Privacy Impact Assessment
for

IBM Facilities and Real Estate Management on Cloud (IBM TRIRIGA)

June 2022

System/Business Owner

Cathy Wicykowski
Support Services Specialist, Business Operations Branch

Reviewing Official

Charles Cutshall
Chief Privacy Officer

I. What information will be collected?

Contact Information	
☒ Business E-mail Address	
Biographical Information	
☒ Name	☒ Group/Org. Membership
☒ Employment Information (e.g., type, title, and what space they occupy)	
Identify any *Biographical Information* is not included above:	
☒ Employment Information (Type and Title, Cardiopulmonary Resuscitation (CPR)/ Automated External Defibrillator (AED) Responder, Floor Warden)	
Active Directory/Device Information	
☒ User Name / No Password	

II. Why is the information being collected?

IBM Tririga (Tririga), a computer-aided facilities management solution, is used by the Commodity Futures Trading Commission (CFTC) to oversee space management and move management. Tririga 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.

The following CFTC privacy notice describes the purposes for which personally identifiable information (PII) is collected, used, maintained, and shared by the information system:

- CFTC-5, *Employee Personnel, Payroll, Time and Attendance* (81 FR 67327)

The following authorities permit the collection, use, maintenance, and sharing of PII:

- 7 U.S.C. including § 12 of the Commodity Exchange Act, at 7 U.S.C. 16, and the rules and regulations promulgated thereunder.
- 44 U.S.C. § 3101, *Records management by agency heads; general duties*.

III. What is the intended use of the information?

This system collects and maintains information necessary for an employee and/or a contractor to onboard or offboard, as well as change offices during their employment at the CFTC. Onboarding staff information is received on CFTC Form 719: New Staff Requirements, distributed as a digital attachment to the Special Agreement Check (SAC) Notice issued by the Security and Emergency Management Unit (SEMU). 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. Staff offboarding notices are generated by the Offboarding System and are also received via email.

All data is manually entered into the cloud-based system by one of two Division of Administration (DA) system administrators. These DA system administrators will also create, update, and delete data in Tririga.

IV. With whom will the information be shared?

PII maintained in the information system may be disclosed:

a) To contractors, grantees, volunteers, experts, students, and others performing or working on a contract, service, grant, cooperative agreement, or job for the Federal government when necessary to accomplish an agency function.

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.

V. How is information in the information system secured?

Records are protected from unauthorized access and improper use through administrative, technical, and physical security measures. Administrative measures include regular review of security procedures and best practices to enhance security, and placing restrictions on computer access to authorized individuals who have a legitimate need to now the information. Technical measures within CFTC 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 measures 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-5, *Employee Personnel, Payroll, Time and Attendance* (81 FR 67327). The SORN was last published in the Federal Register on September 30, 2016.