Privacy Impact Assessment of the Common Data Platform (CDP)

For Questions or Comments, please email: privacy.comments@frb.gov

1. System Overview

The Board of Governors of the Federal Reserve System's (Board) Supervision and Regulation (S&R) Division owns and manages the Common Data Platform (CDP), a cloud-based system that consolidates S&R supervisory data into a single secure environment. The CDP improves data discoverability, accessibility, and shareability, while supporting more efficient management of S&R data across the organization.

S&R data are collected from supervised financial institutions and acquired from other external sources to improve data analysis in support of the Board's supervisory activities (e.g., regulatory report filings, exam documentation, S&P global reports, correspondence), which have been consolidated into CDP.

Consolidation of existing data and analytical functionality into a single platform provides a more seamless experience for users to view and analyze data in one place, while also improving data security and data management capabilities.

In some cases, traditional artificial intelligence (AI), generative artificial intelligence (GenAI), or agentic AI may be leveraged to analyze documents containing personally identifiable information (PII).[1] In accordance with Board policy, certain AI use cases must first be approved by the Board's Chief AI Officer.

2. Information Collected, Sources, and Authority to Collect

2.1 What information about individuals is collected, used, maintained, or disseminated?

Board and Federal Reserve Bank employees, contractors, and customers of supervised financial institutions may include some or all of the following information:

- Name;

[1] PII is information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual. The Office of Management and Budget (OMB), OMB Circular A-130, "Managing Information as a Strategic Resource" (July 28, 2016).

- Business contact information (e.g., title, email address, phone number, employee ID, network ID);
- Supervisor name associated with staff;
- Location (District);
- Examiner Commissioning status (i.e., whether employee is a commissioned examiner);
- Permanent role(s);
- Task assignment(s);
- Knowledge area(s) (expertise and proficiency level); and/or
- Relevant external certification (training and development activities).

Financial institution records related to supervisory activities may include information about customer loans and accounts, including some or all of the following information:

- Customer name; *
- Telephone numbers;
- Home and business address(es);
- Driver's license number;
- Social security number;
- Birth date and place of birth;
- Citizenship information;
- Taxpayer identification number;
- Occupation and employment history;
- Education and professional credentials,
- Customer loan information (e.g., loan amount, loan and account numbers, balances and interest rates). *

*A customer's name and loan information may be present on documents in compliance with regulatory requirements such as Bank Secrecy Act/Anti-Money Laundering, Office of Foreign Assets Control requirements, and other laws and regulations.

Records about key employees and officers with supervised institutions may include the following information:

- Name,
- Contact information (business/home, address, phone, email);
- Details about their financial accounts and compensation; and

Information about compliance with applicable laws and regulations (e.g., illegal or unethical behavior).

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

Customer records are provided to the Board and Federal Reserve Banks by supervised financial institutions and other regulatory agencies during supervisory activities. Information may also be collected from other sources to improve data analysis in support of the Board's supervisory activities (e.g., regulatory report filings, exam documentation, S&P global reports, correspondence).

2.3 What are the legal authorities for this collection?

The Board and Federal Reserve Banks collect this information as part of its supervisory responsibilities under the Federal Reserve Act of 1913, as amended.

3. Use of the information collected

What is the purpose(s) for this information collection?

The information collected from supervised financial institutions is used to evaluate each institution's safety and soundness, and compliance with consumer and community affairs laws and regulations.

4. Data Minimization

How is the information collected and maintained relevant and necessary to accomplish the specified purpose(s)?

Information collected during bank examinations is relevant and necessary for the Board and Federal Reserve Banks to fulfill their supervisory responsibilities. All information collected by S&R and maintained in CDP is directly related to supervisory activities for the purpose of conducting research and analytics to further the mission of the Federal Reserve. Information about customers of supervised institutions is used to evaluate safety, soundness, and compliance with consumer and community affairs laws and regulations.

5. Access to Information

Who has access to this information?

Access is limited to authorized Board and Federal Reserve Bank staff, and other authorized federal, state, and foreign banking regulators who require access for official business purposes.

Information that users are permitted to access is based on their job responsibilities. Periodic reviews are conducted to determine whether users still require access, have the appropriate role, and whether there have been any unauthorized changes in any information maintained in CDP. CDP enforces comprehensive access management controls including data management and metadata tagging.

Disclosures may also be made under the Freedom of Information Act (5 USC §552).

6. Information Sharing and Disclosures

Does the Board share this information with third parties? If so, identify the organization(s) with whom the information is shared, the purpose for which it is shared, and how the information is accessed and used.

Information, including PII, may be shared as needed for conducting supervisory activities with staff of other federal bank regulatory agencies in conjunction with joint supervisory activities (Office of the Comptroller of the Currency (OCC), the Federal Deposit Insurance Corporation (FDIC), the Consumer Financial Protection Bureau (CFPB)), and state and foreign banking regulators, consistent with information sharing agreements.

7. Individual Participation

7.1 Do individuals have an opportunity to decline to provide their information or consent to the use of their information?

No. Individuals and financial institutions are required to provide the requested information, and do not have an opportunity to consent to the particular uses of their information by the Board or Federal Reserve Banks.

7.2 Are individuals able to access their own information?

Individuals are not able to access their own information.

8. Data Quality

What are the procedures for ensuring that the information maintained in the system is accurate, complete, and up-to-date?

Information is collected directly from Board and Federal Reserve Bank employees and contractors, while customer information is obtained from financial institutions during Federal Reserve Bank examinations. The examiner-in-charge, central point of contact, or a designee is responsible for ensuring the accuracy and completeness of the information acquired from financial institutions.

9. Data Retention

How long will the information be retained?

Data purchased from a third-party, acquired from other federal agencies or public sources are retained only as long as they are needed for business purposes, or in accordance with licensing agreements or contracts. Financial and supervisory data (e.g., financial data collected by financial institutions to fulfill their reporting requirements and supervisory data such as ratings, risk analysis, and supervisory findings) are retained indefinitely.

10. Security of Data

What are the administrative and technological controls used to secure the information against unauthorized access?

CDP is required to comply with the security and privacy controls of the "Security Assurance for the Federal Reserve" (SAFR), the Board Trust Model (additional controls for when Board information is processed, stored or transmitted in an information system managed by a Federal Reserve Bank), and the "Federal Risk and Authorization Management Program" (FedRAMP) for cloud systems.[2] SAFR is largely based on the National Institute of Standards and Technology's (NIST) Special Publication 800-53, "Security and Privacy Controls for Information Systems and Organizations."

11. Privacy Act of 1974

Is this a "system of records" (i.e., a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual) under the Privacy Act of 1974 (5 U.S.C. § 552a(a)(5))?

CDP is not a system of records under the Privacy Act since information is not retrieved by a name or personal identifier. Therefore, a system of records notice is not required, and individuals do not have access or amendment rights to their information under the Privacy Act.

Reviewed:

//Signed//
Charles Young
Senior Agency Official for Privacy

06/10/2026
Date

//Signed//
Jeff Riedel
Chief Information Officer

06/10/2026
Date

[2] https://www.fedramp.gov/.