Commodity Futures Trading Commission
Privacy Impact Assessment

System Name: PRISM

Office: Financial Management Branch

Date: January 08, 2018

1. Overview

The CFTC Procurement Team manages the Commission's acquisition needs and oversees and executes all CFTC procurement activities. The team is responsible for drafting and implementing procurement policy for the Commission, serving as business manager for agency contracting activities, and awarding and administering the Commission's contracts in accordance with sound business practices, federal laws and regulations, and agency policies.

The CFTC Procurement Team will use PRISM, a browser-based, Commercial-off-the-Shelf (COTS) software product to manage the contract life-cycle. PRISM includes tools to support requirements generation, approval, workflow processing, and other steps of the procurement process, including closeout. Pursuant to an Interagency Agreement, the Department of Transportation (DOT) Enterprise Service Center (ESC) hosts and provides technical support for CFTC's implementation of PRISM.

2. Data Collected and Stored Within the System

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

The PRISM system contains personally identifiable information (PII) and non-personally identifiable information pertaining to vendors, who are registered within the General Services Administration's (GSA) System for Award Management (SAM) system, and CFTC's core accounting system, DELPHI. PII retained within the PRISM system may include PII where a vendor uses PII in identifying herself or himself in an entrepreneurial capacity. The PRISM system also contains PII from authorized PRISM users for identification and user access purposes.

1. PII Categories	2. Is collected, processed, disseminated, stored and/ accessed by this system or project	3. CFTC Employees	4. Members of the Public	5. Other (e.g. contractors, other government employees)
Name (for purposes other than contacting federal employees)	X	X	X	X
Date of Birth				
Social Security Number (SSN, last 4 digits)	X			X
Tax Identification Number (TIN)	X		X	X
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 some other Health Information				
Financial Account Information	X		X	X
Certificates				
Legal Documents	X		X	X
Device Identifiers				
Web Uniform Resource Locator(s)				
Education Records				
Military Status				
Employment Status				
Foreign Activities				
Other (please be specific, e.g. Tip, Complaint or Referral/TCR number):				

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

PRISM collects information directly from CFTC employees, CFTC contractor employees, the SAM database, and vendors. CFTC employees and contractor employees requiring access to PRISM must provide information to gain access to the system. Data is collected directly from vendors responding to CFTC solicitations. This information often includes information which may contain PII including Taxpayer Identification Numbers (TINs), and contact information.

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

PRISM collects information to manage the acquisition process for the procurement of services and supplies. The information collected from CFTC authorized users (employees and contractors) is necessary to establish accountability and to track workload related processes concerning procurement transactions.

Information collected from CFTC vendors is required by the Federal Acquisition Regulation (FAR) and necessary to accurately document, award, and manage procurement actions, including ensuring vendors are compensated for goods delivered, or services performed.

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

PRISM collects information directly from CFTC users (employee and contractors). If a new end user account is needed, the end user or PRISM Site Administrator completes a User Account Request form, which is signed by the appropriate CFTC supervisor for access to PRISM. The completed and approved form is then emailed to the ESC-Shared Services provider for user profile set-up.

Most vendor information is pre-loaded into PRISM via electronic download of SAM data on a monthly basis through a secure process performed by the DOT ESC-Shared Services team. Vendor file downloads from the ESC-Shared Services providers are uploaded into PRISM as a scheduled batch file, and daily updates are made through the same secure procedure as needed. In some cases, the CFTC requisitioner, contract specialist, or contracting officer, may manually enter notes regarding the procurement into the PRISM system.

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

Yes. The current CFTC procurement process is largely a manual process. The PRISM system allows CFTC to automate the procurement process and accomplish stages of the acquisition process from gathering requirements to contract closeout, workload management and reporting.

Internally - PRISM uses information to create requisitions, solicitations, award documents, contract modification documents, interagency agreements, blanket purchase agreements, and basic ordering agreements. Additionally, PRISM uses information to internally manage the acquisition process by establishing user accounts and tracking workload related processes on procurement transactions. Reports are generated to track and help manage program area workload, provide information in support of CFTC procurement goals and objectives, as well as managing the PRISM system itself.

Externally – PRISM transmits select PRISM information to Federal Procurement Data System–Next Generation (FPDS-NG) to satisfy FAR reporting requirements. It is a FAR requirement to report awarded and executed procurement transactions that meet specific guidelines and thresholds. Federal contract data in FPDS-NG is available to all Federal agencies, Congress, the Office of Management and Budget, and the general public.

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

Authority to collect this information is provided by:
FAR Subpart 4.1102, Policy, requires prospective contractors be registered in the SAM database prior to award of a contract or agreement, which authorizes the use of limited vendor PII as contained in the SAM system.

The Electronic Funds Transfer (EFT) Act requires that most federal payments be made electronically. As a result, any vendor of the Federal government is required to receive payment by EFT which authorizes use of vendor TIN, which may be associated with an individual and is obtained from the SAM.

Additional authority to collect information from CFTC contractors and vendors is authorized by: to 5 U.S.C. 301; Executive Order 9373; the Office of Federal Procurement Policy Act (41 U.S.C. 405)

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?

Procurement records are retained for the life of the contractual action, plus a specified period of time after the action has been completed. The procedures and retention periods for contract files and data is set forth in section 4.805 of the FAR and General Records Schedules 1.1, Item 010, published by the National Archives and Records Administration (NARA). For completed contract files, disposition is required 6 years after final payment or cancellation, but longer retention is authorized if needed for business use.

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

Destruction or disposition of the information retained in the PRISM system will follow the FAR as required, and NARA approved disposition schedules for the records.

User accounts are retained for the life of the system, per GRS 3.2, Item 030. Users who no longer require a PRISM account cannot be deleted from the system, however, the login rights are removed from the account and the account is deactivated. Deletion of user accounts would eliminate pertinent historical elements of the procurement 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)?

CFTC Requisitioners, CORs, and Contracting Specialist/Officers, Senior Procurement Officers have access to the information stored in PRISM. Access to data and information is controlled through role-based and site-based access, as well as the use of security groups within PRISM preventing unauthorized sharing of information. CFTC authorized contracting staff may have access to information in PRISM on a need-to-know basis to fulfill their contracting duties on behalf of CFTC. CFTC contracts that require contractors

to have access to Privacy Act information in PRISM contain the appropriate FAR Privacy Act clauses.

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

PRISM transmits contract data to the Federal Procurement Data System (FPDS-NG) as part of the contract award process. This data generally includes contract number, number of quotes received, vendor name, if CFTC competed the action, the value of the action and the period of performance. The FPDS-NG is managed by the General Services Administration and serves as the current central repository of information on Federal contracting. FAR Part 4.602 requires Federal agencies to report acquisition activities to the FPDS-NG. These secure transmissions are a function within PRISM.

Contract data from the PRISM system may be used to respond to inquiries from Congress, the General Accountability Office (GAO), and Freedom of Information Act (FOIA) requests.

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

Procurement transaction data in FPDS-NG is publically available. PRISM may electronically transmits information that includes an agency identifier, procurement document number, award and expiration dates and/or the business name of a vendor/ consultant operating in their entrepreneurial capacity.

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?

No other datasets are known, or apply to this system at this time.

4.5. Describe how the CFTC will track disclosures of personally identifiable 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.

CFTC is able to track the disclosure of personal information collected from PRISM by tracing the information back from the external request to the initial collection.

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)?

The CFTC implementation of PRISM will be electronically interfaced with the DELPHI Financial System. From a technical perspective, the DELPHI Financial System is managed and secured at DOT ESC, who is responsible at the technical administration level to provide the necessary protection of privacy for individuals in the system that may be affected by the interface.

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?

Notice is provided to CFTC authorized users via the PRISM User Account Request form and PRISM Rules of Behavior provided by DOT. General notice is also provided to CFTC users by the System of Records Notice (SORN).

Vendors who have registered with SAM and provided information through that system are made aware that the information will be shared by Federal agencies as part of the registration process.

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?

CFTC and contractor employees are requested to provide information to access the system. This information is limited to name, work phone and work e-mail address. An individual may decline to provide this information, however, if the information is not provided, the employee cannot be granted access to the PRISM system. The individual grants consent by filling out the required forms to obtain access to PRISM.
Vendors or consultants who decline to submit the required information, will not be able to register in the SAM database, and therefore will not be able to do business with the CFTC.

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?

If individuals would like access to their personal information contained in the system, or request amendment or correction to their information, they should address a written inquiry to the Office of General Counsel, Commodity Futures Trading Commission, Three Lafayette Centre, 1155 21st Street, NW, Washington, DC 20581. Details on submission requirements are located in Commission regulations at 17 CFR Part 146.

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?

Information is protected from unauthorized access and improper use through administrative, technical, and physical security measures. Administrative safeguards include agency and system specific Rules of Behavior, agency-wide procedures for safeguarding personally identifiable information, and required annual privacy and security training. Technical security measures within CFTC include restrictions on computer access to authorized individuals who have a legitimate need to know the

information; required use of strong passwords that are frequently changed; multi-factor authentication for remote access and access to many CFTC network components; use of encryption for certain data types and transfers; firewalls and intrusion detection applications; and regular review of security procedures and best practices to enhance security.

PRISM users can only access the PRISM system through a web browser through the CFTC intranet. The PRISM system requires PIV card authentication to access the system, and the CFTC network is also PIV card enabled providing an added layer of security. Only specifically authorized individuals may access the records in this system of record, and access is limited according to job function, through system-defined security groups Physical measures include restrictions on building access to authorized individuals and 24-hour security guard service. All employees and contractors are made aware of the sensitive nature of PII and proper handling of PII via annual security and privacy training.

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 procurement process relies on accurate and timely information to properly manage the process from contract initiation to closeout. Therefore, appropriate review and verification of the information is built into the procurement process and performed on an ongoing basis driven by the actions required to execute tasks in the contract lifecycle.

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 locate and/or monitor an individual in real-time.

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

Yes. The CFTC follows all applicable Federal Information Security Management Act (FISMA) requirements. PRISM is FedRamp compliant and received an Authority to Operate (ATO) by DO. The DOT security assessment package was inspected by CFTC security staff.

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

Users receive annual privacy and security training, and must abide by IT Rules of Behavior when accessing CFTC information systems. In addition, PRISM has its own set of Rules of Behavior provided by DOT.

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?

Typical retrieval methods are by contract name, or number. If a vendor is using her or his name in an entrepreneurial capacity, the name may be associated with the contract and retrieved by this identifier.

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.

Contractor and Consultant Privacy Act information is this system will be covered by the forthcoming CFTC-51, Contractor and Consultant SORN. CFTC employee information is covered under exiting SORN CFTC-35, General Information Technology Records, and CFTC-5, Employee Personnel, Payroll, Time and Attendance.

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, use, and disclosure of the information in this system have been reviewed by CFTC's Office of General Counsel, and CFTC's Privacy Office and they are consistent with the Commission's 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?

There is a risk of using information in PRISM for reasons outside of its original collection. To mitigate this risk access to PRISM is limited to the minimum access users need to perform their respective functions based on roles, sites, and security groups. This allows users to perform appropriate duties in the system for which they have responsibility and prevents users from seeing more information than is required to perform their job function The PRISM system is only accessible through a browser via the CFTC network, which requires PIV-access for user log-in. The PRISM system also requires PIV card authentication to access the system. All users have or will receive CFTC security training, and PRISM user training prior to being granted access to the system. In addition, changes to user accounts are tracked and audited through the use of transaction history tracking which provides information on data changes made and the specific user who made the change.