Privacy Impact Assessment
for
TeamMate

05/12/21

System/Business Owner

Tony Carr

Reviewing Official
Charles Cutshall
Chief Privacy Officer

1. SYSTEM OVERVIEW

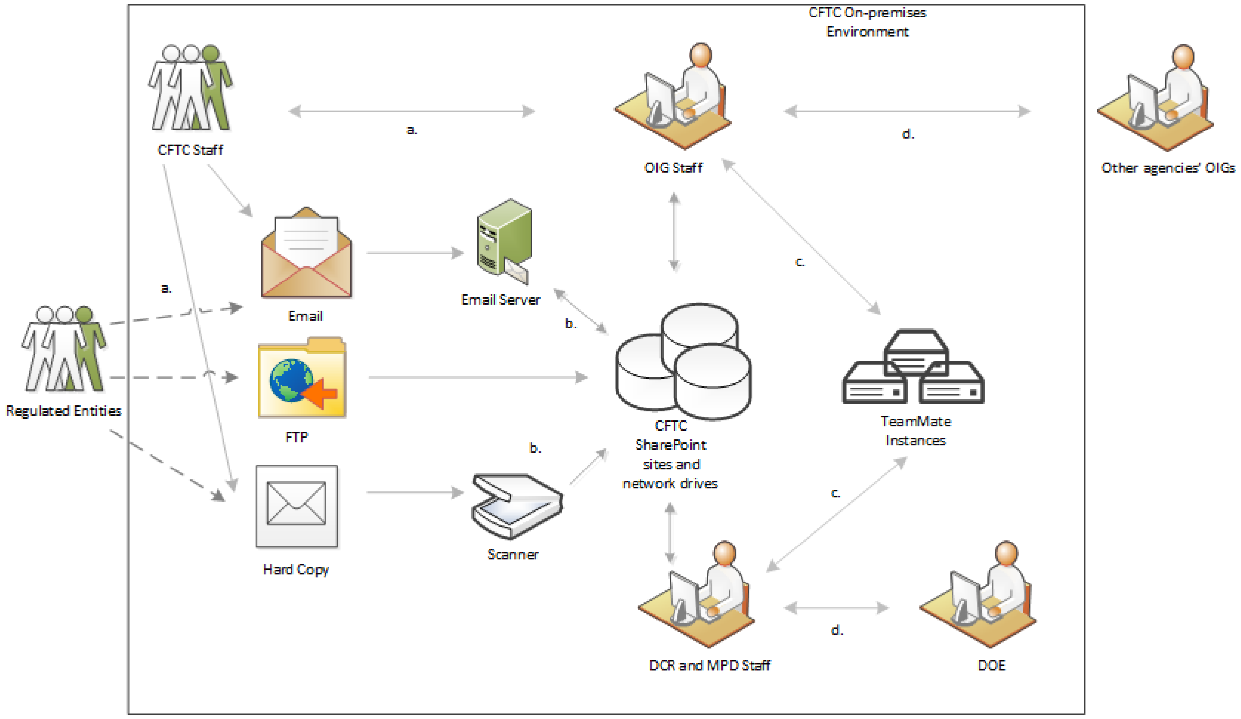
1) Describe the purpose of the system/collection:

   The TeamMate Electronic Work Papers (TeamMate) application is a commercial off-the-shelf audit management system used by the Office of the Inspector General (OIG), Division of Clearing and Risk (DCR), and Market Participants Division (MPD) to collect, store, and manage digital records relating to audits and other reviews within the scope of their respective missions. MPD and DCR process personal information relating to members of the public while conducting periodic audits of regulated entities, whereas OIG processes personal information of Commodity Futures Trading Commission ("CFTC" or "Commission") staff in the context of its oversight function.

   The sources and categories of personal information collected vary by audit, and are contained in notes, documents, spreadsheets, emails, and other documentation collected by the auditors. Users manually upload this documentation to TeamMate or add additional information in note fields within the application.

   TeamMate data is maintained on one server with individual instances installed on workstations. Workstation applications connect to the server via the General Support System. MPD, DCR, and OIG each have unique instances of TeamMate, and access to data residing in each instance is segregated. Access rights are determined by each instance's TeamMate Champion, an individual responsible for configuring and maintaining the application. Appendices 1-3 to this PIA contain additional information specific to each divisions' use of TeamMate.

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) Parties undergoing an audit or examination submit documentation to DCR, MPD, or OIG electronically or in hard copy. DCR and MPD may receive files from regulated entities via secure FTP, while OIG may access information directly from CFTC systems and staff.

b) Audit materials are stored in appropriate databases across the CFTC network.

c) TeamMate data is maintained on one server with individual instances installed on workstations. Workstations applications connect to the server via the General Support System. MPD, DCR, and OIG each have unique instances of TeamMate, and access to data residing in each instance is segregated. DCR, MPD, and OIG auditors upload copies of relevant documents to project files within their respective TeamMate instances and consult them as necessary to complete their examinations. DCR and MPD auditors can access all data within their respective instances, but may only modify project files for which they are responsible. OIG auditors can only access the project file for which they are responsible. Read and write privileges for individual audit files is determined by each instance's TeamMate Champion.

d) OIG may share information with other Federal agencies' OIGs in the context of peer reviews. DCR and MPD may share information with the Division of Enforcement (DOE) as appropriate.

2. 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 (for OIG)
☐ Other:

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: TeamMate links to CFTC's Windows Active Directory (AD) to ensure that only authorized personnel can access the specific project information or documents to which they are assigned. Access rights are determined solely by each instance's TeamMate Champion. Database administrators from the Division of Administration do not have access to information within TeamMate unless so granted by the TeamMate Champion(s).

4) What monitoring, recording, and auditing safeguards are in place to prevent or detect unauthorized access or inappropriate use of the information?

Logs are created recording the sign-in and sign-off times of TeamMate users. The Division of Administration has access to these logs and provides them to MPD, DCR, and OIG upon request.

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

Appendix No. 1: Office of the Inspector General

1. AUTHORITY AND PURPOSE

The Inspector General Act (5 U.S.C. Sections 6 and 8G(g)(1)) authorizes the collection of information by OIG. 13 CFR 101.302 identifies the scope of the Inspector General's authority. Additionally, OIG investigates any reports from Federal contractors of any violation of Federal criminal law involving fraud, conflict of interest, bribery, or a gratuity violation, or a violation of the civil False Claims Act. See Federal Acquisition Regulations (FAR) (73 Fed. Reg. 67064).

To obtain the necessary evidence, the Inspector General and his or her designees have the right to:

- Access all records, reports, audits, reviews, documents, papers, recommendations, and other materials available to CFTC and relating to CFTC's programs and operations;
- Require by subpoena the production of all information, documents, reports, answers, records, accounts, papers, and other data and documentary evidence;
- Administer oaths and affirmations or take affidavits; and,
- Request information or assistance from any Federal, state, or local government agency or unit.

2. INFORMATION TYPES

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

Note: Information in TeamMate is necessarily contextual and will depend on the nature of the audit. TeamMate may therefore contain data elements and information types that are not specifically identified below.

Identifying Numbers	
☐ Social Security Number	☒ Truncated or Partial Social Security Number
☐ Driver's License Number	☐ License Plate Number
☐ Patient ID Number	☒ File/Case ID Number
☐ Student ID Number	☐ Health Plan Beneficiary Number
☐ Passport Number	☐ Federal Student Aid Number
☒ Employee Identification Number	☐ Taxpayer Identification Number
☐ Professional License Number	☐ Legal Entity Identifier
☐ Credit/Debit Card Number	☐ National Futures Association ID
☐ Personal Bank Account Number	☐ Other ID if it can be traced back to an individual
☐ Personal Device Identifiers or Serial Numbers	

Contact Information	
☐ Personal Mobile Number	☒ Business Phone Number
☐ Personal E-mail Address	☒ Business E-mail Address
☐ Home Phone Number	☒ Business Mobile Number
☐ Home Mailing Address	☒ Business Mailing Address
Sole Proprietors	
☒ Business Taxpayer Identification Number	☒ Business Mailing Address
☐ Business Credit Card Number	☒ Business Phone or Fax Number
☐ Business Bank Account Number	☒ Business Mobile Numbers
☐ Business Device identifiers or Serial Numbers	☒ Business Email
Biographical Information	
☒ Name	☒ Gender
☒ Date of Birth	☐ City or County of Birth
☐ Country of Birth	☒ Zip Code
☐ Citizenship	☒ Military Service Information
☐ Spouse Information	☒ Academic Transcript
☐ Group/Org. Membership	☒ Resume or Curriculum Vitae
☒ Location Data (e.g., GPS)	☒ Nationality
☒ Employment Information	☐ Marital Status
☐ Mother's Maiden Name	☐ Children Information
Biometrics/Distinguishing Features/Characteristics	
☐ Fingerprints	☐ Height
☐ Retina/Iris Scans	☐ Voice/Audio Recording
☐ Hair Color	☐ Eye Color
☐ Video Recording	☐ Photos
☐ Weight	☐ Signatures

2) What information relating to TeamMate users will be collected, maintained, used, and/or disseminated?

Active Directory/Device Information	
☒ IP Address	☒ MAC Address
☒ CFTC Asset Number	☒ Device Identifiers or Serial Numbers
☒ User Name	☒ Log data

3. COLLECTING INFORMATION

1) How is the information in this system collected?

OIG auditors receive documents from audited entities by a variety of methods including email, direct database access, and in hard copy. Documents are saved in dedicated SharePoint sites, reviewed by auditors for relevance, and manually uploaded to the respective TeamMate database. Auditors may also enter additional information in note fields within the application or by using Microsoft Word and Excel integrations within TeamMate.

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 is subsequently maintained in TeamMate.

4. INFORMATION USE

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

   Information in TeamMate is organized into separate project folders for each audit. TeamMate does not have a search function that would allow a user to search and retrieve information across multiple project folders or within a single project folder. Project folders may be named according to the audit case number, which in turn is linked to the CFTC office, division, or individual being reviewed. It is also possible for individual document file names to include elements of personal information if so named by the document's author. Microsoft Word, Microsoft Excel, and PDF documents opened in TeamMate have normal search functionalities.

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

   Retrieval of information by OIG is covered by CFTC-32, *Office of the Inspector General Investigative Files* (exempted).

   Retrieval of information relating to CFTC users of TeamMate is covered by CFTC-35, *General Information Technology Records*.

5. INDIVIDUAL PARTICIPATION

1) Is the information collected directly from the individual?

   When the subject of the audit is an individual, some information may be collected directly.

   When the subject of the audit is a CFTC office or division, the information collected often relates to individuals other than the auditor's immediate point of contact, such as employees and contractors within that office or division.

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

The collection of information in the context of an audit conducted by OIG is mandatory. Individuals do not have the opportunity to "opt out" of providing their information for inclusion in TeamMate.

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.

6. 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?

   No other CFTC offices have access to data residing in the OIG instance of TeamMate. The conclusions of OIG audits may be shared with the CFTC division which was the subject of the audit, the Legal Division and the Office of the Chairman together with supporting artifacts in TeamMate.

2) Approximately how many users have access to the system?

   At any given time fewer than five OIG staff members have access to TeamMate. OIG's TeamMate Champion and team supervisor have access to all audit folders within TeamMate and are responsible for managing audit assignments. All other users only have access to the audit folders to which they are assigned.

3) How is the information shared internally?

   Information cannot be directly shared with internal stakeholders using TeamMate. If approved, information can only be exported from TeamMate and subsequently transferred electronically or in hard copy.

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

   The conclusions of OIG audits are sometimes made publicly available on the CFTC website, subject to redaction of information protected from release by law or statute. In addition, OIG periodically shares information in TeamMate with auditors from other Federal agencies' inspectors general in the context of peer reviews conducted in accordance with the Council of the Inspectors General on Integrity and Efficiency (CIGIE) *Guide for Conducting Peer Reviews of the Audit Organizations of Federal Offices of Inspector General*. OIG may also share information in TeamMate with members of the Council of Inspectors General on Financial Oversight Information. Finally, information may be shared externally pursuant to a Freedom of Information Act request, Congressional request, with other regulatory agencies, or law enforcement depending on the circumstances. Information may also be disclosed consistent with routine uses published in CFTC-32, *Office of the Inspector General Investigative Files* (exempted).

5) How is the information shared externally?

Information can only be exported from TeamMate and subsequently transferred electronically or in hard copy. OIG may also take additional measures to protect the confidentiality of information, such as by redacting sensitive information, clearly marking any unredacted information as "confidential," and by transferring electronic information in encrypted form.

7. TRANSPARENCY

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

OIG notifies the supervisor responsible for the CFTC unit, office, or division of the upcoming audit by letter or email. The supervisor may subsequently inform other CFTC staff within their unit at their own initiative.

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. OIG only uses information in TeamMate for the purposes identified in CFTC-32, *Office of the Inspector General Investigative Files* (exempted). Log data relating to CFTC users of TeamMate is only used for the purposes identified in CFTC-35, *General Information Technology Records*.

8. RETENTION

1) What are the retention periods for the information?

Audit case files are cut off at the end of the fiscal year in which the audit is completed. Records in historically significant audit case files are transferred in 5-year blocks to the National Archives 30 years after the cutoff date. All other audit case files are destroyed 10 years after the cutoff date.

9. TRAINING

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

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

10. DATA MINIMIZATION

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

   Audits may require the auditor to engage in multiple rounds of information requests and reviews. At each round, auditors are careful to narrow the requests so that only the information necessary to achieve its purpose is collected.

11. 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:

Appendix No. 2: Market Participants Division

1. AUTHORITY AND PURPOSE

MPD conducts financial and compliance monitoring and risk-based reviews pursuant to Commodity Exchange Act Sections 4b, 4d, and 4f, and CFTC regulations at 17 C.F.R 1.10, 1.12, 1.20-1.32., 22.2, and 30.7.

2. INFORMATION TYPES

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

Note: Information in TeamMate is necessarily contextual and will depend on the nature of the audit. TeamMate may therefore contain data elements and information types that are not specifically identified below.

Identifying Numbers	
☒ Social Security Number	☒ Truncated or Partial Social Security Number
☐ Driver's License Number	☐ License Plate Number
☐ Patient ID Number	☒ File/Case ID Number
☐ Student ID Number	☐ Health Plan Beneficiary Number
☐ Passport Number	☐ Federal Student Aid Number
☐ Employee Identification Number	☒ Taxpayer Identification Number
☐ Professional License Number	☒ Legal Entity Identifier
☐ Credit/Debit Card Number	☒ National Futures Association ID
☐ Personal Bank Account Number	☐ Other ID if it can be traced back to an individual
☐ Personal Device Identifiers or Serial Numbers	
Contact Information	
☐ Personal Mobile Number	☒ Business Phone Number
☐ Personal E-mail Address	☒ Business E-mail Address
☐ Home Phone Number	☒ Business Mobile Number
☐ Home Mailing Address	☒ Business Mailing Address
Sole Proprietors	
☒ Business Taxpayer Identification Number	☒ Business Mailing Address
☐ Business Credit Card Number	☒ Business Phone or Fax Number
☒ Business Bank Account Number	☒ Business Mobile Numbers
☐ Business Device identifiers or Serial Numbers	☒ Business Email
Biographical Information	
☒ Name	☒ Gender
☒ Date of Birth	☐ City or County of Birth
☐ Country of Birth	☒ Zip Code
☐ Citizenship	☒ Military Service Information

☒ Spouse Information	☐ Academic Transcript
☐ Group/Org. Membership	☒ Resume or Curriculum Vitae
☐ Location Data (e.g., GPS)	☐ Nationality
☒ Employment Information	☐ Marital Status
☐ Mother's Maiden Name	☐ Children Information
Biometrics/Distinguishing Features/Characteristics	
☐ Fingerprints	☐ Height
☐ Retina/Iris Scans	☐ Voice/Audio Recording
☐ Hair Color	☐ Eye Color
☐ Video Recording	☐ Photos
☐ Weight	☐ Signatures

2) What information relating to TeamMate users will be collected, maintained, used, and/or disseminated?

Active Directory/Device Information	
☐ IP Address	☐ MAC Address
☐ CFTC Asset Number	☐ Device Identifiers or Serial Numbers
☒ User Name	☒ Log data

3. COLLECTING INFORMATION

1) How is the information in this system collected?

MPD auditors receive documents from audited entities by a variety of methods including email, secure FTP transfer, and in hard copy. Documents are saved in dedicated SharePoint sites, reviewed by auditors for relevance, and manually uploaded to the respective TeamMate database. Auditors may also enter additional information in note fields within the application or by using Microsoft Word and Excel integrations within TeamMate.

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 is subsequently maintained in TeamMate.

4. INFORMATION USE

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

Information in TeamMate is organized into separate project folders for each audit. TeamMate does not have a search function which would allow a user to search and retrieve information across multiple project folders or within a single project folder. Project folders may be named according to the audit case number, which in turn is linked to the regulated entity being reviewed. It is also possible for individual document file names to include elements of personal information if so named by the document's author. Microsoft Word, Microsoft Excel, and PDF documents opened in TeamMate have normal search functionalities.

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

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

Retrieval of information relating to CFTC users of TeamMate is covered by CFTC-35, *General Information Technology Records*.

5. INDIVIDUAL PARTICIPATION

1) Is the information collected directly from the individual?

The information collected often relates to individuals other than the auditor's immediate point of contact within such organization, such as its officers, directors, and clients. To the extent the audit is related to an individual or sole proprietor, their information would be collected directly.

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

The collection of information in the context of an audit conducted by MPD is mandatory. Individuals do not have the opportunity to "opt out" of providing their information for inclusion in TeamMate.

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.

6. 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?

Information in TeamMate may be shared with DOE for use in civil or criminal prosecution of alleged violations of the Commodity Exchange Act and regulations thereunder.

2) Approximately how many users have access to the system?

At any given time approximately 40 MPD staff members have access to TeamMate. MPD users of TeamMate have "read only" privileges for all audit folders; auditors have "read and write" privileges for project folders for which they are responsible. The MPD TeamMate Champion is responsible for managing permissions and audit assignments.

3) How is the information shared internally?

Information cannot be directly shared with internal CFTC stakeholders using TeamMate. If approved, information can only be exported from TeamMate and subsequently transferred electronically or in hard copy.

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

Information in TeamMate may be disclosed externally pursuant to a Freedom of Information Act request, Congressional request, an approved request from another federal agency, or other legal demand. Information may also be disclosed consistent with routine uses published in CFTC-15, *Enterprise Surveillance, Oversight & Risk Management System*.

5) How is the information shared externally?

Information can only be exported from TeamMate and subsequently transferred electronically or in hard copy.

7. TRANSPARENCY

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

MPD notifies registered entities of an upcoming audit by email.

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. MPD only uses information in TeamMate for the purposes identified in CFTC-15, *Enterprise Surveillance, Oversight & Risk Management System*. Log data relating to CFTC users of TeamMate is only used for the purposes identified in CFTC-35, *General Information Technology Records*.

8. RETENTION

1) What are the retention periods for the information?

MPD examination files are cut off when the examination is completed, abandoned, or otherwise final. Documents received from registered entities or intermediaries to facilitate an examination of that entity or intermediary, final reports of examinations, copies of administrative actions, corrective plans, correspondence related to the final report or corrective plan, and, other related records are destroyed 10 years after the cutoff date. Staff working papers and supporting documents are destroyed 5 years after the cutoff date.

9. TRAINING

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

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

10. DATA MINIMIZATION

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

Audits may require the auditor to engage in multiple rounds of information requests and reviews. At each round, auditors are careful to narrow the requests so that only the information necessary to achieve its purpose is collected.

11. 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:

Appendix No. 3: Division of Clearing and Risk

1. AUTHORITY AND PURPOSE

DCR conducts its reviews pursuant to 17 C.F.R. §§ 1.73 and 23.609.

2. INFORMATION TYPES

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

Note: As of the publication date of this PIA, DCR is not using TeamMate for new examinations. DCR auditors may nevertheless use TeamMate to reference documents collected during previous examinations.

Information in TeamMate is necessarily contextual and will depend on the nature of the audit. TeamMate may therefore contain data elements and information types that are not specifically identified below.

Identifying Numbers	
☒ Social Security Number	☒ Truncated or Partial Social Security Number
☐ Driver's License Number	☐ License Plate Number
☐ Patient ID Number	☒ File/Case ID Number
☐ Student ID Number	☐ Health Plan Beneficiary Number
☐ Passport Number	☐ Federal Student Aid Number
☐ Employee Identification Number	☒ Taxpayer Identification Number
☐ Professional License Number	☒ Legal Entity Identifier
☐ Credit/Debit Card Number	☒ National Futures Association ID
☐ Personal Bank Account Number	☐ Other ID if it can be traced back to an individual
☐ Personal Device Identifiers or Serial Numbers	
Contact Information	
☐ Personal Mobile Number	☒ Business Phone Number
☐ Personal E-mail Address	☒ Business E-mail Address
☐ Home Phone Number	☒ Business Mobile Number
☐ Home Mailing Address	☒ Business Mailing Address
Sole Proprietors	
☒ Business Taxpayer Identification Number	☒ Business Mailing Address
☐ Business Credit Card Number	☒ Business Phone or Fax Number
☒ Business Bank Account Number	☒ Business Mobile Numbers
☐ Business Device identifiers or Serial Numbers	☒ Business Email
Biographical Information	
☒ Name	☒ Gender
☒ Date of Birth	☐ City or County of Birth

☐ Country of Birth	☒ Zip Code
☐ Citizenship	☒ Military Service Information
☒ Spouse Information	☐ Academic Transcript
☐ Group/Org. Membership	☒ Resume or Curriculum Vitae
☐ Location Data (e.g., GPS)	☐ Nationality
☒ Employment Information	☒ Marital Status
☐ Mother's Maiden Name	☐ Children Information
Biometrics/Distinguishing Features/Characteristics	
☐ Fingerprints	☐ Height
☐ Retina/Iris Scans	☐ Voice/Audio Recording
☐ Hair Color	☐ Eye Color
☐ Video Recording	☐ Photos
☐ Weight	☐ Signatures

2) What information relating to TeamMate users will be collected, maintained, used, and/or disseminated?

Active Directory/Device Information	
☐ IP Address	☐ MAC Address
☐ CFTC Asset Number	☐ Device Identifiers or Serial Numbers
☒ User Name	☒ Log data

3. COLLECTING INFORMATION

1) How is the information in this system collected?

DCR auditors receive documents from audited entities by a variety of methods including email, secure ad hoc FTP transfer, and in hard copy. Documents are saved in dedicated SharePoint sites, reviewed by auditors for relevance, and manually uploaded to the respective TeamMate database. Auditors may also enter additional information in note fields within the application or by using Microsoft Word and Excel integrations within TeamMate.

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 is subsequently maintained in TeamMate.

4. INFORMATION USE

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

Information in TeamMate is organized into separate project folders for each audit. TeamMate does not have a search function which would allow a user to search and retrieve information across multiple project folders or within a single project folder. Project folders may be named according to the audit case number, which in turn is linked to the regulated entity being reviewed. It is also possible for individual document file names to include elements of personal information if so named by the document's author. Microsoft Word, Microsoft Excel, and PDF documents opened in TeamMate have normal search functionalities.

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

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

   Retrieval of information relating to CFTC users of TeamMate is covered by CFTC-35, *General Information Technology Records*.

5. INDIVIDUAL PARTICIPATION

1) Is the information collected directly from the individual?

   The information collected often relates to individuals other than the auditor's immediate point of contact within such organization, such as its officers, directors, and clients. To the extent the audit is related to an individual or sole proprietor, their information would be collected directly.

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

   The collection of information in the context of an audit conducted by DCR is mandatory. Individuals do not have the opportunity to "opt out" of providing their information for inclusion in TeamMate.

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.

6. 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?

   Information in TeamMate may be shared with DOE for use in civil or criminal prosecution of alleged violations of the Commodity Exchange Act and regulations thereunder.

2) Approximately how many users have access to the system?

Approximately 15 DCR staff members have access to TeamMate. All DCR users of TeamMate have “read only” privileges for all audit folders; auditors have “read and write” privileges for project folders for which they are responsible. The DCR TeamMate Champion and associate directors have administrator privileges and manage access for other users.

3) How is the information shared internally?

Information cannot be directly shared with internal CFTC stakeholders using TeamMate. If approved, information can only be exported from TeamMate and subsequently transferred electronically or in hard copy.

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

Information in TeamMate may be disclosed externally pursuant to a Freedom of Information Act request, Congressional request, an approved request from another federal agency, or other legal demand. Information may also be disclosed consistent with routine uses published in CFTC-15, *Enterprise Surveillance, Oversight & Risk Management System*.

5) How is the information shared externally?

Information can only be exported from TeamMate and subsequently transferred electronically or in hard copy.

7. RETENTION

1) What are the retention periods for the information?

DCR examination files are cut off when the examination is completed, abandoned, or otherwise final. Final reports of examinations, copies of administrative actions, corrective plans, correspondence related to the final report or corrective plan, and, other related records are destroyed 10 years after the cutoff date. Documents received from registered entities or intermediaries to facilitate an examination of that entity or intermediary, staff working papers, and supporting documents are destroyed 5 years after the cutoff date.

8. TRAINING

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

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

9. DATA MINIMIZATION

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

   Audits may require the auditor to engage in multiple rounds of information requests and reviews. At each round, auditors are careful to narrow the requests so that only the information necessary to achieve its purpose is collected.

10. 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: