Evaluation Report
2025-SR-C-005
May 5, 2025

Consumer Financial Protection Bureau

The CFPB Can Improve Its Safeguards for Protecting Confidential Supervisory Information

Office of Inspector General
Board of Governors of the Federal Reserve System
Consumer Financial Protection Bureau

Office of Inspector General
Board of Governors of the Federal Reserve System
Consumer Financial Protection Bureau

Executive Summary, 2025-SR-C-005, May 5, 2025

The CFPB Can Improve Its Safeguards for Protecting Confidential Supervisory Information

Findings

We found that the Consumer Financial Protection Bureau's guidance for confidential supervisory information (CSI) does not effectively limit access to such information in its system of record for supervision activities. We also found that the CFPB's guidance does not sufficiently limit access to CSI used to prioritize supervisory activities. The CFPB can reduce the risk of unauthorized access to CSI by updating its guidance to limit access to such information on a need to know basis and clearly defining when that need to know exists.

Additionally, we found that the CFPB's guidance for managing CSI breaches does not include expectations for assessing and documenting the severity of breaches and determining, enforcing, and documenting consequences for responsible employees. Further, the agency does not conduct trend analysis on the causes of CSI breaches to determine the appropriate adjustments to controls based on reoccurring themes. Without formal guidance for determining the severity of CSI breaches, the CFPB may underestimate the associated risks. Appropriately classifying the severity of CSI breaches will help to promote an effective response. In addition, consistently enforcing appropriate consequences when necessary and analyzing the causes of breaches can help the CFPB reduce the risk of reoccurrence or more severe breaches.

Finally, we found that the CFPB does not have a defined process to notify the affected supervised institutions of CSI breaches. We believe that establishing a process for evaluating potential harm or reputational risk to affected institutions and communicating with them about that harm or risk can better prepare the CFPB to respond to future breaches. We also believe such a process will promote transparency and enable institutions to respond quickly, if needed.

Recommendations

Our report contains seven recommendations designed to improve the CFPB's safeguards for protecting CSI. In its response to our draft report, the CFPB concurs with our recommendations and outlines actions that will be taken to address six of those recommendations. The CFPB indicated that the actions are subject to resource availability. The CFPB did not describe any actions to address recommendation 6 or provide implementation time frames for any of the recommendations. In 90 days, we will request that the agency provide implementation dates for each recommendation. We will follow up to ensure that the recommendations are addressed.

Purpose

In 2023, the CFPB declared a major incident breach that affected about 256,000 consumers and 46 institutions—the first time that the agency declared such an incident. We conducted this evaluation to assess the CFPB's controls for safeguarding CSI.

Background

The Division of Supervision's (Supervision) Office of Supervision Examinations (OSE) supervises and examines depository and nondepository institutions to ensure compliance with federal consumer financial laws. Within OSE, regional staff conduct examinations; perform monitoring activities; and coordinate with federal and state regulators, as necessary. As part of these oversight activities, OSE examiners collect and review CSI from supervised institutions.

Supervision staff also create CSI when they analyze information about institutions, document their conclusions, and conduct the CFPB's annual prioritization process for supervisory activities. The CSI that Supervision staff obtain and create may contain personally identifiable information (PII). Breaches of CSI and PII can expose the CFPB, financial institutions, and individuals to reputational and financial damage.

Recommendations, 2025-SR-C-005, May 5, 2025

The CFPB Can Improve Its Safeguards for Protecting Confidential Supervisory Information

Finding 1: CFPB Guidance Does Not Effectively Limit Examiner Access to CSI in SES

Number	Recommendation	Responsible office
1	Define in policy a. the process that examiners should use to request access to files in SES. b. the criteria that managers and regional analysts should use to assess whether a need to know exists in accordance with the least privilege principle. c. the requirement that regional analysts document an examiner's need to know before granting access to supervision files in SES. d. consequences for accessing CSI without a need to know or providing access to CSI when a need to know does not exist.	Division of Supervision
2	Update the document handling directive to require supervision staff to share files by emailing SES links.	Division of Supervision
3	Develop and require training for CFPB staff involved in the examination process for the policy and guidance resulting from recommendations 1 and 2.	Division of Supervision

Finding 2: CFPB Guidance Does Not Sufficiently Limit Access to CSI Used to Prioritize Supervisory Activities

Number	Recommendation	Responsible office
4	Update the guidance for prioritizing and scheduling examinations to reflect the current link sharing practice and to limit access to the supporting analysis to those with a need to know.	Division of Supervision

Finding 3: CFPB Guidance Does Not Adequately Detail Expectations for Managing CSI Breaches

Number	Recommendation	Responsible office
5	Update the guidance for managing breaches of CSI to include expectations for a. assessing and documenting the level of harm associated with a breach. b. counseling, training, or taking other measures to hold CFPB staff responsible for breaches accountable, as appropriate, and documenting such actions. c. analyzing the causes of breaches to identify trends and implement appropriate control adjustments, as necessary.	Office of Technology and Innovation and Division of Supervision
6	Develop required training on the updated guidance after it is implemented.	Office of Technology and Innovation and Division of Supervision

Finding 4: CFPB Guidance Does Not Define a Process for Notifying Supervised Institutions of CSI Breaches

Number	Recommendation	Responsible office
7	Update the CFPB's CI breach response directive to a. provide guidance for assessing the risk to institutions affected by breaches of CSI and notifying those institutions. b. define the roles and responsibilities for those involved in the process.	Office of Technology and Innovation and Division of Supervision

Contents

Introduction

Objective

In February 2023, the Consumer Financial Protection Bureau became aware that an examiner forwarded confidential supervisory information (CSI) to their personal email account.[1] CFPB officials reviewed the examiner's email history and discovered that the examiner had forwarded to a personal email account about 65 emails from February 2022 through February 2023 containing personally identifiable information (PII)[2] of about 256,000 consumers and CSI belonging to 46 institutions.[3] The CFPB's senior agency official for privacy (SAOP) convened the Breach Response Team (BRT), which declared the breach to be a *major incident* based on the number of affected consumers—the first time that the agency declared such an incident.[4]

We assessed the CFPB's controls for safeguarding CSI.[5] Additional details on our scope and methodology are in appendix A.

Background

The Dodd-Frank Wall Street Reform and Consumer Protection Act established the CFPB to regulate the offering and provision of consumer financial products and services under federal consumer financial laws.

[1] Under 12 C.F.R. 1070.2(i), *CSI* includes, among other things, (1) reports of examination and any information contained in, derived from, or related to such reports; (2) any communications between the CFPB and a supervised financial institution or a federal, state, or foreign government agency related to the CFPB's supervision of the institution; (3) any information provided to the CFPB by a financial institution to enable the CFPB to monitor for risks to consumers in the offering or provision of consumer financial products or services; and (4) information that may be exempt from disclosure under the Freedom of Information Act pursuant to 5 U.S.C. 552(b)(8).

[2] The Office of Management and Budget (OMB) defines *PII* as any information that can be used to distinguish or trace an individual's identity, such as their name; Social Security number; and biometric records alone or when combined with other personal or identifying information that is linked or linkable to a specific individual, such as date and place of birth or mother's maiden name.

[3] We made recommendations to improve the CFPB's tool to protect against the unauthorized exfiltration of sensitive agency information in our *2024 Audit of the CFPB's Information Security Program*, OIG Report 2024-IT-C-019, October 31, 2024. In that report, we recommended that the CFPB finalize an agencywide data classification policy and incorporate those classifications and associated labels into the data loss prevention program.

[4] OMB defined the criteria for *major incidents* as a breach that involves PII that, if exfiltrated, modified, deleted, or otherwise compromised, is likely to result in demonstrable harm to the national security interests, foreign relations, or the economy of the United States, or to the public confidence, civil liberties, or public health and safety of the American people, or any incident that is likely to result in the same. In addition, OMB guidance stated that while agencies should assess each breach on a case-by-case basis to determine whether the breach meets the definition of a major incident, any breach of the PII of 100,000 or more people must be considered a major incident. Office of Management and Budget, *Fiscal Year 2021–2022 Guidance on Federal Information Security and Privacy Management Requirements*, OMB Memorandum M-22-05, December 6, 2021. OMB M-22-05 has since been rescinded, and the most recent applicable guidance is Office of Management and Budget, *Fiscal Year 2025 Guidance on Federal Security Information and Privacy Management Requirements*, OMB Memorandum M-25-04, January 15, 2025.

[5] This evaluation does not serve any investigatory purpose.

The Division of Supervision and CSI

The Division of Supervision (Supervision) ensures compliance with federal consumer financial laws by supervising depository institutions and their affiliates with more than $10 billion in total assets and certain nondepository institutions.[6] Supervision comprises two offices: the Office of Supervision Examinations (OSE) and the Office of Supervision Policy and Operations.[7]

OSE supervises and examines depository and nondepository institutions. OSE has four regional offices: New York (Northeast), Atlanta (Southeast), Chicago (Midwest), and San Francisco (West). OSE regional staff conduct examinations; perform monitoring activities; and coordinate with federal and state regulators, as necessary.

Supervision Collects and Creates CSI

As part of their oversight activities, OSE examiners collect and review CSI from supervised institutions. Supervision staff also create CSI when they analyze information about institutions and document their conclusions. Additionally, Supervision's Reporting, Analytics, Monitoring, Prioritization and Scheduling (RAMPS) team conducts the annual prioritization process for the division's supervisory activities. CSI, which may include PII, is one form of a broader category of information that the CFPB calls *confidential information* (CI).[8]

Supervision Maintains CSI in Its Supervision Examination System and SharePoint Sites

Supervision maintains examination-related materials in the Supervision Examination System (SES), which is its system of record for supervision activities. Examiners cannot access examination materials in SES unless a regional analyst assigns an examiner to the event that houses that information. Examination teams also use event-specific SharePoint sites to document their work, which includes CSI. Similarly, the RAMPS team has a SharePoint site for conducting and sharing its analysis to prioritize supervisory activities.

[6] Among nondepository institutions, the CFPB has the authority to supervise entities in the consumer mortgage lending, payday lending, and private education lending markets regardless of size; larger participants in markets for other consumer financial products or services as defined by the CFPB; and entities the CFPB has reasonable cause to determine, by order, are "engaging, or ha[ve] engaged, in conduct that poses risks to consumers with regard to the offering or provision of consumer financial products or services."

[7] Effective September 1, 2024, the CFPB restructured the former Division of Supervision, Enforcement and Fair Lending into two separate divisions, Supervision and Enforcement. Within Supervision, OSE includes four regional offices, and the Office of Supervision Policy and Operations includes the former OSE headquarters elements.

[8] 12 C.F.R. § 1070.2(f) defines CI at the CFPB as: confidential consumer complaint information, confidential investigative information, CSI, as well as any other CFPB information that may be exempt from disclosure under the Freedom of Information Act pursuant to 5 U.S.C. § 552(b).

The CFPB's Breach Response Process

The SAOP manages the response to breaches involving PII and determines the steps to mitigate potential risks, including notifying affected parties and fulfilling Office of Management and Budget (OMB) reporting requirements, such as informing Congress and the agency's office of inspector general.

Under the direction of the SAOP, the Privacy Office conducts an initial assessment of reported breaches and handles privacy breaches that it determines pose minimal risk, called routine breaches. For higher-risk or more complex breaches, the SAOP convenes and leads the BRT, which includes the chief information officer (CIO); the chief data officer; the chief information security officer; representatives from the Legal Division, the Office of Legislative Affairs, and the Office of Communications; and other internal stakeholders, as needed.

When both PII and CSI are involved, the SAOP coordinates with the Confidential Information Breach Team, which can include representatives from the Privacy Office, Supervision, the Division of Enforcement, and the Legal Division, to determine the appropriate mitigation steps. If a breach only involves CI, the SAOP notifies the CI Breach Team to assess the suspected or confirmed CI breach.

Finding 1: CFPB Guidance Does Not Effectively Limit Examiner Access to CSI in SES

The CFPB lacks a formal process for an examiner who has not been assigned to an examination to request access to SES files for that examination as well as a process for sharing examination files. The National Institute of Standards and Technology's Special Publication 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations* and the Federal Trade Commission's (FTC) *Protecting Personal Information: A Guide for Business* both state that access to information should be limited to those who have a need for the information. Supervision did not limit examiner access to CSI in SES consistent with the least privilege principle.[9] In addition, the CFPB does not have a policy that addresses how examination staff should request access to SES files; how managers and regional analysts should assess examiners' need to know before granting access; how examiners should share files internally; and consequences for accessing CSI without a need to know or providing access to CSI when a need to know does not exist. By implementing a policy and updating existing guidance, the CFPB can reduce the risk of unauthorized access to CSI, thus, protecting the confidentiality of sensitive information and minimizing the reputational risk to the agency and the institutions it supervises.

CFPB Guidance Does Not Describe the Process for Requesting Access to SES Files or Assessing Examiners' Need to Know

Interviewees indicated that examiners occasionally need access to documents from examinations to which they are not assigned, such as memorandums or workpapers involving similar issues or potential violations to promote consistency. CFPB guidance does not outline a formal process for examiners to request such access in SES. Some interviewees indicated that the CFPB follows an informal practice of examiners emailing the regional analyst, explaining the business purpose for their request, and copying their manager on the email. Another interviewee indicated that Supervision leadership submits requests for an examiner to access certain files, not the examiner. CFPB guidance does not describe how managers or regional analysts should assess an examiner's need to know before granting the examiner access to the requested information in SES. Further, CFPB guidance does not require managers or regional analysts to document an examiner's need to know before granting access or include consequences for accessing CSI without a need to know or providing access to CSI when a need to know does not exist.

[9] NIST Special Publication 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations*, defines *principle of least privilege* as the principle that users should only have the necessary privileges to complete their assigned task.

CFPB Guidance Does Not Address How Examiners Should Share Files Internally

Interviewees said that before the major incident, examiners typically shared files as email attachments. An official indicated that after the CFPB deployed a new version of SES in June 2023, Supervision encouraged examination staff to share files as SES links that require authorization to view, which reduced the risk of inadvertently sharing a confidential document with someone who does not have a need to know.[10] Interviewees also indicated that for a recipient to view a file via link, a regional analyst must provide the recipient access to the file in SES, thereby preventing unintended recipients or others without approval or a need-to-know from viewing the file.

In June 2023, the CFPB updated the *Directive on Document Handling* and the user guide for SES. The directive instructs staff to share documents within the system with other stakeholders rather than downloading and sharing documents via email. However, the directive does not address how CFPB employees should share files with examiners who need access to SES files for an examination to which they are not assigned.

Applying the Least Privilege Principle When Granting Access to Sensitive Information Is a Leading Practice

According to leading practices, organizations should grant access to sensitive information on a need-to-know basis. NIST Special Publication 800-53, AC-6: Least Privilege, states that organizations should use the principle of least privilege, allowing only authorized access for users that are necessary to accomplish assigned tasks. The FTC's *Protecting Personal Information: A Guide for Business* recommends that organizations keep track of sensitive information, including which employees have access to the information and whether they need to access the information.

Supervision's Information Sharing Practices Introduce the Risk of Unauthorized Access

Supervision did not limit examiner access to CSI consistent with the least privilege principle. For example, in our review of the major incident, we noted that the examiner who caused the breach had access to documentation that was not directly related to their assigned examinations. Multiple interviewees were not able to explain with certainty why the examiner had access to it. Interviewees noted that requesting documents from other examination teams is common at the CFPB. One interviewee noted that the process for requesting access to examinations is informal and the bar for obtaining access is not high.

The CFPB can reduce the risk of unauthorized access to CSI and future data breaches by clearly defining when a need to know exists, by implementing a policy and updating guidance for accessing and handling documents containing CSI, and by developing and requiring training on the new policy and updated

[10] The official noted that the CFPB began developing the new SES version before discovering the major incident.

guidance. Taking these steps will help the agency to protect the confidentiality of sensitive information and minimize the reputational risk to the agency and the institutions it supervises.

Recommendations

We recommend that the director of Supervision

1. Define in policy
    a. the process that examiners should use to request access to files in SES.
    b. the criteria that managers and regional analysts should use to assess whether a need to know exists in accordance with the least privilege principle.
    c. the requirement that regional analysts document an examiner's need to know before granting access to supervision files in SES.
    d. consequences for accessing CSI without a need to know or providing access to CSI when a need to know does not exist.
2. Update the document handling directive to require supervision staff to share files by emailing SES links.
3. Develop and require training for CFPB staff involved in the examination process for the policy and guidance resulting from recommendations 1 and 2.

Management Response

In its response to our draft report, the CFPB concurs with our recommendations. In response to recommendation 1, the CFPB states that Supervision will develop and implement the appropriate processes. In response to recommendation 2, the CFPB states that Supervision will update the document handling directive to require Supervision staff to share files by emailing SES links. In response to recommendation 3, the CFPB states that Supervision will develop the required training on the policies and procedures implemented in response to recommendations 1 and 2 for CFPB staff involved in the examination process. The CFPB indicates that these actions are subject to available resources and did not provide estimated time frames for implementation.

OIG Comment

The planned actions described by the CFPB appear to be responsive to our recommendations. In 90 days, we will request that the agency provide implementation dates for these recommendations, and we will follow up to ensure that they are addressed.

Finding 2: CFPB Guidance Does Not Sufficiently Limit Access to CSI Used to Prioritize Supervisory Activities

Our analysis of data from the major incident revealed that the examiner who caused the breach had CSI from the CFPB's supervision prioritization process without a clear need to know. NIST Special Publication 800-53 states that organizations should grant access to sensitive information on a need-to-know basis. The CFPB's *Examination Prioritization and Scheduling Standard Operating Procedure* (SOP) defines the stakeholders involved in the prioritization process but does not define who has a need to know the CSI RAMPS uses to determine the CFPB's supervision priorities. Further, the SOP does not reflect the CFPB's current processes for sharing prioritization information. By updating its guidance for prioritizing and scheduling examinations to limit access to the supporting analysis to those with a need to know, the CFPB can reduce the risk of unauthorized access to CSI. Further, the CFPB can reduce the likelihood of another incident and reduce the potential for financial or reputational harm to an individual, an institution, or the agency.

An Examiner Had CSI From the Annual Prioritization Process Without an Established Need to Know

Supervision's RAMPS team leads the CFPB's annual risk assessment and prioritization process, which determines OSE's annual examination schedule. As part of the risk assessment process, the RAMPS team analyzes data about supervised institutions. The data may include CSI from the supervision process as well as consumer complaint data, both of which may contain PII.

The RAMPS team conducts the prioritization and examination scheduling with input from internal Supervision stakeholders and other senior leaders. We learned that senior leaders may occasionally share prioritization information with examiners who are not typically involved in the prioritization process. The examiner who caused the major incident breach had CSI from the prioritization process, which did not contain PII, about institutions from all four regions. The examiner sent that CSI to a personal email account. Multiple interviewees were not able to describe with certainty the examiner's need to know the prioritization information. In our view, the examiner did not have a clear need to know the CSI from the prioritization process.

According to NIST Special Publication 800-53, organizations should grant access to sensitive information on a need-to-know basis. The CFPB's prioritization examination and scheduling SOP states that the RAMPS team develops and shares its prioritization data presentation with Supervision leadership and other senior leaders, who use the data to review and approve the final examination schedule. It further states that the RAMPS team shares the final examination schedule with regional analysts to ensure the regions have uploaded the examination calendar into SES.

We learned that following the major incident, the RAMPS team revised how it distributes information to internal stakeholders. According to an interviewee, the RAMPS team creates and shares multiple reports with the agency's leadership team as links to a SharePoint file. However, the RAMPS team has not updated the CFPB's prioritization and examination scheduling SOP to reflect this new process or defined with whom and how internal stakeholders should share prioritization reports containing CSI. The SOP also fails to mention how the CFPB ensures that only those who have a need to know can view and share CSI the RAMPS team uses in its analysis to determine the final examination schedule.

The CFPB can reduce the risk of unauthorized access to CSI by updating its guidance for examination prioritization and scheduling, thus reducing the likelihood of another incident and reducing the potential for financial or reputational harm to an individual, an institution, or the agency.

Recommendation

We recommend that the director of Supervision, in conjunction with the RAMPS program director,

4. Update the guidance for prioritizing and scheduling examinations to reflect the current link sharing practice and to limit access to the supporting analysis to those with a need to know.

Management Response

In its response to our draft report, the CFPB concurs with our recommendation. Specifically, the CFPB states that Supervision will update the guidance for prioritizing and scheduling examinations to reflect the current link sharing practice and to limit access to the supporting analysis to those with a need to know. The CFPB indicated that these actions are subject to available resources and did not provide an estimated time frame for implementation.

OIG Comment

The planned actions described by the CFPB appear to be responsive to our recommendation. In 90 days, we will request that the agency provide an implementation date for this recommendation, and we will follow up to ensure that it is addressed.

Finding 3: CFPB Guidance Does Not Adequately Detail Expectations for Managing CSI Breaches

The CFPB's process for assessing the severity of CSI breaches and determining, enforcing, and documenting consequences for breaching employees is informal, and the agency does not conduct trend analysis to determine the appropriate adjustments to controls based on reoccurring themes. The CFPB's *Reporting Breaches of Confidential Information* policy states that the CI Breach Team manages and responds to suspected CI breaches, and the *Confidential Information Breach Response Directive* supplements this policy. However, neither the policy nor the directive include expectations for assessing and documenting the severity of breaches and determining, enforcing, or documenting consequences for responsible employees. In addition, CFPB guidance does not require staff to conduct trend analysis on the causes of CSI breaches to determine the appropriate adjustments to controls based on reoccurring themes. Without guidance that clearly establishes the expectations for determining the severity of CSI breaches, the CFPB may be underestimating the risk associated with such breaches. Appropriately classifying the severity of CSI breaches will help to promote an effective response. In addition, by consistently enforcing appropriate consequences and analyzing the causes of breaches, the CFPB can reduce the risk of reoccurrence or more severe breaches.

The CFPB Did Not Document Severity Assessments for Most CI Breaches

While the Privacy Office conducts an initial assessment of all breaches, including those involving CSI, the CI Breach Team is responsible for managing and responding to CI breaches. According to the CFPB, the Division of Supervision, Enforcement and Fair Lending (SEFL) experienced 16 breaches involving CSI and other forms of CI from January 2022 to April 2024.[11] Of those 16, the CFPB documented the risk associated with 1 breach. We determined that almost half of the breaches were inadvertent. For example, an employee mistakenly included a non-CFPB email address in an email chain containing CSI. In another example, a field manager sent a document request to an institution that included CSI from another institution. According to a CFPB official, in December 2023, the Privacy Office implemented a tool that enables users to denote whether a breach is *low*, *medium*, or *high* risk, but the agency is not consistently using it. The official also indicated that the CFPB has not documented this process, including the definitions of these risk categories.

[11] We requested data on breaches from January 2022 through April 2024, before the CFPB restructured SEFL. The CFPB provided data on breaches of CI, which included CSI and confidential investigative information.

The CFPB Did Not Document Its Efforts to Hold Most Breaching Employees Accountable

A CFPB official stated that after a CI breach, the CFPB typically provides the employee who caused the breach refresher training or counseling before closing the matter. The official noted that this refresher training reiterates the importance of safeguarding CI and addresses the specific cause of the breach, such as emailing CI to an unintended recipient. However, our analysis of SEFL's breaches of CI from January 2022 to April 2024 revealed that the agency documented that it provided training to breaching employees for 3 of the 16 reported breaches. In some instances, the CFPB indicated that breaching employees either deleted or were instructed to delete any mishandled information.

The CFPB Does Not Conduct Trend Analysis of the Causes of CSI Breaches

While the SAOP reports routine breaches to the CIO, the CFPB does not conduct trend analysis of the causes of CSI breaches to determine the appropriate adjustments to controls based on reoccurring themes. However, a CFPB official acknowledged that doing so could be beneficial. Although some CSI breaches during our scope period appeared to be inadvertent based on our analysis, any breach involving a supervised institution has the potential to be highly consequential to the agency or the institution.

Leading Practices for Managing Breaches

Several federal agencies have formal guidance for assessing the severity of breaches, holding staff accountable, and performing trend analysis. We identified the following leading practices for managing breaches:

- One financial regulatory agency's breach response plan includes guidance for assessing the risk of harm associated with an incident. The guidance includes risk factors that inform a rating, which determines the agency's mitigation and notification strategy.
- Another agency's insider threat mitigation guidance emphasizes the importance of holding staff accountable. This guidance states that providing staff the opportunity to acknowledge their responsibility in an incident while involving them in addressing the consequences can reduce the potential for reoccurrence.
- A third agency conducts analysis of incident data to identify trends and make recommendations to enhance data protection.

CFPB Guidance Does Not Adequately Address Managing CSI Breaches

The CFPB's *Reporting Breaches of Confidential Information* policy outlines the responsibilities of agency staff to discover, report, and respond to suspected or confirmed breaches of CI, which may include CSI. Similarly, the CFPB's *Confidential Information Breach Response Directive* supplements the policy and

provides additional details relating to a breach response. However, neither the policy nor the directive details expectations for assessing and documenting the severity of a CI breach. According to a CFPB official, the CFPB may use factors included in OMB guidance to assess the severity of a CSI breach, but this approach is not documented. Further, neither the policy nor the directive provide guidance for determining, enforcing, and documenting appropriate consequences for employees who cause breaches, such as counseling, providing additional training, or taking other measures to hold them accountable. An official stated that the consequences for an employee breaching CSI are left to the discretion of Supervision management. Finally, neither the policy nor the directive provides guidance on analyzing the causes of CSI breaches to identify trends.

Without a formal policy that clearly defines the expectations for determining the severity of CSI breaches, the CFPB may be underestimating the risk associated with such breaches. Appropriately classifying the severity of CSI breaches will help to promote an effective response. Further, CFPB staff responsible for breaches may not adjust their behavior without consistent and appropriate consequences to reduce the risk of reoccurrence. Lastly, analyzing the causes of those breaches can help the CFPB identify trends and better position the agency to mitigate the risk of future breaches.

Recommendations

We recommend that the CIO, in conjunction with the director of Supervision

5. Update the guidance for managing breaches of CSI to include expectations for
    a. assessing and documenting the level of harm associated with a breach.
    b. counseling, training, or taking other measures to hold CFPB staff responsible for breaches accountable, as appropriate, and documenting such actions.
    c. analyzing the causes of breaches to identify trends and implement appropriate control adjustments, as necessary.
6. Develop required training on the updated guidance after it is implemented.

Management Response

In its response to our draft report, the CFPB concurs with our recommendations. In response to recommendation 5, the CFPB states that Supervision will update its guidance for managing CSI breaches to include expectations for assessing and documenting the level of harm associated with such breaches; counseling, training, or taking other measures to hold responsible staff accountable and documenting such actions; and analyzing the cause of breaches to identify trends and implement appropriate controls. The CFPB did not describe any actions to address recommendation 6. The CFPB indicated that these actions are subject to available resources and did not provide estimated time frames for implementation.

OIG Comment

The planned actions described by the CFPB appear to be responsive to recommendation 5. In 90 days, we will request that the agency describe its planned actions to address recommendation 6 and provide

implementation dates for recommendations 5 and 6. We will follow up to ensure that both recommendations are addressed.

Finding 4: CFPB Guidance Does Not Define a Process for Notifying Supervised Institutions of CSI Breaches

Following the major incident breach, the CFPB's approach to notifying affected institutions varied by region. According to NIST's Special Publication 800-61, *Computer Security Incident Handling Guide*, organizations should have plans for assessing the risk to affected parties and notifying all affected stakeholders of a breach. The CFPB does not have a defined process to determine the potential harm to supervised institutions affected by a CSI breach and to notify those institutions of the breach. The CFPB also has not outlined the roles and responsibilities of those involved in this process. We believe that establishing a process for evaluating potential harm or reputational risk to affected institutions and notifying them of the breach will better position the CFPB to respond to future breaches. We also believe such a process will promote transparency and enable affected institutions to respond quickly, if necessary.

OSE's Approach for Notifying Supervised Institutions of CSI Breaches Varied by Region

The CFPB does not have a defined process to notify supervised institutions of CSI breaches. We found that each regional office used a different approach to contacting institutions and sharing information about the 2023 major incident breach. One regional office notified institutions via email and later sent a follow-up letter to institutions that provided an overview of the breach, operational and technical steps used to mitigate the breach, and additional steps the agency is taking to protect sensitive data. Other regional offices did not send any written communications and informed institutions about the breach by telephone. In addition, Supervision management judgmentally determined that some institutions did not need to be informed of the breach because, among other rationales, no consumer PII was exposed and the data breached was publicly available information.

NIST Special Publication 800-61 states that organizations should have set guidelines for communicating with outside parties regarding an incident. The CFPB's *Confidential Information Breach Response Directive* states that the associate director for the division that owns the data will determine the breach mitigation steps, such as whether and how to notify potentially affected entities, but does not define specific criteria for determining the risk to institutions from a breach and the steps for communicating with affected institutions when needed. Interviewees had varying understandings of who should handle communications to institutions affected by a breach. Senior officials were unsure whether the CFPB had a written process outlining the expected steps.

Mishandling CSI can lead to potential legal repercussions and damage to an institution's reputation. Similarly, mishandling PII can expose individuals to fraud or financial loss. We believe that by establishing a process for evaluating potential harm or reputational risk to affected institutions and communicating with the institutions about this risk, the CFPB will be better prepared to respond to future breaches. Further, establishing clear roles and responsibilities for assessing risk and notifying institutions will enable

the CFPB to enhance coordination among the SAOP, the BRT, and Supervision when responding to CSI breaches. We also believe such a process will promote transparency and enable affected institutions to respond quickly, if necessary.

Recommendation

We recommend that the CIO, in conjunction with the director of Supervision

7. Update the CFPB's CI breach response directive to
    a. provide guidance for assessing the risk to institutions affected by breaches of CSI and notifying those institutions.
    b. define the roles and responsibilities for those involved in the process.

Management Response

In its response to our draft report, the CFPB concurs with our recommendation. Specifically, the CFPB states that Supervision will develop guidance to establish a process for notifying supervised institutions of CSI breaches and will define the roles and responsibilities for those involved in the process. The CFPB indicated that these actions are subject to available resources and did not provide an estimated time frame for implementation.

OIG Comment

The planned actions described by the CFPB appear to be responsive to our recommendation. In 90 days, we will request that the agency provide an implementation date for this recommendation, and we will follow up to ensure that it is addressed.

Appendix A: Scope and Methodology

Our objective for this evaluation was to assess the CFPB's controls for safeguarding CSI. Specifically, we focused on the CFPB's policies and practices for preventing and responding to breaches of CSI from January 2022 through October 2024. Additionally, our scope included the major incident the CFPB declared on March 16, 2023.

We did not evaluate the CFPB's approach to document classification and labeling or its data loss prevention system; these items were part of our 2024 audit of the CFPB's information security program.[12] In addition, we did not assess the appropriateness of any consequences for the examiner who caused the major incident breach.

To accomplish our objective, we reviewed and analyzed CFPB policies and procedures for safeguarding CSI and for responding to breaches of CSI and PII, such as the *Directive on Document Handling*; the *Examination Prioritization and Scheduling SOP*; the *Privacy Breach Response and Recovery Plan*; the *Reporting Breaches of Confidential Information* policy; and the *Confidential Information Breach Response Directive*. We also reviewed related training materials, manuals for SES, and analyzed the population of routine breaches of CI belonging to SEFL from January 2022 through April 2024, and documentation related to the March 2023 major incident.

We conducted interviews with CFPB officials and staff to gather their perspectives on the CFPB's controls for safeguarding CSI and the 2023 major incident. Specifically, we interviewed Supervision staff familiar with the controls for safeguarding CSI and recent changes to policies and practices in response to the 2023 major incident; select members of the Privacy Office, the Cybersecurity Team, and the BRT; and other CFPB regional officials and staff.

We compared the CFPB's policies and processes to applicable laws, regulations, policies, procedures, guidance, and leading practices of several federal agencies related to safeguarding confidential information.

We conducted this evaluation in accordance with the Council of the Inspectors General on Integrity and Efficiency's *Quality Standards for Inspection and Evaluation*. We conducted this evaluation from April 2024 through December 2024.

[12] Office of Inspector General, *2024 Audit of the CFPB's Information Security Program*, OIG Report 2024-IT-C-019, October 31, 2024.

Appendix B: Management Response

Consumer Financial Protection Bureau

1700 G Street NW, Washington, D.C. 20552

April 14, 2025

Michael VanHuysen
Associate Inspector General for Audits & Evaluations
Board of Governors of the Federal Reserve System
20th Street and Constitution Avenue NW
Washington, DC 20551

Dear Mr. VanHuysen,

Thank you for the opportunity to review and comment on the Office of Inspector General's (OIG) report entitled *The CFPB Can Improve its Safeguards for Protecting Confidential Supervisory Information* (CSI). The Bureau appreciates the time and effort that the OIG put into its evaluation, observations, findings, and recommendations. We note your observations regarding improvements that should be made to improve the CFPB's policies, procedures, and processes for safeguarding CSI. Attached to this letter, please find our responses to the specific recommendations found in the report.

Thank you again for your review and the opportunity to provide comments on this report.

Sincerely,

Cassandra Huggins
Principal Deputy Assistant Director, Supervision Policy & Operations

Christopher Chilbert
Chief Information Officer

consumerfinance.gov

Responses to Specific Recommendations

Recommendations in response to Finding 1: CFPB Guidance Does Not Effectively Limit Examiner Access to CSI in SES (responsible party: director of Supervision)

Response: The responses and timelines to Recommendations 1, 2, and 3 are contingent on the availability of system development resources. Significant development resources are required to implement such access controls, including the ability to control access on a file-by-file basis.

1. **Define in policy**
    a. **The process that examiners should use to request access to files in SES.**

    b. **The criteria that managers and regional analysts should use to assess whether a need to know exists in accordance with the least privilege principle.**

    c. **The requirement that regional analysts document an examiner's need to know before granting access to supervision files in SES.**

    d. **Consequences for accessing CSI without a need to know or providing access to CSI when a need to know does not exist.**

    Response: We agree with this recommendation. Supervision will work to develop and deploy appropriate processes to implement the recommendation, subject to available resources.

2. **Update the document handling directive to require supervision staff to share files by emailing SES links.**
    Response: We agree with this recommendation. Supervision will work to update the document handling directive to require Supervision staff to share files by emailing SES links, subject to available resources.

3. **Develop and require training for CFPB staff involved in the examination process for the policy and guidance resulting from recommendations 1 and 2.**
    Response: We agree with this recommendation. Supervision will work to develop required training for CFPB staff involved in the examination process regarding the policies and processes implemented as a result of recommendations 1 and 2, subject to available resources.

Recommendations in response to Finding 2: CFPB Guidance Does Not Sufficiently Limit Access to CSI Used to Prioritize Supervisory Activities (responsible party: director of Supervision, RAMPS program director)

4. **Update the guidance for prioritizing and scheduling examinations to reflect the current link sharing practice and to limit access to the supporting analysis to those with a need to know.**
   Response: We agree with this recommendation. Supervision will work to update relevant guidance to reflect the current link sharing practice and to limit access to the supporting analysis to those with a need to know, subject to available resources.

Recommendation in response to Finding 3: CFPB Guidance Does Not Adequately Detail Expectations for Managing CSI Breaches (responsible party: CIO, director of Supervision)

5. **Update the guidance for managing breaches of CSI to include expectations for**
   a. **Assessing and documenting the level of harm associated with a breach.**
   b. **Counseling, training, or taking other measures to hold CFPB staff responsible for breaches accountable, as appropriate, and documenting such actions.**
   c. **Analyzing the causes of breaches to identify trends and implement appropriate control adjustments, as necessary.**

6. **Develop required training on the updated guidance after it is implemented.**

   Response: We agree with these recommendations. Subject to available resources, Supervision will work to update its guidance to include expectations for managing breaches of CSI to include expectations for assessing and documenting the level of harm associated with a breach; counseling, training or taking other measures to hold responsible CFPB staff accountable, as appropriate, and documenting such actions; and analyzing the cause of breaches to identify trends and implement appropriate controls as necessary.

Recommendation in response to Finding 4: CFPB Guidance Does Not Define a Process for Notifying Supervised Institutions of CSI Breaches (responsible party: CIO, director of Supervision)

7. **Update the CFPB's CI breach response directive to**
   a. **provide guidance for assessing the risk to institutions affected by breaches of CSI and notifying those institutions.**

b. define the roles and responsibilities for those involved in the process.

Response: We agree with this recommendation. As referenced above, Supervision will work to develop guidance that establishes a process for notifying supervised institutions of CSI breaches and will define the roles and responsibilities for those involved in the process, subject to available resources.

Abbreviations

BRT	Breach Response Team
CI	confidential information
CIO	chief information officer
CSI	confidential supervisory information
FTC	Federal Trade Commission
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
OSE	Office of Supervision Examinations
PII	personally identifiable information
RAMPS	reporting, analytics, monitoring, prioritization, and scheduling
SAOP	senior agency official for privacy
SEFL	Division of Supervision, Enforcement and Fair Lending
SES	Supervision Examination System
SOP	standard operating procedure
Supervision	Division of Supervision

Contact Information

General

Office of Inspector General
Board of Governors of the Federal Reserve System
20th Street and Constitution Avenue NW
Mail Center I-2322
Washington, DC 20551

Phone: 202-973-5000
Fax: 202-973-5044

Media and Congressional

OIG.Media@frb.gov

Hotline

Report fraud, waste, and abuse.

Those suspecting possible wrongdoing may contact the OIG Hotline by mail, web form, phone, or fax.

OIG Hotline
Board of Governors of the Federal Reserve System
20th Street and Constitution Avenue NW
Mail Center I-2322
Washington, DC 20551

Phone: 800-827-3340
Fax: 202-973-5044