Commodity Futures Trading Commission
Privacy Impact Assessment

System Name: LabCFTC

Office: Office of General Counsel

Date: May 16, 2017

1. Overview

LabCFTC is the focal point for the CFTC's efforts to promote responsible Financial Technology (FinTech) innovation and fair competition for the benefit of the American public. The purpose of LabCFTC is twofold: first, to encourage responsible FinTech innovation in the markets the CFTC oversees and second, to help accelerate Commission engagement with FinTech solutions that may enable the CFTC to carry out its mission responsibilities more effectively and efficiently.

LabCFTC includes two main components. These components are: CFTC GuidePoint and CFTC 2.0. GuidePoint offers an additional, dedicated point of contact for FinTech innovators to engage with the CFTC, learn about the CFTC's regulatory framework, and obtain feedback on the implementation of innovative ideas for the market. Such feedback may include information that, particularly at an early stage, could help innovators/entities save time and money by helping them understand relevant regulations and the CFTC's approach to oversight. CFTC 2.0 is a program to foster and help initiate the adoption of new technology within the CFTC's own mission activities through collaboration with FinTech industry and CFTC market participants. CFTC 2.0 is intended to provide the agency opportunities to engage with new technologies to discover ideas and technologies that have the potential to improve the effectiveness and efficiency of the agency in carrying out its day-to-day activities.

To effectively implement and manage these components, the CFTC must be able to communicate with the innovator community. To accomplish this task, CFTC has implemented a secure website portal and dedicated email address to facilitate communications with the FinTech community. The website portal is hosted on Amazon Web Services (AWS) GovCloud environment. The AWS GovCloud environment is a **Federal Risk and Authorization Management Program (FedRAMP)** certified hosting provider, meaning it has been authorized for use under a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services.

The CFTC email system is resides on the CFTC General Support System (GSS), which has its own PIA. The CFTC email system is continuously monitored for operational and security risks by CFTC Office of Data Technology (ODT). Access to the LabCFTC mailbox is restricted to CFTC personnel that have a need to know the information.

2. Data Collected and Stored Within the System

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

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**	
Date of Birth				
Social Security Number (SSN, last 4 digits)				
Tax Identification Number (TIN)				
Photographic Identifiers				
Driver's License				
Mother's Maiden Name				
Vehicle Identifiers				
Mailing Address	**X**		**X**	
E-Mail Address	**X**		**X**	
Phone Number	**X**		**X**	
Medical Records Number				
Medical Notes or some other Health Information				
Financial Account Information				
Certificates				
Legal or Business Documents	**X**		**X**	
Device Identifiers				
Web Uniform Resource Locator(s)	**X**		**X**	
Education Records				
Military Status				
Job Title	**X**		**X**	
Foreign Activities				
Other: email inquiries may include some level of identifying information based on the context of the information submitted	**X**		**X**	

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

Information is collected directly from the individuals who choose to submit an email to CFTC.

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

The information is being collected to enable CFTC to communicate with the FinTech community to encourage responsible innovation in the markets CFTC oversees and second, to help accelerate Commission engagement with FinTech solutions that may enable the CFTC to carry out its mission responsibilities more effectively and efficiently.

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

Individuals choose to submit electronic information directly to CFTC through the dedicated LabCFTC email address.

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 collection of this information is authorized under 7 U.S.C. 5(b).

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 records will be maintained in electronic form. Records for this system will be maintained according to disposition schedules approved by the National Archives.

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

The records will be maintained in accordance with the retention periods in the schedules. After the retention period has expired, the records will be destroyed, or disposed of, according to the disposition schedules. All approved schedules are available at **www.cftc.gov**.

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)?

Only internal CFTC personnel are allowed access to the information. These individuals include employees of the Commission and contractors with a need to know the information to perform their Commission responsibilities.

Certain individuals who are specifically assigned access to CFTC's GSS environment have access to the information for information technology administrative and security purposes only.

Contractors with access to the system are required to comply with the Privacy Act contractually through either FAR terms or other terms and conditions. The Office of the Executive Director's Financial Management Branch (FMB) ensures that the contract between the Commission and contractors contains the provisions necessary to protect and secure information to which the contractors have access.

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

If transferred or shared outside the Commission'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.

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.

Yes. The data may be released to the public, consultants, researchers or other third parties. If the data is released it will be aggregated so that no individual is identified in the release.

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?

Recipients of any aggregated or de-identified information from LabCFTC do not have another dataset that could be used to re-identify the information. CFTC is not aware of any public data set that could be used to re-identify the information if publicly released.

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 this system 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, System Managers)?

No other systems share the information or have access to the information in this system. CFTC's ODT staff, including specifically permitted employees and contractors, regularly monitors the information travelling through and/or stored on CFTC's email system. ODT staff is responsible for raising any potential 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?

Notice to individuals is provided on the LabCFTC web pages of the CFTC's website landing page where the individual can locate the email address to contact CFTC. In addition, the Privacy Policy describes what information is collected and stored automatically; that individuals may choose to submit personal information about themselves to the CFTC; how submitted information may be shared; security; and the purposes of the information collection.

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?

All personal information collected is entirely voluntary. Certain personal data elements collected enable the CFTC to respond to the specific inquiries.

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 an individual would like access to their personal information contained in the system, or requests amendment or correction to the information, they can contact the CFTC Privacy Office at privacy@cftc.gov.

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 is protected from misuse and unauthorized access through administrative, technical and physical security measures. Administrative safeguards include written guidelines on handling LabCFTC information. All CFTC personnel are subject to CFTC agency-wide procedures for safeguarding PII and receive annual privacy and security training. Technical security measures within CFTC include

restrictions on computer access to authorized individuals, required use of strong passwords frequently changed, use of encryption for certain data types and transfers, and regular review of security and access logs to determine anomalous activity, and regular review of security procedures and best practices to enhance security. Physical measures include restrictions on building access to authorized individuals.

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 collected from the system is input directly by the individuals submitting the information. Accuracy of the information is dependent upon the individual providing the information.

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

No. The system does not provide real-time capability to locate or monitor an individual .

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

Yes. The Commission follows all applicable FISMA requirements to ensure that information is appropriately secured. Individuals submit information via a dedicated CFTC email address. The email system resides on CFTC's GSS. The CFTC follows the National Institute of Standards and Technology (NIST) Special Publication 800-53, 'Recommended Security and Privacy Controls for Federal Information Systems' to secure its systems as required by 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.

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 and receive annual privacy and security training. Many staff receive additional training focused on their specific job duties.

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, information in the system can be retrieved by name of correspondent, subject matter, date, or other searchable information provided by the submitter.

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.

The Privacy Act records in this system are coved by the existing CFTC-2 SORN.

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?

The system collects basic contact information necessary to follow up with requests and inquiries. There is a risk that a submitter will use their personal information as contact information instead of a business address, phone number, or email address. CFTC provides notice in plain language of how CFTC handles the collected information on the LabCFTC web pages of the CFTC's website.