Extranet 2.0

Privacy Impact Assessment

July 18, 2025

Consumer Financial Protection Bureau

Overview

The Dodd-Frank Wall Street Reform and Consumer Protection Act, Public Law No. 111-203, Title X (herein referred to as the Act), 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.

To support its work, the CFPB requires the collection, use, and sharing of data as permitted by applicable law. The CFPB uses general information technology (IT) support systems to enable the Bureau to collect, process, disseminate, and store data. This data may include personally identifiable information (PII) of members of the public, consumers, representatives or employees from supervised entities, external partners and stakeholders, and CFPB Staff, among others. The type of PII that CFPB collects varies and is dependent upon the specific program purposes and uses.

Oftentimes, the collection, transmission, and sharing of PII requires secure communications, particularly when larger file attachments or multiple file attachments being sent exceed the maximum allowed size in email. The CFPB meets this need with the Extranet, which is a Federal Risk and Authorization Management Program (FedRAMP) approved software tool. Extranet provides a secure method of file transfer that enables CFPB programs to communicate information requests, receive and intake files from external sources, and direct large files, including information that may contain PII. Extranet collects data through a variety of methods including email, secure file transfer protocol (SFTP), managed file transfer (MFT), and secure forms. It also allows replacement of less secure or less efficient processes such as physically mailing or emailing information. Additionally, the Extranet can be used to transmit data to external entities, instead of exporting data using physical drives.

To use Extranet, CFPB initiates a communication by entering a recipient point of contact, such as a first name and last name and email address. Once entered, Extranet creates a secure communication channel allowing CFPB to input requests for information and transmit data as attachments. When complete, Extranet generates a secure link to the platform for authorized recipients (*i.e.,* internal and external users) to view, upload, or download documents. Extranet provides a secure link to the recipient, who must then register an account within Extranet to send and receive information securely with CFPB, including first name and last name, email address, and the creation of a password to access the Extranet account. The information is only shared for

a specified length of time, as determined by the program office. After the set access time is expired, the communication and attachments are automatically deleted from the tool.

Extranet is authorized pursuant to 12 U.S.C. 5492. It is hosted within a FedRAMP-client vendor environment that provides a secure, cloud hosted environment in which to operate. As an enterprise tool, Extranet is managed by the CFPB Legal Technology Support Team[1] and is currently used by several Bureau offices and programs to conduct their business, including the Office of Civil Rights (OCR), the Office of Consumer Populations (OCP), Division of Enforcement, Division of Supervision, Office of General Law and Ethics, and the Freedom of Information Act (FOIA) programs. The scope of this privacy impact assessment (PIA) is to discuss the use of Extranet as a secure transfer and communications tool in support of CFPB data collection and sharing, and how CFPB mitigates those risks. The specific type of information, including PII, used within Extranet is discussed in program specific CFPB PIAs[2] and, where applicable, in CFPB system of records notices (SORNs)[3]. This PIA updates and replaces the Extranet PIA published on November 7, 2014 by addressing risk assessment associated with the new solution, and adopts the CFPB's newest PIA template.

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[4] and in alignment with Office of Management and Budget[5] (OMB) guidance and the National Institute of Standards

[1] For more information about the CFPB's Legal Technology Support Team please see the Legal Technology Support Team (LTST) v.2 PIA, located at https://www.consumerfinance.gov/privacy/privacy-impact-assessments/.

[2] Please see https://www.consumerfinance.gov/privacy/privacy-impact-assessments/

[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.

and Technology (NIST) standards. This PIA examines privacy risks and describes mitigation measures associated with Extranet that support Bureau programs, offices, and divisions 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.

Extranet provides a secure method of file transfer that enables CFPB programs to communicate information requests, receive files from external sources, and provide files to external parties. Extranet collects PII from the individuals who transfer or receive information, in order to create an account. These individuals may include members of the public, consumers, representatives or employees from covered persons or service providers, external partners and stakeholders, and CFPB Staff, among others. The PII includes the individual's full name, email address, and a password. The files and documents transferred via Extranet may contain PII, depending on the documentation being shared. For example, the Office of Civil Rights (OCR) uses Extranet to securely receive and process claims of discrimination which are directly communicated to OCR by employees, former employees, and applicants[6]. In that context, PII includes name and last name, email addresses, and details specific to the matters that are the subject of the complaint or otherwise related to the complaint. Extranet allows OCR to share and send documents to and from internal and external complainants and complainant representatives.

The specific elements of PII and Bureau uses of the information collected through Extranet are described in CFPB program and system PIAs, such as the OCR Equal Employment Opportunity (EEO) PIA.

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

Extranet allows CFPB to collect information directly from authorized users (either internal or external to CFPB). These authorized users may include members of the public, consumers,

[6] For details about OCR's use of data, please see the OCR Equal Employment Opportunity (EEO) Program privacy impact assessment at https://files.consumerfinance.gov/f/documents/cfpb_office-of-civil-rights-equal-employment-opportunity-system_2023-05.pdf.

representatives or employees from covered persons or service providers, external partners and stakeholders, and CFPB Staff. The specific sources of PII collected, disclosed, and used by CFPB programs, offices, and divisions to communicate within Extranet are described in applicable CFPB program and system PIAs.

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

Information used by CFPB within Extranet may be subject to PRA, and CFPB program office must comply with PRA requirements, as applicable. For example, when CFPB conducts market research it seeks OMB approval under the PRA through one of the Bureau's generic information collection plans or standard clearances (e.g., "CFPB Generic Information Collection Plan for Studies of Consumers using Controlled Trials in Field and Economic Laboratory Settings"), or through separate clearances specific to a program or research project[7].

Specific OMB collection numbers for information collected and used by CFPB programs, offices, and divisions to communicate within Extranet are described in CFPB program and system PIAs and forthcoming appendices to this PIA.

1.4 Discuss how the accuracy of the information is ensured.

Extranet provides the secure communication of information between internal and external users of the system. When leveraging Extranet to conduct business, a program, office or division must identify a recipient point of contact to initiate communication through Extranet. For individuals to respond to CFPB through Extranet, they must use a secure session link to access the tool. The accuracy of this point of contact, along with any information shared through the communication, is validated by the program, office, or division prior to inputting the information in Extranet, and upon receiving information retrieved through Extranet.

Privacy Impact Analysis: Related to Characterization of the Information.

Privacy Risk: There is a risk that Extranet may be used to inadvertently provide information to an unauthorized individual by mistakenly entering the wrong recipient's contact information.

[7] Please see https://files.consumerfinance.gov/f/201412_cfpb_market-research-in-the-field-v1.pdf.

Mitigation: CFPB addresses this risk by verifying the accuracy of recipient information prior to sending out communications using Extranet. Further, Extranet provides a secure link to the recipient, who must then register an account within Extranet to send and receive information securely. Each communication action within Extranet, such as opening an email, opening an attachment, or accessing an Extranet account, requires verification through multi-factor authorization prior to access.

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).

Extranet is a tool used by CFPB to conduct secure communications and data transfers. Individual program offices use Extranet to conduct this business based upon a need to know the information being requested, submitted, or received by an authorized recipient. Extranet requires a first name, last name, and email address to initiate communication. Recipients must register an account within Extranet by providing their first name, last name, and email address along with a password to gain access to the account. This PII is the minimum necessary to securely communicate within Extranet. Communications, attachments, and other forms of data that include PII that traverse Extranet is verified as necessary to accomplish the specified purposes by each program, office, and division as based upon the Bureau's legal authority and needs of CFPB to complete its work.

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.

Data used within Extranet is transitory in nature as the tool provides a secure method of communications. Extranet is not a primary means of storing data, instead it provides a temporary repository for data used within the tool. Data is then removed and used and stored by the program and any copies of the data are deleted within the tool. This transitory nature is covered by General Records Schedule DAA-GRS-2016-0016-0002. Any records collected through the use of the tool follow the applicable records retention schedules assigned to that data within the responsible CFPB program.

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

Privacy Risk: There is a risk that data that traverses Extranet is more than is necessary to conduct business processes.

Mitigation: To mitigate this risk program offices that use Extranet verify that information shared and received within the tool is the minimum necessary to complete the assigned task. Further, all PII contained within communications and attachments in Extranet are viewable only by the CFPB-authorized recipient and CFPB sender, and only shared for a specified length of time, as determined by the program office. After the set access time is expired, the communication and attachments are automatically deleted from the tool. If unnecessary data is submitted or received through the Extranet tool, the system owner has the administrative access to delete communications and attachments as requested by the program.

3. Uses of Information

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

Extranet provides a secure communication and data transfer with internal and external stakeholders for a wide variety of purposes. CFPB offices and programs collect and use PII via Extranet consistent with their legal authorities and business needs; the Extranet only provides the technical capability to request and receive the information. Some of these purposes include collecting information to enforce federal consumer financial protection laws; conduct market analysis and research to fulfill statutory requirements, promote competition in the financial marketplace, and inform consumers; receive and respond to consumer complaints about financial products and services; and supervise covered entities.

Additionally, the Extranet enables administrative functions within CFPB, to include the completion of voluminous FOIA or Privacy Act requests that are too large for email; and process employment-related claims directly communicated by employees, former employees, and applicants.

Lastly, the Extranet can be used to share documents with internal CFPB personnel regarding various internal matters; share relevant documents with other government agencies, third parties, or opposing counsel in the course of investigation or litigation; or submit statutorily required reports regarding Bureau activities to external parties, such as Congress, the Office of Management and Budget (OMB) or others. There may be other use cases or occasional needs where time-sensitive files need to be transmitted that are too large for email, and where recipients are unable to accept files via another secure method.

These uses are addressed in further detail in CFPB program and system PIAs that may use the Extranet as part of its data collection and sharing processes.

PII collected directly by Extranet from CFPB staff is used to provision access to the tool. PII collected from external users is also used to register and provision access to the Extranet for secure transmission and reception of data.

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

Information collected using Extranet is contained within communications and attachments that are viewable only by the CFPB-authorized recipient and CFPB sender, and only shared for a length of time that can be determined by the program sending the communication. The Extranet uses an Application Programming Interface (API) to move files to or from CFPB's SharePoint Online environment. CFPB programs, offices, and divisions may grant access to other program, systems, or projects within SharePoint Online depending upon the type of information received via Extranet. To share data within Extranet, the program office stakeholder must submit a request for another authorized user to be granted access; access can only be granted by the Extranet administrator. The program office may also download data from Extranet and share with other CFPB programs. The type of PII that may be shared via Extranet is specific to respective program offices and is based on the authority and purpose for the collection and a need to know by authorized CFPB stakeholders. Extranet is used by programs to conduct their business within the tool, including sharing of data to and from a user. PII collected from a user for registration and use of the tool is only used for that purpose and is not shared. Sharing of any data used by programs, offices, and divisions is addressed in CFPB program and system PIAs and within appendices to this PIA, as applicable.

Privacy Impact Analysis: Related to Uses of Information

Privacy Risk: There is a risk that CFPB may use information within Extranet in a manner inconsistent with the intended purposes for which it was collected, or share information with those who do not have a need to know.

Mitigation: To mitigate this risk, the CFPB shares information sent or received within Extranet only with CFPB program, offices, and divisions that have an authorized need to know. A limited number of CFPB-authorized users have access to Extranet to initiate and receive communications and data within the tool. CFPB users who are granted access to the tool may select an individual to send information to, and will only have access to information that is sent back to them by the

recipient. Granting access to only authorized users of Extranet ensures that the information is used in a manner consistent with the intended purpose. This limits the risk of an Extranet user being able to see all communications within the tool. To share data within the tool, an authorized CFPB user must send a message to a recipient, who then must register an account with Extranet in order to access the communication and information being sent. This further limits the ability to inadvertently send data. Finally, any communication and data that resides on Extranet is temporary, with CFPB-imposed time limits on how long data may be retrieved. Once time limits expired, data is deleted from the tool, reducing the risk of data being accessed by a future CFPB Extranet user.

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.

CFPB provides a Privacy Act Statement on the Extranet user log-in page that informs the user of the general uses of information for logging into and using Extranet. Notice related to information collected and shared through Extranet is addressed in program and system PIAs and in appendices to this PIA, along with applicable CFPB SORNs.

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.

A notice regarding the collection of information for general login and use of Extranet is provided on the Extranet login page. Users may choose to decline the use of Extranet as a result of this notice and may work with CFPB to identify another method of communication suitable for the information being shared or received, if available. Consent related to information collected and shared through Extranet is addressed in CFPB program and system PIAs and in appendices to this PIA, along with applicable CFPB SORNs.

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

Individuals may seek to access or correct their information maintained in CFPB system of records through the CFPB's FOIA Office in writing in accordance with the Bureau's Disclosure of Records and Information Rules, Subpart E-Privacy Act 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. Additional information may also be found on CFPB's website at https://www.consumerfinance.gov/privacy/.

All or some of the information used by programs, offices, and divisions within Extranet may be exempt from access pursuant to the Privacy Act of 1974 or FOIA to prevent harm to a CFPB investigation or enforcement action.

Privacy Impact Analysis: Related to Individual Notice and Participation

Privacy Risk: There is a risk that an individual may not have an opportunity to opt out or participate in the collection of their information using the Extranet tool.

Mitigation: Notice and participation related to information collected and shared through Extranet can be found in CFPB program and system PIAs and in appendices to this PIA, along with applicable CFPB SORNs. In some cases, individuals' information contained within Extranet communications are part of CFPB matters or covered orders, or are contained within public documents being submitted to the Bureau. In these cases, individuals may not have the opportunity to opt out or participate in the use or sharing of their information as these documents are required pursuant to law and CFPB rulemaking. CFPB has taken steps to mitigate these risks by limiting the collection of PII to only the minimum necessary to complete a CFPB request for information. Individuals may also refer to more information located on CFPB's website at https://www.consumerfinance.gov/privacy/ for information on how to inquire whether their information is used or shared by CFPB, and actions they may take to amend, correct, or remove their PII as appropriate.

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.

Extranet provides CFPB programs, offices, and divisions with the ability to securely transfer information with external parties. Any external disclosure of CFPB data are addressed in further detail in CFPB program and system PIAs, subject to the legal authorities that govern the use of the data, existing sharing agreements in place, and routine uses identified within CFPB SORNs, as applicable. Registration data used to provision access to Extranet is not shared.

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

Information shared externally through communications, attachments, and other forms of data through Extranet is subject to applicable law, the use agreements and requirements as set forth by the CFPB program, office, and division. The Legal Technology Support Team (LTST) manages access to the system and requires a form to be completed for each program user that describes the use case for Extranet and the capabilities required to perform the data collection. Further, LTST places default limits on link and file storage expirations, and files are removed from Extranet after this expiry term. Extranet user profiles are configured to restrict sharing and request functions to only what the program needs to perform the data collection or sharing function. Details about the specific type of information shared externally can be found within CFPB program and system PIAs and in appendices to this PIA, and in SORNs that are applicable to the information.

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

Privacy Risk: There is a risk that information may be shared externally for purposes that are inconsistent with the original collection.

Mitigation: To mitigate this risk, the CFPB has implemented administrative and technical access controls that help to ensure information used within the Extranet tool is used according to the purposes identified in this PIA and by the programs, offices, and divisions responsible for the data. Only CFPB authorized users who have created an Extranet account can send communication and information to CFPB-authorized recipients. Recipients must also create an Extranet account prior to accessing any communications and information provided through Extranet.

Authorized recipients may download communications and data from Extranet for use as authorized by law, and as set forth in data agreements, memoranda of understanding, etc. as established by programs, offices, and divisions who use the data. Specific limits on the external use and sharing of data outside of the Extranet functionality can be found in CFPB program and system PIAs and in appendices to this PIA.

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, the Right to Financial Privacy Act, 27 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. 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 to ensure compliance with all laws, regulations, and policy requirements.

The CFPB adheres to the Office of Management and Budget (OMB) privacy-related guidance and applies the National Institute of Standards and Technology (NIST) Risk Management Framework (RMF) for information technology systems, applications, solutions, and services. The CFPB identifies and applies NIST SP-800-53 security and privacy controls and continuous monitoring of controls to ensure ongoing compliance with information security standards and to protect organizational operations and assets and individuals. For example, CFPB assesses the use of APIs to transfer files from the Extranet to CFPB's SharePoint Online environment to ensure the connection has the appropriate controls in place to protect the data. The Extranet system has obtained an Authority to Operate from the CFPB's authorizing official. New uses of Extranet 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 systems.

Specific to Extranet, LTST has completed train-the-trainer sessions that describe the privacy and security capabilities of the tool. This training provided LTST with the ability to place default limits on link and file storage expirations and configure program use profiles to restrict sharing and request functions to only what the program needs to perform the data collection or sharing function. All CFPB Staff are also 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 Extranet 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. 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.

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" 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. In addition, the CFPB employs role-based access controls. The CFPB uses role-based access controls to ensure CFPB Extranet users 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 Extranet by a CFPB Extranet administrator. Individuals who no longer require access have their credentials removed from the system. In addition, access controls allow CFPB to identify an authorized recipient and CFPB sender, and only share for a CFPB-specified length of time. After the set access time is expired the communication and attachments are deleted from the platform.

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

Privacy Risk: There is a risk that Extranet and the 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 Extranet. As noted above, CFPB Staff cannot access the system without being granted access by the system's Product Owners. 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 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" and complete the privacy and security training within thirty days of their onboarding, 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 review audit logs of the system and applications identified herein to monitor for unusual behavior (e.g., disabling 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 within Extranet 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 in violation of CFPB policy, system access may be revoked. If there is evidence of potential misconduct, the incident will be referred to the appropriate Bureau office for investigation and further review. CFPB Staff will be disciplined accordingly, which could include adverse actions or removal from the CFPB.

Document control

Approval

_____

Christopher Chilbert Chief

Information Officer Date

_____

Kathryn Fong

Chief Privacy Officer Date

_____

Jeffrey Sutorus

System Owner

Date

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