Privacy Impact Assessment
for
IBM Facilities and Real Estate Management on Cloud (IBM TRIRIGA)

September 01, 2021

System/Business Owner
Cathy Wicykowski

Reviewing Official
Charles Cutshall
Chief Privacy Officer
Commodity Futures Trading Commission

I.   SYSTEM OVERVIEW

1) Describe the purpose of the system/collection:

The Computer-Aided Facilities Management (CAFM) System is utilized by the CFTC to oversee space management and move management. The CAFM system is primarily used to monitor building and workspace occupancy at its headquarters in Washington, DC and its three regional offices located in New York, Chicago, and Kansas City. Data that is captured for this purpose is also used to assist with strategic space decisions and the adaptation of space to create the most efficient floor plans from an organizational perspective. Space information is obtained from the Computer Aided Design (CAD) drawings for each location. Information about an individual located in a space is provided by the person's Business Management Specialist or the Contracting Officer's Representative (COR).

There will be approximately 50 users of the CAFM system, all part of the Division of Administration. Members of the Business Operations Branch (BOB) are the primary users of the system, with select members of the IT Branch also having access. The Business Management Specialists (BMS) provide the data associated with each new Federal employee while CORs provide the information for Contractors. The BMS also provides space assignments for the individuals. Whenever moves are to be made, the BMS provides the new location as well as any division or title changes. The BMS also enters any departing staff into the Employee Offboarding System. The system will be updated by two members of the Facility Operational Services Section of BOB and everyone else will have read-only access. The CAFM system maintains information for all active staff. Currently, there are approximately 700 Federal employees, 450 Contractors, 50 Interns, and 6 detailees on staff (collectively referred to as "staff"). Once the system is implemented, historical data will also be retained for all staff who depart from the CFTC.

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.
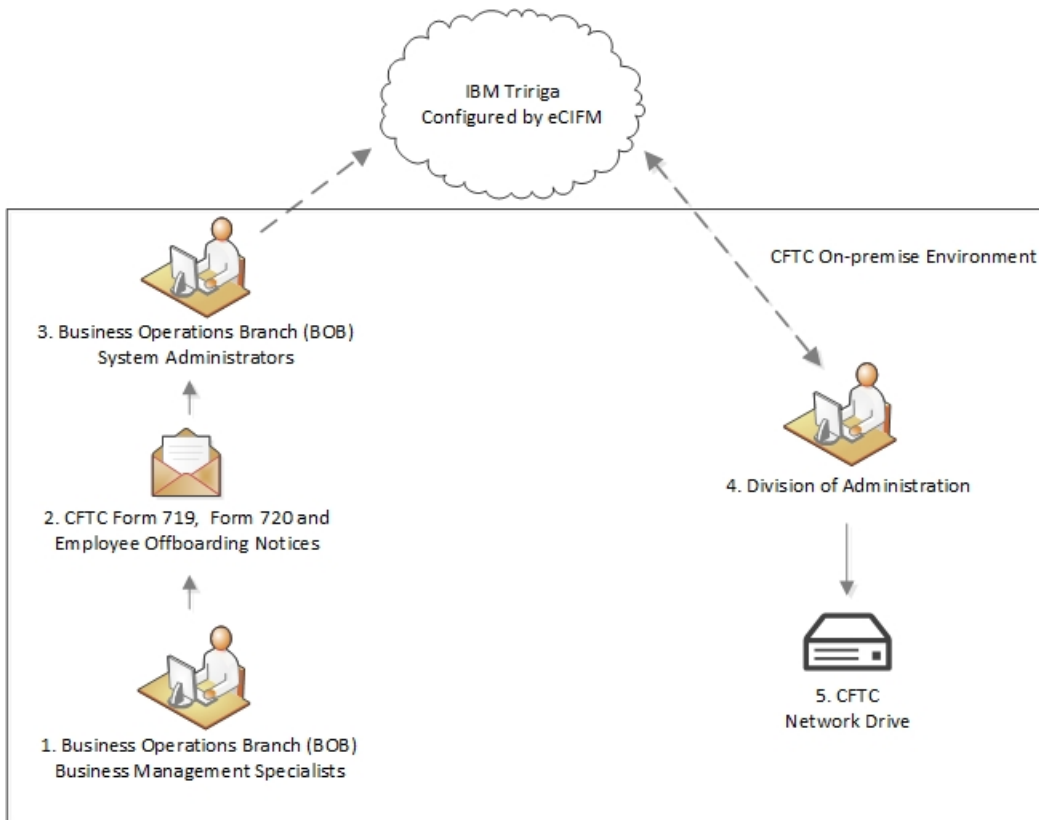
1. Business Management Specialists (BMS) provide the data associated with each new Federal staff member.
2. Staff information is received by system administrators via one of three ways:
   a. Onboarding staff information is received on CFTC Form 719: New Staff Requirements, distributed as a digital attachment to the SAC Notice issued by Security and Emergency Management.
   b. Changes to staff information are received on CFTC Form 720: Employee/Contractor Change, which is automatically generated by the Workforce Change Request System (WCR) and communicated via email.
   c. Staff offboarding notices are generated by the Offboarding System and are also received via email.
3. All data is manually entered into the cloud-based system by one of two system administrators. Information can be retrieved from the cloud-based system by entering the staff name or user ID into a search field.
4. The Division of Administration (DA) is the primary user of the system information in the form of floorplans that show staff name, division indicator, and space information. They may share this information with other division leadership when planning space for reorganizations, division moves, or other related space activity. DA will also create, update, and delete data in Tririga.
5. Information can be shared via email or in printed format, and is stored on the CFTC Network Drive.

II. AUTHORITY AND PURPOSE

1) What is the legal authority to collect, use, maintain, and share information in the system?

5 U.S.C. 6101-6133; 5 U.S.C. 6301-6326; 44 U.S.C. 3101.

III. INFORMATION TYPES

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

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	☐ Personal or Business Fax 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	

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 (e.g., division indicator)	☐ Resume or Curriculum Vitae
☐ Location Data (e.g., GPS)	☐ Nationality
☒ Employment Information (e.g., type, title, and what space they occupy)	☐ Marital Status
☐ Mother's Maiden Name	☐ Children Information

☐ Location Data (Building and office/workstation location)	☒ Employment Information (Type and Title, Special Needs / Handicapped, CPR/AED Responder, Floor Warden)
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 CFTC users of the system 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 / No Password	☐ Log data

IV. COLLECTING INFORMATION

1) How is the information in this system collected?

All data is manually entered into the system by one of two System Administrators using information received via one of three ways:

- Onboarding staff information is received on CFTC Form 719: New Staff Requirements, distributed as a digital attachment to the SAC Notice issued by Security and Emergency Management.
- Changes to staff information are received on CFTC Form 720: Employee/Contractor Change, which is automatically generated by the Workforce Change Request System (WCR) and communicated via email. On rare occasions, an exception to bypass the WCR System is necessary and Form 720 is manually completed, scanned, and emailed to required parties for processing.
- Staff offboarding notices are generated by the Offboarding System and are also received via email.

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.).

Form	Control No. *(If applicable)*	SORN(s) (Please list all that apply.)
CFTC Form 719: New Staff Requirements	N/A	Privacy Act statement not included.

CFTC Form 720: Employee/Contractor Change	N/A	Privacy Act statement not included.

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 will be retrieved from the system by entering the staff name or user ID into a search field. In addition, some staff information can also be retrieved by searching by building location and floor number.

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?

    CFTC-5 *Employee Personnel, Payroll, Time and Attendance*. Categories of records in the system include: records related to telework and requests for reasonable accommodation, business and personal contact information, and employee identification number.

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?

    The Division of Administration (DA) is the primary user of the system information in the form of floorplans that show staff name, division indicator, and space information. Other reports can be generated that would show staff name, staff type, title, and what space they occupy. DA may also share this information with other division leadership when planning space for reorganizations, division moves, or other related space activity.

2) How is the information shared internally?

    Information can be shared via email or in printed format. It is common to print the floorplans on a printer/plotter to get a larger, more readable printout for sharing.

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

    eCIFM Solutions, Inc.: Service provider of IBM Tririga software.

IBM: Cloud Service Provider for Tririga, hosted on a FedRAMP-compliant platform and using FedRAMP-compliant software.

4) How is the information shared externally?

The information can be accessed by the vendor(s) servicing our account via directly logging into the system or via transaction logs. The vendors have signed Non-Disclosure Agreements and any individuals with direct access to the system will have completed a background check and been issued a personnel identity verification (PIV) card by the CFTC. The CFTC may share the information with other entities, such as landlords and the U.S. General Services Administration (GSA), as the Commission explores new space.

VII. TRANSPARENCY

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

CFTC staff are notified of the collection and use of their information through this PIA.

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, CFTC-5 *Employee Personnel, Payroll, Time and Attendance System* is a collection of information concerning CFTC staff. This system contains certain personnel records not covered by government-wide system of records notices, including records related to requests for reasonable accommodation, name, and business contact information.

VIII. INDIVIDUAL PARTICIPATION

1) Is the information collected directly from the individual?

No. The Business Management Specialist completes the forms for Federal Employees and the contracting office representative (COR) handles all forms for Contractors.

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

Data collection is mandatory for an employee and/or contractor to onboard or offboard, as well as change offices during their employment.

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. The individual staff members do not see their onboarding form as it is filled out prior to when they come onboard. Likewise, they do not see any change request forms as the information is input directly into the Workforce Change Request System. Departing staff do get an offboarding notice from the system, but there is no opportunity for them to change any information.

IX. DATA MINIMIZATION

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

Approximately six years ago, the CFTC validated all data being collected and eliminated any PII that was unnecessary to successfully meet the objectives of using a CAFM system. In 2021, the same review took place as the CFTC prepared to build the new database.

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: Monthly physical audit of all space in all locations

XI. RETENTION

1) What are the retention periods for the information?

All allocated space including open space, space relegated to non-staff use and space occupied by staff; the records are maintained in accordance with GRS 5.4, 010, "Facility, space, vehicle, equipment, stock, and supply administrative and operational records." CFTC will retain these records for five (5) years.

Draft, preliminary, intermediate, working, and contract negotiation drawings of facility design, engineering, and construction records are maintained in accordance with GRS 5.4, item 050. CFTC will retain these records until superseded or until project terminates.

Final and as-built drawings, plans, and designs and all other documents of facility design, engineering, and construction records are maintained in accordance with GRS 5.4, item 051. CFTC will maintain these records until they are superseded, the facility is transferred to a new owner, or the structure is removed from Federal inventory.

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:
Please note: Since divisions within CFTC will print out Tririga data for floor planning purposes, access to that printed out information at CFTC requires a badge and a need to know.

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: Security Assertion Markup Language (SAML)

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

The system keeps track of all users who have logged in. Queries can be run to determine who logged in and when.

5) Is this system hosted by a Cloud Service Provider (CSP)? Yes
    a. If yes, which one? IBM Maximo and TRIRIGA on Cloud for US Federal Service
    b. If yes, has the system obtained a FedRAMP Authorization? Yes, FedRAMP Authorization was obtained on December 11, 2018.

XIII.   TRAINING

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

CFTC Annual Cybersecurity Awareness Training and CFTC Annual Privacy Awareness Training.