Commodity Futures Trading Commission
Privacy Impact Assessment

System Name: General Support System

Office: Office of Data and Technology

Date: September 22, 2016

1. Overview

The CFTC General Support System (GSS) is a collection of platforms and systems that form a networked infrastructure to support the CFTC's data processing needs. This infrastructure includes hardware, software, applications, databases, communications and Internet access to support mission and daily operations. Various CFTC major and minor applications reside on or link to the GSS, including financial market and oversight applications, civil law enforcement applications, internal administrative applications, and external-facing applications through which registrants and other individuals submit information. Because the GSS forms the CFTC information technology ("IT") network infrastructure, the information that is processed on or through the GSS can include virtually every type of information that CFTC creates, collects, uses, stores, maintains, disseminates, discloses and disposes of in support of its mission, which is to protect market users and the public from fraud, manipulation, abusive practices and systemic risk related to commodity futures and derivatives that are subject to the CEA, and to foster open, competitive, and financially sound markets.

The GSS components interconnect through a managed and redundant wide area network and host key components for CFTC major and minor applications. The GSS also links the CFTC headquarters to its regional offices in New York City, Chicago and Kansas City, as well as to its primary computing facility (PCF) and its alternate computing facility (ACF). The components of the GSS make up the fundamental hardware and software that provide connectivity, security, storage, communications, Internet access, and data access. The GSS includes client devices through which staff conduct daily work, and also central data storage and management devices.

The GSS routinely compiles and maintains personally identifiable information ("PII") of CFTC current and former network users, i.e., employees, volunteers, interns, contractors or consultants, to enable the network to function effectively, reliably and securely, and for activities to be logged for auditing, system improvement, and security purposes.

While the CFTC GSS contains a broad array of hardware, software, applications, databases, communications tools, and means to access the Internet, this privacy impact assessment (PIA) addresses the GSS components and functions that are likely to collect, compile or process personally identifiable information (PII). This includes:

1. Enterprise Applications: a communications and messaging platforms (e.g., email and instant messaging), database platform, and collaboration platform;
2. Workstations: desktops, laptops, and printers;
3. Telecommunications: telephones, audiovisual equipment, and tablets;
4. Network infrastructure: routers and switches, storage area network (SAN), primary and alternate computing facilities; and
5. Security infrastructure: firewalls, Active Directory (AD), Certificate Authority (CA), remote network access, security patch management, and personal identity verification (PIV).

Note: Other **PIAs available on the CFTC website** address certain other CFTC major and minor applications that collect, compile or process PII.

2. Data Collected and Stored Within the System

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

As noted, the GSS forms the CFTC IT network infrastructure, including hardware, software, applications, databases, communications and Internet access to support both mission and daily operations. Much of the PII processed on or transiting through the GSS relates to network users, e.g., CFTC usernames, contact information and network usage data for IT security purposes. Yet, various CFTC major and minor applications reside on or link to the GSS, including financial market and oversight applications, civil law enforcement applications, internal administrative applications, and external-facing applications through which registrants and other individuals submit information. As a result, and particularly because the GSS contains the CFTC communication platforms, the PII that is processed on or through the GSS can include virtually every type of information that CFTC creates, collects, uses, stores, maintains, disseminates, discloses and disposes of in support of its mission. This includes the following types of PII:

Categories	Is collected, processed, disseminated, stored and/or accessed by this system or project.	CFTC Employees	Members of the Public	Other (e.g. contractors, other government employees)
Name (for purposes other than contacting federal employees)	X	X	X	X
CFTC network username	X	X		X
CFTC contact information, e.g., CFTC email address, desk and mobile phone numbers, office location	X	X		X
Digital Certificates used by network systems	X	X		X
Date of birth	X	X	X	X
Social Security Number (SSN, last 4 digits)	X	X	X	X
Tax Identification Number (TIN)	X	X	X	X
Photographic identifiers	X	X		

Categories	Is collected, processed, disseminated, stored and/or accessed by this system or project.	CFTC Employees	Members of the Public	Other (e.g. contractors, other government employees)
Driver's license				
Mother's maiden name				
Vehicle identifiers				
Personal mailing address	X	X	X	X
Personal e-mail address	X	X	X	X
Personal phone number	X	X	X	X
Medical records number				
Medical notes or some other health information	X	X		X
Financial account information	X	X	X	X
Certificates	X	X	X	X
Legal documents	X	X	X	X
Device identifiers	X	X	X	X
Web uniform resource locator(s)				
Education records	X	X	X	X
Military status	X	X		
Employment status	X	X	X	X
Employment performance ratings or other information	X	X		
Applicant information	X	X	X	
Foreign business activities supervised by the CFTC	X		X	
Trader identities	X		X	
Trader positions	X		X	X
*Reports from individuals of any instance of fraud, waste, and abuse at CFTC	X	X	X	X
Information involved in investigations or complaints handled by the Division of Enforcement or Office of General Counsel	X	X	X	X
Banking data	X	X	X	
Procurement/contracting records	X	X	X	X
Data/information from foreign sources	X		X	
Data/information received through a memorandum of understanding or other sharing arrangement	X		X	
Proprietary or business information	X		X	X

Categories	Is collected, processed, disseminated, stored and/or accessed by this system or project.	CFTC Employees	Members of the Public	Other (e.g. contractors, other government employees)
Other: Communications between CFTC network users, or to or from such users, not already covered	X	X	X	X
Security identifiers of network users (generated by Microsoft Operating Systems)	X	X		X
Information related to CFTC network user activities on the network in identifiable form, e.g., log in and out times of certain CFTC applications and databases, and Internet usage	X	X		X

*Certain applications used by the CFTC Office of the Inspector General to investigate allegations of fraud, waste and abuse at the CFTC reside on the GSS; as a result, some of the related information is processed on or transits through the GSS.

Other **PIAs available on the CFTC website** address certain other CFTC major and minor applications that collect, compile or process PII.

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

The sources of information contained in the GSS are current and former CFTC IT network users, including current and former employees, interns, volunteers, contractors and consultants; individuals communicating with CFTC network users through CFTC communications platforms; information from other CFTC major and minor applications that is processed on or through the GSS, e.g., information from market and oversight, civil law enforcement and internal administrative applications, and from applications through which registrants and other individuals submit information; and CFTC hardware, software and system components that generate information reflecting activity on the CFTC IT network. For example:

- CFTC network user information needed for the GSS and its components to operate efficiently and securely and for the CFTC to control access to software, applications, data and information;
- activity logs, audit trails, identification of devices used to access CFTC systems, Internet sites visited, and information input into sites visited;
- logs of calls to and from a CFTC network user on desk or mobile phones, and similar communication data traffic logs;
- records of the name of authorized CFTC users, PIV card identifiers, user access level, and status (e.g. active/inactive), also including PIV card activity information, including time and CFTC office location of use by card holder;
- information of CFTC registrants or other individuals conducting business in CFTC-supervised financial markets that is collected and stored in other CFTC major or minor applications and transmitted through the GSS; and

- information stored in internal collaboration tools, including but not limited to a staff member's title, business and personal contact information, and organizational chart and hierarchy information.

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

The information is collected, used, maintained and disseminated to enable effective, reliable and secure operation of the IT network to support the CFTC's mission and daily operations. Much of the PII processed on or transiting through the GSS is collected, used, disseminated and maintained for the functioning and security of the IT network. Because the GSS forms the IT network infrastructure and other CFTC major and minor applications reside on or link to the GSS, PII from those other applications can be processed on or transit through the GSS.

Examples of the more specific purposes of PII collection, use, maintenance and dissemination include to: add and delete network users, i.e., enable CFTC employees, interns, volunteers, contractors and consultants to access the IT network and components (e.g., workstations and mobile devices), and when no longer working for the CFTC, to disable their access; enable network users to securely connect, store, and access data within other CFTC applications; monitor usage of and security of network components and applications; ensure the availability and reliability of the CFTC network components and applications; document and/or control access to various network applications; audit, log, and alert responsible CFTC personnel when certain PII is accessed in specified systems; investigate and make referrals for disciplinary or other action if improper or unauthorized use is suspected or detected; enable electronic communications between CFTC network users, and to and from CFTC network users with individuals outside the CFTC.

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

The PII processed on or transiting through the GSS is collected from CFTC network user communications with other network users and with individuals outside the CFTC; and CFTC network user actions on the network, e.g., downloads, uploads, extracts or creation of information from other CFTC applications that is stored on or transits through the GSS. (Information collected by applications that reside on the GSS is contained in PIAs for each individual application.)

GSS components and applications generate information that is personally identifiable reflecting activity on the CFTC network, e.g., security logs of access to applications, Internet use and logs of calls. The GSS also receives information that includes PII from external entities, e.g., the National Finance Center, in general receiving this information via secure file transfer protocol (SFTP), wide-area network (WAN) links and virtual private network connections (VPN).

2.5. Is the system using technologies in ways that the CFTC 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?

The legal authorities for collection are: 5 U.S.C. § 301; Commodity Exchange Act, 7 U.S.C. § 1 et seq. including Section 12 of the Commodity Exchange Act, at 7 U.S.C. § 16, and the rules and regulations promulgated thereunder.

3. Data and Records Retention

3.1.   For what period of time will data collected by this system be maintained and in what form will the data be retained?

The CFTC maintains policies and procedures, and provides training to all network users, designed to ensure that records will be maintained and then disposed of in accordance with **records disposition schedules** for the records involved, as approved by the National Archives and Records Administration (NARA). Information retained in the GSS is maintained in electronic form, primarily within internally accessible systems, but possibly on secure back-up or long-term storage media. Paper records are retained in paper filing methods, such as folders or binders, in secure offices and lockable cabinets.

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

The CFTC maintains policies and procedures, and provides training to all network users, designed to ensure that, once a record's retention period expires and the records are approved for disposal, the records are destroyed using a method appropriate to the format (e.g., shredding of paper records, destruction of media that contain PII, and purging of electronic records).

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)?

The CFTC maintains policies and processes to restrict access to the GSS internally to those network users who have a need to know the information to perform their job duties.

CFTC contractors with access to the GSS, including information security specialists, are required to comply with the Privacy Act and CFTC information usage policies and procedures contractually through either Federal Acquisition Regulation (FAR) terms or other terms and conditions. Many contractors also individually sign non-disclosure agreements. The Office of the Executive Director's Financial Management Branch is responsible for ensuring that the contract between the CFTC and contractors contains the provisions necessary to protect information to which the contractors have access.

The CFTC only shares information contained in the GSS with third parties as authorized by law. This includes, but is not limited to:

- sharing for legal proceedings or law enforcement purposes, e.g., when necessary for arbitration, mediation, litigation, investigations, or enforcement actions;
- sharing with individuals who have made a FOIA request and no exemption applies; and
- sharing with Congress.

The CFTC also provides certain types of information to other government authorities for official purposes, for example, to the National Finance Center to manage financial and human resource matters. The CFTC also shares information for security monitoring purposes, including with an external managed security services provider. Additionally, most CFTC communications transit through the **National Cybersecurity Protection System or "EINSTEIN,"** which detects and can prevent malicious activity.

The CFTC explains its routine uses for sharing information **in its Systems of Records Notices.**

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

The GSS forms the IT network infrastructure; the GSS, by itself, does not automatically share data outside the CFTC, i.e., there are no interconnections with external systems that would result in automated sharing data.

The GSS includes the communication platforms and provides the infrastructure for certain other CFTC major and minor applications. When network users are authorized to share PII processed on or transiting through the GSS, they may use the communication platforms, e.g., email, messaging or "file transfer protocol" (FTP). The CFTC maintains policies that prohibit network users from transmitting sensitive PII (or other types of confidential information) outside the CFTC network in an unencrypted or unsecured manner. The CFTC Privacy Office and ODT Security staff train all CFTC network users at least annually on this policy and on the procedures that can be used to transmit such information in an encrypted or otherwise secure manner.

If PII processed on or transiting through the GSS were printed in hard copy, staff have been directed by CFTC policy and trained to ensure secure delivery.

The GSS contains several one-way and two-way interconnections with other entities, for example with its managed security services provider; and the National Finance Center discussed in section 4.1.

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.

As described in Section 4.1, the information contained in the GSS will not be shared outside the Commission unless authorized by law. In certain instances, the CFTC creates high level aggregations of information for publicly available reports, for example, the Division of Enforcement may publish the number of individuals investigated for Commodity Exchange Act (CEA) violations over a particular period of time. In these instances, the CFTC aggregates the information at a high level to help ensure that the information cannot be re-identified.

4.4 Do the 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?

In the limited situations when the CFTC may publish aggregate or de-identified information, the CFTC 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.

The CFTC Office of General Counsel tracks disclosures for responses to requests from Congress or requests under the Freedom of Information Act (FOIA), and disclosures of information through arbitration, mediation or litigation. The Division of Enforcement tracks disclosures for purposes of investigations and enforcement actions, including any disclosures by the Whistleblower Office. They document, 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 information and by whom, and any restrictions on further dissemination of the requested information. Regular processing of GSS information through third party systems, e.g., information provided to the managed security services provider and communications transiting through the National Cybersecurity Protection System (“EINSTEIN”), is recorded through contract documentation and audit logs of transmissions.

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, and System Managers)?

GSS forms the network infrastructure, and other CFTC major and minor applications reside on or transfer information through the GSS. Other systems and applications interface with parts of the GSS, for example, the CFTC’s network administration database, Microsoft Active Directory. ODT network services personnel and administrators are responsible for protecting the interface between these systems to protect the privacy rights of individuals.

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?

The CFTC maintains this **PIA on the Privacy Office's CFTC website**, and Privacy Act **System of Records Notices available through the website.** Both explain the types of information collected, how the information may be used, possible sharing of the information, retention of the information, security measures, and how individuals may access information about themselves.

Also, all CFTC network users receive the CFTC's IT Rules of Behavior when they begin work at the CFTC. The document describes user responsibilities and expected behavior with regard to information and information system usage, and also reminds users that they have no reasonable expectation of privacy while using CFTC systems. The CFTC also provides a basic notice to users about the collection and use of information in the CFTC network every time they log into the CFTC network.

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?

When the CFTC requests that an individual provide information voluntarily, the individual may decline to provide information. For example, the GSS provides the infrastructure for internal collaboration tools, including the CFTC's intranet. Some network users have agreed to allow the CFTC to post their photograph on the intranet, while other users have not. The CFTC follows the wishes of these individuals. When an individual has a choice about providing information to the CFTC, he or she may grant consent by providing information or expressing consent orally or in writing.

In other situations, information is required for individuals to continue to work for the CFTC. For example, for purposes of network and information security, the GSS components and applications generate logs of network user activity on the network. CFTC network users receive notice of this type of data collection, and are reminded every time they log onto the network that the network is an official US government system, operated by the CFTC, and that they have no reasonable expectation of privacy in their use of the network.

The notices discussed in Section 5.1 above explain the opportunities an individual may have to decline to provide information or to consent to particular uses of the 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?

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?

The information in the GSS is protected from misuse and unauthorized access through various administrative, technical and physical security measures consistent with statutory and regulatory prohibitions on misusing confidential information. 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 information 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 and maintenance of records in lockable offices and filing cabinets. For example, all access to the GSS is on-site or via a secured virtual private network (VPN) connection. Also, CFTC staff regularly review GSS audit records for indications of inappropriate or unusual activity.

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?

Various administrative, technical and physical security measures are in place to help ensure that the information input into the GSS continuously reflects, over time, that information originally input into the system.

Each network user is responsible for the accuracy of information entered into or transmitted by the GSS. Once submitted, the information system security officer (ISSO) for each GSS component listed in Section 1 is responsible for verifying that information contained in the component system or application is accurate, relevant, timely and complete.

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

No, the system does not provide the capability to monitor an individual in real-time. However, the GSS can confirm whether an individual is logging in to the CFTC network from a CFTC desktop as opposed to a remote computer via VPN. Also, the GSS contains mobile device management software that allows specifically designated CFTC IT staff to locate a CFTC mobile device, if such a device is lost or stolen.

6.4 Does this system comply with FISMA requirements to help ensure that information is appropriately secured?

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 Modernization Act (FISMA). The CFTC ODT Security Team conducts security assessments of the GSS in accordance with the **Office of Management and Budget Circular A-130 - Managing Federal Information as a Strategic Resource** and **NIST Special Publication 800-37, Guide for the Security Certification and Accreditation of Federal Information Systems**. The CFTC OED Privacy Office develops privacy controls and conducts privacy assessments in accordance with **Circular A-130, "Managing Information as a Strategic Resource," Appendix II, "Responsibilities for Managing Personally Identifiable Information**" (released July 28, 2016), and **NIST SP 800-53 Rev. 4, Security and Privacy Controls for Federal Information Systems and Organizations**. The GSS is scheduled to be assessed and authorized (A&A) on September 22, 2016. The GSS, if breached, would result in a moderate potential impact on individuals or organizations, as categorized under the **Federal Information Processing Standards (FIPS) 199**.

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

All CFTC network users are subject to CFTC agency-wide policies and procedures for safeguarding PII. They receive privacy and security training and acknowledge the CFTC "Information Technology Rules of Behavior" when they start work at the CFTC and annually thereafter. Many staff receive additional training focused on their specific job duties, for example, system administrators and individuals with access to the security infrastructure 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?

Although CFTC staff may retrieve GSS information by keyword, staff frequently search and retrieve by personally identifiable information, such as an individual's name or phone number. Information related to individual workstations is generally retrieved by an individual's CFTC username, and information from the security infrastructure tools generally is searched based on a combination of internet protocol (IP) address, CFTC-issued device Identifier and/or CFTC 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, the information contained within the GSS is covered by existing SORNs:

- **CFTC-33, Electronic Access Card**
- **CFTC-35, General Information Technology Records**

- **CFTC-47, Internal Electronic Collaboration Tools**

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 **www.cftc.gov**.

The collection, uses and disclosures of the information have been reviewed and are consistent with the privacy policy on **www.cftc.gov**.

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 and maintains strong administrative, technical and physical controls to protect PII created, collected, stored in and/or transiting through the GSS. In addition to the controls noted in Section 6.1 above, for example:

- PII stored in and transiting through the GSS is only viewable by specific employees and contractors with a need to know the information, i.e., employees and contractors who require access to perform their job functions, and who are bound by non-disclosure policies and/or agreements.
- Several applications within the GSS require unique usernames and passwords that are separate from CFTC network usernames and passwords.
- Certain types of data processed on the GSS are encrypted at rest.
- CFTC staff receive training on how to identify and report "insider threats," including being aware of inappropriate requests for access to information, reporting attempts to log into other users' accounts, and other suspicious activity.
- In addition to other training, the CFTC requires that system administrators and staff with access to security infrastructure complete role-based training.