Privacy Impact Assessment
for
Amazon Web Services General Shared Services (AWS GSS)

August 2025

Point of Contact
Dulles Chang
Division of Administration

Reviewing Official
Kellie Cosgrove Riley
Chief Privacy Officer

OVERVIEW

The CFTC's Amazon Web Services General Shared Services (AWS GSS) is a platform as a service (PaaS) in a Virtual Private Cloud (VPC) within the CFTC's AWS cloud tenancy. AWS GSS provides shared services across the three other CFTC ATO portfolios in VPCs within that AWS cloud tenancy: Order Book on Demand/Market Financial Data Cloud (OBOD/MFDC), Portal, and Business Information Systems (BIS).

While there are numerous tools, or shared services, available from AWS GSS, this Privacy Impact Assessment addresses the CFTC's use of the following two shared services, which involve the collection and use of personally identifiable information (PII) about CFTC employees and contractors:

- AWS Directory Service, which manages a replicated version of the CFTC's Active Directory (AD), which allows the CFTC to leverage a broad range of other applications in CFTC's AWS cloud tenancy; and
- AWS Identity & Access Management (IAM) Center, which allows Single Sign-On (SSO) by supporting automatic provisioning (synchronization) of CFTC users and groups.

The Division of Administration – Information Technology (DA-IT) manages the backend AWS infrastructure based on service requirements and the requirements provided by other CFTC Divisions, as well as the AD information that is collected and maintained in AWS GSS to control and facilitate access. The CFTC maintains full control of agency content that is uploaded to AWS GSS and the information about CFTC employees and contractors is only used to enable access to the CFTC infrastructure and provide access to other CFTC services that may be hosted within the CFTC's AWS cloud tenancy.

Besides appropriately cleared CFTC contractors, who have access to AWS GSS and its IT log information in order to troubleshoot incidents that impact the CFTC network infrastructure pursuant to a contract between those vendors and CFTC, no outside persons or entities generally have access to this information system. Role Based Access Controls (RABC) are in place to prevent unauthorized access to the centralized authentication and authorization service.

1. AUTHORITIES AND OTHER REQUIREMENTS

1.1 What legal authority(ies) permit or require the CFTC to collect, use, maintain, or disseminate the information in the system, project, or program?

The Commodity Exchange Act, 7 U.S.C. 1, et seq. (CEA), and the rules and regulations promulgated thereunder authorizes the creation and function of

the CFTC, including the means to operate the Agency in order to achieve its stated mission. AWS GSS is a significant component of CFTC's infrastructure, and forms part of the foundation on which CFTC operates.

1.2 Is there a Privacy Act System of Records Notice(s) (SORN(s)) that applies to the information in the system, project, or program? If yes, please identify it. If no, please explain why not.

Yes. CFTC-35, General Information Technology Records applies to the records in this system. The CFTC's SORNs are available at CFTC.gov/privacy.

1.3 Please identify the applicable accreditation boundary evaluated during the Authority to Operate (ATO) process. If the system, or involved project or program, is hosted by a Cloud Service Provider (CSP), please identify the CSP and state whether the system has Federal Risk and Authorization Management Program (FedRAMP) authorization.

The applicable accreditation boundary is Amazon Web Services General Shared Services, for which an ATO was issued on July 2, 2024, and which was placed into continuous monitoring. Amazon Web Services is a FedRAMP authorized cloud service provider.

1.4 Is there a records retention schedule(s) approved by the National Archives and Records Administration (NARA) that governs the retention of the records maintained in the system, project, or program? If yes, please identify the schedule. If not, please explain.

Yes, the records in AWS GSS are "System Access Records" and are subject to GRS 3.2.030 System access records - Systems not Requiring Special Accountability for Access, and subject to Disposition Authority, DAA-GRS-2013-0006-0003.

1.5 Please list all forms or other information collection instruments that are used to collect the information in the system. If the information collected is subject to the Paperwork Reduction Act, provide the name of the form or information collection and the applicable OMB control number.

CFTC Form 719 is completed by the supervisor of a new employee or the Contracting Officer's Representative (COR) for a new contractor The Paperwork Reduction Act (PRA) does not apply to this collection.

2. INFORMATION

2.1 Identify the information that the system, project, or program collects, maintains, uses, or disseminates.

AWS GSS collects, maintains, uses, and/or disseminates the following information about CFTC employees and contractors: name; username and password; business phone number, email address, fax number, and mailing address; and internet protocol (IP) address, medium access control (MAC) address, log data, and other device identifiers or serial numbers.

2.2 Is the information collected directly from the individual and, if not, what are the sources of information collected. How is the information obtained?

The information in AWS GSS is not collected directly from individuals. It is obtained from the CFTC's Active Directory, which is populated when supervisors of new employees and the CORs for new contractors complete CFTC Form 719 and provide it to the Helpdesk to manually create the CFTC user's AD account in CFTC's on-premises environment. That AD account is then synced with other CFTC instances of AD, including in AWS GSS.. In addition, device identifiers are collected via replication from CFTC Enterprise Domain Controllers.

2.3 What steps are taken to minimize the collection of information in the system, project, or program?

The data elements and quantity of PII collected by AWS GSS is dictated by the minimum data needed to provide CFTC personnel connectivity to the CFTC infrastructure and access to other CFTC services that may be hosted within AWS GSS and to maintain proper security over the CFTC network and CFTC data therein.

2.4 Discuss how the accuracy, integrity, and/or quality of the information identified above are determined.

AWS GSS does not determine the accuracy, integrity, or quality of the PII it collects. If a user needs to update their business contact information stored in this information system, a ServiceNow ticket may be opened with the user's request and tracked within CFTC's IT Service Management Platform. Device identifiers, which are captured automatically and are based on the user's location and assigned system and device, cannot be changed.

In the event that any changes are made to AD information, those changes are automatically replicated across all three of CFTC instances of AD, which includes the AWS GSS VPC.

2.5 Privacy Impact Analysis: Related to the Collection and Characterization of the Information

AWS GSS collects all PII data elements from CFTC's Active Directory. All data elements within Active Directory are collected, in the case of a user's business contact information, from CFTC Form 719, which is completed by the assigned supervisor for the new employee and by the COR for the new contractor, who have an interest in providing accurate information. Device identifiers are collected directly from the CFTC device(s) associated with the employee or contractor and there is little to no possibility that they will be inaccurate. Overall, there is low risk that the information collected by AWS GSS will be inaccurate or unreliable. If that risk is realized, an employee or contractor would likely not be allowed to access the CFTC network or any assets therein, as the user could not be authenticated via SSO, which relies on Active Directory. That risk is readily mitigated by the affected user creating a ServiceNow ticket to initiate the process to change or update their PII in AWS GSS.

3. USE OF THE INFORMATION

3.1 Describe how the information is used internally at the CFTC to support a business purpose.

The information in AWS GSS is used to allow CFTC employees and contractors to access the other VPCs in the CFTC's AWS cloud tenancy in a secure manner.

AWS GSS also supports the operation of the other three CFTC systems in that same cloud environment, MFDC/OBOD, BIS, and Portal, with one or more of the AWS shared services. As one or more of those three CFTC systems need one or more AWS shared services, that system will automatically communicate with AWS GSS, which will then deploy the requested shared services to the other system or systems.

3.2 Identify all programs or offices, and an approximate number of individuals, within the CFTC that have assigned roles and responsibilities with respect to the system, project, or program or with whom information is shared. Explain how each uses the information.

AWS GSS is accessible to the CFTC Customer Support Center and to DA-IT to ensure CFTC users are properly authenticated via SSO for access to CFTC network and assets. In addition, CFTC enterprise security operations center (eSOC) may access AWS GSS when investigating a potential incident or breach.

3.3 Privacy Impact Analysis: Related to the Internal Access and Use

Those in CFTC Customer Support Center and eSOC with defined access to AWS GSS PII have an official need for that access.

While there may be a low risk that individuals who are not authorized to access AWS GSS will gain access, AWS GSS has been configured such that only those with an official need to know that AWS GSS data have access. All access requests and related decisions are sent to the end user's manager for acceptance or denial. Role Based Access Controls are used to limit access to data required by users to perform their duties.

4. INFORMATION SHARING

4.1 Is the information shared outside of the CFTC as part of usual agency operations? If so, identify the organizations or individuals with whom the information is shared, how and *why* it is shared, and how it is to be used.

Information in the system is shared with contractors working onsite at the CFTC and may be shared with external IT providers when troubleshooting incidents that are impacting the CFTC network infrastructure. Information in the system may also be shared with outside agencies, such as the Cybersecurity and Infrastructure Security Agency (CISA) in the event of an incident or breach.

4.2 How is the information sharing described in 4.1 compatible with the purpose for which it was originally collected described in 3.1?

The external sharing described above, to the extent needed, is consistent with the purpose stated in Section 3.1 and with the "Purpose" statement in the applicable SORN, as it is required for maintaining the functional operation and the security of the CFTC network. This external sharing is permitted by various routine uses set forth in CFTC-35 and in the CFTC's Blanket Routine Uses.

4.3 Is the information sharing documented in a Memorandum of Understanding, other information sharing agreement, or a contract?

CFTC contractors may access CFTC PII in AWS GSS pursuant to a contract with CFTC. For example, the current contact requires contractors to manage activities including, but not limited to, configuring, updating, and maintaining Identity and Access Management (IAM) roles, security groups, applicable Active Directory (AD) and local accounts, which would enable contractors to access PII in CFTC AD accounts.

4.4 Are there limitations on re-dissemination of the information by the third party in place, either in the documents identified in 4.2 or otherwise?

The current contract includes the following provisions:

- Section 2.3.2, Clauses Incorporated by Full Text, which includes the FAR Clause 52-224.1 Privacy Act Notification and accordingly incorporates Privacy Act restrictions on dissemination of PII;
- Section 2.12.4 Intrusion Detection and Prevention, which provides that the contractor shall comply with all contractual and Federal information security and privacy requirements applicable to the operation, maintenance or support of the CFTC information system; and
- Section 7 Nondisclosure Agreement (NDA), requires all contractors providing services in support of the contract to sign the NDA provided, which requires, e.g., compliance with the Privacy Act as well as with CFTC policies, procedures and guidelines related to information security and privacy, including but not limited to Safeguarding Personally Identifiable Information and the IT Rules of Behavior.

4.5 Describe how the system, project, or program accounts for and maintains a record of disclosures outside of the CFTC.

Information, including PII, retained by AWS GSS is generally shared internally to those employees and contractors with a need-to-know, pursuant to 5 U.S.C. 552a(b)(1), which is an exception to the accounting of disclosures requirement. For those other instances where AWS GSS PII is shared to external persons or entities, as described in the routine uses identified in SORN CFTC-35, a process has been constructed to comply with the Privacy Act requirement for retaining an accounting of disclosures, whereby for any instance of required disclosure of PII from AWS GSS to any external person, agency, or entity, CFTC will transcribe on a dedicated spreadsheet the date, nature, and purpose for sharing the PII and the name and address of the external person, agency, or other entity to whom the PII will be/is disclosed.

4.6 Privacy Impact Analysis: Related to Information Sharing

All external transfer or sharing of AWS GSS PII is identified and covered by a routine use published in CFTC-35, General Information Technology Records or CFTC's blanket routine uses published at 76 FR 5974.

Because AWS GSS PII is limited to business contact information and CFTC-issued device information, there is low risk of any overcollection or oversharing of this data by external parties. Business contact information is insufficient to steal CTC users' identities or to replicate their access credentials. In theory, some of the business contact information could be changed – as noted above, device identifiers cannot be changed, erased, or

otherwise altered – possibly affecting a CFTC user's ability to be authenticated for purposes of access to the CFTC network or asset therein. In such an event, however, the CFTC user would quickly learn of impaired access and initiate a ServiceNow ticket to correct any inaccurate information in Active Directory.

5. DATA RETENTION

5.1 Explain how long and for what reason the information is retained.

All information collected by AWS GSS, including user information and log-related activity, is stored during a user's engagement with CFTC and for an additional 30 days after that engagement concludes. At that time, the business use for that information generally ceases and the information is subject to destruction or other disposition. As noted above, the information retained is required for CFTC users to access the network and CFTC assets therein, as well as to monitor and ensure the secure operation of the CFTC network. This retention is consistent with the applicable retention schedule identified in Section 1.4.

5.2 Describe how the information is disposed of at the end of its retention period.

When a CFTC user's engagement is ended, that user's Active Directory account will be deleted 30 days thereafter. However, if a business use for PII persists, that information may be retained beyond the initial 30 days after expiration of the retention period. Only a portion of AWS GSS log data is overwritten at a given time, with the oldest data being deleted first.

5.3 Privacy Impact Analysis: Related to Retention

AWS GSS maintains all records in accordance with the above-referenced retention schedule.

The risk associated with excessive retention beyond the period dictated by applicable retention authorities is low. In general, a CFTC user's PII in AWS GSS is only relevant during the period of that user's engagement with CFTC and an additional 30 days thereafter. To the extent a user's data is retained for a longer period without an official business justification, that data cannot be used to steal the user's identity and any effect on that user's ability to authenticate for purposes of accessing CFTC network or related assets is moot because that user is no longer engaged by CFTC.

6. NOTICE

6.1 How are individuals provided notice prior to the collection of their information? If they are not provided notice, please explain why.

No PII in AWS GSS is collected directly from individuals. AWS GSS collects all PII via Active Directory and therefore there is no direct notice provided to CFTC users about the collection of their data. CFTC users instead receive indirect notice of the collection of their data via the SORN applicable to AWS GSS, which is CFTC-35, General Information Technology Records.

6.2 Do individuals have the opportunity to consent to the use of their information or decline to provide their information? Please explain.

CFTC users do not have the opportunity to consent to the collection or any particular use of their PII by AWS GSS because no PII is directly collected by AWS GSS from CFTC users. In any event, the collection of that PII is a requirement of initiating and continuing engagement with CFTC, whether as employee, contractor, or other personnel.

6.3 Privacy Impact Analysis: Related to Notice

CFTC users receive notice of the collection of their data via CFTC-35, General Information Technology Records, which mitigates the risk associated with notice but does not completely remove that risk, since much of the PII collected by AWS GSS originates from Active Directory and is not directly collected from individuals. Individuals do not have the opportunity to consent or object to any particular use of their PII. Individuals' PII collected by AWS GSS, which PII consists entirely of CFTC employment related information and CFTC-issued device identifiers, is used only for providing access to and monitoring user's activity in the CFTC network. Accordingly, the risk associated with notice, although technically not actionable due to the mandatory nature of the collection, appears to be low.

7. REDRESS

7.1 What procedures are in place that allow individuals to access their information?

Because AWS GSS does not collect PII directly from any individuals but through other systems and there is no direct interface for non-administrative users, there are no procedures in place to allow individuals to directly access their information within AWS GSS. However, all CFTC personnel can access their business contact information as stored in the Global Address Book, which is part of Microsoft Outlook, and the information in the Global Address Book is constantly synchronized with the data in all three of CFTC's instances of Active Directory, including that instance of AD data in AWS GSS. CFTC

personnel cannot delete or make any changes to their data within the Global Address Book.

In addition, a Privacy Act request can be made by individuals to gain access to their data held by this information system, pursuant to the directions provided in 17 C.F.R. § 146.3 - Requests by an individual for information or access, as stated in CFTC-35, General Information Technology Records (81 FR 67327) (September 30, 2016).

7.2 What procedures are in place to allow individuals to correct/amend inaccurate or irrelevant information about themselves?

CFTC users can submit a ServiceNow ticket and work with the HelpDesk to obtain any corrections, amendments, or other update to their business contact information in AWS GSS. As noted above, users cannot make any changes to any device identifiers, which are collected directly from the user's CFTC issued equipment. In addition, a Privacy Act request can be made by individuals to correct or amend their data held by this information system, pursuant to the directions provided in 17 C.F.R. § 146.8 – Amendment of a record, as stated in CFTC-35, General Information Technology Records (81 FR 67327) (September 30, 2016).

7.3 How are individuals notified about the procedures for correcting/amending their information?

When a CFTC user begins engagement with CFTC, whether as employee, contractor, or other personnel, they are informed during onboarding how to request changes to their information via a ServiceNow ticket. As provided in SORN CFTC-35, General Information Technology Records, individuals whose PII is collected by AWS GSS, i.e., CFTC employees, contractors, and other personnel, can contact the Office of General Counsel for CFTC to seek an amendment or correction of their PII and must comply with the requirements identified in 17 CFR § 146.8 for such requests to be considered.

7.4 Privacy Impact Analysis: Related to Redress

CFTC personnel do not have access to their own PII in AWS GSS, as identified in response to Question 7.2. During onboarding, all CFTC personnel receive instruction on how to complete a ServiceNow ticket to, e.g., correct any inaccurate or out-of-date information in their AWS GSS profile, in addition to the Privacy Act procedures for amending or correcting PII described in response to question 7.3. Accordingly, individuals' risk of not having the opportunity to learn and seek correction or amendment of their PII is low.

8. AUDITING AND ACCOUNTABILITY

8.1 How is the information in the system secured?

Information security is secured with multiple layers of security including the following:

- Physical controls include onsite guards and ID badges; and
- Administrative controls include access control lists and non-disclosure agreements (NDAs) for vendors and contractors; and
- Technical controls include multifactor authentication (MFA), Federal Risk and Authorization Management Program (FedRAMP) certified data centers, firewalls, and encryption.

CFTC's continuous monitoring program includes AWS GSS.

8.2 Are audit logs generated reflecting access and use of the information in the system? If not, please explain. If so, please describe how often they are reviewed and for what purpose.

AWS GSS includes AWS CloudTrail and AWS VPCFlowLogs as general services that create log data specific to AWS GSS. AWS CloudTrail records and audits AWS user activity including but not limited to application program interface (API) calls, console sign-ins, and service events. AWS VPCFlowLogs records and audits internet protocol (IP) traffic and network connections within the AWS GSS VPC environment. AWS CloudTrail logs include the following PII: IP addresses, identified as the "SourceIPAddress"; and CFTC email addresses, which are included within the larger "UserIdentityPrincipalid" data element; and the UserIdentityPrincipalid data element, which is assigned to the specific individual to which the email address applies. AWS VPCFlowLogs logs include IP addresses, identified as "SrcAddr" and "DstAddr". While those logs indicate what data sources are accessed, they do not indicate how AWS GSS data is used. Those two sets of logs collect data and send it in real time to Sentinel. There is no review of those AWS GSS logs before they are sent to Sentinel. CFTC's Enterprise Security Operations Center (eSOC) reviews Sentinel log data related to alerts received by eSOC and to alerts triggered by the source from which data in the logs are gathered. If any audit logs note suspicious activity, eSOC will follow the CFTC internal playbook guidelines, which are based on the type of event, e.g., malware or unauthorized access, and if meeting the relevant criteria, will report the event to the Cybersecurity and Infrastructure Security Agency (CISA).

8.3. What procedures are in place to determine who has access to the system, and are they documented?

A CFTC staff member's need to access AWG GSS and the data therein, as well as the extent of that access, is dictated by the job role assigned to that person and as approved by that person's assigned manager or supervisor. The manager or supervisor then communicates that approval to the AWS GSS administrative user, who implements the necessary changes in AWS GSS to provide the needed access.

When onboarding a new AWS GSS administrator, a Privileged Access Form is required. That form requires the prospective administrator to make multiple attestations regarding the proper use of, protection of, and access to the system and data therein, and must be signed by user, user's manager, the system owner, and CFTC Chief Information Security Officer (CISO).

8.4 Describe what privacy training is provided to users, either general or specific to this system or project.

Completion of initial and thereafter annual security and privacy awareness training is a prerequisite to a user gaining and maintaining access to the CFTC network. All users must sign the CFTC Information Technology Rules of Behavior Acknowledgment, which memorializes this requirement. Access to the system is limited to those with an official need-to-know.

The requirement to complete security and privacy awareness training is immediately charged to an employee or contractor upon onboarding to CFTC, i.e., after their AD account is created, and must be completed within two days. If the training has not been completed in the two-day period, the user's AD account is automatically disabled, preventing that user from accessing the CFTC network to any degree, and the account remains disabled until the training has been completed.

8.5 Privacy Impact Analysis: Related to Auditing and Accountability

Failure of an audit to detect potential malicious activity or improper access to AWS GSS audit logs risks individuals' PII be deleted or altered, which would negatively affect their access to the CFTC network and assets therein. As noted above, an employee's or contractor's access to the CFTC network and assets therein is a condition of initiating and continuing engagement with CFTC. There is a low risk of stolen identity, because this information is business related and not personal, or of gaining access to the CFTC network, since more than a user's AD profile information is required to gain access to the CFTC network. These risks are mitigated by alerts set up by eSOC to identify any suspicious activity. Once the alert is received, eSOC is notified and immediately responds and remediates any damage caused by the event.