Commodity Futures Trading Commission
Privacy Impact Assessment

System Name: Data Loss Prevention (DLP) Tool

Office: Office of Data and Technology (ODT)

Date: July 11, 2018

1. Overview

The Commission's DLP tool is a commercial off the shelf (COTS) tool designed to analyze, identify, alert and prevent the unintentional or deliberate exfiltration of unprotected sensitive data from an organization's network. The DLP tool is currently being used at the CFTC to discover and protect the unauthorized or accidental transmission of Social Security numbers (SSN) outside of the Commission.

2. Data Collected and Stored Within the System

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

The tool is capable of capturing sensitive information including sensitive personal information which may include Social Security numbers (SSN), dates of birth, financial information, and other personal information that may be linked or linkable to specific individuals. However, the tool only captures information that is related to a violation of the policies and rules that have been defined within the tool to protect CFTC information from unauthorized or accidental transmission outside of the CFTC.

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	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		

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		
Financial Account Information	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)	x	x	x	x
Education Records				
Military Status	x	x		
Employment Status	x	x	x	x
Foreign Activities	x		x	
Other: Communications between CFTC network users, or to or from such users, not already covered	x	x	x	x

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

Sources of data include email sent by CFTC employees, contractors, and volunteers, who have access to CFTC information and systems.

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

The information is being collected to identify, validate, and remediate sensitive data loss to the Commission.

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

The tool monitors CFTC email traffic and captures data that violates the policies and rules set up in the tool to protect data from unauthorized or accidental transmission outside the CFTC.

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

No. The tool is not monitoring individuals in real-time. The tool automates the monitoring of data traffic to determine if there is a policy violation. Data may be later associated with an owner once it has been properly analyzed and validated by authorized staff to determine if the owner is necessary for remediating the violation**.**

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

Privacy Act of 1974 5 U.S.C. § 552a (e)(10), Public Law 113-283 (FISMA); 44 U.S.C. §3553(a)(2), and Office of Management and Budget (OMB) Circular A-130 § 5(f)(1)(d).

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 Commission is in the process of developing a records disposition schedule for this system. Data for this system will be maintained in accordance with the records disposition schedule that is ultimately approved by the National Archives and Records Administration (NARA). The records will be maintained in electronic format.

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

All data will be deleted according to the records disposition schedule that is ultimately approved by NARA. The Commission's records disposition 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)?

Access to the data is limited to a small number of individuals who support the CFTC security operations. An individual's access to data within the system is restricted based on business need and dependent on the role to which they are assigned within the system**.**

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

The data is used for internal purposes only, and there is no intention to share any data outside the Commission's network. If data is required to be shared pursuant to the Privacy Act or other legal obligation, it will be properly secured and protected with appropriate administrative and technical controls.

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.

The data will not be released to the public**.**

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?

The data is not released publically, and there is no known public data set.

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 the DLP tool 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)?

No. Other systems do not share or have access to the information in this system.

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?

Each time a user logs in to the CFTC network they are presented with a notice that the system is monitored for security purposes, and the user provides consent by clicking on the “ok” button to use the network and associated systems.

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?

If a user declines consent to the DLP monitoring the user will not be able to use CFTC systems. The information in the system is only used to reduce the data breach risk associated with the exposure of unprotected sensitive data.

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?

The DLP tool is not considered a system of records under the Privacy Act, therefore provisions of the Privacy Act allowing users to gain access to their information in this system are not applicable. For systems of records that are covered under the Privacy Act, individuals should address written inquiries to the Office of General Counsel, Commodity Futures Trading Commission, Three Lafayette Centre, 1155 21st Street, NW, Washington, DC 20581. See 17 CFR 146.3 for full details on what to include in a Privacy Act access request.

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 various administrative, technical, and physical security measures. Administrative safeguards include agency-wide Rules of Behavior, 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, required use of strong passwords frequently changed, use of encryption for certain data types and transfers, and regular review of security procedures and best practices to enhance security. The DLP application is hosted on the agency's dedicated DLP servers. Because DLP users can access the DLP system through a Web browser, access is only possible via the secured CFTC intranet.

Physical security measures include restrictions on building access to authorized individuals and maintenance of records in lockable offices and filing cabinets.

6.2. While the information is retained in the system, what will the requirements be for determining if the information is still sufficiently accurate, relevant, timely, and complete to ensure fairness in making determinations?

Data is verified for accuracy when held for review.

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

The system does not provide the capacity to track or monitor the location of an individual in real-time. The system may be able to identify an individual and his or her office or geographical location within the Commission at a particular time based on system logs or details contained in the event alert.

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

Yes, the system complies with all applicable Federal Information Security Management Act (FISMA) requirements**.** The tool is part of the CFTC's GSS security boundary that has undergone the required security assessment.

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 systems that contain CFTC information.

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. the data will not be retrieved by a personal identifier in the normal course of business. The tool tracks and provides event alerts that are validated and analyzed and this is the way the information is retrieved.

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.

No. Since the data in the system is not retrieved by a personal identifier, the system is not covered under a 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?

There is a risk that data collected by the DLP tool may be used for a different purpose without notice to the data subject

There is a risk that more information than is necessary will be analyzed in order to determine if an event requires escalation before resolution.

This risk is mitigated by the security team having role-based access to the information and security analysts will only query additional data when necessary and appropriate to resolve an event.

There is a risk that those with authorized access could use their access for unapproved or inappropriate purposes.

To mitigate this risk, the DLP tool contains auditing records of activities performed by all users. These audit logs are reviewed periodically by cleared representatives from ODT and any inappropriate use will be referred to the appropriate internal investigators (such as the Office of Inspector General or others as required) for handling.

There is a risk that authorized users are exposed to PII as a routine part of their official duties. These users may make inappropriate disclosure of this information, either intentionally or unintentionally. To mitigate this risk, all users of the tool are required to take specific training on how to handle PII and for resolving DLP events. Users must also abide by IT Rules of Behavior.

There is a risk that as ODT provides access to and retains increasing amounts of sensitive information, it may become a target for unauthorized outside users (hackers). The DLP tool is hosted on the agency's dedicated DLP servers. Access to the tool is only possible via the CFTC intranet and operates under the FIPS 140-2 compliant Secure Socket Layer (SSL) encryption technology. All transmissions within the DLP system are encrypted to protect the information.