PRIVACY IMPACT ASSESSMENT—AUGUST 2023

ServiceNow Cloud Platform General Support System (GSS)

Does the CFPB use the information to benefit or make a determination about an individual?	No
What is the purpose?	Provide automation, resource management, and shared support services.
Are there controls to enforce accountability?	Yes, all standard CFPB privacy protections and security controls apply.
What opportunities do I have for participation?	Opportunities for notice, consent, access, and redress are documented in this this PIA and related SORNs.

cfpb Consumer Financial Protection Bureau

Overview

The Dodd-Frank Wall Street Reform and Consumer Protection Act (the Act), Public Law No. 111-203, Title X, established the Consumer Financial Protection Bureau (CFPB). CFPB performs a range of functions including, but not limited to, supervising and enforcing financial entities, conducting research on financial markets, and collecting and responding to consumer complaints. Numerous administrative processes, such as human resource recruiting and hiring management, information technology (IT) help desk support, change management, and workplace management, support these CFPB functions. To efficiently manage these internal administrative functions, CFPB leverages ServiceNow.

ServiceNow is a third-party, cloud-based software-as-a-service (SaaS) platform that provides customizable, out-of-the-box applications to automate repeatable day-to-day activities. CFPB's use of ServiceNow is authorized by Sections 1011, 1012, and 1021 of the Dodd-Frank Act. Information in ServiceNow is collected in accordance and compliance with the Dodd-Frank Act, the Paperwork Reduction Act (PRA), and the Privacy Act of 1974. The platform is a Federal Risk and Authorization Management Program (FedRAMP) High authorized cloud environment, providing a security and privacy-compliant environment for CFPB applications and data to reside.

CFPB uses ServiceNow's applications to build and automate tasks and workflows that provide fast and reliable access to CFPB's internal IT data and services, such as:

- Supporting CFPB's IT Service Desk through ticket management and solution processes.
- Automating human resource (HR) workflows by providing a single platform for CFPB HR services.
- Centrally managing the lifecycle of all changes to IT services to minimize service disruptions.
- Managing and tracking security incidents and privacy breach response, which includes supporting the identification and logging of reported events, classifying and prioritizing reported events, assigning reported events to appropriate users or groups, and resolving reported events.
- Planning, prioritizing, and tracking internal projects.
- Supporting employee and contractor health and safety.
- Managing and responding to audit, compliance, and risk management requests.
- Providing automated facilities management services to schedule and reserve workstations, meeting rooms, and collaboration resources.

ServiceNow collects personally identifiable information (PII) of CFPB staff (employees, contractors, detailees, volunteers, employment candidates, and interns) for administrative functions, service desk capabilities, and human resource-related purposes. The PII used by ServiceNow depends on the application and process, but typically includes the following:

- First name;
- Last name;
- Employee ID;
- Email address (work and personal);
- Division and Office;
- Manager/Supervisor information;
- Phone number (work and personal);
- Office location; and
- Contracting officer representative (COR) – if the user is a contractor.

Additional PII that's collected to support the various applications may include, but is not limited to (see Section 2 for more information applications):

- Address (work and home);
- Work region;
- Job title;
- Salary (pay band/range, base salary, and total salary);
- CFPB start date;
- Years of experience; and
- Resume information (past experience - start/end date, former employers, title, hours, etc.).
- Audit management applications may collect evidence from program offices which may include other limited sensitive PII during CFPB's internal audits.

CFPB is conducting this Privacy Impact Assessment (PIA) to document the collection, use, and maintenance of PII in ServiceNow. CFPB applications are developed and managed through CFPB's Change Control Board (CCB) processes and Assessment and Authorization (A&A) documentation. Privacy is addressed within application development to include functional requirements analysis, data governance reviews, detailed design reviews, alternatives analysis, feasibility analysis, benefits/cost analysis, and privacy risk assessments for each ServiceNow application.

Because CFPB continues to develop use cases for different ServiceNow applications,[1] this PIA covers both CFPB applications currently operating on this platform as well as planned applications and data collections in the near future. When an application is added that collects new types of PII in a way that is not identified in this PIA, this new type of collection will be documented as an update to this PIA. CFPB's authority to collect specific information and routine uses of those records are identified in this PIA and Office of Personnel Management (OPM) System of Records Notice (SORN) GOVT-1, General Personnel Records, OPM SORN GOVT-5, Recruiting, Examining, and Placement Records, CFPB.014, Direct Registration and User Management System SORN, CFPB.009, Employee Administrative Records System SORN, and CFPB.029, Public Health and Safety SORN.[2] The PRA does not apply to ServiceNow as the environment sources staff PII from CFPB's internal database, and it does not ask "identical" questions of ten or more persons as per 5 CFR 1320.3(c).

Privacy Risk Analysis

The primary risks associated with PII covered by this PIA are related to the following:

- Purpose of Collection
- Data Minimization
- Security
- Limits on Uses and Sharing of Information
- Accountability and Auditing

Purpose of Collection

CFPB uses ServiceNow to build and operate a number of different applications that help CFPB conduct its internal business processes. There is a risk that CFPB staff PII within ServiceNow is used beyond its intended collection purpose. CFPB mitigates this risk by assessing proposed

[1] An example is utilizing a ServiceNow application to support the creation and management of compensation determination requests in accordance with 2022 Agreement on Compensation Reform Pay Reset.

[2] See https://www.consumerfinance.gov/privacy/privacy-impact-assessments/ for a list of CFPB PIAs and https://www.consumerfinance.gov/privacy/system-records-notices/ for a list of SORNs.

collections of PII to determine the appropriate legal authority to collect the information. In addition, CFPB mitigates risk by confirming that the proposed uses of PII are consistent with a specific, documented purpose and applicable SORN. This confirmation is achieved through project evaluations, CFPB CCB reviews, and other A&A processes to ensure that proposed uses of PII align with existing compliance and development documentation. CFPB also addresses privacy implications during an application development lifecycle. The application development lifecycle includes detailed documentation reviews, which guarantee that privacy risk is managed throughout the development lifecycle. In addition, applications are continuously monitored to ensure that the purpose of collection remains consistent.

Data Minimization

ServiceNow uses the PII collected to internally support CFPB's administrative functions, service desk capabilities, and human resource-related activities. For Service Desk functions, CFPB leverages ServiceNow's out-of-the-box solutions, such as template web forms and standard workflows, that can be used to collect service-related information. These internal web forms may contain data collection fields requiring more PII than necessary to complete a business need. As a result, there is a risk that unnecessary or irrelevant PII may be collected and stored within the platform. CFPB mitigates this risk by assessing proposed uses of standard web forms and workflows and the intended purposes for collecting PII so that ServiceNow collects only the minimum amount of PII required to accomplish the stated purpose. For example, the customization of data fields limits the amount of PII entered by individuals to the minimum amount necessary. If more than the necessary amount of PII is provided, the environment employs processes to remove unnecessary PII before using the data to conduct program activities.

Security

ServiceNow and its applications may be a target for unauthorized access and insider threats. To mitigate this risk, ServiceNow is subject to the appropriate technical, physical, and administrative controls or safeguards as prescribed by federal security and privacy guidelines (e.g., Federal Information Security Modernization Act (FISMA), National Institute of Standards and Technology (NIST) Special Publications, and CFPB policies and procedures). Through this process, safeguards such as encryption for PII maintained within the platform are implemented to reduce the overall risk to the PII in transit or at rest. In addition, security and privacy controls are implemented through a layered approach to restrict access to PII to authorized individuals. CFPB has also implemented security tools to scan ServiceNow to detect malware, phishing, spam, and unsafe links. The ServiceNow Cloud utilizes audit logs for selected user transactions specified by CFPB standards. Security risks are further mitigated by role-based access controls implemented for the ServiceNow platform. This protects sensitive data and ensures employees can only access information and perform actions they need to do their jobs.

Although access to PII is limited to authorized individuals, there is a risk that ServiceNow might lack granular access controls. For example, all personnel with IT service delivery (ITIL) roles have the same access levels to all tickets, including those not assigned to them. CFPB mitigates this risk through implementation of field-level controls that allow access to be further limited to specific data fields. Moreover, CFPB staff who utilize ServiceNow applications to collect, use, share, maintain, and disseminate PII are made aware of their roles and responsibilities through annual and role-based training for protecting PII. Access to ServiceNow follows the principle of least privilege and is strictly maintained by the program leadership via system owner reviews of privileged user access requests (PUAs) to determine the type of access required before authorized individuals gain access.

As a result of this assessment, CFPB's Privacy team is now part of governance and project working groups to assess the privacy implications of systems and applications developed within the ServiceNow platform.

Limits on Uses and Sharing of Information

ServiceNow allows PII to be used in different ways by different applications and workflows. For example, CFPB divisions and offices may request to implement an application that automates a business need but may use existing PII to perform the workflow task. As a result, there is a risk that PII could be exposed to unauthorized individuals who might have access to the platform but are not authorized to use all PII contained within the environment.

CFPB mitigates this risk by ensuring that CFPB staff who use ServiceNow applications to collect, use, share, maintain, and disseminate PII are made aware of their roles and responsibilities through annual and role-based training for protecting PII. CFPB staff undergo specific training such as ServiceDesk training implemented to ensure users are aware of their responsibilities for protecting PII. Further, despite the risk of lack of granular access control as described above, CFPB implements field-level controls to limit access to specific PII data fields.

ServiceNow connects with other CFPB cloud environments to share and store data. For example, CFPB's SailPoint[3] allows CFPB staff PII to be pushed to and from ServiceNow. Information may

[3] SailPoint is an identity management platform used for providing and managing access to CFPB systems. It is covered by the Identity, Credential and Access Management (ICAM) PIA found at https://files.consumerfinance.gov/f/documents/cfpb_icam_pia_2023-03.pdf

also be shared with other applications to support the resolution of requests. As a result, there is a risk that an unauthorized individual may access PII stored within the environment or that a breach within CFPB may impact ServiceNow applications. CFPB mitigates this risk by only sharing PII with other CFPB system and application environments that have achieved an Authority to Operate (ATO). CFPB also assesses connections between other cloud environments to apply role-based environment access controls to ensure the security and privacy of the interconnection. Any proposed data sharing between the cloud environments is also assessed to ensure that only authorized individuals can access data within ServiceNow.

Accountability and Auditing

The ServiceNow environment hosts various business applications with different use cases for PII collection, sharing, and maintenance. Due to the various business applications, the platform maintains different amounts and types of PII for different purposes. As a result, there is a risk that unauthorized individuals may inadvertently access PII. To mitigate this risk, individuals with access to ServiceNow must complete annual role-based training on proper ways of handling CFPB PII and information security. Additionally, internal and independent auditors hold CFPB accountable for complying with CFPB policies and procedures related to processing PII.

CFPB 's Rules of Behavior (RoB) provide guidance and specific rules on the appropriate use of CFPB information systems for individuals granted access to ServiceNow. Individuals must review, acknowledge, and sign CFPB's RoB. Individuals are also only authorized to receive the minimal access required to accomplish assigned core job functions. Individuals requiring privileged access must receive system owner approval by completing a PUA before granting such access. CFPB is committed to taking swift and immediate action if we uncover any violations of law, policies, and procedures.

The technical, physical, and administrative controls implemented to promote individual participation, minimization, and accountability are appropriate and implemented within the ServiceNow platform.

Privacy Risk Management

1. Describe what information the CFPB collects, how the information is collected, and the sources from which the information is collected.

The PII for ServiceNow users is collected directly from CFPB staff or from existing human resource databases. Information captured for HR purposes is collected through account creation and access forms completed by individuals as part of the hiring and onboarding process for CFPB. The information is then shared with SailPoint, which verifies that CFPB staff is authorized to access IT resources. Sharing and syncing user information between SailPoint and the ServiceNow platform enables CFPB staff to request access to applications within ServiceNow.

ServiceNow collects PII from CFPB staff in various ways, depending on the specific application. For example, the Service Desk collects PII through web forms, email, and phone calls when CFPB staff requests service support. Further, OHC may manually enter other HR-related information in their databases that are not automatically synced via SailPoint to support specific activities such as compensation determination. Most applications on the ServiceNow platform typically utilize PII, including:

- First name;
- Last name;
- Employee ID;
- Email address (work and personal);
- Division and Office;
- Manager/Supervisor information;
- Phone number (work and personal);
- Office location; and
- Contracting officer representative (COR) – if the user is a contractor.

Additionally, some applications may require specific PII to fulfill their intended purpose. This PII may include the following:

- Address (work and home);
- Work region;
- Job title;
- Salary (pay band/range, base salary, and total salary);

- CFPB start date;
- Years of experience; and
- Resume information (past experience - start/end date, former employers, title, hours, etc.).

Also, evidence provided during CFPB's internal audits may include other PII such as the financial account and biographic information of members of the public used for that limited purpose. The Office of Inspector General (OIG) requires a full and complete record of evidence as artifact. PII is retained in accordance with specific program office's retention schedule as documented in its PIA and only accessed by authorized CFPB internal auditors and program points of contact.[4]

CFPB staff working remotely to support routine work and business communications may also provide personal contact information such as home address or personal mobile phone. The information described above is the minimum amount necessary to access ServiceNow. Specific uses of PII by ServiceNow's applications are reviewed on a case-by-case basis to ensure PII is minimized to the amount necessary to achieve its intended purpose.

2. Describe the CFPB's objective for the information.

ServiceNow uses PII collected from CFPB staff to support internal administrative, service desk, and human resource-related functions. Such applications include:

- CFPB's Service and Support Portal (Service Desk): Supports technical service requests, reporting technical issues, knowledge management, incident reporting, facilities work orders, space reservations, and wayfinding.
- CFPB's Human Resource Service Delivery (HRSD): Performs HR services such as compensation determination, telework arrangements, and CFPB Next (i.e., return to work) programs. It allows employees, supervisors, and OHC to submit, view, and manage employee-preferred work schedules, location, and designation.
- Information Technology Service Management (ITSM) Application: Performs HR tasks not covered under the HRSD application, such as onboarding, offboarding, internal moves and transfers, etc.

[4] As an example, the Consumer Response office uses ServiceNow's Audit Management application to manage audits of consumer complaints. This will require a full and complete record of evidence as an artifact which may occasionally contain sensitive PII. This specific use is covered by the Consumer Response PIA.

- CFPB Safe Workplace Applications: Supports CFPB staff and contractor health and safety. The applications utilized include Employee Health Screening, Employee Readiness Surveys, Employee Travel Safety, Workplace Safety Management, etc.
- Privacy Breach Response: Supports the Privacy team in tracking and processing privacy breaches from discovery and initial analysis through remediation, mitigation, post-breach review, and closure.
- Cybersecurity Incident Management: Supports the identification and logging of incidents, classifying and prioritizing incidents, assigning incidents to appropriate users or groups, and resolving incidents.
- Workspace Management: Allows CFPB staff to schedule and reserve workstations, meeting rooms, collaboration resources, and submit facility work orders.
- Change Management: Controls the lifecycle of all changes to IT services undertaken by CFPB.
- Strategic Portfolio Management (SPM): Allows CFPB staff to plan, prioritize, and track work with capabilities such as project portfolio management, agile management, and application management to align work to business objectives.
- Integrated Risk Management (IRM): Allows CFPB to manage and respond to business risks quickly. Applications developed include Audit Management, Policy & Compliance Management, and Risk Management.
- Security Operations Management (SecOps): Allows CFPB to record and respond to security incidents and vulnerabilities.
- Information Technology Operations Management (ITOM): Automates discovery of hardware and software for the Configuration Management Database (CMDB).

ServiceNow collects and uses the minimum PII to perform these tasks. When a program needs to collect PII, CFPB assesses the design and purpose of the system and its use to collect, use and store PII. This assessment is completed by a review of ServiceNow's design documents and conducting this PIA to determine whether CFPB has an authorized purpose to collect and use the information, and to ensure that PII used is both relevant and necessary to its intended purpose.

3. Describe how the CFPB shares any of the information with third parties with whom the CFPB shares the information for

compatible purposes, e.g., federal or state agencies, the public, etc.

CFPB may externally share information collected and maintained by ServiceNow on a case-by-case basis as needed to manage CFPB's core business functions in ServiceNow. OHC may also use personnel-related information within ServiceNow to generate reports for Equal Employment Opportunity reporting purposes and responding to Freedom of Information Act requests. In instances where CFPB may have to share PII maintained within ServiceNow with external third parties, that information is only shared with consent from the impacted individuals or when CFPB otherwise pursuant to routine uses published in our SORNs. Sharing of this information by CFPB is covered by and consistent with the routine uses published in, where applicable, the following SORNs: OPM SORN GOVT-1, General Personnel Records; OPM SORN GOVT-5, Recruiting, Examining, and Placement Records; CFPB.014, Direct Registration and User Management System; CFPB.009, Employee Administrative Records System; and CFPB.029, Public Health and Safety [5].

4. Describe what opportunities, if any, individuals to whom the information pertains have to (a) receive notice regarding the CFPB's use of the information; (b) consent to such use; (c) access the information that pertains to them; or (d) obtain redress.

CFPB does not use ServiceNow to collect PII directly from the public. CFPB provides privacy notice to CFPB staff at the point of PII collection, typically during staff onboarding and at the time ServiceNow accounts are subsequently created. A Privacy Notice is also provided within specific CFPB ServiceNow applications to inform staff of why the information is collected and how it is used by that application. CFPB also publishes SORNs and PIAs to inform individuals about the purposes of the collection and how they can access the information used by a particular ServiceNow application.

Where applicable, CFPB allows individuals to request access and amendment to their PII in accordance with the Privacy Act and CFPB's Privacy Act regulations at 12 C.F.R. 1070.50 et seq. Information about Privacy Act requests is published in the associated SORNs. Employees and contractors may also be able to update their information directly.

[5] See https://www.consumerfinance.gov/privacy/privacy-impact-assessments/ for a list of CFPB PIAs and https://www.consumerfinance.gov/privacy/system-records-notices/ for a list of SORNs.

For additional information and analysis related to specific systems, applications, and data collections, applicable SORNs, and individual system/application PIAs are available at www.consumerfinance.gov/privacy.

5. Explain the standards and relevant controls that govern the CFPB's—or any third-party contractor(s) acting on behalf of the CFPB—collection, use, disclosure, retention, or disposal of information.

CFPB manages risks to privacy by complying with the Privacy Act of 1974 and the E-Government Act of 2002; adopts Office of Management and Budget privacy-related guidance as best practice and applies National Institute of Standards and Technology risk management processes for privacy. CFPB conducts a complete security review of the ServiceNow platform based on all applicable federal laws, directives, and standards. CFPB develops and follows a Security Implementation Plan (SIP) identifying the necessary procedures for PII use within each application developed on the platform. ServiceNow maintains an ATO and is hosted and stored in the ServiceNow Government Community Cloud (GCC), which has an Agency FedRAMP High Authorization. Additional controls have been implemented around personnel management in the ServiceNow GCC. Direct access to applications inside of the GCC is restricted to U.S. citizens within the United States. A dedicated team has been established to handle customer technical support for the GCC. Personnel on the customer technical support team servicing the GCC are U.S. citizens residing in the U.S.

All CFPB Federal and Contractor staff are automatically granted access to ServiceNow when onboarded. This allows a basic level of access to ServiceNow to submit incidents, service requests, facilities work orders, and workstation reservations. For non-privileged access beyond those granted to standard users, CFPB follows the User Access Request (UAR) process. Similarly, the PUA process is followed to request elevated or privileged roles in ServiceNow. All users are required to complete mandatory privacy and security training and additional training before gaining access to the ServiceNow platform or any applications within the platform. Users must also complete the user agreement outlining their roles and responsibilities in using the platform and its information. Privacy is carefully considered when applications are developed within the ServiceNow platform to ensure the application design aligns with CFPB's authority to collect, use, maintain, and share PII. Privacy reviews are part of each application design, change, modification, or upgrade to the ServiceNow platform.

CFPB's ability to use ServiceNow involves the appropriate security and privacy controls implemented, tested, and reviewed as part of the agency's information security and privacy programs. These services are subject to the FISMA implementing standards and the most current CFPB regulation guidance.

The unique capabilities of ServiceNow require consistent risk management and continuous monitoring processes. These processes are subject to and maintained by CFPB's Security and Privacy Continuous Monitoring Strategies, which allow for consistent, substantive reviews of the security and privacy controls to ensure the security of the platform and the privacy of the PII residing within it.

CFPB develops applications within ServiceNow using an agile development process to ensure design feasibility and to complete necessary security and privacy compliance requirements prior to implementing the application for use. ServiceNow does not mask or strip direct identifiers but enforces user access controls that ensures access to specific information is based upon a defined role or responsibility. User identities and access rights remain properly managed, secure, and monitored. As a result of this PIA, the ServiceNow platform has been assessed to determine how its applications provide a more secure, automated approach to business operations. Further, due to this PIA, CFPB’s Privacy team is now part of governance and project working groups to assess privacy implications with the use of PII within ServiceNow.

The following technical and administrative controls secure the PII and provide accountability for CFPB's appropriate collection, use, disclosure, and retention of personal information:

- Audit logs and reviews are in place to identify, review, and assess unauthorized access to the ServiceNow platform and the data within its applications.
- CFPB general and role-based privacy training is required prior to granting access to the ServiceNow platform and any applications within the platform. Role-based training includes data handling procedures, incident and breach response procedures, and CFPB's authority to collect and use information in accordance with its regulations.
- CFPB incident response procedures and privacy breach response procedures are in place to address incidents involving data residing in the ServiceNow platform.
- Data quality and integrity checks are performed in accordance with CFPB’s Data Access Policy for any systems using data within the environment.

- Compliance with CFPB cybersecurity policy and procedures is documented within security and privacy implementation plans.
- Role-based Access Controls: CFPB is responsible for assigning and maintaining roles and permissions within ServiceNow and its applications based on an individual's role within the organization and as approved by CFPB Cybersecurity. The following lists examples of the roles and responsibilities within ServiceNow:
    - System Administrator role – A privileged role granted to authorized CFPB staff, giving them full access to manage configuration settings within the ServiceNow platform and manage user account privileges and permissions.
    - Security Administrator role - A privileged role granted to authorized CFPB staff that allows users to update High Security Settings.
    - ITIL role - Performs standard actions for IT service management, including opening, updating, and closing incidents, problems, changes, and configuration management items. By default, only users with the ITIL role can have tasks assigned to them.
    - ITIL Administrator role - Possesses more privileges than the ITIL role and is intended for team leads. This role can delete incidents, problems, changes, and other related entities when the ITIL and ITIL administrator roles are assigned.
    - CFPB Basic User roles - These roles are assigned to all CFPB staff granted access to application(s) on the ServiceNow platform. Permissions are based upon assigned business functions (e.g., COR, Examiner, Investigator, Stakeholder Support, etc.), and security configurations are based on their business and security needs within a specific application.
    - Service Account roles - Service account roles are specific non-system administrator user accounts assigned to authorized CFPB staff. These roles could include roles for the different HR Service Delivery applications organized by administrator, manager, timekeeper, and user roles.
    - Security Incident roles: Responsible for detecting and responding to security incidents as Security Incident Administrators, Analysts, or other individuals working on incident response tasks.
    - Approval Administrator role - This role allows assigned CFPB staff to view or modify approval requests not directly assigned to them.

- SPM roles – These roles depend on the functions within the specific SPM application. They are organized by administrator, manager, and user roles for Project and Portfolio Management, Demand Management, Agile Development, and Test Management applications.
- IRM roles – These roles depend on the different IRM applications organized by administrator, manager, and user roles for Audit Management, Policy & Compliance, and Risk.
- Knowledge Administrator role – Manages the knowledge base by creating, editing, and reviewing knowledge base articles.

- National Archives and Records Administration (NARA) has approved the following records schedules for ServiceNow:
  - Employee Separation Records covers the offboarding function within the OHC ITSM Application; authority: DAA-GRS-2014-0004-0004.
  - Program Management Records covers the various administrative applications within ServiceNow; authority: N1-587-12-6.
  - Facility, Space, Vehicle, Equipment, Stock, and Supply Administrative and Operational Records covers the Workspace Management function; authority: DAA-GRS-2016-0011-0001.
  - Administrative Help Desk Records covers CFPB's use of the Service Desk function; authority: DAA-GRS-2017-0001- 0001.
  - Employee Health and Safety Records covers CFPB's Safe Workplace applications; authority: DAA-GRS-2021-0003-0001.
  - Information Systems Security Records; Privacy and Cybersecurity Incidence Response Information covers the Privacy Breach Response, Cybersecurity Incident Management, and SecOps functions; authority: DAA-GRS-2013-0006-0002.
  - Common Office Records covers the HRSD as well as various administrative functions; authority: DAA-GRS-2016-0016-0001.
  - General Technology Management Records to cover the ITOM, SPM, IRM, Change Management, and some ITSM functions; authority: DAA-GRS-2013-0005-0010.
- Personnel Security, including background checks, is completed for all CFPB employees, contractors, or other individuals authorized to conduct CFPB activities within ServiceNow.

CFPB may use contractors to help support the collection, use, disclosure, or retention of information covered by this PIA, and those contractors are subject to similar controls. For example, contractors with access to direct identifying PII must report suspected or confirmed privacy incidents to CFPB immediately and no later than one hour after discovery. Other requirements placed on contractors may include training on privacy and compliance with federal privacy requirements and Federal Acquisition Regulations (FAR).

6. Discuss the role of third party(ies) that collaborate or partner with the CFPB, if any. Identify any controls used to protect against inappropriate collection, use, disclosure, or retention of information. (This does not include third parties acting on behalf of the CFPB, e.g., government contractors discussed in Question 5.)

ServiceNow allows CFPB to connect CFPB-authorized third-party vendor services, such as CFPB's SailPoint and Splunk, to the platform to support enhanced performance, increased security, data storage needs, and data analytics and visualization capabilities from other CFPB cloud environments. SailPoint is the primary mechanism by which employee information and attributes are synchronized with ServiceNow. It is the identity information management system that manages CFPB's Active Directory for creating and removing users in ServiceNow. This connection allows employee information within SailPoint to be pushed to ServiceNow whenever updated. Also, connection to Splunk facilitates security logging to monitor authorized access to the platform. CFPB may also leverage tools and services within ServiceNow to support various IT requests initiated by employees. These requests may be routed through other third-party vendors for fulfillment.

To identify and mitigate risks before deployment or integration, all third-party cloud systems or environments connecting with ServiceNow are assessed according to CFPB's A&A processes. In addition, CFPB reviews the terms of use and licensing agreements of connecting systems to ensure they do not create a risk to the PII that resides within ServiceNow.

Any hosted applications that support or are developed within ServiceNow are managed through a project governance lifecycle where CFPB's security and privacy teams assess the scope and design of the application to ensure compliance with CFPB policies and procedures, including any tools and components selected from ServiceNow. ServiceNow connects with CFPB-approved third-party cloud services, such as SailPoint and Microsoft O365. In addition to CFPB vetting applications and validating security controls, ServiceNow provides additional application verification before admittance to the platform. Typically, third-party tools and service providers must also be assessed to identify the necessary security and privacy controls that must be implemented and achieve a separate ATO before connection to ServiceNow. Depending on the connection typical controls include:

- Memoranda, information sharing agreements, and authority to use describe the collection, use, maintenance, and sharing of any PII contained within ServiceNow;
- Documented compliance with CFPB cybersecurity policy and procedures;
- Data Quality and Integrity Checks;
- Audit logs and reviews policy and standard operating procedures;
- Role-based access controls within the platform and the applications that reside within the platform.

Document control

Approval

CHRISTOPHE
R CHILBERT

Digitally signed by
CHRISTOPHER CHILBERT
Date: 2023.08.28 14:41:20
-04'00'

Chris Chilbert

Chief Information Officer

Date

KATHRYN
FONG

Digitally signed by
KATHRYN FONG
Date: 2023.08.28
15:43:03 -04'00'

Kathryn Fong

Chief Privacy Officer

Date

WILLIAM
BIRD

Digitally signed by
WILLIAM BIRD
Date: 2023.08.28
13:27:12 -04'00'

Bill Bird

Initiative Owner

Date