



**Privacy Impact Assessment
For
COVID-19 Symptom Screening
Qualtrics XM Directory**

March 2022

System/Business Owner

Dwight Riley
Chief Security Officer

Reviewing Official

Charles Cutshall
Chief Privacy Officer

I. What information will be collected?

General Information/File Types	
<input checked="" type="checkbox"/> Health Information	<input checked="" type="checkbox"/> System Development Information
Identifying Numbers	
<input checked="" type="checkbox"/> Employee Identification Number	
Contact Information	
<input checked="" type="checkbox"/> Personal Mobile Number	<input checked="" type="checkbox"/> Business Phone Number
<input checked="" type="checkbox"/> Personal E-mail Address	<input checked="" type="checkbox"/> Business E-mail Address
<input checked="" type="checkbox"/> City	<input checked="" type="checkbox"/> Department / Division
Biographical Information	
<input checked="" type="checkbox"/> Name	
Biometrics/Distinguishing Features/Characteristics	
<input checked="" type="checkbox"/> Signatures	
Medical/Emergency Information	
<input checked="" type="checkbox"/> Medical/Health Information	
Active Directory/Device Information	
<input checked="" type="checkbox"/> Given Name	<input checked="" type="checkbox"/> Surname
<input checked="" type="checkbox"/> Email Address	<input checked="" type="checkbox"/> Employee ID
<input checked="" type="checkbox"/> Name	<input checked="" type="checkbox"/> Telephone
<input checked="" type="checkbox"/> City	<input checked="" type="checkbox"/> Country
<input checked="" type="checkbox"/> Unique User Identifier	

II. Why is the information being collected?

The Commodity Futures Trading Commission (CFTC) is implementing processes and procedures to allow CFTC employees to safely access CFTC facilities in accordance with Federal guidelines for reopening government facilities during the COVID-19 public health crisis. The CFTC will use Qualtrics XM Directory to (1) distribute, via daily emails, terms and conditions for CFTC employees to respond to prior to reporting to work onsite, and to (2) collect and maintain the responses from CFTC employees.

The following CFTC privacy notices describe the purposes for which personally identifiable information is collected, used, maintained, and shared by the Qualtrics XM Directory information system:

- CFTC Privacy Impact Assessment, *Ensuring a Safe and Healthy Workplace in Response to COVID-19* (Oct. 14, 2020)
- CFTC-54, *Ensuring Workplace Health and Safety in Response to a Public Health Emergency* (85 FR 60981)

In addition, the distributed terms and conditions include a Privacy Act Statement that describes the purposes for which personally identifiable information is collected, used, maintained, and shared.

The following authorities permit the collection, use, maintenance, and sharing of personally identifiable information:

- General Duty Clause, Section 5(a)(1) of the Occupational Safety and Health Act of 1970 (29 U.S.C. § 654)
- Executive Order 14043, *Requiring Coronavirus Disease 2019 Vaccination for Federal Employees* (September 9, 2021)
- Executive Order 13991, *Protecting the Federal Workforce and Requiring Mask-Wearing* (Jan. 20, 2021)
- OMB Memorandum M-20-23, *Aligning Federal Agency Operations with the National Guidelines for Opening Up America Again* (Apr. 20, 2020)

III. What is the intended use of the information?

This information system collects and maintains information necessary to ensure a safe and healthy work environment in response to COVID-19. Symptom screening information stored in Qualtrics is collected directly from CFTC employees and is shared with officers and employees of the CFTC who have a need for the information in the performance of their official duties.

Information collected and maintained in the information system may be shared with the Chairman's Office and the Executive Director in order to maintain situational awareness and to coordinate the sharing of information in response to COVID-19. Information may also be shared with division directors and supervisors when staff become sick or are exposed to COVID-19.

The CFTC has established a Coronavirus Contact Tracing (CVCT) group to follow-up with staff who develop flu like symptoms (or who have any other reason to believe that they may have contracted SARS-CoV-2, the virus that causes COVID-19) after having visited a CFTC facility or interacted in-person with other CFTC staff outside the office for social or other reasons. The CVCT group is composed of staff from the Office of the Executive Director, the Security Emergency Management Unit, Logistics, and Workforce Relations. Information may be shared with staff from any of these offices when necessary to conduct contact tracing.

Information is collected and maintained in accordance with the Americans with Disabilities Act of 1990 and regulations and guidance published by the U.S. Occupational Safety and Health Administration, the U.S. Equal Employment Opportunity Commission, and the U.S. Centers for Disease Control and Prevention.

IV. With whom will the information be shared?

Personally identifiable information maintained in the information system is shared externally, but only when authorized and consistent with the disclosures and routine uses identified in the relevant Privacy Act of 1974 (Privacy Act) and applicable privacy notices. All disclosures not covered by a Privacy Act

exemption, or otherwise required by Executive Branch policy, are compatible with the purposes for which the information was collected.

Personally identifiable information maintained in the information system may be disclosed to:

- (a) To a Federal, State, or local agency to the extent necessary to comply with laws governing reporting of infectious disease;
- (b) To the CFTC staff member's emergency contact for purposes of locating a staff member during a public health emergency or to communicate that the CFTC staff member may have potentially been exposed to a virus as the result of a pandemic or epidemic while visiting a CFTC facility;
- (c) To another Federal agency, to a court, or a party in litigation before a court or in an administrative proceeding being conducted by a Federal agency when the Commission is a party to the judicial or administrative proceeding where the information is relevant and necessary to the proceeding;
- (d) To contractors, performing or working on a contract for the Commission when necessary to accomplish an agency function;
- (e) To the Department of Justice or in a proceeding before a court, adjudicative body, or other administrative body which the Commission is authorized to appear, when:
 - 1. The Commission; or
 - 2. Any employee of the Commission in his or her official capacity; or
 - 3. Any employee of the Commission in his or her official capacity where the Department of Justice or the Commission has agreed to represent the employee; or
 - 4. The United States, when the Commission determines that litigation is likely to affect the agency or any of its components;
- (f) Is a party to litigation or has an interest in such litigation, and the use of such records by the Department of Justice or the Commission is deemed by the agency to be relevant and necessary to the litigation;
- (g) To appropriate agencies, entities, and persons when (1) the Commission suspects or has confirmed that there has been a breach of the system of records, (2) the Commission has determined that as a result of the suspected or confirmed breach there is a risk of harm to individuals, the Commission (including its information systems, programs, and operations), the Federal Government, or national security; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the Commission's efforts to respond to the suspected or confirmed breach or to prevent, minimize, or remedy such harm; or,
- (h) To another Federal agency or Federal entity, when the Commission determines that information from this system of records is reasonably necessary to assist the recipient agency or entity in (1)

responding to a suspected or confirmed breach or (2) preventing, minimizing, or remedying the risk of harm to Individuals, the recipient agency or entity (including its information systems, programs, and operations), the Federal Government, or national security, resulting from a suspected or confirmed breach.

V. How is information in the information system secured?

Information maintained in this information system is protected from unauthorized access and improper use through administrative, technical, and physical security measures. Administrative safeguards include limiting access to the information maintained in the information system to authorized users and the regular review of security procedures and best practices to enhance security. Technical security safeguards include the 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; and, firewalls and intrusion detection applications. Physical safeguards include restrictions on building access to authorized individuals, 24-hour security guard service, and maintenance of records in lockable offices and filing cabinets.

VI. Are records maintained as part of a Privacy Act system of records?

Information processed in this information system is subject to the Privacy Act and is maintained as part of CFTC-54, *Ensuring Workplace Health and Safety in Response to a Public Health Emergency* (85 FR 60981). The SORN was published in the *Federal Register* on September 29, 2020.