OCTOBER 30, 2012

Privacy Impact Assessment

COMPLIANCE ANALYSIS TOOLKIT

Contact Point:
Claire Stapleton
Chief Privacy Officer
1700 G Street, NW
Washington, DC 20552
202-435-7220
claire.stapleton@cfpb.gov

Consumer Financial Protection Bureau

DOCUMENT PURPOSE

The Privacy Impact Assessment or "PIA" provides the public with information about the Consumer Financial Protection Bureau's ("CFPB" or "Bureau") collection and use of personally identifiable information ("PII"). PII is any information "that can be used to distinguish or trace an individual's identity"[1] like a name, address, Social Security number, or place and date of birth. The CFPB uses PIAs to document how the PII it collects is used, secured, and destroyed in a way that protects each individual's privacy. Each PIA is broken out into sections that reflect the CFPB's Privacy Principles. The CFPB's Privacy Principles are a set of nine rules the CFPB follows when it collects or uses PII.

OVERVIEW

PROJECT / SYSTEM NAME: Compliance Analysis Toolkit

PROJECT/SYSTEM INCLUDES INFORMATION ABOUT:

- ☒ Federal Employees
- ☒ Contractors
- ☐ Consultants
- ☒ The Public

PROJECT/SYSTEM INCLUDES:

- ☒ Name and other biographic information (e.g. date of birth)
- ☒ Contact Information (address, zip code, telephone number, email address)
- ☐ Social Security number ("SSN") or other identifier
- ☒ Financial Information
- ☐ User and Online Information
- ☐ Third Party Information
- ☐ Other Information (including biometric information and health or medical information)

The Dodd-Frank Wall Street Reform and Consumer Protection Act (the "Act"), Public Law No. 111-203, Title X, established the CFPB. The CFPB administers, enforces, and implements federal consumer financial protection laws, and, among other powers, has authority to protect consumers from unfair, deceptive, and abusive practices when obtaining consumer financial products or services.

One of the CFPB's primary responsibilities is to supervise companies[2] that provide consumers with financial products or services. Part of the supervision process involves reviewing loan data, which includes information about loans that a supervised company has made or bought and is holding for repayment.

The Compliance Analysis Toolkit (the "CAT") automates and streamlines the collection and

---

[1] Office of Management and Budget (OMB) Memorandum 07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*, May 22, 2007, (OMB M-07-16) defines PII as information which "can be used to distinguish or trace an individual's identity, such as his or her name, social security number, biometric records, etc., alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc."

[2] For the purposes of this PIA, the term "companies" includes all entities the CFPB has authority to supervise under the Act.

analysis of this data by providing a centralized system where supervised companies can securely upload loan file data for analysis by CFPB examiners.

The CFPB is publishing this PIA to document its use of the CAT and its impact on privacy. In addition, PII contained in the CAT is documented in three System of Records Notices ("SORN"), CFPB.002 – CFPB Depository Institution Supervision Database [76 FR 45766], CFPB.003 – CFPB Non-Depository Institution Supervision Database [76 FR 45761], and CFPB.014 – Direct Registration and User Management System [77 FR 24185].

SECTION 1.0 PURPOSE OF COLLECTION

The CFPB will state the purpose and legal authority for collecting PII.

1.1 Why is the information being collected?

The CFPB collects and maintains PII in the CAT to supervise companies under its authority.

1.2 What legal authority and/or agreements allow the information to be collected?

Authority for the CAT is provided by Pub. L. No. 111-203, Title X, Section 1011, 1012, 1021, 1024, and 1025, codified at 12 U.S.C. §§ 5491, 5492, 5511, 5514, and 5515.

1.3 Is the information searchable by a personal identifier – like a name or Social Security number? If so, what Privacy Act System of Records Notice(s) apply/applies to the information being collected?

The CAT is searchable by the name of an employee of a supervised company, of a CFPB employee who is a user of the system (collectively "users"), by a user ID, or by the name of a loan officer associated with a loan file as described in the SORNs for the system.

1.4 Is there a records retention schedule that has been approved by the National Archives and Records Administration (NARA) for the information system(s)? Explain how long and for what reason the information is retained.

The CFPB maintains computer and paper records indefinitely until NARA approves the CFPB's records disposition schedule. Records that fall under a general records schedule will be disposed of according to the applicable schedule.

1.5 Are there any forms or surveys that are associated with the collection of the information that would be covered by the Paperwork Reduction Act (PRA)?

The CAT does not use a form subject to PRA requirements.

1.6 Are there any privacy risks for this system that relate to the purpose of the collection? If so, how will the CFPB

mitigate these risks?

There are no identifiable risks associated with the purpose of this system.

SECTION 2.0 OPENNESS AND TRANSPARENCY

The CFPB will be open and transparent. We should tell individuals about the PII we collect and how we will protect it, use it, and share it. We will provide an easy way for individuals to learn about what is happening to their PII.

2.1 Will individuals be given notice prior to the collection of personal information about them? If not, please explain.

In general, yes. Users create their own account, have it created by their employer on their behalf, or have it created through an automated method, as described in Section 6.1 of this PIA. A Privacy Act statement is available to those who register to use the system and create their own account.

For users who have their account created on their behalf, such as CFPB employees who have their account automatically created, explicit notice may not be provided prior to the collection of personal information. Additionally, loan officers who have their PII uploaded into the system as part of loan file data will not receive explicit notice. The Bureau has provided constructive notice of how it will collect information stored in this system through this PIA and the associated SORNs.

2.2 Will individuals be given notice prior to their information being shared? If not, please explain.

Users are provided a Privacy Act statement only when they create their own account. For individuals who have their account created on their behalf, such as CFPB employees who have their account automatically created, explicit notice is not provided prior to their information being shared. Additionally, loan officers who have their PII uploaded into the system as part of loan file data will not receive explicit notice. The Bureau has provided constructive notice of how it will share information stored in this system through this PIA and the associated SORNs.

2.3 Are there any privacy risks for this system that relate to openness and transparency? If so, how will the CFPB mitigate these risks?

There are no risks associated with openness and transparency for this system.

SECTION 3.0 DATA MINIMIZATION

The CFPB will limit the collection of PII to what is needed to accomplish the stated purpose for its collection. The CFPB should keep PII only as long as needed to fulfill that purpose.

3.1 Whose information is included in the system?

The system includes information, including PII, about users of the system and about loan officers included in loan file data.

3.2 What PII will the system include?

PII about users of the system includes:

- Name (first, last);
- Company/organization employer name and title;
- Business contact information including address, phone (and extension), facsimile number, and email address; and
- Security question and answer for resetting password.

PII about loan officers associated with a particular loan in a loan file includes:

- Name (first, last); and
- Nationwide Mortgage Licensing System identifier ("NMLS ID").

3.3 Why is the collection and use of the PII necessary to the project or system?

PII about users of the system is used to:

- Communicate with users about their account; and
- Validate that individuals should have access to the system on behalf of their employer or the CFPB.

PII about loan officers associated with loan files is used to validate that the loan officer is licensed to represent the supervised company and is licensed to work in the specific state associated with the loan. Section 4.4 discusses the connection with NMLSR that supports this validation.

3.4 Will the system aggregate previously unavailable data about the individual or create new data about the individual? If so, how will this data be maintained and used?

The system does not aggregate data or create new data about individuals.

3.5 What controls exist to protect the consolidated data and prevent unauthorized access?

See Section 3.4 for more information.

3.6 Will the system monitor the public?

The system does not monitor the public.

3.7 Will the system monitor employees or contractors?

Yes, since the system monitors users' use of the system for auditing purposes.

3.8 What kinds of reports can be produced on individuals? Will the data included in the reports produced be made

anonymous?

The system will be able to produce reports about a user's use of the system for auditing purposes. Reporting security is outlined in Section 6.0.

Reports on loan file data will only include information on individuals to the extent that they contain the names of loan officers associated with a loan file.

3.9 Are there any privacy risks for this system that relate to data minimization? If so, how will the CFPB mitigate these risks?

There are no risks associated with data minimization for this system.

SECTION 4.0 LIMITS ON USES AND SHARING OF INFORMATION

The CFPB will publish a notice about how we plan to use and share the PII that we collect from you. We will only share your PII in ways that are compatible with the notice or as stated in the Privacy Act.

4.1 Is the information in the project limited to only the information that is needed to carry out the purpose of the collection?

All information collected is relevant and necessary for the registration and management of users' accounts in the system, or for supervision purposes. Section 3.3 provides more information.

4.2 Will the CFPB share any of the information with other individuals, Federal and/or state agencies, or private sector organizations? If so, how will the CFPB share the information?

Information contained in the CAT about users of the system may be shared as outlined in the SORN, CFPB.014 – Direct Registration and User Management System [77 FR 24185]. Information about loan officers in the system may be shared as outlined in the SORNs, CFPB.002 – CFPB Depository Institution Supervision Database [76 FR 45766] and CFPB.003 – CFPB Non-Depository Institution Supervision Database [76 FR 45761].

4.3 Is the information collected directly from the individual or is it taken from another source?

Generally information is entered directly by the individual seeking access to the system, but may also be entered by another individual acting on their behalf, or through an automated account creation process as outlined in Section 6.1. PII may also be collected through the loan file upload process.

4.4 Will the project interact with other systems, whether within the CFPB or outside of the CFPB? If so, how?

The CAT will interconnect with several other systems both within the CFPB and external to the Bureau.

Inbound connections from external sources include:

- Financial market data information automatically synched from external data sources on a monthly basis for compliance analysis. This information does not include PII; and
- Nationwide Mortgage Licensing System and Registry ("NMLSR") data automatically exported into the CAT on a monthly basis for compliance analysis. This data contains no PII other than the names and NMLS ID's of loan officers. More information is available under Section 3.3. You can learn more about the NMLSR at www.consumerfinance.gov.

Inbound connections from internal systems include:

- Treasury/CFPB Active Directory for syncing to automatically create user accounts for CFPB employees.

Outbound connections to internal systems include:

- Uploaded or modified loan file data aggregated into a single file and, along with compliance analysis reports, exported to the CFPB's General Support System ("GSS") on a nightly basis.

4.5 Are there any privacy risks for this project that relate to use limitation? If so, how will the CFPB mitigate these risks?

There are no risks associated with use limitation for this system.

SECTION 5.0 DATA QUALITY AND INTEGRITY

The CFPB will make reasonable efforts to ensure that all PII it maintains is accurate, relevant, timely, and complete.

5.1 How will the information collected be verified for accuracy and completeness?

In general, users who register to use the CAT are responsible for submitting accurate information in setting up their account.

Additionally, the system has automated technical controls which help reduce erroneous or incomplete information, including:

- First name and last name fields cannot be null and user IDs must be unique;
- Users may only choose from a drop-down list of approved company names rather than type in a company name;
- State names and abbreviations are validated against a list of states within the United States;
- ZIP codes entered are validated for minimum and maximum length;
- Phone numbers are validated for minimum and maximum length; and
- Users are required to submit a valid email address to which an email is sent for registration as described in Section 6.1.

Additionally, CFPB employees may have their account automatically created and validated through the process described in Section 6.1.

Loan file information uploaded by supervised companies is checked for correct format and completeness for analysis by the system; however, the accuracy of information submitted in the files can't be validated by the system. An automatic connection between the CAT and the NMLSR also validates certain information in the loan file data. This is discussed in Sections 3.3 and 4.4.

5.2 Are there any privacy risks for individuals whose information is collected or used by the project that relate to data quality and integrity? If so, how will the CFPB mitigate these risks?

There are no risks associated with data quality and integrity for this system.

SECTION 6.0 SECURITY

The CFPB must protect PII from loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure.

6.1 Who will have access to the data in the project? What is the authorization process for access to the project?

Access to information in the CAT is limited to individuals who demonstrate a *bona fide* need for access, including users and system development and operations staff. Access is managed through non-transferrable usernames and passwords, and assigned user roles.

User Type	Description / Privileges
Covered Person (Supervised Company User)	Can register for access and log in to the loan file submission and validation services. This is the user account used by employees of supervised companies.
Solution Support (CAT Help Desk)	Can add and manage users, provision security settings and modules. Does not have access to any data from any supervised companies. This is the user account used by system operations staff.
Regional Administrator (1/3 CFPB User Types)	Can provision access for examiners to Covered Person (supervised company user) accounts. Can access the Covered Person default settings and profile and has the ability to validate registration information and approve the account. Has access to all data from all supervised companies.
Entity Administrator (1/3 CFPB User Types)	Can provision access for examiners to Covered Person accounts. If assigned by Regional Administrator, can also access the Covered Person default settings and profile and has the ability to validate covered person registration information and approve the account. Can view and edit all of the loan file data and results in all Covered Person accounts and modules that they are assigned.
Examiner (1/3 CFPB User Types)	Has access to the Covered Persons and module(s) they are assigned. Can perform loan file data audits, view the results of the audits for the supervised companies that they have been provisioned for and perform loan file data related calculations.

In general, users may request access to the system through the secure web portal. To request access, they must provide the information outlined in Section 3.2 through the portal's electronic form.

Users must submit a valid email address to which an email is sent. This email includes a one-time confirmation link which a user must click in order to have their registration confirmed, and a determination made about that individual's status as an approved user. An email notification is sent to the user with the decision about their registration.

CFPB employees who are users of the system have the option of having their accounts created through the process outlined above or through an automated process which creates their account based on their CFPB Active Directory profile.

6.2 Has the CFPB completed a system security plan for the information system(s) supporting the project?

The CFPB completed a System Security Plan ("SSP") for the CAT on July 30, 2012. The application has been categorized as "moderate" level system.

6.3 How will the system be secured?

In addition to the user access controls outlined in Section 6.1, the system also includes multiple technical, physical, and administrative controls, including:

- Compliance with all relevant laws and requirements;[3]
- Encrypted data communication networks, private networks and/or encryption technologies used during the transfer of information;
- Integration, performance and user acceptance ("UAT") testing, as well as continuous monitoring testing and Information Technology Contingency Plan ("ITCP") testing;
- Data input validation to ensure that data is being provided in the correct format and does not potentially cause issues that could lead to SQL injection, cross-site scripting, etc.;
- Appropriate warning to the user in the case of incorrect entry of username/password combination;
- Locked accounts after 3 failed login attempts within a 120 minute period;
- Password change limitations - a maximum of 1 time during a 24-hour period;
- Requirements to change user password every 60 days;
- Restrictions on reusing the last 24 passwords;
- Requirements for passwords to contain at least 12 different characters and a combination of letters, numbers and special characters;
- Passwords validation for length, required characters, and previous use;
- Prompts to change password upon initial login;
- Non-printing and non-displaying passwords in the system's reporting functions;
- CFPB users are subject to established Rules of Behavior for the system; and

[3] Although pursuant to 12 U.S.C. 5497(a)(4)(E),, 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.

- Log in occurs through a secure web portal. Remote CFPB users are also required to log in through a secure, two-factor authentication process.

The system also audits transactions, including:

- Successful and unsuccessful login attempts;
- Invalid password login attempts;
- Hardware changes;
- Abnormal system events; and
- Specific actions (e.g. reading, editing, deleting, printing, opening and closing loan files.

6.4 Are there mechanisms in place to identify security breaches? If so, what are they?

The CFPB relies on the Treasury Department's directives related to security and privacy incidents. The CFPB is developing supplemental interim incident-reporting materials, and, upon moving onto its own network infrastructure, will issue new directives related to security and privacy incidents. Additionally, contractors responsible for developing and managing the CAT are obligated to immediately notify an established point of contact at the CFPB in the event that PII in the system is lost or compromised.

6.5 Are there any privacy risks for this system that relate to security? If so, how will the CFPB mitigate these risks?

There are no risks associated with security for this system.

SECTION 7.0 INDIVIDUAL PARTICIPATION

The CFPB will give individuals, in most cases, the ability to access their PII, and allow them to correct or amend their PII if it is inaccurate.

7.1 What opportunities are available for individuals to consent to uses, decline to provide information, or opt out of the project? If no opportunities are available to consent, decline or opt out, please explain.

Users requesting access to the CAT must provide the required information outlined in Section 3.0. Declining to provide this information will result in a denial of system access. Loan officers whose information is included as part of a loan file do not have the opportunity to decline to provide information.

7.2 What procedures will allow individuals to access their information?

CAT users may manage and update certain information in their user account. Otherwise, the CFPB offers a means through the Privacy Act for individuals to access, amend, or correct their records. Information about Privacy Act requests is available in the SORNs for this system, and at www.consumerfinance.gov/foia.

7.3 Can individuals amend information about themselves in the system? If so, how?

Yes. Section 7.2 outlines this process.

7.4 Are there any privacy risks for this system that relate to individual participation? If so, how will the CFPB mitigate these risks?

There are no risks for this system related to individual participation.

SECTION 8.0 AWARENESS AND TRAINING

The CFPB will train all personnel about the proper treatment of PII.

8.1 Describe what privacy training is provided to users, either generally or specifically relevant to the project.

The CFPB offers privacy and security training to all employees of the CFPB, including contractors who handle PII on behalf of the Bureau.

The CAT also requires each user of the system to have a log on ID and password. Additionally, users must agree to the system's Rules of Behavior prior to receiving access.

8.2 Are there any privacy risks for this system that relate to awareness and training? If so, how will the CFPB mitigate these risks?

There are no risks associated with awareness and training for this system.

SECTION 9.0 ACCOUNTABILITY AND AUDITING

The CFPB is accountable for complying with these principles. We will regularly check that we are meeting the requirements and take appropriate action if we are not doing so.

9.1 How does the system ensure that the information is used in accordance with the stated practices in this PIA?

The CFPB, in conjunction with the contractors operating the system, has implemented technical and administrative controls as outlined in this PIA to ensure the confidentiality, accuracy, and integrity of information in the CAT.

9.2 Are there any privacy risks for this system that relate to accountability and auditing? If so, how will the CFPB mitigate these risks?

There are no risks for the CAT that relate to accountability and auditing.