



**Privacy Impact Assessment
for
Stressing Positions at Risk (SPARK)**

June 10, 2021

System/Business Owner

Division of Clearing and Risk (DCR)

Reviewing Official

Charles Cutshall
Chief Privacy Officer
Commodity Futures Trading Commission

I. SYSTEM OVERVIEW

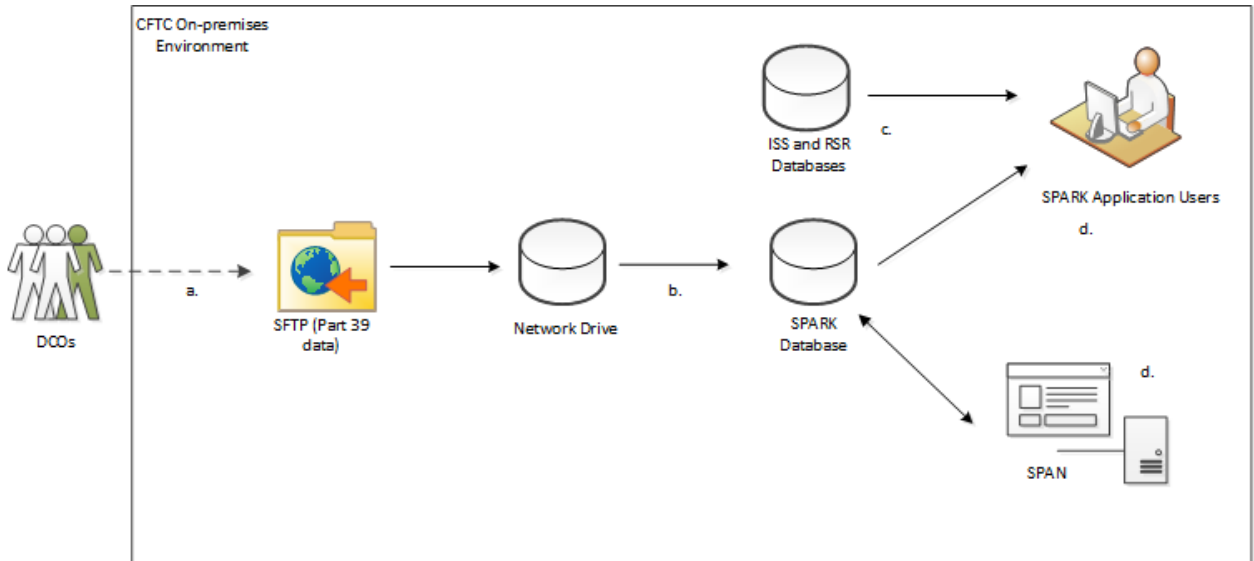
1) Describe the purpose of the system/collection:

Stressing Positions at Risk (SPARK) is used by Commodity Futures Trading Commission (CFTC) staff to identify traders whose positions may pose financial risk to the markets or a clearing firm. Division of Clearing and Risk (DCR) staff analyze an owner's holdings and project the effect of market moves on these holdings. By leveraging the desktop application version of the Standard Portfolio Analysis of Risk (SPAN) software, developed by the Chicago Mercantile Exchange, SPARK allows DCR to perform "what if" analyses to determine the effect of market movement on margin. Through these "what if" scenarios, an analyst can determine if the margin is sufficient.

SPARK uses data from the Integrated Surveillance System (ISS) and data submitted by Derivatives Clearing Organizations (DCOs). A DCO is an entity that enables each party to an agreement, contract, or transaction to substitute, through novation or otherwise, the credit of the DCO for the credit of the parties; arranges or provides, on a multilateral basis, for the settlement or netting of obligations; or otherwise provides clearing services or arrangements that mutualize or transfer credit risk among participants. Pursuant to Part 39 of the CFTC's regulations, DCOs are required to submit daily position information relating to the DCO's clearing members and the clearing member's respective customer accounts.

SPARK comprises both a database for Part 39 data, parts of the ISS database, and a client server application. Limited firm-level financial data is also copied from the Regulatory Statement Review (RSR) system. SPAN is integrated into SPARK via application programming interface (API) such that DCR users do not need to open the desktop application in order to use its functionalities.

2) Provide a data map or model illustrating how information is structured or is processed by the system throughout its life cycle. Include a brief description of the data flows.



- a. DCOs submit daily Part 39 data relating to the DCOs clearing members and the clearing members’ respective customer accounts via secured file transfer protocol (SFTP) to a network drive within the CFTC environment.
- b. The Data Engineering & Processing (DEAP) team within the Division of Data (DOD) is responsible for maintaining loading programs that populate data from the SFTP drop site into the SPARK database.
- c. The SPARK application integrates with certain information from the ISS and RSR databases.
- d. Users of SPARK use the integrated SPAN desktop application to calculate margin risks. Results of analyses created using SPAN are saved to the SPARK database.

II. AUTHORITY AND PURPOSE

- 1) What is the legal authority to collect, use, maintain, and share information in the system?
7 U.S.C. §§ 2, 7a-1, 12a, and 17 C.F.R. § 39.19.

III. INFORMATION TYPES

- 1) What information will be collected, maintained, used, and/or disseminated?

| Identifying Numbers | |
|---|--|
| <input type="checkbox"/> Social Security Number | <input type="checkbox"/> Truncated or Partial Social Security Number |
| <input type="checkbox"/> Driver’s License Number | <input type="checkbox"/> License Plate Number |
| <input type="checkbox"/> Patient ID Number | <input type="checkbox"/> File/Case ID Number |
| <input type="checkbox"/> Student ID Number | <input type="checkbox"/> Health Plan Beneficiary Number |
| <input type="checkbox"/> Passport Number | <input type="checkbox"/> Federal Student Aid Number |
| <input type="checkbox"/> Employee Identification Number | <input type="checkbox"/> Taxpayer Identification Number |

| | |
|--|--|
| <input type="checkbox"/> Professional License Number | <input checked="" type="checkbox"/> Legal Entity Identifier |
| <input type="checkbox"/> Credit/Debit Card Number | <input type="checkbox"/> National Futures Association ID |
| <input type="checkbox"/> Personal Bank Account Number | <input checked="" type="checkbox"/> Other ID if it can be traced back to an individual |
| <input type="checkbox"/> Personal Device Identifiers or Serial Numbers | |
| Contact Information | |
| <input type="checkbox"/> Personal Mobile Number | <input type="checkbox"/> Business Phone Number |
| <input type="checkbox"/> Personal E-mail Address | <input type="checkbox"/> Business E-mail Address |
| <input type="checkbox"/> Home Phone Number | <input type="checkbox"/> Personal or Business Fax Number |
| <input type="checkbox"/> Home Mailing Address | <input type="checkbox"/> Business Mailing Address |
| Sole Proprietors | |
| <input type="checkbox"/> Business Taxpayer Identification Number | <input type="checkbox"/> Business Mailing Address |
| <input type="checkbox"/> Business Credit Card Number | <input type="checkbox"/> Business Phone or Fax Number |
| <input type="checkbox"/> Business Bank Account Number | <input type="checkbox"/> Business Mobile Numbers |
| <input type="checkbox"/> Business Device identifiers or Serial Numbers | |
| Biographical Information | |
| <input checked="" type="checkbox"/> Name | <input type="checkbox"/> Gender |
| <input type="checkbox"/> Date of Birth | <input type="checkbox"/> City or County of Birth |
| <input type="checkbox"/> Country of Birth | <input type="checkbox"/> Zip Code |
| <input type="checkbox"/> Citizenship | <input type="checkbox"/> Military Service Information |
| <input type="checkbox"/> Spouse Information | <input type="checkbox"/> Academic Transcript |
| <input type="checkbox"/> Group/Org. Membership | <input type="checkbox"/> Resume or Curriculum Vitae |
| <input type="checkbox"/> Location Data (e.g., GPS) | <input type="checkbox"/> Nationality |
| <input type="checkbox"/> Employment Information | <input type="checkbox"/> Marital Status |
| <input type="checkbox"/> Mother's Maiden Name | <input type="checkbox"/> Children Information |
| Biometrics/Distinguishing Features/Characteristics | |
| <input type="checkbox"/> Fingerprints | <input type="checkbox"/> Height |
| <input type="checkbox"/> Retina/Iris Scans | <input type="checkbox"/> Voice/Audio Recording |
| <input type="checkbox"/> Hair Color | <input type="checkbox"/> Eye Color |
| <input type="checkbox"/> Video Recording | <input type="checkbox"/> Photos |
| <input type="checkbox"/> Weight | <input type="checkbox"/> Signatures |

2) What information relating to CFTC users of the system will be collected, maintained, used, and/or disseminated?

| | |
|---|---|
| Active Directory/Device Information | |
| <input type="checkbox"/> IP Address | <input type="checkbox"/> MAC Address |
| <input type="checkbox"/> CFTC Asset Number | <input type="checkbox"/> Device Identifiers or Serial Numbers |
| <input type="checkbox"/> User Name / Password | <input checked="" type="checkbox"/> Log data |

IV. COLLECTING INFORMATION

1) How is the information in this system collected?

DCOs submit daily Part 39 in XML format via SFTP to a location within the CFTC environment. The DEAP team within DOD is responsible for maintaining loading programs that populate data from the SFTP drop site into the SPARK database.

SPARK examines the following kinds of data:

- Contracts data: The contracts data is imported from ISS and may include contract market code, name, exchange, and ISS exchange commodity code.
 - Margin rate data for flagship and non-flagship contracts: Margin rates are set by the exchanges for each contract trading on the exchange. Flagship contracts are those that have been identified by CFTC as the largest on an exchange. The data includes margin rates for all flagship and non-flagship contracts and the beginning and end dates of the rates.
 - Top traders by contract data: The largest net long traders and the largest net short traders on the daily price report may include the trader, reporting firm, number of net long and net short contracts, owner ID, trader suffix, reporting firm ID, and account number by contract market.
 - Margin by trader data: The margin requirements for all large trader positions data may include trader, reporting firm, long and short option values, long and short future values, and initial total margin.
 - Hedge fund report and supporting data: Some of the hedge fund data comes from ISS.
 - Firm financial data: The firm financial data, imported from RSR, includes data required by 17 C.F.R. § 1.10(b) and may include excess net capital for futures commission merchants (FCMs) and FCM broker/dealers.
- 2) If any forms are used to collect information that resides in the system, please include the name of such form(s) and any applicable control number (i.e. issued by CFTC, OMB, etc.).

No forms are used to collect information that resides in the system other than those described for ISS.

V. INFORMATION USE

- 1) Will information in the system be retrieved using one or more of the data elements listed in Section III?

Yes, information in SPARK is retrieved using the account owner name, legal entity identifier (LEI), or similar unique identifier.

- 2) If the information in the system is retrieved using one or more of the identifiers, what CFTC System of Records Notice (SORN) covers the information?

Retrieval of information is covered by CFTC-15, *Enterprise Surveillance, Oversight & Risk Monitoring System*.

VI. ACCESS AND SHARING

- 1) With which internal CFTC Offices or Divisions is the information shared? For each Office or Division, what information is shared and for what purpose?

CFTC staff in DCR, DOD, Division of Market Oversight (DMO), Division of Enforcement (DOE), and Office of the Chief Economist (OCE) have access to the SPARK application and database. Each user must be 1) added to several Active Directory groups (including ISS) to open and access the application's menus, and 2) added to specific database user groups for permission to query the data.

- 2) How is the information shared internally?

Information in SPARK can be accessed through the client application or through direct database access via SQL and other database analysis tools. Information in SPARK cannot be edited via SQL.

- 3) With which external organization(s) is the information shared?

Information from SPARK is not shared externally as a regular matter of course. If DCR identifies positions that indicate a possibility of significant market risk, CFTC staff may contact DCOs, clearing members, or account holders to discuss risk mitigation strategies. Limited information from SPARK may be shared in that context, subject to applicable restrictions. To the extent the risk originated from a customer account, the clearing member and DCO would already have any personal information associated with that account.

- 4) How is the information shared externally?

Information from SPARK may be shared via email or orally in the context of discussions with DCOs, clearing members, or account holders.

VII. TRANSPARENCY

- 1) How are individuals notified as to how their information will be collected, used, and/or shared within this system?

If an account is owned by a trader that is also subject to the CFTC's Ownership and Control Rules which is subsequently stored in the ISS database and accessed via the SPARK application, they will have been provided with a Privacy Act statement when filing a Form 40 or Form 102. The form relating to Part 39 data is Form Derivatives Clearing Organizations (DCOs), which is completed by entities applying to become DCOs. They are instructed to describe how they will comply with their daily/monthly/periodic reporting requirements under Part 39.19 in Exhibit J. DCOs may be required to report individual account

information. Individuals are made aware of the disclosure in the Commission's regulations and the publication of this assessment provide further transparency and notice of the collection of the information.

- 2) Is a SORN required? If so, explain how the use of the information in this system is limited to the use specified in the SORN?

Yes. Information is only used for the purposes identified in CFTC-15, *Enterprise Surveillance, Oversight & Risk Monitoring System*.

VIII. INDIVIDUAL PARTICIPATION

- 1) Is the information collected directly from the individual?

No, information is collected from the relevant DCO.

- 2) Is the collection mandatory or voluntary? If voluntary, what opportunities do the individuals have to decline to provide information?

The submission of information relating to periodic position reporting is mandatory. Individuals do not have the opportunity to "opt out" of providing their information for inclusion in SPARK.

- 3) Do individuals have an opportunity to consent to a particular use of the information? If so, how do they provide consent for a particular use?

No, individuals do not have the opportunity to consent to a particular use of the information.

IX. DATA MINIMIZATION

- 1) What steps were taken to minimize the collection of PII in the system?

The reporting instructions to DCOs for Part 39 data specify the fields to be included in the XML file, and no further information is collected.

X. DATA QUALITY AND INTEGRITY

- 1) How is data quality ensured throughout the information lifecycle and business processes associated with the use of the information?

- Cross referencing data entries with other systems
- Third party data verification
- Data taken directly from individuals
- Character limits on text submissions
- Numerical restrictions in text boxes
- Other: Data validation checks

XI. RETENTION

1) What are the retention periods for the information?

Position data and ad hoc reports generated for one-time analysis are deleted when no longer needed.

Lists or rankings of entities and intermediaries whose positions may pose a risk to the markets or clearing firms are deleted after three years.

Data held to evaluate areas of risk and assess market impact, including risk review reports, benchmarking monthly margin reports, and other research or risk oversight records are deleted 10 years after the review or evaluation is completed.

XII. SECURITY

1) What types of administrative safeguards protect the information?

- Contingency Plan
- User manuals for the system
- Rules of Behavior
- Non-Disclosure or other contractual agreement
- Other:

2) What types of physical safeguards protect the information?

- Guards
- Identification Badges
- Biometric
- Cameras
- Physically secured space with need to know access
- Other: None

- 3) What types of technical safeguards protect the information?
- User Identification
 - Firewall
 - Virtual Private Network (VPN)
 - Multi-factor Authentication (MFA)
 - Passwords
 - Encryption
 - De-Identification
 - Anonymization
 - Other: An alert is generated if an unauthorized person attempts to open the application.
- 4) What monitoring, recording, and auditing safeguards are in place to prevent or detect unauthorized access or inappropriate use of the information?

Login, logout, menu selection, and query activity are logged.

- 5) Is this system hosted by a Cloud Service Provider (CSP)? No
- a. If yes, which one?
 - b. If yes, has the system obtained a FedRAMP Authorization?

XIII. TRAINING

- 1) What privacy training is provided to users of the system?

Annual privacy and cybersecurity training is mandatory for all CFTC staff.