Privacy Impact Assessment for ServiceNow

April 2025

Point of Contact
Marty Rison
System Owner

Reviewing Official
Kellie Cosgrove Riley
Chief Privacy Officer

OVERVIEW

ServiceNow is a cloud-based platform that encompasses a variety of modules designed to optimize workflows for enterprise operations, risk management, and service delivery. The Commodity Futures Trading Commission ("CFTC" or "Commission") has adopted ServiceNow to streamline operations by automating workflows in a variety of information technology and administrative contexts. This Privacy Impact Assessment (PIA) is being conducted because many of the modules in use on the ServiceNow platform involve the collection and use of information about Commission employees, contractors, and others.

ServiceNow processes and stores data necessary for IT and other business operations, including, but not limited to, user details, asset information, vulnerability data, and risk assessments. The platform is configured to ensure the privacy and security of this information, with stringent access controls, encryption, and auditing capabilities.

The use and deployment of the various modules on the ServiceNow platform is managed by the CFTC's Division of Administration - Information Technology (DA-IT), with support from ServiceNow contractors regarding the design, development, and deployment of solutions on the platform, and from the ServiceNow Corporate Office regarding deployment of new modules and continuous improvements to the platform.

Within DA-IT, the ServiceNow System Administrators are responsible for the overall administration, configuration, and maintenance of the ServiceNow platform. They manage user access, security and privacy controls, and system performance. Various other groups within DA-IT make up the majority of those that use the ServiceNow modules in their day-to-day business. These include:

- Network Operations, which uses ServiceNow's IT Service Management (ITSM) and IT Operations Management (ITOM) modules to manage day-to-day IT services.

- User Operations, which uses ITSM to manage the CFTC's Customer Support Center (CSC), providing timely assistance with IT issues and service requests, and to oversee telecommunications and audio-visual support and services, providing communication and conferencing capabilities for the Commission.

- Client Engineering, which is responsible for packaging and deploying commercial off-the-shelf (COTS) applications and uses ServiceNow to ensure that third-party software products are properly configured, tested, and distributed across the CFTC's environment.

- Security Operations Team, which engages with the Security Operations (SecOps) module and its integration with Qualys to manage vulnerabilities, track remediation efforts, and respond to security incidents.

- Systems Team, which uses the App Engine platform to design and develop a variety of custom applications tailored to CFTC's operational needs and to help streamline internal workflows, automate business processes, and improve overall service delivery across multiple departments within the Commission.

In addition to DA-IT, all CFTC staff, to include employees and contractors, use and benefit from the services managed within ServiceNow. CFTC staff interact with ServiceNow through a Self-Service portal, which is designed to limit exposure to sensitive data while ensuring ease of use for service requests and issue reporting. Direct use of ServiceNow by CFTC staff includes:

- Submitting incident tickets, service requests, and change requests through the Self-Service portal, allowing the IT department to manage and resolve issues efficiently.

- Requesting IT services, equipment, and software through the Self-Service portal, enhancing user autonomy and satisfaction.

- Completing forms developed in the App Engine module or otherwise, including certain human resources forms, forms to request information needed for investigations, and forms necessary to efficiently equip newly onboarded staff.

The use of ServiceNow is governed by strict access controls, ensuring that only authorized personnel within CFTC have direct access to the system. Access is granted based on role and need, and external contractors are bound by security and privacy agreements to protect organizational data.

This PIA includes appendices that provide further details on each ServiceNow module in use at the Commission. The types of information collected by ServiceNow depends on the business purpose for its use. This may include information about the IT system, software, or technology-related information, and/or information about individuals. As additional ServiceNow modules are added in the Commission's environment, the appendices will be updated.

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 CFTC is authorized to collect the information within ServiceNow pursuant to a variety of general authorities related to agency operations and more specific authorities pertaining to the function and purpose of specific modules and application in use on the platform. These include, but may not be limited to, the Commodity Exchange Act, particularly 7 U.S.C. § 16, and its implementing regulations; 5 U.S.C. § 301; 44 U.S.C. § 3534; OMB Circular A-130; and authorities pertaining to Federal government personnel administration and management found in Title 5 of the U.S. Code and in Office of Personnel Management regulations and guidance.

Additional authorities may apply to specific modules or applications within ServiceNow and will be addressed where relevant in the appendices.

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.

Various SORNs may apply to the information collected or maintained in ServiceNow depending on the specific module or application. These include, for example, CFTC-35, General Information Technology Records, 81 FR 67327; OPM/GOVT-1 General Personnel Records, 77 Fed. Reg. 79694 as modified by 87 FR 5874 and 88 FR 56058; CFTC-5, Employee Personnel, Payroll, Time, and Attendance, 81 FR 67327; and CFTC-10 Investigatory Records, 76 FR 5973.

Where relevant, additional SORNs may be identified in the appendices.

1.3 Please identify the applicable accreditation boundary evaluated during the Authority to Operate (ATO) process. If the system 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.

ServiceNow is hosted in the Government Community Cloud (GCC) and provided as a Platform as a Service (PaaS) which is a FedRAMP® certified cloud environment. The ServiceNow ITSM module received an ATO in March 2023; that ATO is currently under review to expand the boundary to include the complete ServiceNow platform and all of the modules implemented by the CFTC.

1.4 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.

The information collected in ServiceNow is generally not subject to the PRA as information is not collected directly from members of the public. To the extent any of the applications built in ServiceNow via the use of the App Engine module or otherwise result in an information collection subject to the PRA that will be addressed in the applicable appendices.

2. INFORMATION

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

Depending on the module, ServiceNow collects various information, including information about individuals and information about IT systems, software, and other technology-related information. This information is detailed in the appendices of this PIA, as are the sources of the information, the steps taken to minimize the collection of information, and how the accuracy, integrity, and/or quality of the information is determined.

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

There is a risk that more information will be collected than is necessary to meet the business needs addressed by ServiceNow. This risk is mitigated by establishing effective procedures to collect only the information necessary, via the use of clear instructions to users and minimizing the use of free text fields.

There is also a risk that the information collected may not be accurate. This risk is minimized by collecting relevant information from trusted sources or, where possible, directly from the individual who has an interest in providing accurate information to obtain requested services for DA-IT or from other offices for whom DA-IT has established applications and workflows.

To the extent the use of any particular module or application within ServiceNow presents any specific additional risks related to the information collection, they will be addressed in the applicable appendices.

3. USE OF THE INFORMATION

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

The uses of the information collected within ServiceNow varies according to the business purpose for which a particular ServiceNow module was implemented or for which a particular application was built. This information is detailed in the appendices of this PIA, as are the roles and responsibilities of those within the CFTC who have access to ServiceNow and for what purpose.

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

There is a risk that the information in the system will be accessed by an unauthorized user or accessed by an authorized user for a purpose that is not authorized or is inconsistent with the purpose for which it is being collected and maintained in ServiceNow.

This risk is mitigated through the use of Role Based Access Controls (RBAC) comprised of user provisioning, permissions management, and access controls. User access is also mapped to organizational duties performed to ensure that users are only processing data specific to their authorized functions. Additionally, all users must agree to Rules of Behavior prior to being granted access to the system.

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 from ServiceNow is generally not shared outside of the CFTC but may be accessed or shared with contractors who are working with CFTC employees and who have a role in the automated workflows implemented via the various ServiceNow modules. To the extent any future ServiceNow module facilitates sharing outside of the CFTC, that will be documented in the applicable appendices.

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?

While the purpose for which the information in ServiceNow varies across the modules, as noted in Section 3, any sharing with or access by a contractor is done only to achieve the business purpose that prompted the collection of the information. Each Privacy Act system of records notice covering the various records in ServiceNow contains a routine use permitting disclosure to contractors under these circumstances.

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

Yes, the relevant contract or contracts outline the duties of the contractor and its employees with respect to CFTC information.

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?

Yes, the relevant contract or contracts include limitations concerning the use and sharing of CFTC information. In addition, all contractors are required to sign Rules of Behavior and a Nondisclosure Agreement.

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

ServiceNow generates audit logs indicating who accessed information in the system and for what purpose.

4.6 Privacy Impact Analysis: Related to Information Sharing

There is a risk that information will be shared outside of the agency and used for a purpose that is not compatible with the business need for which it was originally collected. This risk is mitigated because the system is not designed for external sharing and the contractors who have direct access to the system are required to adhere to the terms of the contract. In addition, the role-based access controls limit contractor access to only the information they need to know to fulfill their contractual obligations.

5. DATA RETENTION

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

The information in ServiceNow is subject to various retention requirements. How long and for what reason the information is retained within each module is detailed in the appendices.

When any new modules or features are developed within ServiceNow, the ServiceNow team will meet with the Records and CUI Office to discuss the applicable retention schedules.

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

All records are destroyed using the correct destruction method (deletion) as outlined within the CFTC Records Management Manual using the Records

Destruction Approval form. ServiceNow has configured an automated process where all records within ServiceNow that have reached their retention period are automatically deleted. The deleted records are then held within logs (maintained within ServiceNow) which contain in eXtensible Markup Language (XML) files of the actual data that was deleted in case the records needed to be restored. The ServiceNow team is working with the Records and CUI Office to ensure that these logs are permanently deleted according to the appropriate time frame as identified by the Records and CUI Office.

5.3 Privacy Impact Analysis: Related to Retention

There is risk that information in ServiceNow may be retained longer than is necessary to meet the business need for which it was collected. This risk is mitigated by adhering to the applicable records schedule, which addresses the business need to retain the information. When records are scheduled for destruction based on the retention schedule, the information is deleted securely and completely as part of the automated deletion process. This risk is not fully mitigated, however, pending the ServiceNow team identifying with RCO the appropriate retention for the XML files referenced above.

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.

General notice regarding the collection and use of individuals' information within ServiceNow is provided via publication of this PIA. Additional information regarding the collection and use of certain records about individuals that may ultimately be collected and used in ServiceNow is provided via publication of applicable Privacy Act systems of records notices.

More direct notice is provided within ServiceNow in those instances where the information is provided directly by the individual, via the Self-Service Portal or otherwise, through a Privacy Act statement or other notice available to the individual.

The appendices further describe what notice, if any, is provided to individuals within the various ServiceNow features and modules.

6.2 Privacy Impact Analysis: Related to Notice

There is a risk that individuals are not aware that ServiceNow collects and uses their information. This risk is mitigated through the publication of this PIA and applicable

SORNs. In addition, for those ServiceNow features and modules where individuals provide their information directly in the system, they may also receive a Privacy Act statement or other notice.

7. REDRESS

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

Individuals may request access to records about themselves that are included in the relevant systems of records by following the procedures outlined in the respective SORNs. Further information about redress, including how an individual can request that their information be corrected, is provided where applicable the appendices.

7.2 Privacy Impact Analysis: Related to Redress

There is a risk that individuals may not be able to access information about themselves that is contained within ServiceNow nor be afforded adequate opportunity to correct that information. This risk is mitigated by providing individuals, where required and appropriate, with an opportunity to obtain access to and request amendment of their records.

8. AUDITING AND ACCOUNTABILITY

8.1 How is the information in the system secured?

The ServiceNow solution is hosted in the GCC and is, therefore, accessible only from CFTC devices within the Commission's enterprise, enhancing the physical, technical, and administrative safeguards built into the system.

Physical safeguards include secure data centers. The GCC hosting ServiceNow operates in physically secure data centers with strict access controls, surveillance, and monitoring protocols managed by the cloud provider. Only Commission-approved and secured devices can access the CFTC’s ServiceNow instance, further limiting physical access points.

Technical safeguards specific to GCC include network restrictions, including configuration that only allows connections from within the Commission’s enterprise network, ensuring that data traffic is isolated from other environments. Commission devices accessing the ServiceNow solution are protected with endpoint security measures, such as device-level encryption, antivirus software, and compliance checks. The GCC meets stringent Federal security and compliance standards, including FISMA, FedRAMP, and NIST SP 800-53, which involve advanced technical controls like continuous monitoring and automated threat detection. Lastly,

administrative safeguards in place include enterprise access policies which are enforced to ensure devices meet security baselines before accessing ServiceNow.

By leveraging a Software as a Service (SaaS) model in the GCC and restricting access to only CFTC devices within the enterprise, the security framework provides a controlled and compliant environment for protecting information.

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.

Audit logs for ServiceNow are generated for specific actions and are used to detect malicious users, track unusual activity, and comply with requirements to track access changes. Audit log guidance is provided in ServiceNow documentation and can be tailored for specific requirements. Audit logs are currently reviewed as needed or upon request. Access control lists are reviewed within logs any time a change is made to the system to ensure that only the individuals who need access are granted access.

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

Access to CFTC's ServiceNow environment is limited to users who are listed in CFTC Entra ID (Active Directory) and who are granted access via Single Sign On (SSO). If a new hire (CFTC employee or contractor resource) needs access to ServiceNow it would be noted on their respective HR Form 719. If there is an existing resource that requires access to ServiceNow, a ticket is opened and the system owner approves or denies the request. In addition, users must be on the CFTC network, either directly or via the CFTC virtual private network (VPN), to reach CFTC's Self-Service Portal and ServiceNow instances. Access to CFTC ServiceNow and the various modules, applications, features, and data contained in it is controlled through user access groups that are assigned different combinations of roles and discrete privilege, based on the role and function of the person. At the most basic level, all CFTC staff are in the "CFTC – Dynamic Active Users" group. This provides the ability to submit ServiceNow requests through the Self-Service Portal, view pending approval requests, view the user's asset information, and read posted Knowledge Base articles. There are several groups specifically for approvers of various kinds e.g., access requests. There are also several groups and subgroups for the fulfillment of various kinds of requests e.g., hardware provisioning, infrastructure changes, security incident reporting. In most cases, management approval is required for inclusion in CFTC Entra ID (Active Directory) groups. Elevated or administrative roles are granted strictly on the basis of business function and require supervisor or leadership approval.

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

All users are required to complete Cybersecurity and Privacy Awareness Training prior to obtaining access to the Commission's network and systems and annually thereafter. A user's failure to complete the annual training requirement will result in their network access being terminated. a prerequisite and annual requirement for access to ServiceNow.

8.5 Privacy Impact Analysis: Related to Auditing and Accountability

There is a risk that the audit logs and access control lists will not be used effectively to maintain the security of the ServiceNow platform. This risk is mitigated through the logs being carefully designed and controlled and access control lists being reviewed within logs any time a change is made to the system to ensure that only the individuals who need access are granted access. There is also a more general risk that those with access to ServiceNow will not understand their obligations with respect to the privacy and security requirements pertaining to the information in the system. This risk is mitigated through annual training requirements.

Appendix A: ServiceNow IT Support Management (ITSM) Module

PURPOSE

The ServiceNow Information Technology Support Management (ITSM) module is used by the CFTC as its IT Support Services ticketing system. ServiceNow ITSM is primarily used by the Customer Support Center (CSC) Agents to track IT issues and requests from staff and contractors at its headquarters in Washington, DC and its three regional offices located in New York, Chicago, and Kansas City. In addition, Facility Operations Services (FOS) and Cybersecurity also maintain workspaces, or separate help desks, within ITSM to track and monitor issues and requests related to their respective business areas.

Part of the ITSM module functionality allows for interaction with an internal facing portal, known as the Self-Service Portal, where CFTC employees and contractors can interact with the CSC Agents. They can submit tickets and other requests and receive information and alerts associated with the Commission's IT infrastructure.

The key features of ServiceNow's ITSM module that the CFTC is using include:

- Incident Management, which allows IT teams to capture, prioritize, and resolve issues quickly and efficiently, reducing the impact on business operations.
- Change Management, which manages the lifecycle of all IT system and network changes to facilitate those changes with minimal disruption.
- Service Catalog, which allows users to easily request IT services and track the status of their requests.
- Configuration Management Database (CMDB), which stores information on IT assets and their relationships. (The CMDB receives asset information from EAMS.)

SYSTEM ACCESS

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.

Within the Commission, multiple programs and offices have assigned roles and responsibilities regarding the ITSM module. Due to the diverse nature of services and functions supported by ITSM, many individuals potentially interact with or "touch" ITSM tickets within the system. These interactions occur for a variety of purposes, including but not limited to ticket resolution, approval processes, technical assessments, compliance checks, and audit reviews.

Given the breadth of functions managed through ServiceNow, ITSM module users include personnel from IT Operations, Customer Support, Application Development and Deployment, Privacy, Security, Change Management, Vulnerability Management, and various business units. Each of these offices may have different roles and responsibilities, such as:

- CFTC Staff and Contractors: Everyone at the Commission has access to CFTC's Self-Service Portal on the Intranet to report IT issues or request hardware and software.
- IT Operations and Customer Support: Personnel from these offices are primarily responsible for managing incident tickets, resolving technical issues, deploying software, and providing support services.
- Systems Development Teams: These teams focus on addressing system changes, enhancements, and debugging within the platform.
- Business and Functional Units: Various business teams engage in ticket approval processes, initiate service or application requests, and monitor task completion for their respective projects or programs.
- Privacy and Security Teams: These teams ensure compliance with privacy and security standards by monitoring access controls, auditing activities, and addressing incidents.

Information generated via the ITSM module is shared in a controlled manner based on role-based access controls (RBAC). These controls ensure that individuals only have access to information relevant to their specific responsibilities. For instance:

- IT Staff and Support Teams access information needed for ticket resolution and system administration tasks.
- Approval Authorities have access to ticket details related to requests and changes that require their authorization.
- Change Advisory Board Members have access to all IT Change Requests and related ticket and associated documentation.
- CFTC Staff and Contractors who submit information and requests via the Self-Service Portal have access only to their own information and tickets.

Through these controlled access policies, the system maintains data integrity, security, and privacy while enabling collaboration across the Commission's various offices and programs.

TYPES OF INFORMATION IN THE SYSTEM

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

To create a ticket, information such as the individual requester's phone number (provided directly from the CFTC staff), business email address, manager, office location (by state), job title, department, CFTC branch, CFTC division, CFTC section, and CFTC unit is pulled from CFTC Entra ID (Active Directory). In instances where government furnished equipment, such as a laptop or business cell phone, need to be sent to a CFTC staff member's residence, the individual who needs the GFE provides their first and last name, home address, phone number, and personal email address required for shipping. This information is maintained within the comments section of the ticket request. ITSM does not otherwise request information directly from the individual.

An individual's name and asset (GFE) they are assigned to may be pulled from the ServiceNow Enterprise Asset Management System (EAMS), if a CSC agent needs to determine what asset an CFTC Staff member is assigned to in order to fulfill a ticket.

Any comments or work notes on tickets handling Cloud Assured Managed Services or Cloud Security are sent to the ServiceNow Cloud Assured Managed Services (CAMS). This allows the CAMS Team (contractors) to handle/manage those tickets. ITSM still remains the authoritative source of the ticket.

Changes to staff information, such as when an employee transfers to another office within the CFTC, are received on HR Form 720, *Employee/Contractor Change*, which is populated within the Management and Administrative Enterprise Database (MAED) (a separate CFTC information system) the information from the form is then populated into an automated email that is sent from MAED to ServiceNow ITSM. The information on HR Form 720, which includes name (last, first, middle), region, official title, grade, employment type, organization/department, pay status (paid, unpaid), standard form (sf) 52 request for personnel action form number, room/office number, and a list of any special furnishings needed (beyond the standard furniture), is ingested into a new ticket within ITSM to track the work necessary to fulfill a change in position for an employee or contractor.

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

ITSM collects information for the purpose of tracking IT issues and requests. Most of the information collected for this purpose is pulled from CFTC Entra ID (Active Directory) when the CFTC staff use the Self-Service portal. When CFTC staff call the

CSC to report an issue or make a request, the CSC Agent populates the ticket information in ITSM. The HR form 720 is received from MAED (a separate information system) with the information populated from that system and is sent to the CSC via an email and a ticket is created in ITSM. Information is also directly collected from CFTC staff during interactions with the CSC. The information collected from CFTC staff is entered into the comments section of a support ticket by the technician or end user directly. For example, CSC may collect information when Government Furnished Equipment (GFE) is being shipped to the end user's residence or where the CFTC staff member provides a personal home or cell number for the CSC Agent to contact them regarding an IT Issue in the process of troubleshooting and resolution.

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

ITSM collects only the information necessary to track IT issues, requests from staff and staff changes. The information that is received from HR form 720 includes only that which is necessary to effectuate the transfer of the employee and ensure the proper equipment and access is issued.

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

ITSM receives information from CFTC Entra ID (Active Directory), MAED (a separate CFTC information system), COR, Business managers, and directly from CFTC staff (via the Self-Service Portal). In specific cases such as the need to ship a GFE to a remote CFTC staff member's residence, additional information may be collected directly from the individual. Each of these are trusted sources and sources that have an interest and need to provide accurate information to ensure they receive the requested service. If a CFTC staff member provides information within the text box of a ticket request or submits attachments, it is the responsibility of the CFTC staff member to ensure the accuracy of that information. If information were to be outdated or inaccurate, a new ticket can be submitted, and the comments sections of the ticket would then contain the accurate information. Any information received from the HR Form 720 that is determined to be inaccurate can be corrected at the point of collection within MAED (a separate information system).

Connections to Other Modules within ServiceNow and CFTC Information Systems

ServiceNow ITSM has connections to the following systems:

- CFTC Entra ID (Active Directory)
- CAMS
- EAMS
- MAED

RELEVANT SORNS

CFTC-35, General Information Technology Records 81 FR 67327
OPM/GOVT-1, General Personnel Records, 80 FR 74815
CFTC-5, Employee Personnel, Payroll, Time, and Attendance, 81 FR 67327

NOTICE

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

General notice regarding the collection and use of individuals' information within ServiceNow is provided via publication of this PIA. Additional information regarding the collection and use of certain records about individuals that may ultimately be collected and used in ServiceNow is provided via publication of applicable Privacy Act systems of records notices.

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

For the collection of information directly from CFTC staff when they submit a ticket through the Self-Service portal or via interaction with a CSC Agent, consent is implied as the CFTC staff member voluntarily provides their information (such as phone number and address) to make their request or report an issue. In other instances, such as the submission of the Form 720 and collection of information from CFTC Entra ID (Active Directory), there is no opportunity to consent but the use of the information is consistent with the reason for its initial collection from the individual.

RECORD RETENTION

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, records within ITSM are governed by the following General Records Schedules:

- GRS 3-1-010 Information technology development project records - Infrastructure project records

- GRS 3-1-020 Information technology operations and maintenance records

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

Records are kept in accordance with their applicable retention schedules as identified above. The records are retained under Disposition Authority DAA-GRS-2013-0005-0006 and DAA-GRS-2013-0005-0004 respectively, which requires that the records within ITSM be destroyed 5 years after project is terminated and 3 years after agreement, control measures, procedures, project, activity, or transaction is obsolete, completed, terminated or superseded.

REDRESS

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

CFTC staff may access the information they submit about themselves and any requests they've made through the Self-Service portal. They may also more generally request access to records about themselves that are included in the relevant systems of records by following the procedures outlined in the respective SORNs.

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

The information collected within ITSM is for a point in time use, collected for the purpose of submitting a ticket for an issue or shipping GFE's to CFTC staff and contractors when applicable. If information were to be outdated or inaccurate, a new ticket can be submitted to correct the information or the comments sections of the ticket can be amended to correct information about, e.g., shipping information.

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

Individuals receive information about submitting tickets via ITSM in CFTC Communications and interactions with the CSC; to the extent they discover errors in those tickets the CSC Agents can provide guidance. More generally, they may request amendment to records about themselves that are included in the relevant systems of records by following the procedures outlined in the respective SORNs.

Privacy Impact Analysis:

No additional specific risks have been identified for this module.

Appendix B: Service Now IT Operations Management (ITOM)

PURPOSE

The IT Operations Management (ITOM) Visibility module will enable the implementation of a Configuration Management Database (CMDB). The CMDB will serve as a centralized repository for tracking and managing IT assets, services, and their relationships. ITOM Visibility tools, such as Discovery and Service Mapping, will provide detailed insights into the Commission's infrastructure and ensure accuracy and accountability in managing IT resources.

The key features of ServiceNow's ITOM Visibility module include:

- Discovery: Automatically discovers assets across infrastructure.
- Service Mapping: Maps and visualizes the relationship between IT components.

SYSTEM ACCESS

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.

Network Operations uses ITOM to manage day-to-day IT services, including asset management.

TYPES OF INFORMATION IN THE SYSTEM

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

CFTC Entra ID (Active Directory) information is collected for the purpose of allowing users to sign into the ITOM module via SSO. Any asset information that is collected includes information about what assets a particular CFTC Staff members is assigned to and is provided from EAMS (a separate ServiceNow module authorized within a separate ATO boundary) into the ITSM module. The ITSM module then provides that asset information to ITOM for the purpose of creating a complete, accurate, and up-to-date record of configuration items throughout the Commission.

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

Information is not collected directly from the individual. For those users who have permissions to access ITOM, their credentials are pulled from CFTC Entra ID (Active Directory). Any asset assignment information (i.e. what asset is assigned to what CFTC staff member) is provided from EAMS into the ITSM module. The ITSM module then provides that asset information to ITOM.

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

All information obtained from Entra ID is mandatory and the minimum necessary to be able to allow users access to the module via SSO. Any asset assignment information (i.e. what asset is assigned to what CFTC staff member) pulled from the ITSM module is only that needed for the creation of the up-to-date record of all IT assets and infrastructure within the Commission.

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

The ServiceNow ITOM module receives information from Entra ID (Active Directory) and EAMS (via ITSM). The information from Entra ID (Active Directory) is presumed to be accurate as is the asset assignment information (i.e. what asset is assigned to what CFTC staff member) that is pulled from the EAMS through ITSM. To ensure the accuracy and quality of the data from EAMS, EAMS data within ITSM is refreshed nightly and ITOM reads this information daily.

CONNECTIONS TO OTHER MODULES WITHIN SERVICENOW AND CFTC SYSTEMS

ServiceNow ITOM has connections to the following:

- MID Server – CFTC Network
- Microsoft Endpoint Configuration Manager (MECM)/ Service Graph Connector (SCCM) – Does not provide or receive PII from ITOM
- Intune - Does not provide or receive PII from ITOM
- Azure Cloud Service Graph Connector - Does not provide or receive PII from ITOM
- AWS Cloud Service Graph Connector - Does not provide or receive PII from ITOM
- EAMS
- CFTC Entra ID (Active Directory)

RELEVANT SORNS

CFTC-35, General Information Technology Records, 81 FR 67327.

NOTICE

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

General notice regarding the collection and use of individuals' information within ServiceNow is provided via publication of this PIA. Additional information regarding the collection and use of certain records about individuals that may ultimately be collected and used in ServiceNow is provided via publication of applicable Privacy Act systems of records notices. No direct notice is provided to individuals concerning the inclusion of their information in ITOM but the use of the Entra ID and asset assignment information is consistent with the purpose for which it was collected.

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

In the case of the ServiceNow ITOM Module, information is not collected directly from individual (CFTC staff) therefore, individuals do not have the opportunity to consent to the use of their information in ITOM.

RECORD RETENTION

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 within ITOM are governed by the following General Records Schedules:

- GRS 6-3-020 Enterprise architecture records

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

Records are kept in accordance with their applicable retention schedules as identified above. The records are retained under Disposition Authority DAA-GRS-2017-0009-0002 which requires that the records within ITOM be destroyed 7 years after creating a new iteration of the enterprise or information architecture.

REDRESS

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

Individuals do not have direct access to ITOM nor to the asset management information contained therein. CFTC staff may request access to records about themselves that are included in the relevant systems of records by following the procedures outlined in the respective SORNs.

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

CFTC Staff do not have direct access to their information within the ServiceNow ITOM Module. If a CFTC staff member needed to update their personal information, that CFTC staff member would need to update their information within CFTC Entra ID (Active Directory); any correction of assigned assets could be addressed via the CSC. Individuals may also more generally request amendment of records about themselves that are included in the relevant systems of records by following the procedures outlined in the respective SORNs.

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

The procedures for submitting a request to correct information are outlined in the applicable SORNs.

Privacy Impact Analysis:

No additional specific risks have been identified for this module.

Appendix C: ServiceNow Security Operations (SecOps)

PURPOSE

The Security Operations (SecOps) module is an enhancement to the ServiceNow ITSM module that helps manage and respond to security incidents, including threat detection, incident response, and vulnerability management. The Security Operations module is integrated with Qualys (contained in a separate ATO boundary) to bolster the Commission's Vulnerability Management program. This integration enables automated detection and management of vulnerabilities across the IT landscape, providing real-time visibility into security risks and enhancing the ability to mitigate threats. The module allows for a streamlined workflow from detection through remediation, ensuring rapid response to emerging vulnerabilities.

The key features of ServiceNow's SecOps module include:

- Security Incident Response: Manages and resolves security incidents.
- Vulnerability Response: Prioritizes and remediates vulnerabilities.
- Threat Intelligence: Collects and analyzes threat data.

SecOps will be used by the Enterprise Security Operations Center (eSOC) team and the CSC to help manage tickets dealing with the CFTC's cybersecurity posture and for preventing, detecting, and responding to threats. If any ticket is created within ITSM that indicates the need for eSOC review and handling, the ticket will be sent to ServiceNow SecOps.

SYSTEM ACCESS

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.

The following Cyber Security group(s) have access to the ServiceNow SecOps module:

- eSOC (approximately 13 users): This group is responsible for the day-to-day monitoring and management of security incidents, threats, and vulnerabilities.
- eSOC Approvers (approximately 3 users): This group includes individuals responsible for reviewing and approving specific actions or escalations within the SecOps module, ensuring that appropriate workflows and protocols are followed.
- Insider Risks (approximately 2 users): This group is tasked with identifying and addressing insider threats, focusing on monitoring and investigating activities that could indicate potential internal risks.

- Leads (approximately 3 users): This group comprises team leaders or managers overseeing the operations and ensuring the effective functioning and compliance of the SecOps module.
- ServiceNow Developers (approximately 6 users): Individuals responsible for configuring and managing the SecOps module, ensuring it is properly customized, updated, and maintained to meet operational needs.

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

The ServiceNow SecOps module contains CFTC Entra ID (Active Directory) SSO information for individuals within the CSC and eSOC who access the module. CFTC staff members' name, business phone number, business email, personal cell phone, and location (if the individual is a remote employee) may be provided within tickets that are received from ITSM for the purpose of reporting a security incident. CFTC staff members' name and business email may also be included within phishing email security incidents that Sentinel (a separate information system) provides to SecOps.

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 collected for the CSC agents and the eSOC team to access SecOps is collected from Entra ID. Any information relating to CFTC Staff is provided from the ServiceNow ITSM Module ticket, which can include information received directly from the individual about a security issue, or from Sentinel (to provide SecOps with phishing email security incident information).

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

All information collected for the CSC agents and the eSOC team to access SecOps obtained from Entra ID is mandatory and the minimum necessary to be able to allow users access to the module via SSO. Other information relating to CFTC Staff and their ticket submission is generally the minimum necessary to address the issue, though the possibility exists that individual will provide additional information in the comments section of a ticket.

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

Any information relating to CFTC Staff is provided from the ServiceNow ITSM module ticket is presumed to be accurate given that it was submitted by the individual only for the purpose of fulfilling a request, as is information from

Sentinel provided in order to provide SecOps with phishing email security incident information.

CONNECTIONS TO OTHER MODULES/FEATURES WITHIN SERVICENOW AND CFTC SYSTEMS

ServiceNow SecOps has connections to the following:

- Qualys- does not send or receive PII from SecOps
- Microsoft Sentinel
- ServiceNow ITSM
- CFTC Entra ID (Active Directory)

RELEVANT SORNS

SORN CFTC-35, General Information Technology Records, 81 FR 67327.

NOTICE

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

In the case of ServiceNow SecOps information is not collected directly from individuals (CFTC staff) and, therefore, no notice is provided directly to the individual from SecOps but may be provided when an individual submits a ticket with ServiceNow ITSM. General notice regarding the collection and use of individuals' information within ServiceNow is provided via publication of this PIA. Additional information regarding the collection and use of certain records about individuals that may ultimately be collected and used in ServiceNow is provided via publication of applicable Privacy Act systems of records notices.

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

Information is not collected directly from individuals (CFTC staff) and, therefore, there is no opportunity for individuals to consent to the collection and use of their information in SecOps. When individuals submit a ticket for resolution, their consent to use that information however is necessary to resolve the ticket is implicit.

RECORD RETENTION

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 within SecOps are governed by the following General Records Schedules:

- GRS 3-2-010 Systems and data security records

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

Records are kept in accordance with their applicable retention schedules as identified above. The records are retained under Disposition Authority DAA-GRS-2013-0006-0001 which requires that the records within SecOps will be destroyed 1 year(s) after system is superseded by a new iteration or when no longer needed for agency/IT administrative purposes to ensure a continuity of security controls throughout the life of the system.

REDRESS

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

CFTC staff do not have direct access to SecOps. CFTC may access their ITSM ticket information through the ServiceNow Self-Service Portal.

CFTC staff may request access to records about themselves that are included in the relevant systems of records by following the procedures outlined in the respective SORNs.

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

CFTC staff do not have direct access to their information ServiceNow SecOps. If a CFTC staff member needed to update their personal information, that CFTC staff member would need to update their information within CFTC Entra ID. If any information were to be outdated or inaccurate within a ticket, CFTC staff would have to submit a new ticket within ServiceNow ITSM and the comments sections of the ticket would then contain the accurate information.

CFTC staff may also request amendment of records about themselves that are included in the relevant systems of records by following the procedures outlined in the respective SORNs.

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

Individuals receive information about submitting tickets via CFTC Communications and interactions with the CSC; to the extent they discover errors in those tickets the CSC Agents can provide guidance. More generally, they may request amendment to records about themselves that are included in the relevant systems of records by following the procedures outlined in the respective SORNs.

Privacy Impact Analysis:

No additional specific risks have been identified for this module.

Appendix D: ServiceNow App Engine

PURPOSE

ServiceNow App Engine is an application development program used to by the CFTC to create custom business applications without extensive development cycles. This capability is used only by DA-IT Systems Team to build, deploy, and manage low-code applications.

The key features of ServiceNow's App Engine include:

- Custom Application Development: Develops applications specific to business needs.
- Integration Hub: Facilitates integration with third-party apps and data sources. (Not currently in use.)
- Flow Designer: Automates and manages workflows across applications.
- UI Builder: Designs user interfaces for custom applications.

SYSTEM ACCESS

The Systems Team, with support from the ServiceNow Development team, and the are the only teams within the CFTC that have the capability to develop applications and solutions using App Engine.

TYPES OF INFORMATION IN THE SYSTEM

No information pertaining to individuals is collected or used directly within the App Engine development platform itself; however, as ServiceNow App Engine's purpose is to create applications, depending on the created application's design and purpose, custom applications may collect, maintain, and/or use a broad range of information about individuals that is collected, used, and maintained in the ServiceNow platform.

Currently, App Engine has been used to develop the following applications:

- Internet Data Collection Requests (eLaw Forensics)(Initially developed with App Engine, later iterations of the forms were created using ITSM standard form and workflow development tools.)
- Workforce Schedules
- Telework Applications Solutions

This appendix will be updated as new applications are developed.

Identify the information that the system, project, or program collects,

maintains, uses, or disseminates.

Internet Data Collection Requests (eLaw Forensics)
There are two internet data collection request forms that were created by App Engine to support the CFTC Forensics team (made up of five individuals) and the Division of Enforcement (DOE), for website collections when conducting investigations.

Workforce Schedules
All CFTC employees are required to submit their work schedule to their supervisor for approval. The Workforce Schedules Application is an automated form that collects the following information: first and last names, first and second line supervisors, and the CFTC employee's requested work schedule. This form allows supervisors to document and manage staff work schedules.

Telework Applications Solutions
The Telework Application Solution is an automated form that is completed by CFTC federal employees requesting to telework. The Telework Application Form collects first and last name, supervisor name, telework location (address, city, state, zip code), telework location phone number (which may be a personal cell phone number), and the type or telework requested (regular, episodic, medical, hardship). The information provided on the form is used by the Commission primarily to determine whether the employee making the request may participate in the requested telework arrangement and to document and manage such arrangements.

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

Internet Data Collection Requests (eLaw Forensics)
Staff in DOE provide the information requested on the internet data collection request forms via the Self-Service Portal by entering it directly into the application in ServiceNow. This includes information about individuals who are the subject of an investigation.

Workforce Schedules
The name of the employee and the name of their supervisor is populated within the form by CFTC Entra ID (Active Directory). The employee manually enters their requested schedule directly within the form itself through the Self-Service Portal.

Telework Applications Solutions
The first and last name of the CFTC federal employee and the name of their supervisor is populated within the form by CFTC Entra ID (Active Directory). The CFTC federal employee then populates the days of the week on which they're

requesting to telework, telework location (address, city, state, zip code), telework location, phone number (which may be a personal cell phone number), and the type or telework requested (regular, episodic, medical, hardship) directly within the form itself through the Self-Service Portal.

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

Internet Data Collection Requests (eLaw Forensics)
The information that is received from the Internet Data Collection Request Forms is collected for law enforcement purposes and the general requirement to minimize data collection is less stringent here as to what will be needed for an investigation is often not known at the outset.

Workforce Schedules
Only the information necessary for the CFTC to determine the CFTC federal employee's schedule request is collected and there is no free text data field where an individual employee or might inadvertently submit unnecessary information.

Telework Applications Solutions
The application is designed to collect only the information necessary for the CFTC to determine whether the employee making the request may participate in telework arrangements and to document and manage such arrangements and there is no free text data field where an individual employee or might inadvertently submit unnecessary information.

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

Internet Data Collection Requests (eLaw Forensics)
The information that may be populated within the Internet Data Collection Requests come directly from DOE staff who have an interest in providing and obtaining relevant information to obtain accurate search results.

Workforce Schedules
The information collected within the Workforce Schedules Automated Form comes from CFTC Entra ID (Active Directory) and is entered directly by the employee who has an interest in providing accurate information. If inaccurate information is submitted, or accurate information becomes outdated, the employee can submit a corrected form via the Self-Service portal.

Telework Applications Solutions

The information collected within the Telework Applications Solutions Form comes from CFTC Entra ID (Active Directory) and is entered directly by the employee who has an interest in providing accurate information. If inaccurate information is submitted, or accurate information becomes outdated, the employee can submit a corrected form via the Self-Service portal.

CONNECTIONS TO OTHER MODULES WITHIN SERVICENOW AND CFTC SYSTEMS

ServiceNow App Engine has connections to the following:

- CFTC Entra ID (Active Directory)

RELEVANT SORNS

Internet Data Collection Requests (eLaw Forensics)
CFTC-10, Investigatory Records, 76 FR 5973.

Workforce Schedules
CFTC-5, Employee Personnel, Payroll, Time, and Attendance, 81 FR 67327, and OPM/GOVT-1, General Personnel Records, 77 Fed. Reg. 79694 as modified by 87 FR 5874 and 88 FR 56058.

Telework Applications Solutions
SORNs CFTC-5, Employee Personnel, Payroll, Time, and Attendance, 81 Fed. Reg. 67327, and OPM/GOVT-1, General Personnel Records, 77 Fed. Reg. 79694 as modified by 87 FR 5874 and 88 FR 56058.

Additional SORN coverage may be added to this list as new applications are developed within App Engine.

NOTICE

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

Internet Data Collection Requests (eLaw Forensics)
No notice is provided to the subjects of investigations whose records are included in this form and form whom information is not directly collected.

Workforce Schedules
Individuals receive notice in the form of the following Privacy Act statement when they complete the Workforce Schedule form.

PRIVACY ACT STATEMENT

"This notice is being provided pursuant to the Privacy Act, 5 U.S.C. 5 552a(e)(3), to inform you about why the Commodity Futures Trading Commission ("Commission") is collecting this information from you. Authority: The Commission's authority to collect this information derives from 5 U.S.C. Chapter 61 and relevant government-wide guidance from the Office of Personnel Management. Purpose: The information you provide on this form will be used by the Commission primarily to document and manage your work schedule. Routine Uses: In addition, it is possible that the Commission may disclose the information that you provide to a third party pursuant to a "routine use" where such a disclosure is required by law or otherwise deemed necessary and appropriate. A complete list of "routine uses" may be found in the relevant system of records notice(s), OPM/GOVT-1. General Personnel Records, 77 Fed. Reg. 79694 as modified by 86 Fed. Reg. 68291) and/or CFTC-5, Employee Personnel, Payroll, Time, and Attendance, 81 Fed. Reg. 67327. Effect of Not Providing the Information: Providing this information is voluntary; but if you do not provide the information requested, you and your supervisor may not be able to establish and manage your work schedule."

Telework Applications Solutions

Individuals receive notice in the form of the following Privacy Act statement when they complete the Telework Application form:

PRIVACY ACT STATEMENT

"This notice is being provided pursuant to the Privacy Act, 5 U.S.C. § 552a(e)(3), to inform you about why the Commodity Futures Trading Commission ("Commission") is collecting this information from you. Authority: The Commission's authority to collect this information derives from 5 U.S.C. Chapter 61, 5 U.S.C. § 6502, and relevant government-wide guidance from the Office of Personnel Management. Purpose: The information you provide on this form will be used by the Commission primarily to determine whether you may participate in telework arrangements and to document and manage such arrangements. Routine Uses: In addition, it is possible that the Commission may disclose the information that you provide to a third party pursuant to a "routine use" where such a disclosure is required by law or otherwise deemed necessary and appropriate. A complete list of "routine uses" may be found in the relevant system of records notice(s), CFTC-5, Employee Personnel, Payroll, Time, and Attendance, 81 Fed. Reg. 67327, and/or OPM/GOVT-1, General Personnel Records, 77 Fed. Reg. 79694 as modified by 86 Fed. Reg. 68291. Effect of Not Providing the Information: Providing this information is voluntary; but if you do not provide the information requested, you may not be able to participate in a telework arrangement."

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

Internet Data Collection Requests (eLaw Forensics)
For the internet data collection request forms, individuals who are the subject of investigations are not the source of information, therefore the opportunity to consent is not provided.

Workforce Schedules
As noted in the Privacy Act statement provided to the individual, an individual can decline to provide information, but failing to provide the information may impact their ability to establish their work schedule:

"Effect of Not Providing the Information: Providing this information is voluntary; but if you do not provide the information requested, you and your supervisor may not be able to establish and manage your work schedule."

Consent is implied when the individual voluntarily provides their information within the Workforce Schedules form.

Telework Applications Solutions
As noted in the Privacy Act statement provided to the individual, an individual can decline to provide information, but failing to provide the information may impact their ability to telework:

"Effect of Not Providing the Information: Providing this information is voluntary; but if you do not provide the information requested, you may not be able to participate in a telework arrangement."

Consent is implied when the individual voluntarily provides their information within the Telework Applications Form.

RECORD RETENTION

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 collected via applications created within ServiceNow App Engine are governed by the following General Records Schedules:

Internet Data Collection Requests (eLaw Forensics)

- GRS 5-2-020 Intermediary records

Workforce Schedules
- GRS 2-4-030 Time and attendance records

Telework Applications Solutions
- GRS 2-3-040 Telework/alternate worksite program case files

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

Internet Data Collection Requests (eLaw Forensics)
Records are kept in accordance with their applicable retention schedules as identified above. The records are retained under Disposition Authority DAA-GRS-2017-0003-0002 which requires that the records within the Internet Data Collection Requests will be destroyed upon creation or update of the final record.

Workforce Schedules
Records are kept in accordance with their applicable retention schedules as identified above. The records are retained under Disposition Authority DAA-GRS-2019-0004-0002 which requires that the records within Workforce Schedules will be destroyed when 3 years old.

Telework Applications Solutions
Records are kept in accordance with their applicable retention schedules as identified above. The records are retained under Disposition Authority DAA-GRS-2018-0002-0004 which requires that the records within the Telework Applications Solutions will be destroyed when superseded or obsolete or 1 year after end of employee's participation in program, whichever is sooner.

REDRESS

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

Internet Data Collection Requests (eLaw Forensics)
For the internet data collection request forms, the records in this system that refer or relate to records contained in CFTC-10, Investigatory Records (exempted), have been exempted by the Commission from certain provisions of the Privacy Act of 1974 pursuant to the terms of the Privacy Act, 5 U.S.C. 552a(k)(2), and the Commission's rules promulgated thereunder, 17 CFR 146.12. These records are exempt from the notification procedures, records access procedures, and record contest procedures.

Workforce Schedules

CFTC federal employees may access the information they provided within the form by going into the ServiceNow Self-Service Portal where they can view their submitted form. CFTC staff may also request access to records about themselves that are included in the relevant systems of records by following the procedures outlined in the respective SORNs.

Telework Applications Solutions
CFTC federal employees may access the information they provided within the form by going into the ServiceNow Self-Service Portal where they can view their submitted form. CFTC staff may also request access to records about themselves that are included in the relevant systems of records by following the procedures outlined in the respective SORNs.

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

Internet Data Collection Request Forms:
For the internet data collection request forms, the records in this system that refer or relate to records contained in CFTC-10, Investigatory Records (exempted), have been exempted by the Commission from certain provisions of the Privacy Act of 1974 pursuant to the terms of the Privacy Act, 5 U.S.C. 552a(k)(2), and the Commission's rules promulgated thereunder, 17 CFR 146.12. These records are exempt from the notification procedures, records access procedures, and record contest procedures.

Workforce Schedules
CFTC employees can submit amended, corrected, or updated workforce schedules for approval via the ServiceNow Self-Service Portal. They may also request amendment of records about themselves that are included in the relevant systems of records by following the procedures outlined in the respective SORNs.

Telework Applications Solutions
CFTC employees can submit amended, corrected, or updated telework applications for approval via the ServiceNow Self-Service Portal. They may also request amendment of records about themselves that are included in the relevant systems of records by following the procedures outlined in the respective SORNs.

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

Internet Data Collection Request Forms:

For the internet data collection request forms, the records in this system that refer or relate to records contained in CFTC-10, Investigatory Records (exempted), have been exempted by the Commission from certain provisions of the Privacy Act of 1974 pursuant to the terms of the Privacy Act, 5 U.S.C. 552a(k)(2), and the Commission's rules promulgated thereunder, 17 CFR 146.12. These records are exempt from the notification procedures, records access procedures, and record contest procedures.

Workforce Schedules
Through CFTC Communications and interaction with supervisors and human resources staff, CFTC employees are instructed concerning the use of the Self-Service Portal. They are also instructed on procedures specific to correcting information within the form during the Mandatory Training for Telework and Work Schedules.

More generally, the procedure for requesting amendment to records about themselves is included in the relevant SORNs.

Telework Applications Solutions
Through CFTC Communications and interaction with supervisors and human resources staff, CFTC employees are instructed concerning the use of the Self-Service portal. They are also instructed on procedures specific to correcting information within the form during the Mandatory Training for Telework and Work Schedules.

More generally, the procedure for requesting amendment to records about themselves is included in the relevant SORNs.

Privacy Impact Analysis:

There is a risk that individuals are not aware how the Workforce Schedules and Telework Applications Solutions automated forms use their information. The risk is mitigated primarily through providing a robust Privacy Act statement on the Telework Applications Solutions Form and the Workforce Schedules Automated Form at the time of collection.

Appendix E: HR Form 719 Automation ServiceNow App

PURPOSE

The HR Form 719 Automation ServiceNow App was created to automate the Human Resources (HR) Form 719 that handles new staff requirements related to onboarding. The automated form once filled out, turns into a ticket and tracks onboarding tasks.

SYSTEM ACCESS

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.

CFTC Contracting Officer Representative (COR) and business managers access and use the HR Form 719 Automation ServiceNow App to fill out information on behalf of their federal employee or contractor for the purpose of onboarding. FOS and Human Resources also use the information to assist in onboarding tasks.

TYPES OF INFORMATION IN THE SYSTEM

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

The HR Form 719 Automation ServiceNow App collects and maintains CFTC staff onboarding information. The automated form collects the following information pertaining to an individual: name (last, first, middle), phone number, email, region, employment type, organization/department, pay status (paid, unpaid), standard form (SF) 52 request for personnel action form number, room/office number, appointment type, VIP status, and a list of any special furnishings needed (beyond the standard furniture). Employee ID, location, organization, employee supervisor ID, employment type, division, name (first, middle, last), date CFTC join (date employee joined the CFTC), proposed on board date, proposed estimated end date, communication (phone number, email), communication type, employee communication value (personal phone number and or email), employee contract ID (if contractor), contract number, COTR employee ID (COR employee is assigned to), alternate COR employment type desc, employment category, appointment type ID (paid/unpaid) employment subtype ID, division, grade, position, grade number, position name, and employment sub type description is pulled from MAED (a separate system within the CFTC). This information then goes through the ServiceNow MID Server HR Form 719 which works as a conduit to the cloud environment where the application is hosted. This information from MAED is then

automatically populated within the form. Then individuals COR (if a contractor) or business managers (if a federal employee) go into the ServiceNow Self-Service Portal where they access the Form 719 and populate the rest of the information such as room number and list of any special furnishings needed (beyond the standard furniture). The information within the form is then created as a ticket to track the work necessary to onboard a FED or Contractor. The ticket is also used to create a network or CFTC Entra ID (Active Directory) account, email account, image a laptop, deploy hardware to the workspace if they'll be onsite, etc. When all the tasks are completed, and the user is onboarded or off boarded, the ticket is then closed.

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

CFTC staff information within the HR Form 719 Automation ServiceNow App is collected from MAED (a separate CFTC Information system), and from CORs or business managers. Information is not collected directly from the individual to whom the information pertains.

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

The information that is received from the HR Form 719 is limited to that which is necessary to onboard CFTC federal employees and contractors.

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

The information pulled from MAED (a separate information system) to populate the automated form is presumed to be accurate. All other information that is provided by the COR or business manager is also presumed to be accurate as they have an interest in providing accurate information to ensure a smooth onboarding process. It is the COR or business manager’s responsibility to ensure the accuracy of the information.

CONNECTIONS TO OTHER MODULES WITHIN SERVICENOW AND CFTC SYSTEMS

The ServiceNow HR Form 719 Automation ServiceNow App has connections to the following:

- CFTC Entra ID (Active Directory)
- ServiceNow MID Server

- MAED

RELEVANT SORNS

OPM/GOVT-1, General Personnel Records, 77 Fed. Reg. 79694 as modified by 87 FR 5874 and 88 FR 56058.

CFTC-35, General Information Technology Records, 81 FR 67327.

NOTICE

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

CFTC staff information within the HR Form 719 Automation ServiceNow App is collected from MAED (a separate CFTC Information system), and from COR or business managers. Notice and consent indirectly occurs when an individual accepts employment with the CFTC and provides their information but no direct notice is provided regarding the Form 719.

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

No. Individuals do not have the opportunity to consent to the inclusion of their information on Form 719. It is required of the CORs and Business Managers to enable effective onboarding.

RECORD RETENTION

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 within HR Form 719 Automation ServiceNow App are governed by the following General Records Schedules:

- GRS 3-2-030 System access records - Systems not requiring special accountability for access

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

Records are kept in accordance with their applicable retention schedules as identified above. The records are retained under Disposition Authority DAA-GRS-

2013-0006-0003 which requires that the records within the HR Form 719 Automation ServiceNow App will be destroyed when business use ceases.

REDRESS

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

For the CFTC staff information within the HR Form 719 Automation ServiceNow App, CFTC staff may request access to records about themselves that are included in the relevant systems of records by following the procedures outlined in the respective SORNs.

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

For the CFTC staff information within the HR Form 719 Automation ServiceNow App, CFTC staff may request amendment of records about themselves that are included in the relevant systems of records by following the procedures outlined in the respective SORNs.

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

The procedures for submitting a request to correct information are outlined in the applicable SORNs.

Privacy Impact Analysis:

No additional specific risks have been identified for this module.

Appendix F: ServiceNow Qualys Integration for Vulnerability Management

PURPOSE

The ServiceNow Qualys Integration allows the CFTC to automate and streamline their vulnerability management process. Qualys sends vulnerability information to ServiceNow and the information is used to create tickets and update the dashboard information.

No PII is within the system as Qualys does not identify the various data formats/patterns that would indicate PII.

The key features of ServiceNow's App Engine include:

- Vulnerability Identification: Identifies security vulnerabilities in the IT infrastructure.
- Remediation Tracking: Manages and tracks the remediation of vulnerabilities.