Compliance Tool v.#3

Privacy Impact Assessment

November 2024

Consumer Financial Protection Bureau

Overview

The Dodd-Frank Wall Street Reform and Consumer Protection Act (The Act) established the Consumer Financial Protection Bureau (CFPB or Bureau).[1] The CFPB is a 21st century agency that implements and enforces federal consumer financial law and ensures that markets for consumer financial products are fair, transparent, and competitive.

In accordance with the CFPB's supervisory authority provided in the Act, Pub. L. No. 111-203, Title X, §§1011, 1012, 1021, 1024, 1025, and 1026, codified at 12 U.S.C. §§5491, 5492, 5511, 5514, 5515, and 5516, the CFPB Supervision Division (Supervision) is authorized to collect information to monitor and evaluate supervised entities in the offering or provision of consumer financial products or services. Supervised entities include banks, savings associations, credit unions and nonbank institutions, and entity service providers and affiliates (hereinafter referred to as "supervised entity or entities"). Part of the supervision process involves collecting and reviewing mortgage loan information (hereinafter referred to as "loan information or documents") for covered loans that a supervised entity has issued or purchased and is holding for repayment. Covered loans include those covered under:

- Truth in Lending Act ("TILA") of 1994[2]
- Real Estate Settlement Procedures Act ("RESPA") of 1974[3]
- Home Ownership and Equity Protection Act ("HOEPA") of 1994[4]
- Secure and Fair Enforcement for Mortgage Licensing Act ("SAFE Act") of 2008[5]
- Integrated Mortgage Disclosures Under the Real Estate Settlement Procedures Act (Regulation X) and the Truth In Lending Act (Regulation Z) ("TRID Rule") of 2013[6]

Supervision has procured use of a vendor-owned automated mortgage compliance tool (Compliance Tool) for the purpose of analyzing loan information to ensure supervised entities remain compliant with all applicable federal and regulatory laws that protect consumers from unfair,

---

[1] Public Law No. 111-203, Title X

[2] 15 U.S.C. 1601 *et. seq.*

[3] 12 U.S.C. 2601 *et. seq.*

[4] Public Law No. 103-325, 108 Stat. 2190

[5] 12 U.S.C. § 5101 *et. seq.*

[6] Title 12 Code of Federal Regulations (CFR) 226

deceptive, and abusive practices in the mortgage market. The Compliance Tool provides a centralized system for CFPB examiners to automate and streamline the collection and analysis of loan information or documents collected from supervised entities. CFPB examiners manually enter loan information contained in mortgage loan documents into the Compliance Tool to include personally identifiable information (PII) on loan officers or the equivalent (hereinafter referred to as "entity employees") and statistical and demographic data on borrowers of covered loans. The tool is used to conduct quantitative analysis on the loan data elementws entered to ensure that what was disclosed to the consumer at the time of loan origination was accurate. For example, if can be used to recalculate the annual percentage of a loan based on the individual loan fees entered. The CFPB uses the analysis to make informed decisions, gain insights, and ensure that supervised entities are in complkiance with consumer-protection laws and regulations.

The Compliance Tool is not a system of records under the Privacy Act of 1974,[7] as the records maintained therein are not retrieved by a personal identifier. The Compliance Tool contains information from mortgage loan documents that have been entered by the CFPB examiner. Copies of the loan information or documents are maintained in the CFPB's Supervision and Examination System (SES).[8] Supervised entities provide these documents to the CFPB during the course of an examination via the Supervision Portal.[9] While the Compliance Tool is not itself a system of records, System of Records Notice (SORN) coverage for these documents is provided under the corresponding SORN for SES, CFPB.002 Supervision and Examination Records (SER) SORN.[10]

In addition, the Compliance Tool collects account information about Compliance Tool users, which include CFPB Staff.[11] This information includes full names, contact information (*e.g.*, business email address) and associated agency information, usernames and passwords, and system access records. These records are covered under the CFPB.014 – Direct Registration and User Management System SORN, which provides coverage for records (*e.g.*, access records) associated with authorized

---

[7] 5 U.S.C. § 552a.

[8] *See* CONSUMER FINANCIAL PROTECTION BUREAU, SUPERVISION AND EXAMINATION SYSTEM PRIVACY IMPACT ASSESSMENT (May 2023) and subsequent updates, *available at*, https://www.consumerfinance.gov/privacy/privacy-impact-assessments/.

[9] *Id*. The Supervision Portal is a secure external-facing portal that allows supervised entities to upload documents that contain PII securely within the CFPB network.

[10] *See* CBP.002 – SUPERVISION AND EXAMINATION RECORDS, SYSTEM OF RECORDS NOTICE, 89 Fed. Reg. 73077 (Sept. 9, 024) and subsequent updates, *available at*, https://www.consumerfinance.gov/privacy/system-records-notices/ (hereinafter SER SORN).

[11] CFPB Staff is defined as all employees, interns, volunteers, consultants, contractors, and detailees assigned to CFPB.

system users.[12]

The original Privacy Impact Assessment (PIA) for the Compliance Tool was published on October 30, 2012, to document the CFPB's use of the vendor-owned tool and its impact on privacy and was last updated on April 28, 2018. The CFPB is publishing this PIA update in a new template to document the Compliance Tool's migration to the Amazon Web Services Cloud environment, to clarify the information collected regarding borrowers and entity employees and the sharing of information with external parties, to update SORN coverage and access and correction procedures, and to expand on the privacy protections in place for security, auditing, and accountability.[13]

Privacy Analysis and Risk Management

The CFPB conducts Privacy Impact Assessments (PIAs) on both programs and information technology systems, pursuant to the E-Government Act of 2002, Section 208[14] and in alignment with Office of Management and Budget[15] (OMB) guidance and the National Institute of Standards and Technology (NIST) standards. This PIA examines privacy risks and describes mitigation measures associated with Supervision's Compliance Tool pursuant to the Fair Information Practice Principles. This includes the design and implementation of administrative, technical, or physical safeguards or controls, as applicable.

1. Characterization of Information

1.1 Identify the information the CFPB collects, uses, disseminates, or maintains, and the individuals about whom the information pertains.

---

[12] *See* CBP.014 – DIRECT REGISTRATION AND USER MANAGEMENT SYSTEM, SYSTEM OF RECORDS NOTICE, 83 Fed. Reg. 23435 (June 21, 2018) and subsequent updates, *available at*, https://www.consumerfinance.gov/privacy/system-records-notices/.

[13] *See* CONSUMER FINANCIAL PROTECTION BUREAU, AMAZON WEB SERVICES GENERAL SUPPORT SERVICES PRIVACY IMPACT ASSESSMENT, (Dec. 2022) and subsequent updates, , https://www.consumerfinance.gov/privacy/privacy-impact-assessments/.

[14] 44 U.S.C. § 3501 note.

[15] Although pursuant to section 1017(a)(4)(E) of the Dodd Frank Wall Street Reform and Consumer Financial Protection Act, Public Law 111-203, the CFPB is not required to comply with OMB-issued guidance, it voluntarily follows OMB privacy-related guidance as a best practice and to facilitate cooperation and collaboration with other agencies.

This section has been updated to clarify the information collected for borrowers and entity employees. The Compliance Tool collects the below information on the following categories of individuals, and may vary based on the type of exam and analysis being conducted:

Borrowers:

- City, County, State and Zip Code of the borrower's property address
- Income and asset information
- Loan information (e.g., amount, type of loan, purpose for loan, maturity term, dates of disclosures)
- Gender
- Race

Entity Employees (e.g., loan originators):

- Loan Originator Nationwide Mortgage Licensing System identifier ("NMLS ID")
- Loan Originator Full Name

CFPB Personnel

- Name (First and Last)
- Contact Information (business email address)
- Employer name
- Usernames and passwords

1.2 What are the sources of information and how is the information collected?

Apart from information collected directly from Compliance Tool users, all other information is collected from the supervised entity at the request of the CFPB exam team for an examination. Upon request, the supervised entity will upload the relevant mortgage loan documents to SES via the Supervision Portal. CFPB examiners then manually enter only the relevant information into the Compliance Tool for analysis and review. This includes information collected on borrowers and entity employees. The supervised entity collects the information during the normal course of business directly from entity employees and borrowers during the mortgage loan process. This information is then shared with the CFPB during the supervision examination process.

1.3 If the information collection is covered by the Paperwork Reduction Act (PRA), provide the OMB Control number for the collection.

In accordance with the Paperwork Reduction Act of 1995, as amended, the CFPB has reviewed the information collection and determined that the information maintained in the Compliance Tool does not modify or create any new collections.

1.4 Discuss how the accuracy of the information is ensured.

The CFPB collects information on entity employees and borrowers directly from the supervised entity to ensure information maintained in the Compliance Tool is accurate and up to date. The CFPB relies on the supervised entity to provide accurate and up to date information at the time of collection. Additionally, the supervised entity collects the information directly from the entity employee during the course of employment and from the borrower during the mortgage loan process. Direct collection increases the likelihood that the information provided is accurate. While the CFPB does not independently verify that the information is up to date, this does not impact or interfere with the analysis process as the information is used to ensure the supervised entity is compliant.

Privacy Impact Analysis: Related to Characterization of the Information.

Privacy Risk: There is a risk that the information collected from supervised entities is inaccurate or not up to date.

Mitigation: As noted above, the CFPB relies on the supervised entity to provide accurate information on entity employees and borrowers at the time of collection. For borrowers, the information provided includes the borrower's race, gender, the city and zip code associated with the borrower's property, and other loan and income information. As noted above, this information is collected directly from borrowers during the mortgage loan process.

Additionally, the information provided on borrowers is a statistical or demographic data set (without the borrowers' names) and CFPB examiners only use this information to analyze and ensure that the supervised entity is in compliance with consumer-protection laws. More importantly, no benefit or determination about a borrower is made based on the information collected from the supervised entity and thus, will not negatively impact the borrower.

For entity employees, the information provided includes the entity employee's name and NMLS

identifier. While the information is collected directly from the entity employee, this information can also be verified through the NMLSR system (if applicable).[16] If the results of an analysis conducted on the information indicate a potential compliance problem, the CFPB validates the information during the examination outside of the Compliance Tool to ensure the information is accurate.

2. Limits on Information Collection and Retention

2.1 Explain how the CFPB only collects and maintains the information that is directly relevant and necessary to accomplish the specified purpose(s).

The information the CFPB collects and maintains in the Compliance Tool is handled in a manner that is consistent with the purposes necessary to perform and support the examination and analysis processes. To ensure that supervised entities remain in compliance with federal law and regulation, the CFPB collects and maintains mortgage loan documents during the supervision examination process, which are maintained in SES. CFPB examiners then manually enter only the information that is needed for analysis into the Compliance Tool.

For example, the SAFE Act is designed to enhance consumer protection and reduce fraud by encouraging states to establish minimum standards for the licensing and registration of state-licensed and federal mortgage loan originators (MLO).[17] The Safe Act prohibits individuals from engaging in the business of a residential MLO without first obtaining and maintaining annually a registration and license and NMLS identifier. Information collected on entity employees includes the names, along with the MLO's NMLS identifier. The CFPB examiner uses and enters this information into the Compliance Tool as part of reviewing a mortgage loan file. It allows the CFPB examiner to ensure the loan originator who originated the borrower's loan is properly registered and maintaining a loan originator license via NMLSR, where nonexempt.

---

[16] *See* CONSUMER FINANCIAL PROTECTION BUREAU NATIONWIDE MORTGAGE LICENSING SYSTEM AND REGISTRY PRIVACY IMPACT ASSESSMENT (Sept. 27, 2012) and subsequent updates, *available at*, https://www.consumerfinance.gov/privacy/privacy-impact-assessments/.

[17] Mortgage loan originator means an individual who: (i) takes a residential mortgage loan application; and (ii) offers or negotiates terms of a residential mortgage loan for compensation or gain. MLOs are employees of depository institutions, or a subsidiary that is: (A) owned and controlled by a depository institution; and (B) regulated by a federal banking agency; or (C) an institution regulated by the Farm Credit Administration, as set forth in 12 USC § 5102.

2.2 Describe the records retention requirements for the information. Has the retention schedule been approved by the CFPB and the National Archives and Records Administration (NARA)? If so, include the retention schedule.

The records collected and maintained in the Compliance Tool are retained in accordance with the CFPB Supervision Examination and System Records Schedule, DAA-0587-2013-0011, Items 001-0010. Records will be disposed of in accordance with the records schedule Item No and disposed of up to 20 years.[18]

Privacy Impact Analysis: Related to Limits on Information Collection and Retention

Privacy Risk: There is a risk that the CFPB collects more information than is necessary for the purpose(s) of collection.

Mitigation: To mitigate this risk, the CFPB only collects a limited amount of information about supervised entity employees and borrowers that is narrowly tailored to effectively carry out the CFPB's purpose(s) and use(s) for collection. As noted above, supervised entities provide mortgage loan documents and CFPB examiners identify only the relevant information required for analysis and *manually* enter that information into the corresponding data fields in the Compliance Tool. For example, the names of borrowers are not entered into the Compliance Tool because this information is not necessary to determine whether the supervised entity is compliant. The race and gender of borrowers is entered and maintained in the Compliance Tool as supervised entities are required to provide the same mortgage rates to all borrowers under the SAFE Act. The CFPB examiner may analyze this information about borrowers to ensure that mortgage rates do not fluctuate based on their gender or race.

Additionally, the Compliance Tool is designed to include only the data fields required for the various types of information required for analysis. The tool does not include free text fields or allow for the inclusion of other PII. The information entered into the Compliance Tool is mostly quantitative, such as numbers for associated loan fees or the date disclosures provided to borrowers. For example, TILA requires lenders to provide the consumers (*i.e.*, borrower) with loan cost information so borrowers can comparison shop for certain types of loans and adhere to

[18] https://www.archives.gov/research/guide-fed-records

disclosure requirements to protect consumers against inaccurate and unfair credit billing. CFPB examiners use and enter certain loan information (*e.g.*, dates of disclosure) provided by supervised entities into the Compliance Tool to ensure the required loan disclosures (*e.g.*, estimates, final amount disclosures) are timely provided to the borrower within the defined time periods throughout the course of the mortgage loan process. Within the Compliance Tool, the dates entered will be flagged if the time of such disclosure is outside of the regulatorily allowable timeframe.

3. Uses of Information

3.1 Describe the purpose of the information and how the CFPB uses it.

Pursuant to the CFPB's supervisory authority provided in the Act, Pub. L. No. 111-203, Title X, §§1011, 1012, 1021, 1024, 1025, and 1026, codified at 12 U.S.C. §§5491, 5492, 5511, 5514, 5515, and 5516, the CFPB is authorized to collect information to monitor and evaluate supervised entities in the offering or provision of consumer financial products or services. The information collected and maintained in the Compliance Tool is used to conduct and coordinate examinations and reports, supervisory evaluations and analyses, and enforcement actions, including both CFPB activities and collaborations with other regulatory agencies.

For example, RESPA requires lenders, mortgage brokers, or servicers of home loans to provide borrowers with pertinent and timely disclosures regarding the nature and costs of the real estate settlement process, and prohibits specific practices, such as kickbacks, and places limitations upon the use of escrow accounts (*e.g.*, restrictions on force-placed insurance). CFPB examiners enter the loan information into the Compliance Tool to compare the initial loan estimate disclosure of fees against the final closing disclosure of fees charged at loan consummation. This ensures that specific categories of fees do not increase substantially, as prohibited by regulation, throughout the course of the loan transaction.

In addition, this information is used to support the conduct of investigations or to be used as evidence by the CFPB or other supervisory or law enforcement agencies, which may result in the initiation of administrative or federal court actions, or criminal referrals, such as to the Federal Reserve Office of Inspector General. For example, when assessing HOEPA addresses abusive practices in refinancing and home equity mortgage loans with high interest rates or high fees by establishing specific disclosure requirements and restrictions on prepayment penalties and certain other loan terms, and regulated lender practices (*e.g.*, extending credit without regard to a consumer's ability to pay). Additionally, HOEPA provides for enhanced remedies for violations of law, a mechanism to consumers to rescind covered loans that included certain prohibited terms

and obtain higher damages, and increased liability to purchasers.

CFPB examiners enter loan information into the Compliance Tool to analzye and identify whether the loan fees delineate the loan as a "high-cost mortgage loan" as defined under HOEPA. If yes, the MLO is required to provide additional disclosure(s) within a prescribed time period through the loan process. The Compliance Tool first flags the "high-cost mortgage loan" category, and then collects the date(s) when the required disclosure(s) were provided to the borrower.

Finally, the information is used to manage internal business processes. The Compliance Tool allows CFPB to examine and analyze information collected from loan documents inspected during the performance of CFPB's statutory duties, and for administrative purposes to ensure quality control, performance, and improving management processes.

3.2 Is the information used or shared with other CFPB programs, systems, or projects?

Generally, information collected and maintained in the Compliance Tool is not shared outside of Supervision. Information will only be shared with other program offices or divisions to support CFPB mission operations in accordance with all laws, regulations, and policies. On occasion, loan information may be shared with the Division of Research, Monitoring, and Regulations (RMR) for research and marketing purposes, such as to help inform the Bureau's market-monitoring efforts, including research regarding particular markets and the risk to consumers presented in such markets. Any such internal sharing is subject to CFPB data governance procedures.

Privacy Impact Analysis: Related to Uses of Information

Privacy Risk: There is a risk that PII collected and maintained in the Compliance Tool will be shared with individuals that do not have a need to know, and used in a manner that is inconsistent with the original purpose(s) for collection.

Mitigation: To mitigate this risk, the CFPB only shares information maintained in the Compliance Tool in accordance with laws, regulations, policies and CFPB SORNs. As noted above, while used to support examinations and investigations, the information maintained in the Compliance Tool is generally not shared with other CFPB program offices and divisions. Only CFPB personnel within Supervision are granted access to the Compliance Tool. Access is based on the individual's job function and duties, such as CFPB examiners who require access to conduct analyses of mortgage loan information to ensure supervised entities remain compliant with all

applicable federal and regulatory laws. Additionally, Compliance Tool users must enter a username and password to access the tool.

Finally, all CFPB Staff with access to CFPB systems and technologies, such as the Compliance Tool, must sign the CFPB "Acceptable Use of CFPB Information Technology Resources" policy.[19] This policy establishes the user's responsibilites and the requirements to safeguard information technology resources and information. This includes protecting PII and other sensitive or confidential information. All CFPB personnel are required to take annual privacy training. For example, CFPB examiners must adhere to CFPB privacy policy and complete the confidentiality and privacy briefing when they initially onboard and on an annual basis thereafter. CFPB privacy training stresses the importance of appropriate and authorized use of personal information in government information systems.

4. Individual Notice and Participation

4.1 Describe what opportunities, if any, individuals to whom the information pertains receive notice prior to the collection of information. If notice is not provided, explain why not.

General notice is provided by the CFPB through its rulemakings, this PIA, and applicable SORN(s). As noted above, the information collected and maintained in the Compliance Tool is manually entered by CFPB examiners from information contained in loan documents and maintained within SES. This information, including information regarding entity employees and borrowers, is collected directly from supervised entities via the Supervision Portal.

In addition, a Privacy Act Statement is provided on the Supervision Portal prior to collection of information. The Privacy Act Statement identifies the CFPB's authority under which the information is collected, the principal purpose(s) for which the information is intended to be used, and the sharing of information, including the applicable SORN(s) that applies.

[19] *See* ACCEPTABLE USE OF CFPB INFORMATION TECHNOLOGY RESOURCES, Operational Policy No. OPS-T&I-2023-07, Ver. 3.0 (April 9, 2013), and subsequent updates (hereinafter AUP).

4.2 Describe what opportunities are available for individuals to consent to use, decline to provide information, or opt out of the CFPB's collection and use of the information.

In general, individuals do not have opportunities to consent to CPFB's collection and use of the information. The information is provided to CFPB as part of the examination process; CFPB does not collect the information directly from indivdiuals. In the exercise of the CFPB's supervisory authorities, supervised entities are required to produce information to the CFPB pursuant to §§ 1024, 1025, and 1026 of the Dodd-Frank Act, codified at 12 U.S.C. §§ 5514, 5515, and 5516.

4.3 What are the procedures that allow individuals to access their information or correct inaccurate information?

While the Compliance Tool is not considered a Privacy Act system of record, the CFPB.002 Supervision and Examination SORN provides coverage for records maintained within SES. Therefore, regardless of citizenship, individuals may access or correct their information maintained in SES by contacting the CFPB's Freedom of Information Act (FOIA) Office[20] in writing in accordance with the Bureau's Disclosure of Records and Information Rules, Subpart E-Privacy Act,[21] promulgated at 12 C.F.R. 1070.50 et seq. If you have any questions, please contact the CFPB FOIA Office via FOIA@CFPB.gov or at (855) 444-3642.

Records compiled for law enforcement purposes may be exempt from access pursuant to the Privacy Act or FOIA.

Privacy Impact Analysis: Related to Individual Notice and Participation

Privacy Risk: There is a risk that individuals may not have the opportunity to participate in or consent to the collection of their information.

Mitigation: The three primary groups of individuals whose PII is maintained in the Compliance

[20] https://www.consumerfinance.gov/foia-requests/submit-request/

[21] eCFR 12 CFR Part 1070 - Disclosure of Records and Information

Tool are borrowers, entity employees, and Compliance Tool users. Compliance Tool users include CFPB Staff. Information regarding Compliance Tool users is limited to what is required to obtain authorized access to the CFPB network, systems, and tools, such as the Compliance Tool. Additionally, this enables CFPB system owners to audit users who access the tool to ensure compliance with all security and privacy requirements.

Borrowers and entity employees do not generally have an opportunity to consent or participate in the collection and maintenance of their information. Supervised entities provide this information to the CFPB as required by law to ensure that supervised entities comply with federal consumer financial protection laws. Importantly, only a limited amount of borrower information is required for analysis and examination. For example, the information maintained in the Compliance Tool does not include identifying information, such as names and physical addresses, but only the city and zip code in which the borrower's property is located, demographic information (*e.g.*, race, gender), and other loan information.

5. External Sharing and Disclosure of Information

5.1 Does the CFPB share this information with external entities or partners? If so, identify the organization or third-party and how the information is accessed and used.

Not applicable. This section has been updated to clarify the sharing of information maintained in the Compliance Tool. External parties do not have direct access to the Compliance Tool. Only CFPB Staff have user accounts. Additionally, information maintained within the Compliance Tool is not shared with external parties, including other federal, state, and local regulators. While the Compliance Tool is used to support examinations and the investigative process, the sharing of information related to an examination will occur outside of the Compliance Tool, such as through SES and in accordance with applicable SORNs.

5.2 Does the CFPB place limitations on information sharing and/or re-dissemination of the information?

Not applicable.

Privacy Impact Analysis: Related to External Sharing and Disclosure of Information

Not applicable.

6. Accountability, Auditing, and Security

6.1 How does the CFPB secure the information to ensure that it is used in accordance with stated practices in this PIA?

The CFPB complies with the Privacy Act of 1974,[22] the Right to Financial Privacy Act,[23] Section 208 of the E-Government Act of 2002,[24] and other applicable laws. To ensure compliance, and that PII and other sensitive information is protected, the CFPB adopts the Fair Information Practice Principles (FIPPs) as the framework for its privacy policy.[25] The FIPPs apply throughout the CFPB for the collection, use, maintenance, disclosure, and destruction of PII, and any other activity that impacts the privacy of individuals, regardless of citizenship, to ensure compliance with all laws, regulations, and policy requirements.

The CFPB adheres to the Office of Management and Budget's (OMB) privacy-related guidance [26] and applies the National Institute of Standards and Technology (NIST) Risk Management Framework (RMF)[27] for information technology systems, applications, solutions, and services. The CFPB identifies and applies NIST SP-800-53[28] security and privacy controls

---

[22] 5 U.S.C. § 552a.

[23] 12 U.S.C. §§ 3401 *et seq*.

[24] 44 U.S.C. § 3501 note.

[25] *See* CFPB PRIVACY POLICY (Dec. 6, 2012), and subsequent updates.

[26] More information regarding OMB guidance is available at, https://www.whitehouse.gov/omb/information-regulatory-affairs/privacy/.

[27] *See* NIST, Risk Management Framework (RMF) For Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy, SP-800-37 Revision (Rev.) 2 (December 2018). For more information visit https://www.nist.gov.

[28] *See* NIST, Security and Privacy Controls for Information Systems and Organizations, SP-800-53, Rev. 5 (September 2020). For more information visit https://www.nist.gov.

and continuous monitoring of controls to ensure on-going compliance with information security standards and protect organizational operations and assets and individuals.

The Compliance Tool has obtained an Authority to Operate from the CFPB's authorizing official.

6.2 Describe what privacy training is provided to users either generally or specifically relevant to CFPB information system.

All CFPB Staff are required to adhere to all CFPB cybersecurity and privacy policies and take mandatory annual training. For example, CFPB Staff are required to take the CFPB Privacy Training and Security Awareness Training before being granted access to the Compliance Tool and annually thereafter. The privacy training ensures that CFPB Staff understand their responsibilities to safeguard PII, and to identify and report suspected or confirmed privacy breaches within twenty-four hours of discovery. CFPB Privacy Office is notified of CFPB Staff that fail to complete the annual privacy training, at which time, their access is terminated until their annual privacy training is complete.

6.3 What procedures are in place to determine which users may access CFPB information systems and how the CFPB provides access?

CFPB Staff with access to CFPB information and systems and facilities are required to proceed through background investigations for suitability and security clearance determinations. This ensures compliance with all federal laws and that individuals supporting the CFPB are deemed reliable, trustworthy, and suitable for the role they will fulfill. Other requirements placed on federal contractors may also include those associated with Federal Acquisition Regulations.

CFPB Staff must properly obtain and present credentials to gain access to CFPB facilities and systems. The CFPB's secure access controls policy, "Secure Access Controls via Multi-Factor Authentication"[29] Policy applies to CFPB Staff that have logical and/or physical access to CFPB facilities, information systems or applications, and/or information (in physical or electronic form).

[29] *See* SECURE ACCESS CONTROLS VIA MULTI-FACTOR AUTHENTICATION, NO. OPS-ADMIN-2024-01 (Nov. 6, 2023), and subsequent updates.

This ensures the CFPB maintains a secure operating environment and protects our systems against potential external threats.

In addition, the CFPB employs role-based access controls. The CFPB uses role-based access controls to ensure CFPB Staff only have access to the system and/or information necessary and relevant to their assigned duties. System access is granted on the user's role within the Compliance Tool. Individuals who no longer require access have their credentials removed from the system.

Privacy Impact Analysis: Related to Accountability, Auditing, and Security

Privacy Risk: There is a risk that the Compliance Tool and information maintained therein may be accessed by unauthorized individuals.

Mitigation: To mitigate this risk, the CFPB has implemented the above technical, physical, and administrative controls to safeguard PII and other sensitive information maintained in the Compliance Tool. For example, access to the Compliance Tool is limited to CFPB Staff who have a need to know the information in the performance of their duties. As noted above, CFPB Staff that require elevated privileges to complete their job functions must sign and electronically submit the *Privileged User Access (PUA) Form* to the CFPB ServiceDesk to obtain elevated access to NBR and review and acknowledge the *Rules of Behavior for Privileged Users*.

In addition, the CFPB has established oversight controls through robust auditing features to identify and support accountability for unauthorized use/misconduct. CFPB's "Information Governance" Policy[30] outlines the established rules on the intake, management, disclosure, and disposition of information (in its various formats) at CFPB and applies to all CFPB users. As noted above, CFPB Staff are required to review and sign the CFPB's "Acceptable Use of CFPB Technology Resources Policy"[31] and complete the privacy and security training, and annually thereafter, before access is granted to a CFPB system.

Suspicious and/or unauthorized access is monitored and logged, thereby discouraging users from inappropriate access to CFPB systems. Security administrators are notified of unusual

[30] *See* CFPB POLICY ON INFORMATION POLICY ON INFORMATION GOVERNANCE AT THE CFPB, No. OPS-OCDO-2023-18, 2.0 (Sept. 26, 2023), and subsequent updates.

[31] AUP, *supra* note 16.

behavior (e.g., disablement of security, login times, number of login attempts, failed login attempts) or misconduct (e.g., unauthorized removal of data) by authorized users. For example, the CFPB employs extract logging and 90-day reviews to identify user behavior and staff actions around particular events, such as changes in the information or data, warnings, or errors that are unexpected, which are reviewed in relation to their job roles and workflow. If the system administrator notices that anyone has used a system or application in violation of CFPB policy, system access may be revoked. If there is evidence of potential misconduct, the incident may be referred to the appropriate CFPB office for investigation and further review and appropriate action.

Document Control

Approval

Chris Chilbert	**Kathryn Fong**
Chief Information Officer	**Chief Privacy Officer**
Katie Day	**Katelyn Sellers**
Program/Product Owner	**Program Director**

Original, signed document on file with the CFPB Privacy Office.