN CFTC-17, Litigation Files-OGC, and are retained and disposed of pursuant to CFTC-16 and/or CFTC-17; and
(b) Investigatory records not disclosed in such proceedings are retained in exempt SORN CFTC-10, Investigatory Records, and disposed of on the same schedule as the related non-exempt records under CFTC-16 or CFTC-17.

All Investigatory Records remain exempt from disclosure under the Privacy Act.

Internal Administrative Information collected to monitor CFTC user use of the Internet for investigations, including access, system event usage logs, will be retained and destroyed in accordance with GRS 20, Items 1a and 1c, which require that information is destroyed when CFTC determines it is no longer needed for administrative, legal, audit, or other operational purposes.

Disposal of all CFTC information collected for the purposes stated in this PIA will be conducted in accordance with Office of Management and Budget ("OMB"), NIST and NARA Guidelines.

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 will have access to the information, are Federal Acquisition Regulations (FAR) clauses 24.104 (Contract clauses), 52.224-1 (Privacy Act Notification), and 52.224-2 (Privacy Act), included in the contract?

Individuals who seek information about how social media sites collect, use, disclose and make accessible their PII should review the Site's terms of service or terms of use agreement, and its privacy policies.

All CFTC employees and many contractors have access to the names and organizations of authors of material disseminated internally through the news clips. Because the authors' names and organizations are publicly-available information, no confidentiality restrictions apply.

Information collected for Enforcement purposes and maintained in SORN CFTC-10 Investigatory Records (Exempted) and/or CFTC-16 Enforcement Case Files, may be disclosed in accordance with the blanket routine uses that appear at the beginning of the Commission's compilation of its systems of records notices, Federal Register notice 66 Fed. Reg. 41842 (2001), and any other specific routine uses identified for these SORNs, as they may be amended. Records maintained in the Enforcement Case Files may be shared publicly through enforcement proceedings brought in administrative tribunals or courts.

Internal Administrative Information will be accessible internally and shared with those who need to know the information for legitimate business purposes. In usual circumstances, the information may be added to a system of records, for example, Internet Security Gateway Systems, CFTC-36; Commission Investigatory Records, CFTC-10 (Exempted); or Enforcement Case Files, CFTC-16 (e.g., if needed for evidentiary purposes

to support an enforcement action). If this occurs, the information will be accessible and shared as provided in the applicable system of records notice.

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

Individuals who seek information about how a SMS transfers and shares their PII should review the Site's terms of service or terms of use agreement, and its privacy policies.

When PII is collected, maintained or disseminated by the CFTC for the internal news clipping service, the names and organizations of reporters are publicly available and not subject to confidentiality restrictions. It may be shared with others by paper or electronic means, as publicly-available news stories, blogs and SMS posts are generally shared. Any records used for purposes of an investigation or enforcement proceedings will be subject to SORN CFTC-10, Investigatory Records (Exempted), which is exempt from certain provisions of the Privacy Act, as noted above. Records used for enforcement proceedings brought in administrative tribunals or courts will be subject to SORN CFTC-16, Enforcement Case Files, and shared according to the rules and orders of the applicable tribunal. If added to a system of record, Internal Administrative Information may be shared as stated in an applicable system of records notice.

4.3. Do other systems share the information or have access to the information? 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, or System Managers)?

Individuals who seek information about how a SMS shares their PII or makes it accessible to other systems should review the Site's terms of service or terms of use agreement, and its privacy policies.

For Public Affairs purposes, in the only situations in which PII may be collected, maintained or disseminated by the CFTC, the names and organizations of authors of publicly available web content are not subject to confidentiality restrictions. Other CFTC systems may access the news clips posted on the intranet. This information is available to CFTC employees and contractors on the CFTC intranet and through CFTC-wide email.

Any records used for Enforcement purposes, will be subject to SORN CFTC-10, Investigatory Records (Exempted), which is exempt from certain provisions of the Privacy Act, as noted above. Records used as part of Enforcement Case Files may be shared with Commission enforcement and litigation systems, and if so, personnel in the Division of Enforcement and Office of Information Technology Services will be responsible for securing the information and protecting individual rights, as provided in CFTC-16, Enforcement Case Files.

Internal Administrative Information collected by the CFTC is only available to systems administrators unless used for an investigation.

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?

Individuals who seek information about how a SMS collects, uses, discloses and makes accessible their PII should review the Site's terms of service or terms of use agreement, and its privacy policies.

The information collected by the CFTC is from publicly available sources and collected directly from the Internet, except in certain limited enforcement investigations during which a CFTC user may act as a member of the public in seeking information pertaining to a business opportunity from an individual or entity.

The Commission provides notice to individuals about the Commission's collection, use, sharing and other processing of personal data through this PIA, the Commission's privacy policy and System of Record Notice for Investigatory Records, and the Commission's privacy notice available on SMS when feasible.

CFTC staff are notified of the collection and use of Internal Administrative Information through this PIA, CFTC log-in banners and internal policies and procedures.

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?

Each SMS determines what information it collects from an individual or allows an individual to post, and whether there is an opportunity or right not to provide that information, in order to obtain an account and become a user. The information collected by the Commission is offered to the Commission with the consent of an Internet user or is from publicly available sources, collected directly from the Internet and often voluntarily posted by the individual whose PII will be maintained, except in limited Enforcement investigations as explained above. For information publicly available on the Internet, individuals do not have an opportunity or right to consent to a particular use of the information collected by the CFTC.

In certain limited Enforcement investigations, information about a business opportunity that may violate applicable law may be sought directly from an individual or entity, just as a member of the public could request such information. For example, a Division of Enforcement staff member, using a username and profile not affiliated with the CFTC and acting as a member of the public, may send a request for information concerning a business opportunity. If an individual provides information under such circumstances, he or she will be providing it voluntarily and will have the opportunity to decline to provide it.

CFTC staff who are using the Off-Network Computers do not have an opportunity to consent to the collection or particular use of Internal Administrative Information.

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?

Most SMS require registered users to enter their login ID (e.g., an email address) and password at the SMS home page to gain access to their SMS account and change or update their account information. SMS typically explain in their privacy policies and screen language how users may access and update their accounts.

Internal news clips and Internal Administrative Information about CFTC staff's use of the Internet are not retrieved by an individual identifier, and therefore, no right of access or amendment exist. If Internal Administrative Information is added to a system of records, individuals may follow the procedures in the applicable system of records notice to gain access and request amendment to their records.

Information maintained in the CFTC Investigatory Record system have been exempted by the Commission from certain provisions of the Privacy Act of 1974 pursuant to the terms of the Privacy Act, 5 U.S.C. 552a(k)(2), and the Commission's rules promulgated thereunder, 17 CFR 146.12. Such 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. Records used in enforcement proceedings brought in administrative tribunals or court may be accessed and their accuracy may be questioned pursuant to the rules of the applicable tribunal, e.g., through discovery, evidentiary motions and testimony.

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?

The Commission provides secure access to the Internet and SMS via multiple high-speed Internet connections through:

- staff's assigned desktop computers and laptops linked to the CFTC's production network; and

- a handful of separate computers that are logically and physically isolated from the CFTC's production network ("Off-Network Computers").

All of these computers are secured within CFTC offices. The connections from Off-Network Computers to the Internet are isolated from the production network to eliminate risks to the network, and many are registered anonymously and are not traceable to the CFTC, allowing designated CFTC staff to conduct investigations as members of the public, simulating the customer experience.

To ensure that only approved content is disseminated through the CFTC SMS account for Public Affairs, only a select group of CFTC staff will have login credentials (username and password) that allow them to access CFTC SMS pages and make content edits.

When PII is collected and maintained as stated herein, the records will be protected from unauthorized access and misuse through various administrative, technical and physical security measures in accordance with applicable law. Technical security measures within CFTC 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. Physical measures include restrictions on building access to authorized individuals only and maintaining records in lockable offices and filing cabinets. Also, all employees are made aware of the sensitive nature of investigatory information.

6.2. While the information is retained, 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 collected by CFTC staff will not be systematically checked for accuracy and timeliness. Information available on the Internet is subject to frequent change. Information collected by staff is considered an accurate representation of the content as of the point-in-time it was collected. Standard security precautions exist to ensure that the information collected, e.g., information to be used in enforcement proceedings, is not altered inside CFTC's systems.

When the CFTC conducts an Enforcement investigation based on information obtained from the Internet, the records involved in such investigation will become part of the Investigatory Record system and therefore, have been exempted by the Commission from certain provisions of the Privacy Act of 1974 pursuant to the terms of the Privacy Act, 5 U.S.C. 552a(k)(2), and the Commission's rules promulgated thereunder, 17 CFR 146.12.

Internal Administrative Information is subject to review and audit by the Office of Information Technology Services.

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

No.

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

The CFTC follows all applicable Federal Information Security Management Act (FISMA), Privacy Act of 1974 and Commodity Exchange Act requirements to ensure that the information maintained is appropriately secured.

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

All CFTC personnel are subject to CFTC agency-wide procedures for safeguarding PII. They receive annual privacy and security training, in addition to periodic training specific to roles and responsibilities. Division of

Enforcement staff will receive mandatory training focused on the procedures for reviewing the Internet for investigatory purposes.

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?

No, information obtained for Public Affairs (e.g. news clips) and Internal Administrative Information about CFTC use of the Internet are not retrieved by a personal identifier in the normal course of business. In unusual circumstances, Internal Administrative Information may be added to a system of records and become retrievable by a personal identifier.

The investigation records for Enforcement purposes may be retrieved by personal identifiers. See CFTC-10, Investigatory Records (Exempted) and CFTC-16, Enforcement Case Files.

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.

For Public Affairs (e.g. internal news clips), the authors' names are not covered in a "system of records" as defined under the Privacy Act and therefore, no System of Records Notice applies.

Investigation related records for Enforcement purposes are covered under SORN CFTC-10, Investigatory Records, which are exempted by the Commission from certain provisions of the Privacy Act of 1974 pursuant to the terms of the Privacy Act, 5 U.S.C. 552a(k)(2), and the Commission's rules promulgated thereunder, 17 CFR 146.12. Such 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. Records used in enforcement proceedings brought in administrative tribunals or court are covered under SORN CFTC-16, Enforcement Case Files.

Internal Administrative Information is not covered in a "system of records" as defined under the Privacy Act and therefore, no System of Records Notice applies. In unusual situations, such information may be added to a system of records, and if so, the applicable system of records notice would apply.

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 CFTC's Privacy Policy on CFTC.gov.

The **www.cftc.gov** privacy policy has been updated to reflect these uses of the Internet.

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?

Privacy risks associated with the collection of PII for Public Affairs and Enforcement purposes have been mitigated by internal policies and procedures.

Internal policies allow Commission staff to only collect information offered to the Commission with consent or publicly-available information. The publicly-available information the CFTC may collect is the same as that which the public might collect or retrieve when accessing the Internet from their homes, offices or mobile devices or when otherwise researching or requesting information about a commodity or futures related business opportunity. The only exception is for certain limited enforcement investigations which meet specific criteria and follow specific written internal procedures and processes to allow the staff to simulate the experience of any prospective market participant searching the Internet or SMS and, if needed, request

additional information about a business opportunity that may violate applicable law. CFTC staff will document their activities and the information accessed. Staff will request information about the business deal available to potential market participants, not personal information about customers.

To further minimize privacy risks, the CFTC provides clear notice of its investigatory activities to the public on the Internet, as stated in this PIA, in its **www.cftc.gov** privacy policy and, when technologically feasible, on certain specific SMS. Internally at the Commission, only a select number of CFTC staff with a true "need to know" the information to perform their job duties will be allowed to access such investigatory information. Such staff have received annual privacy and security training in addition to special training concerning the sensitive nature of investigatory information. Moreover, administrative, technical and physical security measures secure the investigatory information maintained, and all Federal information security laws are followed.

Privacy risks associated with the collection of Internal Administrative Information is minimal and is consistent with similar computer usage information collected through the CFTC production network for administrative, management and review purposes.

PIA Publication Date: July 15, 2011