United States Government Accountability Office

Report to the Ranking Member, Committee on Finance, U.S. Senate

January 2022

PRIVACY

Federal Financial Regulators Should Take Additional Actions to Enhance Their Protection of Personal Information

Accessible Version

GAO-22-104551

GAO Highlights

Highlights of GAO-22-104551, a report to the Ranking Member, Committee on Finance, U.S. Senate

January 2022

PRIVACY

Federal Financial Regulators Should Take Additional Actions to Enhance Their Protection of Personal Information

Why GAO Did This Study

Federal financial regulators are agencies that supervise the products provided by financial institutions. As part of their oversight responsibilities, many regulators collect and maintain a large amount of consumers' PII. Increased collection and use of PII by agencies can pose challenges in ensuring the protection of individuals' privacy.

GAO was asked to review regulators' handling of PII. This report examines (1) what mission-related PII selected federal financial regulators collect, use, and share, and (2) the extent to which selected regulators ensure the privacy of the PII they collect, use, and share, in accordance with federal requirements and guidance.

GAO selected for review five regulators based on their authority to enforce consumer protection laws and the amount of PII they collect. For each of these entities, GAO analyzed privacy documentation to determine methods by which regulators handle PII, and compared regulators' key practices for handling PII to federal guidance. GAO interviewed officials from these regulators on their handling of PII. GAO also reviewed available agency inspector general reports addressing privacy issues.

What GAO Recommends

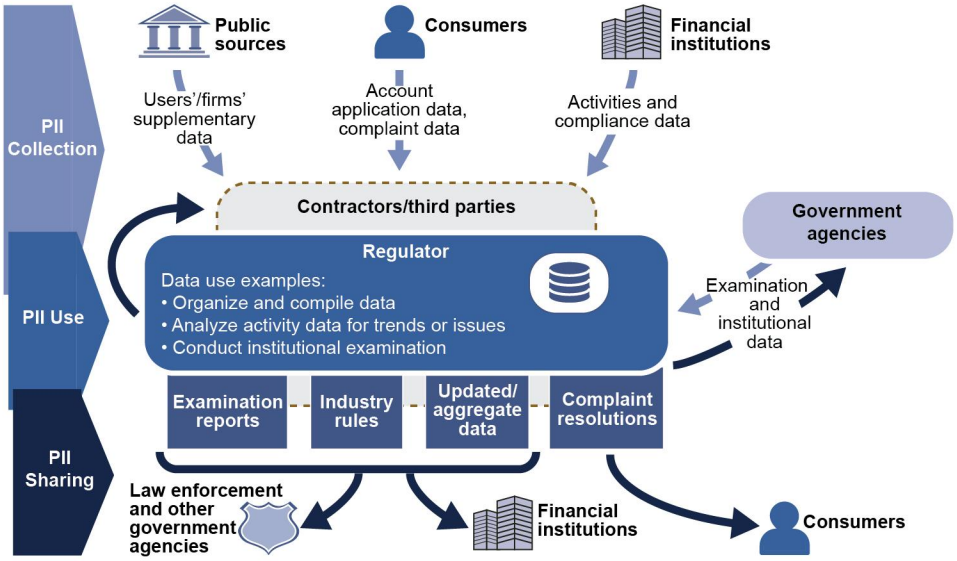
GAO is making eight recommendations to federal financial regulators to better ensure the privacy of the PII they collect, use, and share. FDIC generally agreed with the recommendation it received. Federal Reserve, NCUA, and OCC did not agree or disagree with the recommendations they received, but each described steps they planned to take to implement them.

View GAO-22-104551. For more information, contact Nick Marinos at (202) 512-9342 or MarinosN@gao.gov, or Alicia Puente Cackley at (202) 512-8678 or CackleyA@gao.gov.

What GAO Found

The five federal financial regulators GAO reviewed have built more than 100 information system applications that regularly collect and use extensive amounts of personally identifiable information (PII)—information that can be used to locate or identify an individual—to fulfill their regulatory missions. These regulators collect and share PII with entities such as banks or service providers, contractors and other third parties, and other federal and state regulators. The regulators also collect PII directly from individuals and from financial institutions. Regulators use the PII to conduct supervisory examinations of financial institutions and to receive and respond to complaints or inquiries from customers (see figure).

Collection, Use, and Sharing of Personally Identifiable Information (PII) at Selected Federal Financial Regulators



Source: GAO. | GAO-22-104551

All five financial regulators have created privacy programs that generally take steps to protect PII in accordance with key practices in federal guidance. For example, regulators fully addressed key practices for establishing privacy programs, conducting privacy training for staff, and implementing incident response procedures. However, four of the regulators did not fully implement key practices in other privacy protection areas. For example, the Board of Governors of the Federal Reserve System (Federal Reserve) and National Credit Union Administration (NCUA) did not maintain a full PII inventory for all agency-owned applications, and did not document steps they took to minimize the collection and use of PII. Also, the Federal Deposit Insurance Corporation (FDIC) and Federal Reserve did not establish agencywide metrics to monitor privacy controls, and the Federal Reserve and the Office of the Comptroller of the Currency (OCC) had not fully tracked decisions by program officials on the selection and testing of privacy controls. Until these regulators take steps to mitigate these weaknesses, the PII they collect, use, and share could be at increased risk of compromise.

Contents

Figure

Abbreviations

CAG	Customer Assistance Group
CFPB	Consumer Financial Protection Bureau
FDIC	Federal Deposit Insurance Corporation
FIPPs	Fair Information Practice Principles
HMDA	Home Mortgage Disclosure Act
IT	information technology
NCUA	National Credit Union Administration
NIST	National Institute of Standards and Technology
OCC	Office of the Comptroller of the Currency
OMB	Office of Management and Budget
PCM	privacy continuous monitoring
PIA	privacy impact assessments
PII	personally identifiable information
SORN	system of records notice

U.S. GOVERNMENT ACCOUNTABILITY OFFICE
441 G St. N.W.
Washington, DC 20548

January 13, 2022

The Honorable Mike Crapo
Ranking Member
Committee on Finance
United States Senate

Dear Senator Crapo:

The increasingly sophisticated ways in which the federal government obtains and uses personally identifiable information (PII) has the potential to assist in performing critical functions, such as helping to detect and prevent terrorist threats and enhancing online interactions with citizens.[1] However, these technological developments can also pose challenges in ensuring the protection of citizens' privacy. While bringing significant benefits, federal agencies' dependence on information technology (IT) can also create vulnerabilities that can result in, among other things, the compromise of sensitive personal information through inappropriate use, modification, or disclosure.

Data breaches at federal agencies, as well as at large organizations in the private sector, have resulted in the potential compromise of millions of Americans' PII, which could lead to identity theft and other serious consequences. Such incidents highlight the importance of ensuring the security and privacy of PII collected and maintained by those entities. As part of their oversight responsibilities over depository institutions such as banks and credit unions, federal financial regulators, including the Consumer Financial Protection Bureau (CFPB) and the four federal prudential regulators—the Federal Deposit Insurance Corporation (FDIC), the Board of Governors of the Federal Reserve System (Federal Reserve), the National Credit Union Administration (NCUA), and the Office of the Comptroller of the Currency (OCC)—collect and maintain a large amount of consumers' PII.

You asked us to examine the handling of PII at federal financial regulatory agencies. This report examines (1) what PII selected federal financial regulators collect, for what mission purposes they collect it, and how they

[1]Personally identifiable information is information that can be used to locate or identify an individual, such as names, aliases, Social Security numbers, biometric records, and other personal information that is linked or linkable to an individual.

use and share it; and (2) the extent to which selected federal financial regulators ensure the privacy of the PII they collect, use, and share for key mission applications, in accordance with federal requirements and guidance.[2]

For both objectives, we selected a subset of five federal financial regulators—CFPB, FDIC, the Federal Reserve, NCUA, and OCC. In addition to their large-scale PII collections, we selected these regulators based on their authority to enforce consumer protection laws in the financial sector.

For our first objective, we determined the methods by which each regulator collects, uses, and shares PII, the types of PII each regulator collects, the purposes for which regulators collect PII, and the methods by which each regulator provides notice to individuals whose PII the regulator collects. We also compared processes for sharing PII across the five regulators to determine common sources and destinations for the PII collected and shared by mission applications, as well as common uses of PII in these applications.

For our second objective, we analyzed federal laws and guidance to identify key practices for collecting, using, and sharing PII. The key practices we selected were in the areas of general privacy requirements; considerations for managing PII; use of contractors and third parties; privacy impact assessments; training and accountability; incident response; and use of a risk management framework. We then assessed agencywide policies and practices at each regulator for the collection, use, and sharing of PII against the key practices.

For each of the five regulators, we selected three or four applications for further review. We selected these applications based on factors including centrality to the regulator's mission, and their collection and use of large amounts of PII.[3] Across all five regulators, we selected 18 key mission applications. Among these, we included several functions that have a

[2]For this review, we focused on the PII collected by regulators in mission applications. For the purposes of this report, a mission application is any agency data system that collects and maintains PII for mission purposes, and for which an agency has conducted a privacy impact assessment. We did not focus, for instance, on applications with an internal focus, such as human resources applications.

[3]The list of key mission applications, and the purpose of each application, is listed in appendix VI.

common purpose across regulators, such as conducting regulatory examinations or fielding customer complaints. For each key mission application, we analyzed evidence of each regulator's practices for collection, use, and sharing of PII and compared this evidence with key practices in federal laws and guidance.[4] Appendix I includes additional information about our objectives, scope, and methodology.

We conducted this performance audit from October 2020 to January 2022 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Background

Organizations in the financial services sector such as depository institutions, equities and derivatives markets, and the providers of critical financial market utilities, are regulated based on the services they provide. Depository institutions are the primary providers of wholesale and retail payments services, such as wire transfers, checking accounts, and credit and debit cards. At the federal level, primary regulatory responsibility for depository institutions is carried out by four regulators—the Federal Deposit Insurance Corporation (FDIC), the Federal Reserve, the National Credit Union Administration (NCUA), and the Office of the Comptroller of the Currency (OCC).

These four regulators, known as prudential regulators, supervise depository institutions for the safety and soundness of their financial condition. Safety and soundness refer to a broad range of issues that relate to the health of an institution, including capital requirements, risk management, the quality and diversification of an institution's portfolio, liquidity and funds management, and adequate procedures for internal controls.

The jurisdiction of each regulator depends on the type of charter an institution chooses (including banks, savings associations or credit

[4]Mission applications, in the context of this review, are information systems or groups of information systems that process data. Mission applications include services or other mechanisms regulators use regularly to gather information.

unions) and the origin of the charter (federal or state). Table 1 explains the basic functions of the four prudential regulators, and their missions.

Table 1: Basic Functions and Missions of Federal Prudential Regulators

Agency	Basic function	Mission
Federal Deposit Insurance Corporation	Supervises insured state-chartered banks that are not members of the Federal Reserve System, as well as state savings associations and any insured state chartered branches of foreign banks; insures the deposits of all banks and thrifts that are approved for federal deposit insurance; has the authority to conduct backup examinations for any insured institution; resolves all failed insured banks and thrifts and, if appointed receiver by the Secretary of the Treasury, has authority to resolve certain large bank holding companies and nonbank financial companies.	To maintain stability and public confidence in the nation's financial system by insuring deposits, examining and supervising financial institutions for safety and soundness and consumer protection, making large and complex financial institutions resolvable, and managing receiverships.
Board of Governors of the Federal Reserve System	Supervises state-chartered banks that choose to be members of the Federal Reserve System; bank and thrift holding companies, and the non-depository institution subsidiaries of those institutions; nonbank financial companies designated by the Financial Stability Oversight Council (FSOC) for consolidated supervision and enhanced prudential standards; and certain financial market utilities designated as systemically important by the FSOC. Supervises state-licensed branches and agencies of foreign banks and regulates the U.S. nonbanking activities of foreign banking organizations.	To foster the stability, integrity, and efficiency of the nation's monetary, financial, and payment systems so as to promote optimal macroeconomic performance.
National Credit Union Administration	Charters and supervises federally-chartered credit unions and insures savings in federal and most state-chartered credit unions.	To provide, through regulation and supervision, a safe and sound credit union system, which promotes confidence in the national system of cooperative credit.
Office of the Comptroller of the Currency	Charters and supervises national banks, federal savings associations, and federally-chartered branches and agencies of foreign banks.	To ensure that national banks and federal savings associations operate in a safe and sound manner, provide fair access to financial services, treat customers fairly, and comply with applicable laws and regulations.

Source: Federal regulators' documentation. | GAO-22-104551

In addition to the four prudential regulators, the Bureau of Consumer Financial Protection—also known as the Consumer Financial Protection Bureau (CFPB)—regulates the offering and provision of consumer financial products or services under federal consumer financial laws. CFPB has exclusive examination authority over depository institutions with more than $10 billion in assets and their affiliates, and has primary enforcement authority for federal consumer financial laws. CFPB's mission is to implement and enforce federal consumer financial law

consistently to ensure that markets for consumer financial services and products are fair, transparent, and competitive, among other things.

CFPB interacts with the prudential regulators, which also have responsibility for overseeing federal consumer financial laws. The prudential regulators have consumer compliance examination authority for insured depository institutions with $10 billion or less in assets. The *Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010* requires CFPB to coordinate its supervisory actions and examinations of large depository institutions with the prudential regulators.

Federal Laws and Guidance Set Requirements for Privacy Protection

Federal laws and guidance specify requirements for federal agencies to protect systems and data, including systems used or operated by a contractor or other organization on behalf of a federal agency. CFPB and the four prudential regulators are also among the agencies that regulate and examine the use and sharing of consumer information under federal law. The *Privacy Act of 1974* and other statutes establish protections for personal information accessed or held by federal agencies.[5] These laws establish agency responsibilities with regard to protecting personal information. The Fair Information Practice Principles (FIPPs), which served as the basis for the *Privacy Act*, provide a framework of principles for balancing the need for privacy with other public policy interests, such as national security, law enforcement, and administrative efficiency.

The *Privacy Act* places limitations on the collection, disclosure, dissemination, and use of personal information maintained in "systems of records," or groups of records under the control of any agency from which information is retrieved by individual name or identifier.[6] The *Privacy Act* also requires agencies to notify the public in the *Federal Register* when

[5]The *Privacy Act of 1974*, 5 U.S.C. § 552a.

[6]5 U.S.C. § 552a. According to the *Privacy Act,* a ''record'' means any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, his or her education, financial transactions, medical history, and criminal or employment history and that contains his or her name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph. A ''system of records'' means 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.

they establish or make changes to a system of records. Among the things this notice must identify are: the categories of records collected; the categories of individuals about whom information is collected; the intended routine uses of data; and procedures that individuals can use to review and correct information about them.

The *E-Government Act of 2002* established privacy requirements for federal agencies through its requirement that agencies conduct privacy impact assessments before developing, using, or contracting for an IT system that contains personal information.[7] These assessments are analyses of how personal information is collected, stored, secured, and managed in a federal system.

Agencies must conduct privacy impact assessments (PIAs) (1) before developing or procuring information technology that collects, maintains, or disseminates information that is in identifiable form or (2) before initiating any new data collections of information in an identifiable form that will be collected, maintained, or disseminated using information technology if the same questions are asked of 10 or more people. Other federal guidance from the Office of Management and Budget (OMB) also requires agencies to conduct PIAs when a system change creates new privacy risks; for example, changing the way in which personal information is being used.

In July 2016, OMB published Circular A-130, *Managing Information as a Strategic Resource*, which established general policy for federal information, including the management of IT resources, for which it designates responsibilities to agency heads.[8] Circular A-130 provides guidance to agencies on many details of their privacy programs. Table 2 lists information on individual FIPPs as described in Circular A-130.

[7]Pub. L. No. 107-347, § 208, 116 Stat. at 2921 (2002) (codified at 44 U.S.C. § 3501 note). The privacy provisions of the *E-Government Act* apply to "information in identifiable form," which OMB has defined as information in an information technology system or online collection (i) that directly identifies an individual (e.g., name, address, Social Security number or other identifying number or code, telephone number, email address, etc.) or (ii) by which an agency intends to identify specific individuals in conjunction with other data elements, i.e., indirect identification. See Office of Management and Budget, *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*, Memorandum M-03-22 (Washington, D.C.: Sept. 26, 2003).

[8]OMB, *Managing Information as a Strategic Resource,* Circular A-130 (Washington, D.C.: July 2016).

Table 2: OMB Circular A-130 Fair Information Practice Principle (FIPP) Descriptions

FIPP	Office of Management and Budget Circular A-130 principles' descriptions
Access and amendment	Agencies should provide individuals with appropriate access to personally identifiable information (PII) and appropriate opportunity to correct or amend PII.
Accountability	Agencies should be accountable for complying with these principles and applicable privacy requirements, and should appropriately monitor, audit, and document compliance. Agencies should also clearly define the roles and responsibilities with respect to PII for all employees and contractors, and should provide appropriate training to all employees and contractors who have access to PII.
Authority	Agencies should only create, collect, use, process, store, maintain, disseminate, or disclose PII if they have authority to do so, and should identify this authority in the appropriate notice.
Minimization	Agencies should only create, collect, use, process, store, maintain, disseminate, or disclose PII that is directly relevant and necessary to accomplish a legally authorized purpose, and should only maintain PII for as long as is necessary to accomplish the purpose.
Quality and integrity	Agencies should create, collect, use, process, store, maintain, disseminate, or disclose PII with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to ensure fairness to the individual.
Individual participation	Agencies should involve the individual in the process of using PII and, to the extent practicable, seek individual consent for the creation, collection, use, processing, storage, maintenance, dissemination, or disclosure of PII. Agencies should also establish procedures to receive and address individuals' privacy-related complaints and inquiries.
Purpose specification and use limitation	Agencies should provide notice of the specific purpose for which PII is collected and should only use, process, store, maintain, disseminate, or disclose PII for a purpose that is explained in the notice and is compatible with the purpose for which the PII was collected, or that is otherwise legally authorized.
Security	Agencies should establish administrative, technical, and physical safeguards to protect PII commensurate with the risk and magnitude of the harm that would result from its unauthorized access, use, modification, loss, destruction, dissemination, or disclosure.
Transparency	Agencies should be transparent about information policies and practices with respect to PII, and should provide clear and accessible notice regarding creation, collection, use, processing, storage, maintenance, dissemination, and disclosure of PII.

Source: Office of Management and Budget, *Managing Information as a Strategic Resource*, Circular A-130. | GAO-22-104551

Appendix II of Circular A-130 also describes agency responsibilities for managing PII, and outlines general responsibilities for federal agencies managing information resources that involve PII. For example, Circular A-130 requires agencies to ensure that terms and conditions in contracts and other agreements incorporate privacy requirements for the protection of federal information, and to maintain an inventory of systems that create, collect, use, process, store, maintain, disseminate, disclose, or dispose of PII. Of the nine primary areas of privacy guidance listed in appendix II of Circular A-130, table 3 describes seven key areas that

focus on primary privacy program components and assessment of privacy risks.[9]

Table 3: Privacy Responsibility Areas in Office of Management and Budget Circular A-130 Appendix II

Privacy responsibility area	Description of elements included in each area
General requirements	Agencies shall have comprehensive privacy programs that ensure compliance with applicable privacy requirements, develop and evaluate privacy policy, and manage privacy risks.
Considerations for managing PII	Agencies' privacy programs shall maintain an inventory of personally identifiable information (PII), regularly review all PII maintained by the agency, and comply with applicable requirements regarding the creation, collection, use, processing, storage, maintenance, dissemination, disclosure, and disposal of PII. In addition, agencies' privacy programs shall impose, where appropriate, conditions on other agencies and entities to which PII is being disclosed that govern the creation, collection, use, processing, storage, maintenance, dissemination, disclosure, and disposal of the PII.
Contractors and third parties	Agencies' privacy programs shall ensure that entities that create, collect, use, process, store, maintain, disseminate, disclose, or dispose of information on behalf of a federal agency, or that operate or use information systems on behalf of a federal agency, comply with the privacy requirements in law and OMB policies.
Privacy impact assessments	Agencies shall conduct privacy impact assessments—analyses of how PII is handled—in accordance with the *E-Government Act*, and make the assessments available to the public.
Training and accountability	Agencies' privacy programs shall develop, maintain, and provide agencywide privacy awareness and training programs for all employees and contractors. In addition, the privacy program shall establish rules of behavior for employees and contractors with access to PII and hold agency personnel accountable for complying with applicable privacy requirements and managing privacy risks.
Incident response	Agencies' privacy programs shall develop and implement incident management and response capabilities.
Risk management framework	The National Institute of Standards and Technology risk management framework (RMF) provides a disciplined and structured process that integrates information security, privacy, and risk management activities into the information system development life cycle. The RMF includes steps for categorizing information systems, selecting and implementing security and privacy controls for each system, assessing the controls to determine if they are implemented correctly and operating as intended, and monitoring the controls on an ongoing basis.

Source: Office of Management and Budget, *Managing Information as a Strategic Resource*, Circular A-130. | GAO-22-104551

GAO Previously Recommended That CFPB and OCC Take Actions to Improve Processes for Protecting Consumer Data

In September 2014, we analyzed the scope, uses, and authorities of CFPB's collection of consumer financial data, and its compliance with

[9]The other two areas in appendix II of Circular A-130 are budget and acquisition and workforce management.

laws and federal requirements.[10] CFPB had taken steps to protect and secure these collections, such as implementing access controls and establishing a risk management process for its information systems. However, additional efforts were needed in areas such as developing written procedures for its processes to protect consumer data and further implementing privacy control steps and information security practices. We made 11 recommendations to CFPB, including recommendations to establish written procedures for assessing and managing privacy risks, to obtain independent reviews of its privacy practices, and to implement an evaluation of compliance with contract provisions related to securing this information. We also made a recommendation to OCC to seek timely approval from OMB for their collections of credit card and mortgage data, including data received as part of a sharing agreement with CFPB. CFPB and OCC concurred with these recommendations and implemented them.

Recent Inspector General Reports Included Recommendations on Regulators' Privacy Practices

Agency inspectors general have also assessed privacy protections at each of the five regulators. In many cases, inspectors general assessed privacy protections as part of a larger review of regulators' information security practices, as required annually by the *Federal Information Security Modernization Act of 2014* (FISMA).[11]

As a result of these reviews, the inspectors general made a variety of recommendations regarding regulators' privacy practices. For example, a December 2019 report from the FDIC Office of Inspector General recommended that the FDIC chief privacy officer clarify the role of the senior agency official for privacy in reviewing and approving categorizations for information systems containing PII, and to develop privacy plans for all systems containing PII. A separate report in 2019 by the NCUA Office of the Inspector General recommended that the senior

[10]GAO, *Consumer Financial Protection Bureau: Some Privacy and Security Procedures for Data Collections Should Continue Being Enhanced*, GAO-14-758 (Washington, D.C.: Sept. 22, 2014).

[11]FISMA requires agencies to develop, document, and implement an agencywide information security program to secure federal information systems. FISMA defines information security as protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction, including means for protecting personal privacy and proprietary information. The federal approach and strategy for securing information systems is grounded in the provisions of FISMA.

agency official for privacy implement a process to review and update privacy-related policies and procedures on at least a biennial basis.

Federal Financial Regulators Collect, Use, and Share PII for Many Mission-Oriented Purposes

CFPB and the four prudential regulators together use more than 100 information system applications that regularly collect and use PII.[12] Many different types of PII are collected and used in these applications according to specific purposes and needs in each regulator's mission, such as the supervision of financial institutions, enforcement of regulations for those institutions, and the fielding of consumer complaints. The five regulators regularly share PII as a part of fulfilling their missions. For example, regulators share PII with federal and state government, financial institutions, as well as with third parties such as contractors or loan service providers. Regulators also take steps to provide individuals with appropriate notice regarding the PII they collect, use, and share.

Financial Regulators Collect PII from a Variety of Sources

CFPB and the four prudential regulators collect extensive amounts of PII to use in their mission applications. The five regulators collect PII from individuals; financial institutions, such as banks or service providers over which the regulators have oversight; and other government agencies, such as federal and state regulators and law enforcement agencies. Table 4 shows the number of mission applications at each regulator that collect PII from each of several common sources.

Table 4: Sources for Applications at Selected Federal Financial Regulators That Collect Personally Identifiable Information (PII) for Mission Purposes

PII sources	Consumer Financial Protection Bureau	Federal Deposit Insurance Corporation	Board of Governors of the Federal Reserve System	National Credit Union Administration	Office of the Comptroller of the Currency
Individuals	16	8	7	13	4
Financial institutions	13	20	8	9	4

[12]These systems include a subset of key mission applications that have purposes central to each regulator's primary mission, for which we assessed practices for collection, use, and sharing of PII as part of this review. For a list of these key mission applications for each of the five regulatory agencies, as well as the general mission purpose for each application, see appendix VI.

PII sources	Consumer Financial Protection Bureau	Federal Deposit Insurance Corporation	Board of Governors of the Federal Reserve System	National Credit Union Administration	Office of the Comptroller of the Currency
Other agencies	8	10	4	4	2
Third parties	9	15	2	7	0
Total number of mission applications using PII	**29**	**41**	**15**	**19**	**7**

Source: GAO analysis of privacy impact assessments from federal regulators. Privacy impact assessments are generally available on agency websites. | GAO-22-104551

Note: Because individual systems can collect data from multiple sources, totals for individual collection types may not add to the overall mission applications total.

In addition to these sources, regulators may also collect PII from other third-party sources. For example:

- **CFPB** obtains data from providers of consumer financial products and services, debt counselors, and service providers to detect and assess risks to consumers and markets for consumer financial products and services.
- **FDIC** obtains PII in its role of receiver in the resolution of a failed institution. In this role, FDIC collects information from failed and acquiring financial institutions as well as various servicers contracted with FDIC including loan, marketing, and legal servicers.
- **Federal Reserve** collects mortgage data used to support supervisory stress testing models and for continuous monitoring efforts through an external vendor contracted specifically to interact with the reporting financial institutions.
- **NCUA** also collects PII from service providers and vendors, which provide information needed to pay claims or services during the liquidation process of failed credit unions.

Regulators Use a Diverse Array of PII to Fulfill Mission Needs

To fulfill their individual missions, CFPB and the four prudential regulators use many different types of PII. The types of PII the five regulators use, and the frequency with which certain types of PII are used, vary based on their mission responsibilities. PII types most commonly used by regulators include name, address, email, phone number, Social Security number, and information related to individual financial transactions. For example, Social Security numbers are collected by CFPB to connect data points in better understanding consumer financial decision-making, by NCUA as part of screening prospective credit union officials, and by OCC as part of information required to be collected on key management personnel of

financial institutions. Other types of PII commonly collected and used by regulators include education information; employment information such as employer name or job status; demographic data, such as gender and ethnicity; and background investigation results.

The extent to which regulators use PII varies among mission applications.

- In some cases, regulators' mission applications use PII as source information, but do not generate reports or other output that include PII. For example, a CFPB mission application does not typically allow users to query its data by personal identifier, and an NCUA mission application assigns a unique, anonymous case number, which is the only retrievable identifier.
- In some mission applications, the collection of PII may be an incidental part of receiving other needed data. For example, Federal Reserve documentation for one of its systems states that the system is not designed to capture PII, but certain financial institution records collected as part of the supervision process may contain it, and the PII that does exist in the system may be used to support analyses and findings.

The regulators use PII in their information system applications to fulfill a range of mission-related activities. For example:

- All five regulators use PII in their roles overseeing and conducting supervisory examinations of financial institutions.[13] Examinations commonly focus on ensuring the safety and soundness of financial institutions, as well as consumer compliance examinations that assess, among other things, a financial institution's policies, procedures, and internal controls for implementing financial privacy laws and regulations. For example, regulators may examine consumer transaction data including PII related to use of credit cards and home mortgage lending to ensure compliance with consumer financial laws.
- All five regulators use PII in conducting enforcement activities over financial institutions, for example, using and storing sensitive PII obtained as part of investigations of compliance with financial statutes and regulations.

[13]PII obtained during the supervisory process is generally not specifically referenced by examiners, but may be used to support analyses and examination findings. For example, individual data may be used to support aggregate analysis of issues raised during the course of the supervision process.

- All five regulators use PII in receiving, responding to, or referring complaints or inquiries regarding consumer financial products or services.

Regulators also use PII in mission applications for other, more agency-specific reasons. For example, NCUA and OCC use PII to approve charters—a license to operate—for financial institutions, which requires detailed information on the operations of the institution. Two regulators also use PII to administer the resolution process of failed institutions. FDIC and NCUA conduct analysis, administration, and servicing of loans and real estate acquired from failing financial institutions. Processes in this area include determining creditor claims, resolving liquidations, and maintaining failed financial institution records, such as customers' contact information. Agencies also commonly use PII in mission-related activities such as public outreach and consumer education. Table 5 shows the total number of mission applications using PII at the five regulators, and the number of applications tied to each major purpose type.

Table 5: Mission Purposes for Applications at Selected Federal Financial Regulators That Use Personally Identifiable Information (PII)

Purpose	Consumer Financial Protection Bureau	Federal Deposit Insurance Corporation	Board of Governors of the Federal Reserve System	National Credit Union Administration	Office of the Comptroller of the Currency
Supervision[a]	13	7	11	5	2
Enforcement[b]	5	9	1	3	1
Consumer complaint and inquiry	3	1	1	2	1
Receivership	N/A	19	N/A	5	N/A
Other (public outreach, education, chartering, training, etc.)	15	6	3	6	3
Total number of mission applications using PII	**29**	**41**	**15**	**19**	**7**

Legend: N/A = not applicable.

Source: GAO analysis of privacy impact assessments from federal regulators. Privacy impact assessments are generally available on agency websites. | GAO-22-104551

Notes: Because individual systems can serve multiple purposes, adding totals for individual purposes may not add to the overall mission applications total.

Based on their missions, receivership/liquidation responsibilities are limited to only two regulators, FDIC and NCUA.

[a]The supervision category includes research and market monitoring activities. The Consumer Financial Protection Bureau (CFPB) treats the supervision and research and market monitoring categories as distinct. CFPB has seven applications in the supervision category and five in the research and market monitoring category. One application supports both supervision and research and market monitoring activities using data from other CFPB systems.

[b]The enforcement category includes litigation, fraud prevention, whistleblower activities and other legal activities.

Regulators Share PII with Other Financial Regulators, Contractors, and Other External Entities

As part of fulfilling their missions, CFPB and the four prudential regulators share PII with external entities and enter into agreements that establish specific parameters to ensure that the PII shared will be protected. The extent to which regulators share information varies with the purpose of the sharing. For example:

- As part of their supervisory and oversight responsibilities, prudential regulators share information collected during their examinations of financial institutions. For example, the Federal Reserve shares information received during financial institutions' banking examinations with other members of an interagency council that sets standards for regulatory examinations, to facilitate joint supervisory initiatives, such as compliance with laws over which multiple agencies have jurisdiction. Members of this council include other regulatory agencies, such as the OCC and FDIC, and state banking regulators.
- As part of their responsibility to enforce consumer financial laws, the five regulators share PII with authorized contractors, law enforcement partners, and other state and federal agencies, as well as entities in the judicial arena such as courts, opposing counsel, defendants, and expert witnesses.
- FDIC shares PII with financial advisors; third-party partners, such as property management contractors and vendors; attorneys; and insurance providers in its role of receiver in the resolution of failed institutions.
- NCUA shares PII with vendors and servicers, claimants, correspondents, and asset purchasers that relate to the liquidation of credit unions.

Table 6 shows the number of mission applications in which each of the five regulators share PII with external parties.

Table 6: Applications at Selected Federal Financial Regulators That Share Personally Identifiable Information (PII) for Mission Purposes

	Consumer Financial Protection Bureau	Federal Deposit Insurance Corporation	Board of Governors of the Federal Reserve System	National Credit Union Administration	Office of the Comptroller of the Currency
Number of mission applications where PII is shared with external parties	22	26	10	11	2
Information is shared with government/law enforcement agencies	19	10	9	9	2
Information is shared with other third parties	8	21	9	6	1
Total number of mission-related applications	**29**	**41**	**15**	**19**	**7**

Source: GAO analysis of privacy impact assessments from federal regulators. Privacy impact assessments are generally available on agency websites. | GAO-22-104551

Regulators may use various types of agreements, such as information sharing agreements, confidentiality agreements, and memoranda of understanding to protect the PII they share.[14] Agencies use these agreements to define the purpose, use, and restrictions on data shared in accordance with agency guidance. The agreements require agencies to ensure that disclosure of aggregated data will not result in disclosure of any PII or identification, directly or indirectly, of any financial institution or person. Agreements for enforcement-related information include provisions for using secure channels, such as encrypted email, to limit access to authorized users.

For example, CFPB has information sharing agreements with OCC, FDIC, the Federal Reserve, and NCUA. These agreements describe what information the agencies agree to share, how the data will be shared, the security safeguards required to protect the data, and processes for requesting data or sharing data with additional parties in executing their supervisory responsibilities. CFPB also established a memorandum of understanding with the Department of Justice to coordinate enforcement of federal consumer financial laws. Together, the two agencies agreed to establish and maintain physical, electronic, and procedural safeguards

[14]As stated above, the federal approach and strategy for securing information systems is grounded in the provisions of FISMA. FISMA requires agencies to develop, document, and implement an agencywide information security program to secure federal information systems.

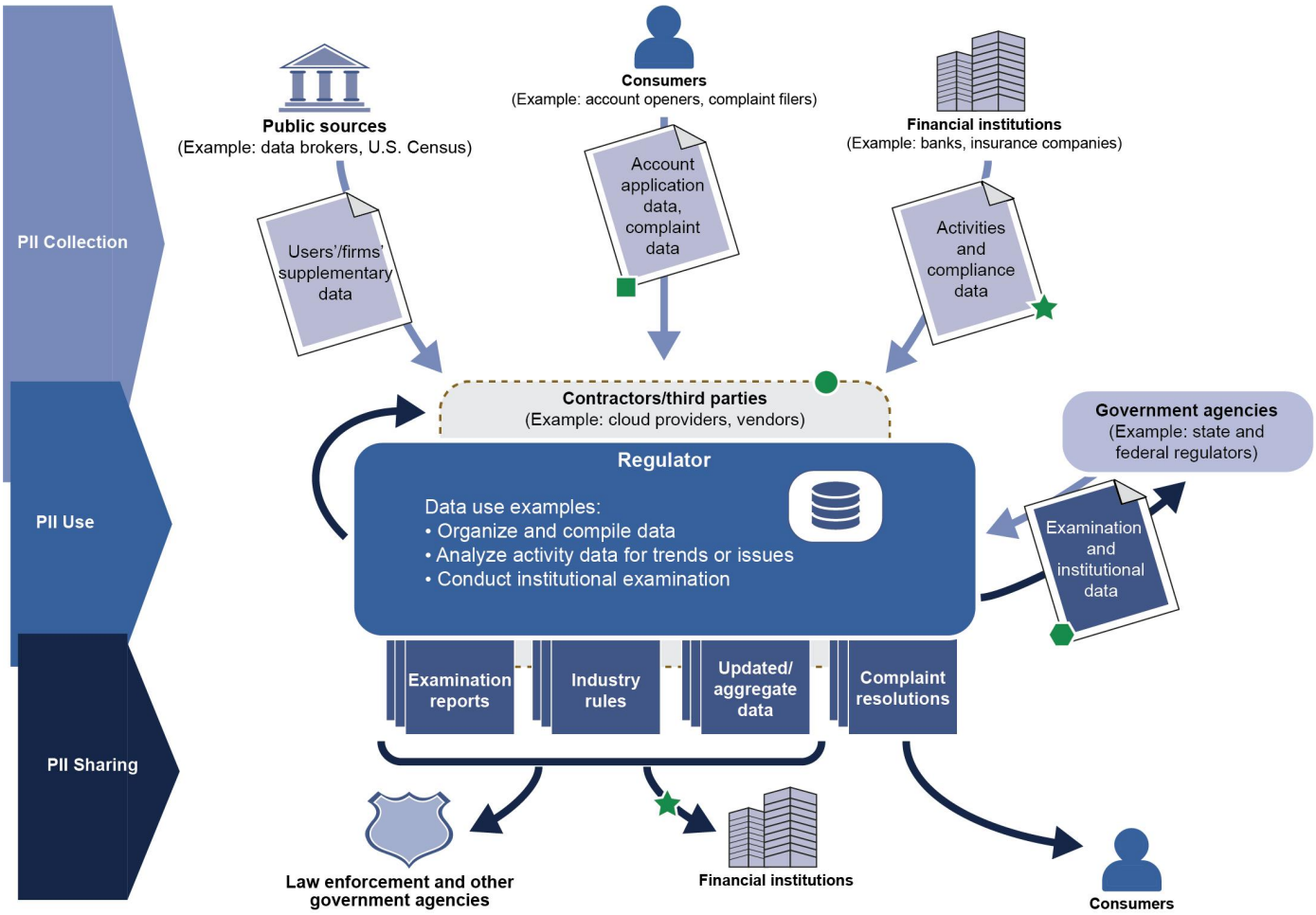
appropriately to protect PII that may be shared against loss, theft, unauthorized access, or other improper actions.

Similar to sharing arrangements with other external entities, contracts with contractors and service providers specify privacy and security requirements. For example,

- FDIC requires contractors who support its insurance determinations and payouts process to sign a contractor confidentiality agreement; and
- For all applications that include PII, NCUA also requires all contractor personnel to agree to nondisclosure agreements and rules of behavior, and to comply with contract and *Privacy Act* requirements prior to gaining access to NCUA's network and application.

The five regulators collect and share PII with similar types of entities. For instance, the five regulators all collect PII from consumers, and both collect and share PII with financial institutions and other regulators. Figure 1 highlights typical external partners for financial regulators in the collection, use, and sharing of PII, and the connections among them.

Figure 1: Collection, Use, and Sharing of Personally Identifiable Information (PII) at Selected Federal Financial Regulators[a]



Legend:

- Agencies provide *Privacy Act* statements and notices prior to collection
- Regulated through nondisclosure agreements and contract clauses
- Legally authorized to collect data
- Based on memoranda of understanding

Source: GAO. | GAO-22-104551

[a]The regulators are the Consumer Financial Protection Bureau, the Federal Deposit Insurance Corporation, the Federal Reserve, the National Credit Union Administration, and the Office of the Comptroller of the Currency.

Regulators Have Processes in Place to Provide Notice Regarding Their Handling of Individuals' PII

CFPB and the four prudential regulators also take steps to provide individuals with appropriate notice regarding the PII they collect, use, and share. The five regulators are required to publish a system of records notice (SORN) for each system of records they maintain and must also provide notice when collecting information from an individual for a system of records.[15] As stated above, the *Privacy Act* defines a system of records as 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 characteristic. For example, NCUA published a *Privacy Act* SORN for its Credit Union Service Organization Registry, an application through which organizations that provide services to credit unions share certain operational and financial information with NCUA. The SORN states that NCUA may share information with appropriate federal or state financial supervision authorities for communication and authentication purposes.

The *Privacy Act* notice requirements do not apply to systems, including systems that may contain PII, that do not meet the definition of a system of records. For example, while the Federal Reserve's Document Management System may include PII that is received from financial institutions as part of the supervision process, according to the Federal Reserve, this system does not meet the definition of a system of records because the PII maintained in the Document Management System is not retrieved by reference to an individual's name or other personal identifier.

In addition to publishing a SORN, when an agency collects information from an individual for a system that meets the *Privacy Act's* definition of a system of records, the agency is required to inform the individual from whom information is being collected

- the authority under which the information is collected,

[15]Each agency that maintains a system of records shall publish in the *Federal Register* (when establishing or revising a system of records) a notice that includes, among other things, the name and location of the system, the categories of individuals and records in the system, and each routine use of the records contained in the system. 5 U.S.C. § 552a (e)(4).

- the principal purpose or purposes for which the information is intended to be used,
- the routine uses which may be made of the information,[16] and
- the effects on the individual, if any, of not providing all or any part of the requested information.[17]

This information is commonly referred to as a *Privacy Act* statement. The *Privacy Act* statement can be provided at the point where information is requested from the individual. For example, in OCC's Customer Assistance Group (CAG) Remedy system, consumers supply their PII as a function of initiating a complaint against their financial institution. The online complaint form typically used by consumers to initiate complaints contains a *Privacy Act* statement.

In addition to its collection requirements, the *Privacy Act* also generally prevents agencies from disclosing PII contained in systems of records without written consent from affected individuals, unless one of the twelve statutory exceptions is met. One key exception is to allow for routine uses, meaning the use of a record compatible with the purpose for which it was collected, and which agencies document in their published SORNs. According to agency officials, the routine use exception covers many of their PII disclosures.

Financial Regulators' Handling of PII Generally Reflect Guidelines and Key Practices, but a Few Weaknesses Remain

CFPB and the four prudential regulators have each created privacy programs with responsibility for managing the risks stemming from their collection, use, and sharing of PII, including for key mission-related applications. Agency privacy programs generally take steps to protect PII in accordance with key practices in each of seven primary protection areas in federal guidance: privacy program general requirements, tracking and managing holdings of PII, contractors and third parties, privacy impact assessments, training and accountability, incident response, and use of a risk management framework. However, guidelines

[16]For example, a routine use may involve the sharing of PII with partner agencies who have an operational need for it.

[17]5 U.S.C. § 552a (e)(3).

and key practices for ensuring the protection of the PII were not implemented fully in three of the seven primary privacy protection areas.

Regulatory Agencies Established Privacy Program General Requirements

According to OMB Circular A-130, agencies shall implement a program for managing privacy risks that is sufficient to comply with federal requirements, maintain a plan to implement the privacy program, designate officials with responsibility to implement the elements of the plan, and conduct assessments of planned uses of PII for each key mission application in accordance with the plan. Each of the five regulators developed an agencywide privacy program and plan sufficient to comply with federal requirements for the handling of PII, performed privacy risk assessments to determine the likelihood that individuals can be identified using linkable information, and conducted and published SORNs according to federal laws and guidance.

Two Regulators Did Not Fully Follow Guidance for Tracking and Managing Their Holdings of PII

According to Circular A-130, agencies' privacy programs shall perform actions related to tracking and managing their holdings of PII, including maintaining an inventory of PII, regularly reviewing all PII maintained by the agency, and complying with applicable requirements regarding the handling of PII. While regulators generally performed these actions, two regulators did not fully meet all of these practices. One did not maintain a PII inventory, and two did not fully document the steps they took to minimize handling of PII. Table 7 shows the extent to which the five regulators had fully incorporated the A-130 key practices in this area.

Table 7: Assessment of Agency Incorporation of Office of Management and Budget Practices: Considerations for Managing Personally Identifiable Information (PII)

Key practice	Consumer Financial Protection Bureau	Federal Deposit Insurance Corporation	Board of Governors of the Federal Reserve System	National Credit Union Administration	Office of the Comptroller of the Currency
Maintain an inventory of agency information systems that involve PII	fully satisfies	fully satisfies	fully satisfies	demonstrated progress	fully satisfies
Take steps to limit collection of Social Security numbers	fully satisfies	fully satisfies	fully satisfies	fully satisfies	fully satisfies

Key practice	Consumer Financial Protection Bureau	Federal Deposit Insurance Corporation	Board of Governors of the Federal Reserve System	National Credit Union Administration	Office of the Comptroller of the Currency
Limit handling of PII in accordance with fair information practice principles	fully satisfies	fully satisfies	demonstrated progress	demonstrated progress	fully satisfies
Require external partners to maintain information systems according to a PII confidentiality level	fully satisfies	fully satisfies	fully satisfies	fully satisfies	fully satisfies
Impose conditions on external parties for handling of PII through written agreements	fully satisfies	fully satisfies	fully satisfies	fully satisfies	fully satisfies

Legend:

● indicates that an agency provided evidence that fully satisfies a criterion.

◐ indicates that an agency demonstrated progress in meeting key elements of a criterion.

○ indicates that an agency did not demonstrate progress in meeting elements of a criterion.

Source: GAO analysis of privacy program documentation from federal regulators. | GAO-22-104551

Note: Scores are intended only to show regulators' performance in meeting individual criteria, and thus cannot be used to provide an exact comparison between agencies on an area-by-area basis.

In particular:

- NCUA did not fully implement the requirement to create and maintain a systems inventory that allows it to regularly review and ensure the accuracy of PII holdings. While NCUA maintains and updates PIAs that document which applications contain PII, these documents must be reviewed individually to assess the agency's PII holdings. Thus, they do not constitute a true agencywide inventory of the agency's PII that can be regularly reviewed to ensure its accuracy and timeliness. CFPB, FDIC, the Federal Reserve, and OCC each maintain an automated or partially automated system that allows for querying of PII information across all of their applications.

  NCUA officials stated that they have begun transitioning their privacy threshold analyses—which determine whether a PIA needs to be conducted—and their PIAs into a new system that will enable additional analysis across applications, for example, through greater use of standardized information entry and by inquiring about related compliance requirements. However, NCUA could not provide specific details on plans or timeframes for implementation of this new system. Without an inventory that allows it to regularly review its PII holdings to ensure that they are accurate and complete, NCUA cannot ensure that privacy protections are consistently applied across its systems.

- While other regulators generally had procedures for documenting the steps they took to minimize the PII collected and used by their applications, NCUA and the Federal Reserve did not specify in

privacy documentation the actions taken or decisions reached for minimizing the PII used in each system. For example, CFPB has an internal team that reviews each new PII collection in consultation with programs and system owners to better ensure that PII use is minimized. The results of this process are documented in its PIAs, which explain, for example, steps taken to limit the amount of PII produced in reports and shared. OCC requires that owners answer specific detailed questions in completing privacy assessments for each of its applications, including on whether an analysis was done prior to collection on which PII types were relevant and necessary to meet the system's requirements.

NCUA specifies required minimization steps for Social Security numbers, and its privacy threshold analyses list protections planned for Social Security numbers if used in a system. However, NCUA does not specify in policy or in its PIAs decisions on the steps it plans to take, or has taken, to minimize other types of PII. Without documenting these steps, it may be difficult for NCUA to ensure consistent implementation of its efforts to minimize PII.

Federal Reserve policy documentation states that privacy threshold analysis reviews are the point at which planned use of Social Security numbers and other PII for a system are reviewed to determine if use can be minimized. According to officials at the Federal Reserve, determinations for how to minimize use of Social Security numbers and other PII are made through discussions between the agency's senior agency official for privacy and stakeholders. However, resulting decisions or analyses associated with these discussions are not recorded in privacy threshold analyses or other documentation. Without documenting the results of these discussions, decisions on minimizing the collection of PII may not be tracked to ensure they are implemented consistently across the agency.

Two Agencies Did Not Include Information on Systems Operated by Contractors and Third Parties in Their PII Inventory

According to Circular A-130, agencies' privacy programs shall ensure that entities that handle information on behalf of a federal agency, or that operate or use information systems on behalf of a federal agency, comply with the privacy requirements in law and OMB policies. While regulators generally met key practices in this area, two regulators did not fully develop an agencywide PII inventory that included information on contractor systems. Table 8 shows the extent to which the five regulators had fully incorporated the A-130 key practices in this area.

Table 8: Assessment of Agency Incorporation of Office of Management and Budget Practices: Contractors and Third Parties

Key practice	Consumer Financial Protection Bureau	Federal Deposit Insurance Corporation	Board of Governors of the Federal Reserve System	National Credit Union Administration	Office of the Comptroller of the Currency
Ensure contract terms for handling PII incorporate privacy requirements and are sufficient to meet federal requirements for information protection	fully satisfies	fully satisfies	fully satisfies	fully satisfies	fully satisfies
Develop agencywide privacy training program	fully satisfies	fully satisfies	fully satisfies	fully satisfies	fully satisfies
Implement policies and procedures for privacy oversight of contractors	fully satisfies	fully satisfies	fully satisfies	fully satisfies	fully satisfies
Ensure incident response procedures are in place for systems used by contractors	fully satisfies	fully satisfies	fully satisfies	fully satisfies	fully satisfies
Ensure *Privacy Act* requirements apply to contractor-operated systems of records	fully satisfies	fully satisfies	fully satisfies	fully satisfies	fully satisfies
Conduct oversight over information systems used or operated by contractors on behalf of the federal government	N/A	fully satisfies	fully satisfies	fully satisfies	fully satisfies
Ensure that contractors' privacy controls for systems operated on behalf of the government comply with National Institute of Standards and Technology standards and guidelines	fully satisfies	fully satisfies	fully satisfies	fully satisfies	fully satisfies
Include information on contractor systems operated on behalf of the government in agencywide PII inventory	N/A	fully satisfies	did not demonstrate progress	demonstrated progress	fully satisfies

Legend:

● indicates that an agency provided evidence that fully satisfies a criterion.

◐ indicates that an agency demonstrated progress in meeting key elements of a criterion.

○ indicates that an agency did not demonstrate progress in meeting elements of a criterion.

N/A = not applicable.

Source: GAO analysis of privacy program documentation from federal regulators. | GAO-22-104551

Notes: The Consumer Financial Protection Bureau does not currently have mission-related information systems that contain PII and are operated by contractors.

Scores are intended only to show regulators' performance in meeting individual criteria, and thus cannot be used to provide an exact comparison between agencies on an area-by-area basis.

Specifically, the Federal Reserve does not currently maintain an inventory of PII held within contractor systems outside of the initial privacy threshold analysis process. Federal Reserve officials stated they are considering solutions to add these elements to their inventory of systems. As stated above, NCUA's method of tracking PII does not constitute a true inventory of the agency's PII, including for contractor-run systems, due to its reliance on review of individual PIAs to assess the agency's PII holdings. Without including PII from contractor-led systems in an inventory that

allows for regular review of PII holdings, the Federal Reserve and NCUA may not be able to monitor fully the extent of PII held by contractors to ensure compliance with privacy protection policies.

Regulators Conducted Privacy Impact Assessments in Accordance with Law and Guidance

According to Circular A-130, agencies shall conduct PIAs and make them available to the public in accordance with the *E-Government Act*. A PIA is an analysis of how PII is handled to ensure that handling conforms to applicable privacy requirements, determine the privacy risks associated with an information system or application, and evaluate ways to mitigate privacy risks. A PIA is both an analysis and a formal document detailing the process and the outcome of the analysis.

All five regulators created PIAs for their mission applications in response to the requirements in the *Act* and their own privacy policies. For example, CFPB's privacy program plan requires its chief privacy officer to ensure that information systems holding PII have risk assessments completed through its PIA process. Overall, the five regulators have created PIAs for each of more than 100 mission applications, and maintain these PIAs on their websites.

Regulators Developed and Implemented Programs for Privacy Training

According to Circular A-130, agencies' privacy programs shall develop, maintain, and implement mandatory agencywide privacy awareness and training programs for internal employees as well as contractors and third parties. The five regulators implemented privacy awareness and training programs according to guidance in Circular A-130, and provided reasonable assurance that all staff receive privacy training consistent with agency policies. For example, the Federal Reserve requires both general training to introduce basic privacy concepts, and role-based training for employees that deal with privacy issues as part of their job function, and delineates required contractor privacy training as a standard part of its contracts.

Regulators Maintained Response Capabilities for Privacy Incidents

According to Circular A-130, agencies should maintain formal incident response capabilities and mechanisms, implement incident management policies to coordinate incident handling, and ensure that incident

response and reporting procedures are operating correctly. The five regulators had policies and procedures in place in the area of incident response. In particular:

- All five regulators maintain formal incident response capabilities and mechanisms, implement formal incident management policies, and periodically test incident response procedures to ensure effectiveness.
- All five regulators have a breach response plan or incident response plan that provides procedures for information systems used or operated by contractors or other entities on behalf of the agency, including timelines for notification of affected individuals.
- All five regulators established roles and responsibilities for agency and contractor personnel to oversee and coordinate incident response activities and to document, report, investigate, and handle privacy incidents.

Three Regulators Did Not Fully Implement Key Elements of a Privacy Risk Management Framework

According to Circular A-130, agency privacy programs should implement a risk management framework to guide and inform the categorization of federal information and information systems; the selection, implementation, and assessment of security and privacy controls; the authorization of information systems and common controls; and the continuous monitoring of information systems. While regulators generally met key practices in this area, three regulators did not fully meet A-130 risk management framework requirements in the areas of (1) the identification of metrics to evaluate implementation of privacy controls, (2) use of a written privacy continuous monitoring (PCM) strategy to catalog privacy controls, or (3) participation of the agency's privacy office in the authorization process for information systems. Table 9 shows the extent to which the five regulators had fully incorporated the A-130 key practices in this area.

Table 9: Assessment of Agency Incorporation of Office of Management and Budget Practices: Risk Management Framework

Key practice	Consumer Financial Protection Bureau	Federal Deposit Insurance Corporation	Board of Governors of the Federal Reserve System	National Credit Union Administration	Office of the Comptroller of the Currency
Implement risk management framework for the categorization, selection, and assessment of privacy controls	fully satisfies	fully satisfies	fully satisfies	fully satisfies	fully satisfies
Ensure policies contain risk categorization schema according to National Institute of Standards and Technology guidelines	fully satisfies	fully satisfies	fully satisfies	fully satisfies	fully satisfies
Policies define a process to select and implement privacy controls	fully satisfies	fully satisfies	fully satisfies	fully satisfies	fully satisfies
Policies identify metrics to evaluate implementation of privacy controls	fully satisfies	demonstrated progress	demonstrated progress	fully satisfies	fully satisfies
Policies define a frequency for assessment of privacy controls	fully satisfies	fully satisfies	fully satisfies	fully satisfies	fully satisfies
Maintain a written privacy continuous monitoring (PCM) strategy that catalogs privacy controls	fully satisfies	fully satisfies	demonstrated progress	fully satisfies	fully satisfies
Categorize the risk level to personally identifiable information in information systems in accordance with risk management framework	fully satisfies	fully satisfies	fully satisfies	fully satisfies	fully satisfies
Select and implement privacy controls according to guidance, including National Institute of Standards and Technology guidance	fully satisfies	fully satisfies	fully satisfies	fully satisfies	fully satisfies
Involve privacy office in the review and approval of privacy plans throughout authorization process	fully satisfies	fully satisfies	fully satisfies	fully satisfies	demonstrated progress
Conduct and document privacy control assessments with respect to requirements	fully satisfies	fully satisfies	fully satisfies	fully satisfies	fully satisfies
Ensure that controls are monitored according to an agency-defined assessment frequency	fully satisfies	fully satisfies	fully satisfies	fully satisfies	fully satisfies
Correct deficiencies identified through privacy assessments	fully satisfies	fully satisfies	fully satisfies	fully satisfies	fully satisfies
Maintain program to implement PCM strategy and maintain ongoing awareness of threats and vulnerabilities	fully satisfies	fully satisfies	fully satisfies	fully satisfies	fully satisfies
Senior agency official for privacy or designee reviews authorization package	fully satisfies	fully satisfies	fully satisfies	fully satisfies	fully satisfies

Legend:

● indicates that an agency provided evidence that fully satisfies a criterion.

◐ indicates that an agency demonstrated progress in meeting key elements of a criterion.

○ indicates that an agency did not demonstrate progress in meeting elements of a criterion.

Source: GAO analysis of privacy program documentation from federal regulators. | GAO-22-104551

Note: Scores are intended only to show regulators' performance in meeting individual criteria, and thus cannot be used to provide an exact comparison between agencies on an area-by-area basis.

In particular:

- Regulators had mixed results in identifying and documenting metrics to evaluate the implementation of privacy controls. For example, CFPB and NCUA each have policies requiring assessment methodologies and metrics to aid in determining whether privacy controls are correctly implemented. In particular, CFPB describes in its continuous monitoring plan specific qualitative and quantitative performance metrics that it reviews annually, such as suspected and actual breaches of PII, and measurements of completion of privacy training. The NCUA privacy team tracked and defined a set of monthly metrics, such as the number of PIAs approved and the number of reported privacy breaches.

  OCC established a requirement for developing, monitoring, and reporting on the results of performance measures, and has also defined metrics related to privacy controls, such as a percentage of systems in which a privacy threshold analysis has been conducted and the percentage of employees that have taken privacy awareness training. Officials stated that they are in the process of implementing a new system to integrate privacy metrics such as these with its agencywide metrics dashboard.

  FDIC and the Federal Reserve, however, did not identify metrics to evaluate the implementation of privacy controls. FDIC established frequencies and parameters for its privacy controls, and has tracked corrective actions based on the results of control tests. For instance, FDIC tracks which individual systems do not have updated privacy impact assessments, or do not have procedures in place for the secure deletion of PII. However, FDIC has not established metrics to measure its overall implementation of privacy controls. Unless it develops metrics that apply across systems, it may be more difficult for FDIC to monitor and report on the extent to which its controls are sufficient to manage privacy risks.

  The Federal Reserve has not established metrics showing the status of privacy controls agencywide. Officials at the Federal Reserve stated that its tracking of corrective actions to resolve issues uncovered in its documented annual control test process is sufficient to ensure the proper implementation of privacy controls. However, without the establishment of metrics as part of its continuous monitoring plan that measure and report on the overall status of privacy controls, it may be more difficult for the Federal Reserve to gauge the effectiveness of its controls and ensure compliance with applicable privacy requirements agencywide.

- The Federal Reserve has not included key details on privacy controls as part of its plan for continuous monitoring. In particular, while the Federal Reserve's privacy policy, which includes its plan for privacy continuous monitoring, contains details of the workflows during the early part of the continuous monitoring process, such as privacy threshold analyses, PIAs, and SORNs, it does not provide information, such as detailed test steps or test frequencies, for the privacy controls it has in place as part of continuous monitoring. Federal Reserve officials stated that the Federal Reserve plans to integrate privacy controls into its already-existing security control program as part of an upcoming transition to Revision 5 of the National Institute of Standards and Technology's (NIST's) control catalog.[18] However, the Federal Reserve has not yet defined a time frame for this transition. Until Federal Reserve's policies for continuous monitoring integrate information on the privacy controls it plans to use, it may not be able to ensure that its privacy controls are monitored and tested appropriately.
- OCC does not document approvals by its privacy office or its senior agency official for privacy for approval of intermediate risk management decisions that occur after the completion of PIAs and SORNs but prior to the final authorization to operate. These decisions include the final selection of controls to be tested for each application, which is recorded in system privacy plans, and the details on testing steps that are performed, which are recorded in security assessment reports. OCC officials stated that the chief privacy officer reviews all final authorizations and approves the agencywide scope and schedule of controls to be assessed, but that officials outside the privacy office, such as system owners or authorizing officials, provide intermediate approvals for individual applications. Officials also stated that OCC is planning to add formal chief privacy officer approval for intermediate milestones such as system privacy plans, but were unable to provide a timeline in which a plan that includes that requirement would be implemented. Until OCC requires its chief privacy officer to validate decisions made during intermediate milestones, it may not be able to ensure that planned protections for PII are sufficient.

[18]National Institute of Standards and Technology, *Security and Privacy Controls for Information Systems and Organizations,* Special Publication 800-53, Revision 5 (Gaithersburg, Md.: Sept. 2020). Unlike previous iterations of SP 800-53, Revision 5 includes both security and privacy controls.

Conclusions

CFPB and the four prudential regulators we reviewed maintain more than 100 mission-related information system applications that collect and use consumer PII. Applications at the five regulators use PII, primarily in their role overseeing supervisory examinations of financial institutions, but also for other mission purposes such as enforcement of consumer financial laws and the processing of consumer complaints. These five regulators also regularly share PII with partners such as other government agencies, law enforcement and judicial entities, and with third parties such as contractors, vendors, and service providers.

The five regulators have each created privacy programs, which have processes to ensure privacy protections for the PII they collect, use, and share in accordance with key practices in federal guidance. However, four of the five regulators did not fully perform key practices such as maintaining a systems inventory that allow it to ensure the accuracy of its PII holdings, documenting steps taken to minimize PII collected and used by applications, identifying and documenting metrics to evaluate the implementation of privacy controls, and documenting key decisions and approvals for the selection and testing of privacy controls. As a result, regulators are less likely to be fully aware of the extent of PII they handle or the controls that are in place internally and externally to protect it. Until regulators take steps to mitigate weaknesses in performing key practices in federal law and guidance, the PII they collect, use, and share could be at increased risk of compromise.

Recommendations for Executive Action

We are making a total of eight recommendations, including one to FDIC, four to the Federal Reserve, two to NCUA, and one to OCC:

The Chair of FDIC should identify and specify metrics to determine whether privacy controls are implemented correctly and operating as intended. (Recommendation 1)

The Chair of the Federal Reserve should define a process for documenting the actions the Federal Reserve takes to minimize collection and use of PII. (Recommendation 2)

The Chair of the Federal Reserve should include information from systems maintained by Federal Reserve contractors in the Federal Reserve's inventory of information systems that handle PII. (Recommendation 3)

The Chair of the Federal Reserve should identify and specify metrics to determine whether privacy controls are implemented correctly and operating as intended. (Recommendation 4)

The Chair of the Federal Reserve should establish a timeframe for including information on privacy controls to be tested within the Federal Reserve's written privacy continuous monitoring strategy. (Recommendation 5)

The Executive Director of NCUA should enhance NCUA's ability to query information from an agencywide inventory of information systems containing PII, including contractor-run systems, to facilitate regular reviews of the inventory for accuracy and completion. (Recommendation 6)

The Executive Director of NCUA should define a process for documenting the actions NCUA takes to minimize collection and use of PII. (Recommendation 7)

The Comptroller of the Currency should require OCC privacy program officials to review intermediate process documentation, such as system privacy plans and security assessment plans. (Recommendation 8)

Agency Comments and Our Evaluation

We provided a draft of this report to CFPB, FDIC, Federal Reserve, NCUA, and OCC. FDIC, Federal Reserve, NCUA, and OCC provided written comments that are reprinted in appendices II through V. FDIC officials stated that they generally agreed with our recommendation. Federal Reserve officials stated that they agreed with the importance of the key practices we identified and would evaluate potential enhancements to address our recommendations. NCUA officials stated that they had efforts underway and planned to implement enhancements to NCUA's privacy program that would address our recommendations. OCC officials described specific updates that they planned to make to OCC standard operating procedures to address our recommendation. We also received technical comments from officials at CFPB and the Federal

Reserve. We incorporated technical comments in the report, where appropriate.

We are sending copies of this report to the appropriate congressional committees, the Director of CFPB, Chairman of FDIC, Chairman of the Federal Reserve, Chairman of NCUA, and the Comptroller of the Currency. In addition, the report is available at no charge on the GAO website at https://www.gao.gov.

If you or your staff have any questions about this report, please contact or Nick Marinos at (202) 512-9342 or MarinosN@gao.gov, or Alicia Puente Cackley at (202) 512-8678 or CackleyA@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. GAO staff who made key contributions to this report are listed in appendix VII.

Sincerely yours,

Nick Marinos
Director, Information Technology and Cybersecurity

Alicia Puente Cackley
Director, Financial Markets and Community Investment

Appendix I: Objectives, Scope, and Methodology

The specific objectives of our review were to (1) determine what personally identifiable information (PII) selected federal financial regulators collect, for what mission purposes they collect it, and how they use and share it; and (2) determine the extent to which selected federal financial regulators ensure the privacy of the PII they collect, use, and share for key mission applications, in accordance with federal requirements and guidance.

For both objectives, we selected a subset of federal agencies that regulate consumer financial institutions and collect significant amounts of PII. Specifically, we selected the Consumer Financial Protection Bureau (CFPB), the Federal Deposit Insurance Corporation (FDIC), the Board of Governors of the Federal Reserve System (Federal Reserve), the National Credit Union Administration (NCUA), and the Office of the Comptroller of the Currency (OCC). In addition to their large-scale PII collections, we selected these regulators based on their authority to enforce consumer protection laws in the financial sector. To gain background information on the status of privacy programs at these regulators, we reviewed recent inspector general reports that addressed the handling of privacy or PII concerns, including annual security-related audits with a privacy component.

On this engagement, we focused on the PII collected by regulators in mission applications. For the purposes of this report, a mission application is any agency data system that collects and maintains PII for mission purposes, and for which an agency has conducted a privacy impact assessment. We did not focus, for instance, on applications with an internal focus, such as human resources applications.

For our first objective, we analyzed privacy impact assessments (PIAs) and system of records notices (SORNs), which are required documentation under federal laws and guidance, for all mission-related applications. From this analysis, we determined the methods by which each regulator collects, uses, and shares PII, the types of PII each regulator collects, the purposes for which regulators collect PII, and the methods by which each regulator provides notice to individuals whose PII the regulator collects. We also determined the types of PII commonly

collected by regulators. We compared processes for sharing PII across the five regulators to determine common sources and destinations for the PII collected and shared by mission applications, as well as common uses of PII in these applications.

For our second objective, we analyzed federal laws and guidance to identify key practices for collecting, using, and sharing PII. Our primary source for key practices was Office of Management and Budget (OMB) Circular A-130.[1] We also identified key practices from the *Privacy Act of 1974,* the National Institute of Standards and Technology (NIST)[2], and other OMB guidance.[3] We organized the key practices according to the main sections of OMB Circular A-130, Appendix II, which focus on privacy practices at federal agencies. Of the nine sections in Circular A-130, the key practices we selected used elements of seven sections: general privacy requirements; considerations for managing PII; use of contractors and third parties; privacy impact assessments; training and accountability; incident response; and use of a risk management framework. Our purpose in selecting these sections was to focus on basic privacy program elements, potential weaknesses in third-party privacy practices, and the assessment process for privacy risks.

We then assessed agencywide policies and practices at each regulator for the collection, use, and sharing of PII against the key practices. For each of the five regulators, we selected three or four applications with purposes central to their regulator's missions, and that collect and use PII. Across all five regulators, we selected 18 key mission applications. Several of the applications have a common purpose across regulators, such as regulatory examinations and the fielding of customer complaints. The list of key mission applications, and the purpose of each application, is in appendix VI.

[1]Office of Management and Budget, *Managing Information as a Strategic Resource,* Circular A-130 (Washington, D.C: July 2016).

[2]National Institute of Standards and Technology, *Security and Privacy Controls for Federal Information Systems and Organizations,* Special Publication 800-53, Revision 5 (Gaithersburg, Md.: Sept. 2020); *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy,* Special Publication 800-37, Revision 2 (Gaithersburg, Md.: Dec. 2018);

[3]Office of Management and Budget, *Preparing for and Responding to a Breach of Personally Identifiable Information*, Memorandum M-17-12 (Jan. 3, 2017); *Role and Designation of Senior Agency Officials for Privacy,* Memorandum M-16-24 (Sept. 15, 2016).

For each key mission application, we also assessed each regulator's practices for collection, use, and sharing of PII, and artifacts indicative of these practices, against key practices in federal laws and guidance. For key mission applications maintained by external contractors, we compared requirements in documentation, such as contract specifications, with identified key practices.

We conducted this performance audit from October 2020 to January 2022 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Appendix II: Comments from the Federal Deposit Insurance Corporation

FDIC

3501 Fairfax Drive, Arlington, VA 22226-3500 Chief Information Officer & Chief Privacy Officer

December 13, 2021

TO: Nick Marinos
Director, Information Technology and Cybersecurity Issues
Government Accountability Office

Alicia Puente Cackley
Director, Financial Markets and Community Investment
United States Government Accountability Office

FROM: Sylvia Burns
Chief Information Officer and Chief Privacy Officer
Director, Division of Information Technology

SYLVIA BURNS Digitally signed by SYLVIA BURNS Date: 2021.12.13 18:08:03 -05'00'

Zachary Brown
Chief Information Security Officer
Office of the Chief Information Security Officer

ZACHARY BROWN Digitally signed by ZACHARY BROWN Date: 2021.12.13 22:59:18 -05'00'

SUBJECT: Management Response to the Draft Audit Report Entitled *Privacy- Federal Financial Regulators Should Take Additional Actions to Enhance Their Protection of Personal Information*

Thank you for the opportunity to review and comment on the Government Accountability Office's {GAO) draft report entitled *Privacy- Federal Financial Regulators Should Take Additional Actions to Enhance Their Protection of Personal Information,* issued on November 10, 2021. The FDIC's Privacy Program is critical to the agency's goal to protect the personal information of our customers and employees, and the FDIC is committed to enhancing protections for personal information.

In its report, the GAO audit team made one recommendation to the FDIC Chair, with which we concur. We expect that FDIC actions in progress, and the new action we are undertaking in response to this draft report, will further improve and strengthen the FDIC's protections of personal information.

MANAGEMENT RESPONSE

Recommendation

3501 Fairfax Drive, Arlington, VA 22226-3500 Chief Information Officer & Chief Privacy Officer

The Chair of FDIC should identify and specify metrics to determine whether privacy controls are implemented correctly and operating as intended.

Management Decision: Concur

Corrective Action:

The FDIC currently relies on an assessment and authorization process to select, monitor, assess and ensure that privacy controls are implemented and working as intended at both the agency and program levels. As recommended by the GAO, the FDIC will identify and specify privacy metrics to enhance FDIC's ability to evaluate the implementation of its privacy controls, and will, accordingly, update its Privacy Program Plan or Privacy Continuous Monitoring Strategy to align with NIST 800-53 Rev 5.

Estimated Completion Date: 6/30/2022

If you have questions regarding this response, please contact Montrice Yakimov, Chief, IT Risk Governance and Policy, Enterprise Strategy Branch, at MONYAKIMOV@FDIC.GOV.

cc: E. Marshall Gentry, Chief Risk Officer, Office of Risk Management and Internal Controls
Elroy Holden, Manager, Office of Risk Management and Internal Controls
Mark Mulholland, Acting Deputy Director, Enterprise Strategy Branch

Text of Appendix II: Comments from the Federal Deposit Insurance Corporation

December 13, 2021

TO: Nick Marinos

Director, Information Technology and Cybersecurity Issues Government Accountability Office

Alicia Puente Cackley

Director, Financial Markets and Community Investment United States Government Accountability Office

FROM: Sylvia Burns

Chief Information Officer and Chief Privacy Officer Director, Division of Information Technology

Digitally signed by SYLVIA BURNS Date: 2021.12.13

Zachary Brown

Chief Information Security Officer

Digitally signed by ZACHARY BROWN

Office of the Chief Information Security Officer

SUBJECT:

Management Response to the Draft Audit Report Entitled Privacy- Federal Financial Regulators Should Take Additional Actions to Enhance Their Protection of Personal Information

Thank you for the opportunity to review and comment on the Government Accountability Office's {GAO) draft report entitled Privacy- Federal Financial Regulators Should Take Additional Actions to Enhance Their Protection of Personal Information, issued on November 10, 2021. The FDIC's Privacy Program is critical to the agency's goal to protect the personal information of our customers and

employees, and the FDIC is committed to enhancing protections for personal information.

In its report, the GAO audit team made one recommendation to the FDIC Chair, with which we concur. We expect that FDIC actions in progress, and the new action we are undertaking in response to this draft report, will further improve and strengthen the FDIC's protections of personal information.

MANAGEMENT RESPONSE

Recommendation

The Chair of FDIC should identify and specify metrics to determine whether privacy controls are implemented correctly and operating as intended.

Management Decision: Concur Corrective Action:

The FDIC currently relies on an assessment and authorization process to select, monitor, assess and ensure that privacy controls are implemented and working as intended at both the agency and program levels. As recommended by the GAO , the FDIC will identify and specify privacy metrics to enhance FDIC's ability to evaluate the implementation of its privacy cont rols, and will, accordingly, update its Privacy Program Plan or Privacy Continuous Monitoring Strategy to align with NIST 800-53 Rev 5.

Estimated Completion Date: 6/30/2022

If you have questions regarding this response, please contact Montrice Yakimov, Chief, IT Risk Governance and Policy , Enterprise Strategy Branch, at MONYAKIMOV@FDIC.GOV.

cc: E. Marshall Gent ry, Chief Risk Offi cer , Office of Risk Managem ent and Internal Controls Elroy Holden, Manager, Office of Risk Management and Internal Controls Mark Mulholland , Acting Deputy Director, Enterprise Strategy Branch

.

Appendix III: Comments from the Board of Governors of the Federal Reserve System

BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM
WASHINGTON, DC 20551

DIVISION OF
INFORMATION TECHNOLOGY

December 8, 2021

Nick Marinos, Director, Information Technology and Cybersecurity Issues
Alicia Puente Cackley, Director, Financial Markets and Community Investment
United States Government Accountability Office
441 G Street, NW
Washington, DC 20548

Dear Mr. Marinos and Ms. Cackley:

Thank you for providing the Board of Governors of the Federal Reserve System ("Federal Reserve" or "Board") with an opportunity to review the final draft of the Government Accountability Office ("GAO") report titled: *Privacy: Federal Financial Regulators Should Take Additional Actions to Enhance Their Protection of Personal Information* (GAO-22-104551). The GAO's report examines what mission-related personally identifiable information ("PII") federal financial regulators collect, use, and share, as well as the extent to which the regulators ensure the privacy of the PII they collect, use, and share, in accordance with federal requirements and guidance. We appreciate the report's recognition that the Federal Reserve has developed an agencywide privacy program that complies with federal requirements for the handling of PII.

The GAO's report makes four recommendations to the Federal Reserve:

www.federalreserve.gov

- The Chair of the Federal Reserve should define a process for documenting the actions it takes to minimize collection and use of PII. (Recommendation 2)

- The Chair of the Federal Reserve should include information from systems maintained by Federal Reserve contractors in its inventory of information systems that handle PII. (Recommendation 3)

- The Chair of the Federal Reserve should identify and specify metrics to determine whether privacy controls are implemented correctly and operating as intended. (Recommendation 4)

- The Chair of the Federal Reserve should establish a timeframe for including information on privacy controls to be tested within its written privacy continuous monitoring strategy. (Recommendation 5)

The Board's Privacy Program implements policies, procedures, and practices designed to safeguard PII, and in particular, sensitive PII. The Federal Reserve continually assesses the effectiveness of its Privacy Program to enhance the protection of PII and ensure the Program remains in compliance with applicable requirements including those issued by the Office of Management and Budget. With respect to the report's recommendations, the Federal Reserve recognizes the importance of implementing the key practices identified by GAO for collecting, using, and sharing PII. Consequently, the Board will evaluate potential enhancements to its Privacy Program to best address the GAO's recommendations.

We appreciate the GAO's review of the financial regulators' privacy practices, for their professional approach to the review, and for the opportunity to comment.

Sincerely,

SHARON MOWRY Digitally signed by SHARON MOWRY Date: 2021.12.08 09:47:15 -05'00'

Sharon Mowry
Director
Division of Information Technology

Text of Appendix III: Comments from the Board of Governors of the Federal Reserve System

December 8, 2021

Nick Marinos, Director, Information Technology and Cybersecurity Issues Alicia Puente Cackley, Director, Financial Markets and Community Investment

United States Government Accountability Office 441 G Street, NW

Washington, DC 20548

Dear Mr. Marinos and Ms. Cackley:

Thank you for providing the Board of Governors of the Federal Reserve System ("Federal Reserve" or "Board") with an opportunity to review the final draft of the Government Accountability Office ("GAO") report titled: Privacy: Federal Financial Regulators Should Take Additional Actions to Enhance Their Protection of Personal Information (GAO-22- 104551). The GAO's report examines what mission-related personally identifiable information ("PII") federal financial regulators collect, use, and share, as well as the extent to which the regulators ensure the privacy of the PII they collect, use, and share, in accordance with federal requirements and guidance. We appreciate the report's recognition that the Federal Reserve has developed an agency wide privacy program that complies with federal requirements for the handling of PII.

The GAO's report makes four recommendations to the Federal Reserve:

- The Chair of the Federal Reserve should define a process for documenting the actions it takes to minimize collection and use of PII. (Recommendation 2)
- The Chair of the Federal Reserve should include information from systems maintained by Federal Reserve contractors in its inventory of information systems that handle PII. (Recommendation 3)
- The Chair of the Federal Reserve should identify and specify metrics to determine whether privacy controls are implemented correctly and operating as intended. (Recommendation 4)
- The Chair of the Federal Reserve should establish a timeframe for including information on privacy controls to be tested within its written privacy continuous monitoring strategy. (Recommendation 5)

The Board's Privacy Program implements policies, procedures, and practices designed to safeguard PII, and in particular, sensitive PII. The Federal Reserve continually assesses the effectiveness of its Privacy Program to enhance the protection of PII and ensure the Program remains in compliance with applicable requirements including those issued by the Office of Management and Budget. With respect to the report's recommendations, the Federal Reserve recognizes the importance of implementing the key practices identified by GAO for collecting, using, and sharing PII. Consequently, the Board will evaluate potential enhancements to its Privacy Program to best address the GAO's recommendations.

We appreciate the GAO's review of the financial regulators' privacy practices, for their professional approach to the review, and for the opportunity to comment.

Sincerely,

Sharon Mowry Director

Division of Information Technology

Appendix IV: Comments from the National Credit Union Administration

National Credit Union Administration
Office of the Executive Director

December 9, 2021

SENT VIA EMAIL

Nick Marinos (MarinosN@gao.gov)
Director, Information Technology and Cybersecurity Issues
US Government Accountability Office

Alicia Puente Cackley (CackleyA@gao.gov)
Financial Markets and Community Investment
US Government Accountability Office

Dear Mr. Marinos and Ms. Cackley,

Thank you for the opportunity to review and comment on the GAO's draft report (GAO-22-104551) on financial regulators' privacy practices. The NCUA embraces the Fair Information Practice Principles and adheres to both the letter and the spirit of federal privacy laws and regulations. These items serve as the foundation of our privacy program, as stated in our privacy program plan and evidenced in our strategic goals, action plans, training materials, and continuous monitoring program.

You identified two areas in which there is room for improvement; (1) our facility in tracking personally identifiable information (PII) across systems, including contractor-run systems, to ensure the accuracy and completion of our inventory reviews, and (2) identification of a defined process for documenting our actions to minimize the collection and use of PII.

We are confident that our program already meets the requirements associated with the suggested improvements, but are committed to continuing to enhance our program. As we mentioned during our interviews, such efforts are well underway. We expect full implementation of technology-assisted assessment and authorization tools to be completed in 2022. This will address the enhancements you identified.

The NCUA is committed to meeting its responsibilities to protect PII consistent with the federal government privacy risk management framework. Thank you again for the opportunity to review and comment on the draft report.

Sincerely,

LARRY FAZIO
Digitally signed by LARRY FAZIO
Date: 2021.12.09 08:47:59 -05'00'

Larry Fazio
Executive Director

1775 Duke Street – Alexandria, VA 22314-6113 – 703-518-6320

Text of Appendix IV: Comments from the National Credit Union Administration

December 9, 2021

Nick Marinos (MarinosN@gao.gov)

Director, Information Technology and Cybersecurity Issues US Government Accountability Office

Alicia Puente Cackley (CackleyA@gao.gov) Financial Markets and Community Investment US Government Accountability Office

Dear Mr. Marinos and Ms. Cackley,

Thank you for the opportunity to review and comment on the GAO's draft report (GAO-22- 104551) on financial regulators' privacy practices. The NCUA embraces the Fair Information Practice Principles and adheres to both the letter and the spirit of federal privacy laws and regulations. These items serve as the foundation of our privacy program, as stated in our privacy program plan and evidenced in our strategic goals, action plans, training materials, and continuous monitoring program.

You identified two areas in which there is room for improvement; (1) our facility in tracking personally identifiable information (PII) across systems, including contractor-run systems, to ensure the accuracy and completion of our inventory reviews, and (2) identification of a defined process for documenting our actions to minimize the collection and use of PII.

We are confident that our program already meets the requirements associated with the suggested improvements, but are committed to continuing to enhance our program. As we mentioned during our interviews, such efforts are well underway. We expect full implementation of technology-assisted assessment and authorization tools to be completed in 2022. This will address the enhancements you identified.

The NCUA is committed to meeting its responsibilities to protect PII consistent with the federal government privacy risk management framework. Thank you again for the opportunity to review and comment on the draft report.

Sincerely,

Larry Fazio Executive Director

Appendix V: Comments from the Office of the Comptroller of the Currency

Office of the Comptroller of the Currency

Washington, DC 20219

December 8, 2021

Mr. Nick Marinos
Director, Information Technology and Cybersecurity Issues
Ms. Alicia Puente Cackley
Director, Financial Markets and Community Investment
U. S. Government Accountability Office
Washington, DC 20548

Dear Mr. Marinos and Ms. Cackley,

Thank you for providing the Office of the Comptroller of the Currency (OCC) an opportunity to review the Government Accountability Office's (GAO) draft report titled *Privacy: Federal Financial Regulators Should Take Additional Actions to Enhance Their Protection of Personal Information*. Technical edits have been provided separately.

As part of this review, the GAO has provided the following recommendation:

The Comptroller of the Currency should require OCC privacy program officials to review intermediate process documentation, such as system privacy plans and security assessment plans.

To address this recommendation, the OCC plans to update its Standard Operating Procedures for the review and approval of system security and privacy plans and security assessment plans to include Chief Information Security Officer/Chief Privacy Officer (CISO/CPO) approval. Updates to the Standard Operating Procedures will ensure intermediate documentation includes privacy oversight by the CISO/CPO as part of the overall OCC Risk Management Framework process. In addition, the OCC is updating its Information Security and Cyber Protection Program policy to require CISO/CPO approval of system security and privacy plans and security assessment plans. Both the changes to the Standard Operating Procedures and policy are planned to be completed by the end of the 2nd Quarter of Fiscal Year 2022 (March 2022).

If you need additional information, please contact me at (202) 649-6800 or the OCC Privacy Program Manager, Ron Shelden at (202) 649-5780.

Sincerely,

Calliope K. Murphy

Digitally signed by Calliope K. Murphy
Date: 2021.12.07 16:27:39 -05'00'

Kathy K. Murphy
Senior Deputy Comptroller for Management and Chief Financial Officer

Text of Appendix V: Comments from the Office of the Comptroller of the Currency

December 8, 2021

Mr. Nick Marinos

Director, Information Technology and Cybersecurity Issues Ms. Alicia Puente Cackley

Director, Financial Markets and Community Investment

U. S. Government Accountability Office Washington, DC 20548

Dear Mr. Marinos and Ms. Cackley,

Thank you for providing the Office of the Comptroller of the Currency (OCC) an opportunity to review the Government Accountability Office's (GAO) draft report titled Privacy: Federal Financial Regulators Should Take Additional Actions to Enhance Their Protection of Personal Information. Technical edits have been provided separately.

As part of this review, the GAO has provided the following recommendation:

The Comptroller of the Currency should require OCC privacy program officials to review intermediate process documentation, such as system privacy plans and security assessment plans.

To address this recommendation, the OCC plans to update its Standard Operating Procedures for the review and approval of system security and privacy plans and security assessment plans to include Chief Information Security Officer/Chief Privacy Officer (CISO/CPO) approval.

Updates to the Standard Operating Procedures will ensure intermediate documentation includes privacy oversight by the CISO/CPO as part of the overall OCC Risk Management Framework process. In addition, the OCC is updating its Information Security and Cyber Protection Program policy to require CISO/CPO approval of system security and privacy plans and security assessment plans. Both the changes to the Standard Operating Procedures and policy are planned to be completed by the end of the 2nd Quarter of Fiscal Year 2022 (March 2022).

If you need additional information, please contact me at (202) 649-6800 or the OCC Privacy Program Manager, Ron Shelden at (202) 649-5780.

Sincerely,

Kathy K. Murphy

Senior Deputy Comptroller for Management and Chief Financial Officer

Appendix VI: List of Key Mission Applications at Federal Financial Regulators

Among the more than 100 information systems applications that collect and use PII at five selected federal financial regulators—the Consumer Financial Protection Bureau, the Federal Deposit Insurance Corporation, the Board of Governors of the Federal Reserve System, the National Credit Union Administration, and the Office of the Comptroller of the Currency—are a subset of applications with purposes central to each regulator's primary mission. Table 10 lists these key mission applications, as well as the general mission purpose for each application.

Table 10: Key Mission Applications for Selected Federal Financial Regulators

Regulatory Agency	Application name	Application Purpose	Application description	Summary of personally identifiable information (PII) in this application
Consumer Financial Protection Bureau (CFPB)	Home Mortgage Disclosure Act (HMDA) Data Collection	Market Research	Tracks information from financial institutions on collection, recording, reporting, and disclosure information about their mortgage lending, in response to legislation.	PII collected in this application can include personal identifiers and demographic data for borrowers, and information on property subject to the loan; the type, purpose, amount of the loan; and approval decisions for loans. PII is used to determine the extent to which institutions are serving housing needs of their communities, as required in HMDA.
	Litigation and Investigation Support Toolset	Enforcement, Litigation	Collects, stores, processes, transmits, and maintains critical information related to investigations and litigation.	This application collects, maintains, and processes PII including name, contact information, Social Security number and financial information for enforcement and litigation activities.
	Matters Management System	Enforcement, Litigation, Rulemaking	Creates a searchable repository for information on legal and regulatory issues, and organizes, distributes, tracks, and reports on this information.	PII such as name, address, phone, and filing/case numbers are searchable in this application, primarily to be able to look up parties relevant to a matter.
	Scheduling and Examination System	Supervision	Stores documents related to the examination and supervisions process, including examination planning documents and rating information derived from the examination process.	PII in this application is generally limited to documentation used to conduct regulatory examinations. This includes contact information for customers, institutions, and CFPB employees, and can include account or transaction information.

Regulatory Agency	Application name	Application Purpose	Application description	Summary of personally identifiable information (PII) in this application
Federal Deposit Insurance Corporation (FDIC)	Claims Administration System	Resolution/ Receivership	Obtains PII from failing/failed financial institutions during the bank closing process for the purpose of processing insurance claims and supporting the manipulation and storage of claims data.	Datasets in this application containing depositor information can contain PII such as bank customer name and financial account information, Social Security number, and address as part of an overall transfer of depositor information files to FDIC during the bank closing process.
	Enterprise Public Inquiry and Complaints System	Consumer Complaint/ Inquiry	Manages complaints and inquiries and allows staff to receive, respond to, track, and report on individual cases received from constituents, including financial institutions.	As part of the complaint/inquiry process, PII such as full name, address, telephone number, e-mail address, and financial information may be collected by this application, related to complaint submitted by the individual via incoming calls, a Web portal, mail, fax, and online forms.
	Examination Tools Suite	Supervision	Creates, processes, and shares examination work papers and a final report of examination.	Examiners obtain financial records in this application such as commercial and consumer loan data from financial institutions, including PII such as borrower's full name, account numbers, outstanding balance(s), interest rates, and payment information.
	Regional Automated Document Distribution and Imaging System	Supervision, Enforcement	Provides an electronic document imagining, distribution, and storage system for final financial institution correspondence and examination work paper documents.	Examination work papers and reports, correspondence, and information related to enforcement and supervisory activities can contain PII such as name, address, Social Security number, and other personal information pertaining to financial institution officials and investigated persons of interest.
Board of Governors of the Federal Reserve System	Consumer Complaint and Inquiry System	Consumer Complaint	Supports the business processes for receiving, responding to, monitoring, and reporting consumer complaints, and inquiries related to financial institutions supervised by the Board.	PII such as contact information for consumers including name, mailing address, phone number, and email address as well as consumer's transaction information is collected and maintained in this application in order to process consumer complaints and inquiries.
	Federal Reserve Application Name Check	Supervision	Maintains information about designated individuals in connection with the Federal Reserve System's processing of applications, notices, or proposals associated with various types of financial institutions.	PII such as name, Social Security number, address, citizenship, occupation and roles is collected and maintained in this application to assist in evaluating the proposed officers, directors, principal shareholders, or others associated with financial institutions in evaluating various regulatory applications, notices, or proposals.
	Studies to Develop and Test Consumer Regulatory Disclosures	Compliance Research	Collects data from consumers for use in rulemaking, policy development, and produces information resources for the public.	PII such as name, home address, email address, and telephone number is used in this application to locate and contact consumers with relevant experience to participate in a research study.

Regulatory Agency	Application name	Application Purpose	Application description	Summary of personally identifiable information (PII) in this application
National Credit Union Administration	Automated Integrated Regulatory Examination System	Supervision	Collects, stores, and processes information that is used while conducting the examination and supervision of credit unions.	Information including PII such as member information, name, account number, date of birth, encrypted Social Security number, home address, share and loan information, credit score, and payment history is used in this application to determine risks present at the credit union as part of the examination and supervision process.
	Consumer Assistance Center	Consumer Complaint	Collects, stores, and processes information to address and manage consumer complaints by consumers against federally insured and state chartered credit unions.	PII data such as individual names, addresses, email addresses, unique identifiers, case numbers and consumer phone numbers is used by this application to respond to, report on, and locate submitted communications, including consumer complaints and inquiries.
	Credit Union Online	Supervision	Collects and stores information from credit unions, including contact information and information about credit union officials.	PII in this application is used to contact officials for examination-related discussions, mailing of an examination report, the monitoring and mitigating of risks, and for congressional reporting.
Office of the Comptroller of the Currency (OCC)	Central Application Tracking System	Chartering	Captures, monitors, facilitates, and reports on the processing of fillings submitted, including bank charters, conversions, branch openings/closings/relocations, acquisitions, and subsidiary activities.	PII stored in this application, such as name, date and place of birth, Social Security number, citizenship status, addresses, and criminal background information are required to be maintained by FDIC for all directors, senior executives, and key management personnel of financial institutions examined by the OCC.
	Customer Assistance Group Remedy	Consumer Complaint	Stores institutional data and information and provides access related to consumer complaints involving financial institutions.	This application collects PII such as name, address, telephone, bank and federal savings associations account numbers, and Social Security numbers to support the processing of and responding to consumer complaints.
	Summation Enterprise	Enforcement, Litigation	Searches, retrieves, codes/annotates, and organizes information and produces electronically stored information responsive to discovery requests for investigation and litigation-related tasks.	PII such as names, addresses, telephone numbers, email addresses, birth dates, Social Security numbers, and personal financial information may be collected by this application as part of financial transaction data, banking records, employee records, and email records obtained as part of investigations and other legal activities.
	Supervisory Information System – Examiner View	Supervision	Manages the supervision of institutions and bank examiners and assists bank examiners in preparing and conducting supervisory activities for financial institutions.	PII is collected by this application during the bank examination process, and can include names, addresses, and information on banking relationships.

Source: Privacy impact assessments from federal regulators. Privacy impact assessments are generally available on agency websites. | GAO-22-104551

Appendix VII: GAO Contacts and Staff Acknowledgments

GAO Contacts

Nick Marinos at (202) 512-9342 or MarinosN@gao.gov

Alicia Puente Cackley at (202) 512-8678 or CackleyA@gao.gov

Staff Acknowledgments

In addition to the contacts above, John de Ferrari (Assistant Director), Kay Kuhlman (Assistant Director), Shaun Byrnes (Analyst-in-Charge), Alexander Bennett, Nancy Glover, Marc Molino, Akiko Ohnuma, Aubrey Nguyen, Monica Perez-Nelson, Jessica Sandler, Priscilla Smith, Andrew Stavisky, and Adam Vodraska made key contributions to this report.

GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through our website. Each weekday afternoon, GAO posts on its website newly released reports, testimony, and correspondence. You can also subscribe to GAO's email updates to receive notification of newly posted products.

Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's website, https://www.gao.gov/ordering.htm.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

Connect with GAO

Connect with GAO on Facebook, Flickr, Twitter, and YouTube.
Subscribe to our RSS Feeds or Email Updates. Listen to our Podcasts.
Visit GAO on the web at https://www.gao.gov.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact FraudNet:

Website: https://www.gao.gov/about/what-gao-does/fraudnet

Automated answering system: (800) 424-5454 or (202) 512-7700

Congressional Relations

A. Nicole Clowers, Managing Director, ClowersA@gao.gov, (202) 512-4400, U.S. Government Accountability Office, 441 G Street NW, Room 7125, Washington, DC 20548

Public Affairs

Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, DC 20548

Strategic Planning and External Liaison

Stephen J. Sanford, Managing Director, spel@gao.gov, (202) 512-4707
U.S. Government Accountability Office, 441 G Street NW, Room 7814,
Washington, DC 20548