Privacy Impact Assessment
For

Azure General Support System

April 2022

System/Business Owner

Lamar Dunn

Reviewing Official

Charles Cutshall
Chief Privacy Officer

I. What information will be collected?

General Information/File Types	
☒ Security Management Information	☒ Personal Identity & Authentication Information
Contact Information	
☒ Business E-mail Address	☒ Business Phone Number
Biographical Information	
☒ Name	
Biometrics/Distinguishing Features/Characteristics	
☒ Signatures	
Active Directory/Device Information	
☒ IP Address	☒ Log data
☒ User Name / Password	

II. Why is the information being collected?

In support of the CFTC's mission and in response to the continued growth in demand for data storage and processing, the Commodity Futures Trading Commission ("CFTC" or "Commission") is implementing a hybrid, multi-cloud strategy that will minimize the Commission's on-premises footprint while augmenting its use of secure, third-party Infrastructure as a Service (IaaS) and Platform as a Service (PaaS) solutions.

This assessment covers the CFTC's use of Azure General Support System (GSS) as an IaaS solution. More specifically, the assessment focuses on Azure Active Directory (Azure AD), Azure Sentinel, and Privileged Identity Manager (PIM), all Azure GSS IaaS components that process personally identifiable information (PII). Notably, this assessment does not cover the CFTC's use of Azure GSS as a PaaS solution. Applications and services offered through the Azure GSS PaaS are considered subsystems and are assessed separately. Details on the specific purposes for which PII is collected, used, maintained, and shared by each PaaS application and service are described in privacy notices associated with each of those subsystems and are documented in the respective assessment findings (e.g., privacy impact assessment).

III. What is the intended use of the information?

Azure Active Directory (Azure AD) processes Personal Identity & Authentication Information. Azure AD uses a structured data store as the basis for a logical, hierarchical organization of directory information. The database (or directory) contains critical information about CFTC's environment, including the users and computers operating on the network. For example, Azure AD centrally manages all CFTC identities and access to all CFTC applications and its enterprise identity service provides single sign-on, multifactor authentication.

Azure Sentinel processes Security Management Information as a scalable, cloud-native, security information and event management (SIEM) and security orchestration, automation, and response (SOAR) solution. Azure Sentinel provides a single solution for attack detection, threat visibility, proactive hunting,

and threat response. The intended use of the information is to collect, index, and search log files from across the CFTC network. It will generate automated alerts based upon events within various indexed datasets; allow automated and ad hoc searching of CFTC log files; and create greater visibility into the day-to-day security condition of the CFTC network.

Privileged Identity Manager (PIM) processes Personal Identity & Authentication Information that enables the CFTC to manage, control, and monitor access to important information resources in the Commission. These resources include Azure AD and other Microsoft Online Services such as Microsoft 365 and Microsoft Intune. PIM is the backend tool that CFTC users use when logging into Azure. The intended use of the information is to specify the privilege level for the users logging into the Azure Portal.

IV. With whom will the information be shared?

PII maintained in the information system is shared internally for the purpose of detecting, correlating, and responding to use limitation potential malicious activity on CFTC information technology (IT) devices, networks, and systems.

PII maintained in the information system is shared externally, but only when authorized and consistent with the disclosures and routine uses identified in the 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, were reviewed by the CFTC privacy program and are compatible with the purposes for which the information was collected.

Records processed by the information system are maintained as part of CFTC Privacy Act system of records CFTC-33, *Electronic Access Card* (76 FR 5973) and CFTC-35, *General Information Technology Records* (81 FR 67327). The applicable routine uses for records maintained as part of CFTC-33, *Electronic Access Card* (76 FR 5973) include:

- Information contained in this system may be disclosed to any person for their use of maintenance or service of data processing systems.

In addition, records maintained in CFTC-33 and CFTC-35 may be disclosed in accordance with the following blanket routine uses (76 FR 5973):

- At the discretion of the Commission staff, information may be given or shown to anyone during the course of a Commission investigation if the staff has reason to believe that the person to whom it is disclosed may have further information about the matters discussed therein, and those matters appear relevant to the subject of the investigation.

- Where information, either alone or in conjunction with other information indicates a violation or potential violation of law—criminal, civil, or regulatory in nature—the relevant information may be disclosed to the appropriate Federal, State, local, territorial, Tribal, or foreign law enforcement authority or other appropriate entity charged with the responsibility for investigating or prosecuting such violation or charged with enforcing or implementing such law.

- Information may be disclosed 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.

- Information may be disclosed to appropriate agencies, entities, and individuals when:
    - The Commission suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised;
    - The Commission has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, identity theft or fraud, or harm to the security or integrity of this system or other systems or programs (whether maintained by the Commission or another agency or entity) that rely upon the compromised information; and
    - The disclosure made to such agencies, entities, and individuals is reasonably necessary to assist in connection with the Commission's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.

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 safeguards include restrictions on computer access to authorized individuals who have a legitimate need to know the information as well as regular reviews of security procedures and best practices to enhance security. Technical 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 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-33 and CFTC-35.

CFTC-33, *Electronic Access Card* (76 FR 5973): This system includes records showing the name of the assigned CFTC user, electronic access card number, access level, and status. It also includes card activity information, including time and location of use by card holder.

CFTC-35, *General Information Technology Records* (81 FR 67327): This system includes certain records that CFTC computer systems routinely compile and maintain about users of those systems to enable the information technology network to operate and function effectively, reliably, and securely, including but not limited to: network user information, network activity information including activity logs, audit trails, identification of devices used to access CFTC systems, Internet sites visited, and information input into sites visited.