Geographic Information System

Privacy Impact Assessment

December 2024

Consumer Financial Protection Bureau

Overview

The Dodd-Frank Wall Street Reform and Consumer Protection Act, Public Law No. 111-203, Title X, established the Consumer Financial Protection Bureau (CFPB or Bureau). 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.

The Geographic Information System (GIS) technology provides the CFPB with a geospatial data, analytics, geocoding, and mapping software tool to support analysis conducted by CFPB program, including the Home Mortgage Disclosure Act (HMDA) program, the Small Business Lending (SBL) program, the Division of Research, Monitoring, and Regulation (RMR), the Supervision Division (SUP), and Enforcement Division (ENF)[1]. The CFPB's use of GIS technology is authorized by Section 1021(c)(6) of the Dodd-Frank Act,[2] which authorizes the CFPB to perform such support activities as may be necessary or useful to facilitate other functions of the Bureau.

The CFPB's GIS technology provides the following capabilities and functionalities:

- Mapping and visualization: allows CFPB users to use an address/location data to visualize data spatially on a map and share those visualizations to help improve business decisions.
- Increasing efficiency: allows concurrent use of geocoding and geolocation capabilities.
- Analytics: provides advanced analytics tools to help users identify patterns, trends, and anomalies in their data.
- Data management: GIS tools have their own data store and allow authorized users to connect to other existing data stores and leverage ready-to-use storage, such as those hosted within CFPB's Amazon Web Services (AWS) Alto environment.
- Security: provides a secure, browser-based enterprise system that allows users to control, store, and access data.
- Authentication: allows user management and authentication with Single Sign-On (SSO).

[1] Please see https://www.consumerfinance.gov/privacy/privacy-impact-assessments/ for program specific privacy impact assessments.

[2] 12 U.S.C. 5511(c)(6).

The data used by the GIS technology includes information, including personally identifiable information (PII), previously collected by CFPB programs such as location of loans (e.g., home or business address), loan application/borrower information, bank branch locations, address of loan applications, and analysis of trends and actions associated with type of loans, along with publicly available location data, such as Census data or other official data mapping layers that are used as a resource and standard data for various programs performing spatial analysis.

The CFPB-employed GIS technology stack has three components: desktop software, online/public portals, and an Enterprise deployment for managing and controlling GIS product use within the organization. GIS users load data into and conduct analysis in the desktop software. It allows users to conduct analysis, create visualizations, and manage geospatial data for a variety of uses at the CFPB. The online portal is solely used for license/entitlement administration by the geospatial administrators. The Enterprise deployment is comprised of various components: the Enterprise Server powers mapping and analysis; the Enterprise Portal is a central internal hub where users can create, share, and manage maps, apps, and spatial data and share with internal collaborators; the Enterprise Data Store provides data storage; and the Enterprise Web Adaptor integrates the server and portal with CFPB infrastructure. The Enterprise technology allows a greater number of users to access the GIS software and utilize geocoding services concurrently without license restrictions. The online instance of the GIS tool is FedRAMP Moderate certified and provided through Amazon Web Services (AWS).

Currently the CFPB uses only the desktop software with a limited use of the online/public portals for license management. As part of this Enterprise deployment, the CFPB will enable the GIS Enterprise technology mentioned above. The online component will be integrated in the future for specific use cases and will be documented in separate privacy impact assessment (PIA) appendices or updates.

The Office of Regulation Technology (RegTech), which manages the HMDA and SBL programs, remains current on state-of-the-art technology that supports fair, competitive, and transparent consumer financial market. As such, RegTech owns and manages the GIS technology for Bureau-wide use; however, other CFPB offices with a need to know are granted access to the technology and the resource data stored on the server, such as the publicly available Census data.

While PII such as home addresses may be entered into the GIS technology to gather information related to a geographic location, the GIS technology is not used by CFPB to retrieve records about individuals (e.g., homeowners); therefore, it is not a system of records. The data used by the GIS technology may be sourced from a Privacy Act of 1974 covered system of record. Program specific system of record notices (SORN) detail how personal information is managed within those source

systems[3]. Should the CFPB choose to configure the tool to retrieve records using PII, the technology will be reassessed for compliance with the Privacy Act and SORN coverage will be provided prior to the functionality being implemented.

This is the CFPB's first PIA of the GIS technology. The CFPB is publishing this PIA to analyze and document privacy risks and mitigations related to the Bureau's use of the GIS technology. This PIA identifies all current use cases of this technology and will be updated with any subsequent uses.

Privacy Analysis and Risk Management

The CFPB conducts PIAs on both programs and information technology systems, pursuant to Section 208 of the E-Government Act of 2002[4] and in alignment with Office of Management and Budget[5] (OMB) guidance and the National Institute of Standards and Technology (NIST) standards. This PIA examines privacy risks and describes mitigation measures associated with the [program and/or information technology systems] that support the [program or project] 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.

The GIS technology does not collect data directly from consumers, financial institutions, or others. Users instead upload existing data collected by CFPB programs to perform a geocoding, visualization, or mapping task.

---

[3] Please see https://www.consumerfinance.gov/privacy/system-records-notices/.

[4] 44 U.S.C. § 3501 note.

[5] 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.

The PII used within the GIS technology relates to consumers and is sourced from HMDA, SBL, SUP, ENF, RMR, financial institutions database, consumer complaint data, audit datasets, and examination datasets. The actual PII data elements are dependent on specific business use cases; however, examples of PII may include but is not limited to:

- Home or property street address of loan applicant or borrower;
- Age of applicant and co-applicant, if available;
- Race, sex, and ethnicity of applicant and co-applicant, if available;
- Credit score;
- Other information related to a borrower's loan application, such as:
    - Loan amount;
    - Debt to income ratio;
    - Property value;
    - Total units;
    - Multifamily affordable units;
    - Loan type;
    - Type of credit;
    - Census tract;
    - North American Industry Classification System (NAICS) code (for business loans);
    - Use of credit; and
    - Discharge status

Certain publicly available datasets are available for GIS users to use in their analysis, such as Census aggregate demographic information at different levels of geography (block group, tract, county, state, etc.). These datasets are spatially enabled, meaning they are already converted into a format that is usable by the GIS technology. These datasets are hosted on the server for ease of access and convenience for our users. While the technology allows CFPB users to match and layer CPFB data with these public datasets to gain additional insights and context into a specific geographic location, no new PII is generated about individuals using this technology.

CFPB staff are provisioned access to GIS technology by using CFPB Staff name, business address, telephone number, email address, internet protocol (IP) address, office location, and CFPB billing

information to license the GIS technology to CFPB. This PII is used to authenticate users, provide support and deliver specialized services.

Eventually CFPB will integrate the online/public portals into its Enterprise deployment, which could enable the publication of anonymized, aggregated data to the public in accordance with applicable legal requirements and data release standards.

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

The information, including PII, uploaded in the GIS technology is sourced from existing CFPB systems. They include, but are not limited to, the CFPB's systems for the HMDA program, SBL program, RMR, SUP, and ENF. These Bureau systems are maintained within on-premise servers and within the Amazon Web Services (AWS) hosted cloud.

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

The GIS technology is employed by several Bureau programs, offices, and divisions such as HMDA, SBL, SUP, ENF, and RMR. Information used by CFPB within GIS technologies may be subject to PRA, and CFPB programs, offices, and divisions must comply with PRA requirements. If required, OMB approval must be obtained through one of CFPB's generic information collection plans or full clearance.

Specific OMB collection numbers for information collected by CFPB programs, offices, and divisions and used to perform spatial analysis are described in the program specific CFPB PIAs.

1.4 Discuss how the accuracy of the information is ensured.

The GIS technology relies on the accuracy of the data input to execute the desired functions. The accuracy of the information is managed by the source system (i.e., the system where the data originates). These systems have integrated checks to ensure the accuracy of the data that is entered by financial institutions and consumers and is detailed in their respective PIAs.

Privacy Impact Analysis: Related to Characterization of the Information.

Privacy Risk: Since the GIS technology is not the initial point of collection for the data required to perform spatial analytics work, there is a risk that the data may be inaccurate, which would affect the integrity of the output.

Mitigation: This risk is mitigated by utilizing information from authoritative source systems. These systems have controls such as automated quality assurance/quality control processes and auditing to ensure that data remains current and accurate to the greatest extent possible. Additionally, data that come from financial institutions directly are certified to be accurate by the financial institutions under penalty of law.

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 GIS technology is limited in the type of data they process and analyze. The technology is designed to leverage location data to produce trends, mapping, visualizations, and analyses. While CFPB programs may collect and maintain a variety of information specific to their purpose and authority, the information used by GIS technology is limited to the location data needed to execute the required output or analysis.

As noted above, the information collected by the system may include information that is not location based such as demographic information, income, and loan amounts. The analysis of demographic information and other PII in the context of location is directly relevant and necessary for the Bureau to promote fair, transparent, and competitive consumer financial products. The PII is retained on the server for analysis until the final output is transmitted to permanent program-appropriate data storage on the CFPB network. Within a week after the final output has been transmitted, the PII is deleted from the GIS server.

The PII collected regarding CFPB Staff is required to create user accounts, manage billing, authenticate users, provide support, and deliver specialized services. The information is also used in audit logs that may be used to verify compliance with the CFPB's privacy and security policies. This information is retained for the life of the user account.

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 CFPB's Records and Information Management program collaborates with program managers to develop records retention schedules and submits to the National Archives and

Records Administration (NARA) for appraisal. NARA provides the authority to disposition when records retention schedules are approved.

Data used for input is intermediate data and considered transitory in nature and the GIS technology output is retained pursuant to the record schedules for each program office. As a practice, users are trained to remove intermediate and non-critical information in the CFPB's existing GIS technology within a week after the final output has been transmitted back to other permanent program-appropriate data storage on the CFPB's network. Further, users are trained to move data out of private folders to the server where program specific retention schedules apply. Output data without PII, such as the aforementioned Census aggregate demographic information, are kept for repeated use only as necessary and with restricted access.

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

Privacy Risk: There is a risk that information maintained in the GIS technology may be retained longer than necessary to accomplish the purpose for which it was originally collected.

Mitigation: Data used within the GIS technology is considered transitory. Program specific record schedules outline the retention period for the data used for input and the resulting output. This risk is further mitigated by documented internal processes that require the deletion of PII and/or sensitive intermediate data within one week after the final output is processed.

Privacy Risk: There is a risk that the GIS technology collect more information than is necessary for the purpose of spatial analysis.

Mitigation: To mitigate this risk, the CFPB has established technical controls and privacy safeguards to ensure only a limited amount of information is entered into the GIS technology. For instance, users are provided a guidance document that covers the principle of using the least amount of data required for analysis. Additionally, the GIS technology is not used for direct data collection at the CFPB. It only leverages the data already collected by various CFPB programs which allows program offices to be deliberate about the inputs needed to obtain the desired output.

3. Uses of Information

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

The GIS technology is a geospatial data management, analytics, research, geocoding, and mapping software tool. The CFPB uses the GIS technology to support several primary business lines, and below are examples of how the technology is used:

1. In RegTech, HMDA Ops, RMR, SUP, and Fair Lending the technology is used to support prioritization of examinations. For example, the technology may be used to geocode the addresses of loan applications, to identify the location/census tract of a particular applicant for fair lending examination analysis, or as an input to the prioritization process. It is also used to conduct spatial analyses, such as cluster analyses or interpolation.

2. In ENF, in addition to the geocoding and spatial analyses mentioned above, the technology is used to display relevant case data (e.g., loan location, bank branch locations, census tracts with demographic indicators, etc.) on a map to present during trials.

3. In RMR, the technology is used to better understand the distribution of spatial phenomena (e.g., mapping clusters of borrowers across a city, creating weather maps of high and low-interest rate areas, overlaying Census or other maps over our data for additional analyses, calculating the effects of flood risk on mortgage prices, etc.).

GIS tasks are also performed across other divisions and offices such as the Office of Technology and Innovation and Consumer Response. The technology allows maps to be presented in a static PDF format and as interactive web-maps and web-apps that can be accessed internally by the staff involved, as well as published for the public where it is appropriate or legally required.

Data can be uploaded into the GIS technology and geocoded so that further analysis can be performed. Alternatively, authorized users can leverage pre-geocoded data and intersect those points with additional information such as census tract, population, and other demographics. The geocoded output takes the form of either a csv file or map that is further analyzed for program-specific purposes once transferred to the respective server.

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

Access to data that is geocoded by the GIS technology, such as HMDA data, may be granted to Bureau users who request it and have a business purpose or need to know. This internal sharing eliminates the hours of work needed to geocode data for analysis. In the desktop instance, outputs are stored in private folders on the CFPB network that are only accessible by the user and GIS administrators. However, a user can request an administrator to add an additional user to a private folder for collaborative purpose. Additionally, the Enterprise instance allows for multiple-user groups where information can be shared within a team or across the Bureau. Authorized GIS users are comprised of Bureau employees and contractors.

Data are shared between programs as deemed appropriate by those program offices.

Privacy Impact Analysis: Related to Uses of Information

Privacy Risk: There is a risk that information may be shared with individuals who do not have a need to know and used in a manner that is inconsistent with the purpose for which it was originally collected.

Mitigation: This risk is mitigated by users having restricted access to certain data sets. Access to information, such as HMDA data, requires authorization and a legitimate need to know prior to being granted access. Each program office has a GIS owner who must sign off on users who require access. The access and use of data must be consistent with the authority that governs the program.

User output is placed into a private folder where only the user and administrators have access. If another user attempts to access others' private folder, an error message pops up and access is denied. In the Enterprise instance, user groups and permissions are assigned by administrators to ensure that only individuals with a need to know have access to groups and the data being shared.

Additionally, all CFPB Staff with access to CFPB systems, such as the GIS technology, must sign the CFPB "Acceptable Use of CFPB Information Technology Resources" policy. This policy establishes the user's responsibilities and the requirements to safeguard information technology resources and information. This includes protecting PII and other sensitive or confidential information. Finally, all CFPB Staff are required to complete privacy training 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.

Information uploaded into the GIS technology is not collected directly from the consumer. Rather, it is derived from existing Bureau systems. As such, where applicable, notice is provided

at the point of collection by the program that initially collected the data. Notice is also provided in this PIA, as well as in the program specific PIAs and SORNs[6].

CFPB Staff information that is collected for the purpose of authentication is covered by CFPB.014 – Direct Registration and User Management System (DRUMS) SORN.

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.

Individuals generally do not have the opportunity to opt out or decline to have their information included in the GIS technology. Where applicable, individuals are provided notice at the point of collection regarding how their information will be used. Additional information regarding consent is provided in the program specific PIAs.

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

The GIS technology is not the source or authoritative system for the information; any output is in aggregate and not specific to any individual. Individuals seeking access to their information must follow the procedures outlined in the program specific PIA and/or SORN that covers the collection of their information.

In general, individuals may access or correct their information maintained in CFPB systems by writing to the CFPB's Freedom of Information Act (FOIA) Office[7] in accordance with the Bureau's Disclosure of Records and Information Rules, Subpart E-Privacy Act,[8] promulgated at 12 C.F.R. 1070.50 *et seq.* If an individual has questions about their information, they may contact the CFPB FOIA Office via FOIA@CFPB.gov or at (855) 444-3642.

Privacy Impact Analysis: Related to Individual Notice and Participation

---

[6] Please see https://www.consumerfinance.gov/privacy/system-records-notices/ for program specific privacy impact assessments.

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

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

Privacy Risk: There is a risk that individuals whose information used in GIS technology do not have an opportunity to opt out or participate in the collection of their information used in the GIS technology.

Mitigation: The information used in GIS technology is uploaded from existing CFPB datasets and not collected directly from individuals. Therefore, individuals do not have the opportunity to opt out or opt in to participate in the GIS tool's use of their information. This risk is mitigated by notice being provided, where applicable, at the original point of collection by the respective program offices.

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.

The GIS technology output may be shared, in aggregate, in various publications and to support regulatory requirements, as appropriate. For instance, the SBL rule requires the publication of aggregate level data to "enable communities, governmental entities, and creditors to identify business and community development needs and opportunities for women-owned, minority-owned, and small businesses."[9] The CFPB, as part of the Federal Financial Institutions Examination Council (FFIEC), also publishes HMDA data, including some geospatial components of the aggregated data. The output may take the form of a trend analysis or maps, for instance, but only aggregate data is shared. No identifying information is shared externally. There is no sharing directly from the GIS technology to external entities.

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

They CFPB typically only publishes aggregated and de-identified information that includes GIS technology output. Any GIS technology output must first be transmitted back to a CFPB on-premise server where it is analyzed and contextualized before being published or shared.

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

9 *See* 12 CFR 1002.101(b)(2).

Privacy Risk: There is a risk that information may be shared in a manner that is inconsistent with the original collection or that may identify individuals.

Mitigation: Data is not stored within the GIS vendor environment. It is stored on CFPB servers which sit behind the Bureau's firewall and have a baseline of controls to ensure the security of the data. The CFPB controls the installation, patches, and updates to the technology. Further, the GIS vendor does not have access to the data. These measures ensure that the CFPB is in full control of the data and can prevent the external sharing or exposure of the data.

The risk of re-identification of individuals is mitigated by data only being shared in aggregate. Published datasets, such as HMDA or eventually SBL, are subject to further analyses to understand re-identification risk and implement mitigations such as data redaction.

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,[10] the Right to Financial Privacy Act,[11] Section 208 of the E-Government Act of 2002, 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.[12] 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 (OMB) privacy-related guidance[13] and applies the National Institute of Standards and Technology (NIST) Risk Management

[10] 5 U.S.C. § 552a.

[11] 12 U.S.C. §§ 3401-3423.

[12] *See* CFPB PRIVACY POLICY (Oct. 10, 2024), and subsequent updates.

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

Framework (RMF)[14] for information technology systems, applications, solutions, and services. The CFPB identifies and applies NIST SP-800-53[15] security and privacy controls and continuous monitoring of controls to ensure on-going compliance with information security standards and protect organizational operations and assets and individuals. The GIS technology is obtaining an Authority to Operate from the CFPB's authorizing official. New uses of GIS technology are assessed to identify new impacts to privacy, and updates to this PIA and appendices to this PIA will be completed to address these new risks.

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 GIS technology and annually thereafter. The Privacy Training ensures that CFPB Staff understand their responsibilities to safeguard PII and identify and report suspected or confirmed privacy breaches within twenty-four hours of discovery. The 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.

Additionally, GIS users are required to read a document outlining server best practices, data security measures, appropriate behavior, and acceptable use. This document outlines good data management and privacy principles and reinforces that they are subject to their division guidelines on storage and handling of sensitive information.

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

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 GIS technology.

---

[14] *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.

[15] *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.

Users with elevated privileges must sign and electronically submit the *Privileged User Access (PUA) Form* to the CFPB ServiceDesk to obtain elevated access to the GIS and review and acknowledge the *Rules of Behavior for Privileged Users*. Individuals who no longer require access have their credentials removed from the system.

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"[16] 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). This ensures the CFPB maintains a secure operating environment and protects our systems against potential external threats.

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

Privacy Risk: There is a risk that unauthorized CFPB Staff may access the GIS technology or associated output.

Mitigation: To mitigate this risk, the CFPB has implemented the above technical, physical, and administrative controls to safeguard PII and other sensitive information used in and derived from the GIS technology. For example, access to the GIS technology is limited to CFPB Staff who have a need to know the information in the performance of their duties. 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 the GIS technology and review and acknowledge the *Rules of Behavior for Privileged Users*. Additionally, PIV+PIN authentication and authorization is enforced on the Enterprise GIS technology deployment.

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

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[17] 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. CFPB Staff are required to review and sign the CFPB's "Acceptable Use of CFPB Technology Resources Policy"[18] 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 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.

[17] *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.

[18] AUP, *supra* note 16.

Document control

Approval

_____

Christopher Chilbert

Chief Information Officer

_____

Kathryn Fong

Chief Privacy Officer

_____

Monica Shelton

Application Owner

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

Change Control

Version	Summary of material changes	Pages affected	Date of change
1.0	Initial Publication	All	