Supervision and Examination System (SES) PIA

Does the CFPB use the information to benefit or make a determination about an individual?	No.
What is the purpose?	To carry out its supervision activities.
Are there controls to enforce accountability?	Yes, all standard CFPB privacy protections and security controls apply.
What opportunities do I have for participation?	Generally applicable: Appropriate opportunities for notice, consent, access, and redress.

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). The CFPB administers, enforces, and implements federal consumer financial protection laws and protects consumers from unfair, deceptive, and abusive practices when obtaining consumer financial products or services. One of the CFPB's primary responsibilities is supervising entities that provide consumers with financial products or services, such as loans or deposit accounts. The CFPB has supervisory authority over multiple depository entities with over $10 billion in assets and includes large banks, credit unions, and their affiliates. It also has authority over non-depository entities including mortgage entities, brokers and servicers, payday lenders, and private education lenders[1]. The CFPB supervises entities by gathering and evaluating information, which can include PII, to determine if they are in compliance with federal consumer financial laws.

The CFPB uses the Supervision and Examination System (SES) to conduct its supervision activities and facilitates the collection and sharing of relevant information. CFPB also uses it as an information repository for compliance rating information. Outcomes from a supervisory activity can include an Examination Report, which contains a compliance rating that reflects the CFPB's assessment of the effectiveness of the institution's compliance management program to ensure compliance with consumer protection laws and regulations and reduce the risk of harm to consumers.

The SES resides within the Salesforce[2] cloud platform and leverages the capabilities of the cloud architecture including the automated collection of information requests, concurrent collaboration between internal assessments, and tracking of document reviews during the examination process. The SES established the CFPB Supervision Portal to facilitate the secure exchange of communication and files between external entities and state regulators. This portal allows authorized entity representatives to view and respond to requests for information, data, and documentation from state regulators. Identification and provisioning of these entity representatives is completed within the SES application by limited sets of CFPB users designated

[1] See 12 U.S.C. §§ 5514-5516.

[2] See https://files.consumerfinance.gov/f/documents/cfpb_salesforce-platform-cloud-environment_pia_2022-05.pdf

with permissions to perform the provisioning. Additionally, the SES securely connects to CFPB's Microsoft O365[3] SharePoint environment for further data processing and storage capabilities, centering around document management.

Though supervisory exams focus on the institution, not individual consumers, the CFPB may need limited access to consumer personally identifiable information (PII) to carry out its work. The majority of PII in SES is collected through examination requests where PII is indirectly part of an entity's response to CFPB. However, there are situations when the CFPB may directly contact consumers to verify their PII for accuracy and completeness.

The CFPB collects and maintains limited PII using SES including:

- PII about consumers who are past, present, or potential consumers of depository and non-depository entities under the authority of the CFPB.
- PII about entity employees who are submitters of the information requested by CFPB.
- PII about CFPB employees who are involved in the supervision process.

The type and extent of PII collected depends on the type of examination being conducted. Information collected through Supervision and Examination activities and maintained in the SES is covered by the following System of Records Notices (SORNs): CFPB.002 – Depository Institution Supervision Database and CFPB.003 – Non-Depository Institution Supervision Database[4].

The CFPB conducts this privacy impact assessment (PIA) to document its use of the SES and to identify associated privacy risks and mitigations. The scope of this PIA is limited to the privacy risks and technical controls associated with the maintenance and use of PII within the SES.
The SES collects data that are related to administrative actions, investigations, and/or audits.[5] The collected data are not subject to requirements of the Paperwork Reduction Act (PRA).

[3] See https://files.consumerfinance.gov/f/documents/cfpb_microsoft-cloud-gss_pia_2022-07.pdf

[4] See https://www.consumerfinance.gov/privacy/system-records-notices/ for a list of SORNs

[5] *See* 5 CFR 1320.4(a)(2).

Privacy Risk Analysis

The primary risks identified in this PIA are related to the following:

- Limits on Uses and Sharing of Information
- Individual Participation
- Data Minimization
- Security.

Limits on Uses and Sharing of Information

The CFPB examination personnel request information, which may include PII, from supervised entities to conduct supervision activities. There is a risk that the examination personnel may misuse the PII, or use the PII in a way that is inconsistent with the purpose of collection.

To mitigate this risk, the CFPB provides training to examination personnel prior to access to PII so they understand their responsibility in collecting, handling, and safeguarding the data. CFPB examination personnel must review the relevant policies and engage in other formal and non-formal training forums to learn how the CFPB business process works and how to appropriately use the information that is collected during examinations. For example, examination personnel are trained to securely store information pertaining to investigations in Microsoft O365 SharePoint, and not on individual IT system equipment assigned to them. Additionally, those with access to the SES receive training that includes a briefing on confidentiality before they are granted access to the system. This briefing includes a reminder to employees that the PII contained within the system may be subject to the Privacy Act.

Examination personnel are also required to conduct the examinations within a specified scope. Once the scope of the exam is set, the Examiner in Charge (EIC) works to customize the information requests for a particular entity. These requests are approved by senior management before sending to the entity. CFPB examination personnel also rely on role-based permissions in the SES to make sure that all information collected is used for its intended purpose.

PII within the SES may also be shared with other cloud environments for data storage and document collaboration. For example, the SES is built on the Salesforce[6] cloud platform and Microsoft[7] 0365 facilitates document collaboration and management for SES. CFPB's Amazon Web Services (AWS) environment also acts as a staging area for files that have not yet been virus-scanned pending transfer to Microsoft O365. This presents a risk that PII stored within another cloud environment may be accessed by an unauthorized individual or that a breach within the cloud environment may impact business operations within the SES.

The CFPB mitigates this risk by sharing the SES data only with systems that have achieved an Authority to Operate (ATO) based upon the CFPB A&A processes. Connections between other cloud environments are assessed by the CFPB 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 only authorized entities can access data within the SES. The CFPB also configures security controls at a granular level within each application to prevent sharing of PII externally. For example, CFPB disables external sharing within Microsoft O365 SharePoint, prohibiting any linked document from being opened outside the CFPB environment.

Individual Participation

The PII collected in SES is typically provided by an entity pursuant to applicable laws and regulations, rather than directly by consumers. Consumers therefore do not have opportunities to opt out or decline to share PII in this context, and there isa risk that individuals are not aware that their information is collected by CFPB, and that CFPB cannot provide a way for individuals to access records that are submitted by supervised entities. However, given the nature of the information collection, the PII included in the SES cannot be accessed or amended by the public because allowing access would jeopardize a pending CFPB examination, investigation, or enforcement action. This risk is acceptable because the supervision of entities is required by the Dodd-Frank Act, the CFPB needs to request information from entities that may contain PII to sufficiently meet this statutory requirement, and PII in the SES system is not collected for the purpose of analyzing specific consumers.

[6] See https://files.consumerfinance.gov/f/documents/cfpb_salesforce-platform-cloud-environment_pia_2022-05.pdf

[7] See https://files.consumerfinance.gov/f/documents/cfpb_microsoft-cloud-gss_pia_2022-07.pdf

Furthermore, CFPB offers a means through the Privacy Act for individuals to access, amend, or correct, their records at their request. However, PII in the SES cannot be accessed or changed if doing so would impact the CFPB's ability to supervise an entity or if doing so would harm a pending investigation or enforcement action. Information about Privacy Act requests is available in the SES SORNs, CFPB.002 – Depository Institution Supervision Database and CFPB.003 – Non-Depository Institution Supervision Database for the SES and at https://www.consumerfinance.gov/foia-requests/.

Data Minimization

There is a risk that documents or other information provided by entities to the CFPB during the examination process may include unnecessary PII about consumers or employees of the entity. To help mitigate this risk, the CFPB trains examiners to collect only relevant and necessary information, as well as how to properly handle and protect sensitive, confidential, and personal information. Examiners must complete the confidentiality and privacy briefing when they initially onboard and on an annual basis thereafter. Where practicable, the CFPB uses de-identified information or information that does not contain name or other direct identifier of the consumer to conduct the examination. The CFPB works directly with the entities it supervises to limit the amount of sensitive information shared during the examination process.

Security

There is a risk that the substantial amounts of information on consumers and their financial transactions in the SES may be a target for hackers, identity thieves, and other cyber threats. The CFPB mitigates this risk by implementing extensive security controls and safeguards for the SES and the GSS that hosts it to protect the information in the system against unauthorized disclosure and access. All employees at CFPB are required to use a Personal Identity Verification (PIV) card to log into their device. After logging in, examination personnel may log in to the SES utilizing ingle sign on and two factor authentication methods. Once they attempt to sign in the user is prompted via Okta Verify on their CFPB-provided cellphone to confirm they did make that action. This then allows the user into the system.

There is also a risk that unauthorized individuals may gain access to the information in the SES. The CFPB mitigates this risk by only granting access to the system to authorized users who, based on their need to know, will be restricted to the minimal amount of PII required or appropriate to carry out their assigned job responsibilities. Access is terminated or reduced as necessary should the authorized CFPB staff no longer have a need to know the information, change job functions, is terminated, or resigns.

In addition, the CFPB issues authorized personnel non-transferable usernames to SES as required for fulfilling official duties. This access is only issued after employees have completed the system's training seminar, which includes confidentiality and privacy briefings. Since access to all information included in the SES may not be necessary for all CFPB employees with supervision responsibilities, the system has unique user roles. For example, employees who supervise other employees with examination responsibilities may require access to human resources systems associated with scheduling, whereas employees tasked with non-examination duties may not require such access. The user roles assigned to each employee when they are granted access to the system reflect their individual needs for information in the system.

The CFPB is also aware of the importance of interconnection security. As mentioned in previous sections above, the CFPB only shares SES data with systems that have achieved an ATO based upon the CFPB A&A process. The SES connections with cloud environments are assessed by role-based environment access controls.

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

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 SES contains PII regarding consumers of depository and non-depository entities products as well as employees of those entities serving as points of contact. It also contains information about CFPB staff assigned to duties related to the supervision of these entities. CFPB staff collectively refers to employees, contractors, detailees, consultants, volunteers, and interns. The PII collected by the SES is indirectly requested from entities the CFPB supervises. The CFPB also collects PII directly from consumers of supervised entities, from consumer complaints, and from employees of the CFPB. The CFPB may use PII to contact consumers to collect and verify additional information required for supervision activities. The CFPB is required by statute to primarily use, to the fullest extent possible, information available from other agencies or reported publicly before contacting the supervised entity to gather additional information.

Depending on the type of examination, consumer PII may be provided by the entity in response to a request for information by CFPB. PII may include, but is not limited to:

- Names
- Account numbers
- Addresses
- Phone numbers
- Email addresses
- Transactional histories
- Information related to complaints they have filed with the CFPB through the Consumer Response System[8].

Additionally, PII such as unsolicited social security numbers and dates of birth may sometimes be provided by entities even though the CFPB does not request it as part of information requests during examinations. When it is necessary to request consumer information, CFPB will, generally, request de-identified consumer information such as demographic information, credit score, and loan information from supervised entities that is not associated with a consumer name or other elements of PII.

The sources where PII may be collected or included as part of CFPB's supervisory activities may include:

- Information collected from supervised entities used to monitor and assess risk and other potential issues.
- Prior scope summary, supervision plan, or similar document produced by state or prudential regulators.
- Prior examination reports/supervisory letters and supporting workpapers (internal and from prudential regulator(s), state regulator(s), or other agencies).
- Information about prior supervisory actions, consumer remediation, and responses to examination reports/supervisory letters.
- Information on enforcement or other public actions (if applicable).
- Correspondence from prudential or state regulator(s) and CFPB correspondence files.

[8] For more information on the CFPB's Consumer Response System, visit www.consumerfinance.gov/privacy.

- State licensing information for the entity.
- The CFPB consumer complaint database.
- Federal Trade Commission (FTC) Consumer Sentinel database.
- Uniform Bank Performance Report (UBPR) and call reports.
- Previous years' FFIEC Home Mortgage Disclosure Act Loan Application.
- Registers (Home Mortgage Disclosure Act Loan Application Register).
- Home Affordable Modification Program data.
- Fair lending analysis.
- Office of the Comptroller of the Currency (OCC) Federal Housing Home Loan Data System (FHHLDS) report.
- Mortgage Call Report (MCR) from the Nationwide Mortgage Licensing System (NMLS)
- Registration or licensing information for mortgage originators (Secure and Fair Enforcement for Mortgage Licensing Act (SAFE Act) from public information or third-parties.
- Institution securities filings, its offered securitizations, and similar public records.
- Industry publications showing credit ratings, product performance, and areas of profitability.
- Newspaper articles, web postings, or blogs that raise examination related issues.
- The Department of Housing and Urban Development's Neighborhood Watch System[9]: https://entp.hud.gov/sfnw/public/.
- Service provider programs.
- Content of the supervised entity's website.
- Current and former directors, officers, employees, agents, shareholders, and independent contractors of depository and non-depository entities.
- Current and former consumers of depository and non-depository entities.
- Current and former CFPB employees assigned to coordinate examinations, provide analysis, or other duties related to the supervision of these entities.

[9] Neighborhood Watch is intended to aid HUD/FHA staff in monitoring lenders and our programs, and to aid lenders and the public in self-policing the industry. *See* https://entp.hud.gov/sfnw/public/.

The system includes information about CFPB employees assigned tasks related to supervision. This may include examination scheduling information, login and use information related to the system, and workflow information. Information about CFPB employees and authorized contractor staff may include:

- Names
- Titles and/or roles within the CFPB
- Contact information such as work address, phone number, and email address.
- The elements of PII collected as part of an entities' submission detailing its interaction with a consumer.

PII requested by CFPB as part of the examination process is the minimum necessary to conduct examinations of a supervised entities' compliance management program and form conclusions about the regulated entity's practices in serving consumers.

2. Describe CFPB's objective for the information.

One of the CFPB's chief responsibilities is supervising entities that provide consumer financial products and services. The CFPB communicates with entities responsible for developing, selling, marketing, and administering these products and services, through entity point of contacts responsible for managing the entity and its legal compliance responsibilities. During these communications, CFPB examiners may collect PII about the entity employees to the extent necessary to identify them and to facilitate further communications. As part of the examination process, CFPB examiners review individual transaction records while determining whether an entity is conducting business in accordance with applicable federal laws. Those transaction records can contain PII about consumers who have been offered or who have purchased the products and services being examined. The records, including PII, are particularly important if the conclusion is that an entity has not been properly following the law, because in those instances, the CFPB may order the entity to correct its mistakes. For example, corrective actions may require identifying consumers whose accounts reflect non-compliance and taking specific steps to remedy the non-compliance.

Internally, the CFPB may share information from the SES, in the form of reports or through access to the system, with members of the enforcement and fair lending teams[10]. The CFPB only shares

[10] Please see CFPB's Certain Supervision, Enforcement, and Fair Lending (SEFL) Data Used for Market Research, https://www.consumerfinance.gov/f/201407_cfpb_PIA_certain-sefl-data-used-for-market-research.pdf

information with authorized users through secure channels, such as online portals like Microsoft O365 SharePoint or through encrypted email, and only with individuals what are authorized to review the reports.

3. Describe how 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.

The CFPB may share PII from the SES with other regulators with authority over the entity in order to help those agencies fulfill their statutory or regulatory obligations. In some cases, the Dodd-Frank Act requires the CFPB to share supervision and examination information with certain agencies. In other cases, the CFPB has chosen to work with related agencies, which may involve sharing information derived from the examination process. Consumers can learn about how the CFPB shares information derived from the examination process in the CFPB Bulletin found at https://files.consumerfinance.gov/f/2012/01/GC_bulletin_12-01.pdf. Additionally, the CFPB only shares PII as authorized in the routine uses published in CFPB.002 –Depository Institution Supervision Database and CFPB.003 – Non-Depository Institution Supervision Database[11].

4. Describe what opportunities, if any, individuals to whom the information pertains must (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 provides individuals the ability to request access to and amend 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 are published in CFPB.002 –Depository Institution Supervision Database and CFPB.003 – Non-Depository Institution Supervision Database [12] and at https://www.consumerfinance.gov/foia-requests/. CFPB maintains exemptions for certain records contained within these SORNs to the extent that records contain investigatory materials compiled for law enforcement purposes, where the disclosure of such material would reveal the

[12] The CFPB.002 –Depository Institution Supervision Database and CFPB.003 – Non-Depository Institution Supervision Database is found at https://www.consumerfinance.gov/privacy/system-records-notices/.

identity of a source who CFPB holds in confidence. Because PII collected during the examination process provided by an entity pursuant to applicable laws and regulations, employees of entities and consumers do not have the opportunity to opt out or decline to provide their PII that is collected in this context.

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.

The CFPB complies with the Privacy Act of 1974, the Right to Financial Privacy Act, and the E-Government Act of 2002; adopts Office of Management and Budget privacy-related guidance as best practice;[13] and applies National Institute of Standards and Technology risk management processes for privacy. The CFPB uses the following technical and administrative controls to secure the information and create accountability for CFPB's appropriate collection, use, disclosure, and retention of the information:

- Audit logs and reviews
- CFPB Personnel Privacy Training
- CFPB Privacy Breach Response and Recovery Plan
- Compliance with CFPB cybersecurity policy and procedures
- Data quality and integrity checks
- Extract logging and 90-day reviews
- Policy and Standard Operating Procedures
- Role-based access controls: The CFPB is responsible for assigning and maintaining roles and permissions within the Salesforce cloud platform and its applications based on an individual's role within the organization and as approved by Cybersecurity. The following lists examples of the roles and responsibilities within the Salesforce cloud platform:
    - System administrator and system administrator roles - These are performed by authorized CFPB employees and contractors. These roles have full access to

[13] Although pursuant to Section 1017(a)(4)(E) of the Consumer Financial Protection Act, Pub. L. No. 111-203, the CFPB is not required to comply with Office of Management and Budget (OMB)-issued privacy guidance, it voluntarily follows OMB privacy-related guidance as a best practice and to facilitate cooperation and collaboration with other agencies.

manage security configuration settings within the Salesforce cloud platform environment, including management of user account privileges and permissions. Security controls such as session time-outs ask the user to continue working or log out after a period of inactivity.

  - CFPB basic user roles - This role is assigned to all CFPB employees and contractors who are granted access to application(s) in the Salesforce cloud platform. Permissions are based upon assigned business function (e.g., Contracting Office Representative (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 accounts roles are specific non-system administrator user accounts assigned to authorized CFPB employees and contractors that are used for data synchronization, managing API credentials, and to synchronize identity information.
- Federal committee on statistical methodology government-wide statistical standards
- Guidelines for ensuring and maximizing the quality, objectivity, utility, and integrity of information disseminated by federal agencies
- National Archives and Records Administration (NARA) has approved the following records schedules for SES:
  - Supervision and Examination System Records - Master Files
    - Authority: DAA-0587-2013-0011 Item 5.1
    - Disposition Instructions: TEMPORARY. Destroy 15 year(s) after cutoff.
  - Supervision and Examination System Records - Supervisory Document Depository
    - Authority: DAA-0587 -2013-0011 Item 5.2
    - Disposition Instructions: TEMPORARY. Destroy 7 year(s) after cutoff.
  - Supervision and Examination System Records - Final examination reports, and supervision and enforcement recommendations (Historic)
    - Authority: DAA-0587 -2013-0011 Item 5.3
    - Disposition Instructions: Transfer to the National Archives 15 years after cutoff.
- Personnel security, including background checks.

The 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 the 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.

As a result of conducting this PIA the CFPB thoroughly reviewed the SES system interconnections Microsoft O365 and AWS Alto. Salesforce cloud platform provides the CFPB with the ability to connect to these authorized third-party vendors services to support enhanced performance. Salesforce's cloud platform connections are secured using the appropriate controls, OKTA and CFPB's enterprise identity management service. The CFPB mitigates this third-party vendor risk by sharing the SES data only with systems that have achieved an ATO based upon the CFPB A&A processes. Connections between other cloud environments are assessed by the CFPB 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 only authorized entities can access data within SES. The CFPB also configures security controls at a granular level within each application to prevent sharing of PII externally. For example, CFPB disables external sharing within Microsoft O365 SharePoint, prohibiting any linked document from being opened outside the CFPB environment.

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.)

CFPB utilizes a variety of third-party tools that support SES functions. For example, the SES connects the Salesforce cloud platform with other CFPB authorized third-party tools such as AWS[14] and Microsoft O365 SharePoint to parse, cleanse, and standardize data, and to protect the Salesforce cloud platform environment from malicious viruses that could be sourced from external individuals that submit file attachments into the Salesforce cloud platform applications. The CFPB creates and secures internal connections with integration tools like MuleSoft, which allows CFPB to create reusable network connections with application programming interfaces (APIs) to move information between systems and environments. These connections are secured

[14] Please see the Microsoft/Office 365 General Support Services (GSS) PIA found at https://www.consumerfinance.gov/privacy/privacy-impact-assessments/

using both the Salesforce cloud platform controls and access and authentication tools through CFPB's enterprise identity management services. These services are reviewed by CFPB security and privacy teams prior to their employment.

Document control

Approval

CHRISTOPHER CHILBERT

Digitally signed by CHRISTOPHER CHILBERT
Date: 2023.05.31 17:28:15 -04'00'

Chris Chilbert
Chief Information Officer
Date

Kathryn Fong

Digitally signed by Kathryn Fong
Date: 2023.06.01 07:43:08 -04'00'

Kathryn Fong
Acting Chief Privacy Officer
Date

DANG PHAM

Digitally signed by DANG PHAM
Date: 2023.05.26 13:16:21 -04'00'

Danny Pham
Initiative Owner
Date