Office of the Comptroller of the Currency
Supporting Statement
Computer-Security Incident Notification
OMB Control No. 1557-0350

A. Justification.

1. Circumstances that make the collection necessary:

To promote the timely notification of computer-security incidents that may materially and adversely affect Office of the Comptroller of the Currency (OCC)-supervised institutions, 12 CFR part 53 prescribes regulations for the reporting and disclosure of computer security incidents. A "computer-security incident," as defined by § 53.2(b)(4) is an "occurrence that results in actual harm to the confidentiality, integrity, or availability of an information system or the information that the system processes, stores, or transmits."

In accordance with § 53.3, a banking organization[1] must report to the OCC the occurrence of a notification incident at the banking organization. "Notification incident," as defined in § 53.2(b)(7), means "a computer-security incident that has materially disrupted or degraded, or is reasonably likely to materially disrupt or degrade, a banking organization's ability to carry out banking operations, activities, or processes, or deliver banking products and services to a material portion of its customer base, in the ordinary course of business; business line(s), including associated operations, services, functions, and support, that upon failure would result in a material loss of revenue, profit, or franchise value; or operations, including associated services, functions and support, as applicable, the failure or discontinuance of which would pose a threat to the financial stability of the United States."

Additionally, § 53.4 requires a bank service provider[2] to notify at least one bank-designated point of contact at each affected banking organization customer as soon as possible when the bank service provider determines that it has experienced a computer-security incident that has materially disrupted or degraded, or is reasonably likely to materially disrupt or degrade, covered services provided to such banking organization for four or more hours. This disclosure requirement for bank service providers is important because banking organizations have become increasingly reliant on third parties to provide essential services.[3] A banking organization may also authorize or contract with a bank service provider to notify the OCC of such an incident on its behalf.

2. Use of the information:

The computer-security incident information collected under part 53 allows the OCC to (1) have early awareness of emerging threats to banking organizations and the broader financial system, (2) better assess the threat a notification incident poses to a banking organization and take appropriate actions to address the threat, (3) facilitate and approve requests from banking organizations for assistance through U.S. Treasury Office of Cybersecurity and Critical Infrastructure Protection (OCCIP), (4) provide information and guidance to banking organizations, and (5) conduct horizontal analyses to provide targeted guidance and adjust supervisory programs.[4]

---

[1] Section 53.2(b)(1) defines a banking organization as "a national bank, Federal savings association, or Federal branch or agency of a foreign bank; provided, however, that no designated financial market utility shall be considered a banking organization."

[2] Section 53.2(b)(2) defines a bank service provider as "a bank service company or other person that performs covered services; provided, however, that no designated financial market utility shall be considered a bank service provider."

[3] 86 FR 66425 (Nov. 23, 2021).

[4] *Id.*

3. Consideration of the use of improved information technology:

Not applicable.

4. Efforts to identify duplication:

There is no duplication.

5. If the collection of information impacts small businesses or other small entities, describe any methods used to minimize burden.

Not applicable.

6. Consequences to the federal program if the collection were conducted less frequently:

Not applicable.

7. Special circumstances that would cause an information collection to be conducted in a manner inconsistent with 12 CFR part 1320:

Not applicable.

8. Efforts to consult with persons outside the agency:

The OCC issued a 60-day *Federal Register* notice on November 27, 2024, 89 FR 93827. No comments were received.

9. Payment or gift to respondents:

None.

10. Any assurance of confidentiality:

The information will be kept private to the extent permitted by law.

11. Justification for questions of a sensitive nature:

There are no questions of a sensitive nature.

12. Burden estimate:

Reporting: 100 Respondents[5] x 3 hours = 300 hours
Disclosure: 832 Respondents[6] x 3 hours = 2,496 hours

[5] The estimated number of respondents for the reporting requirement is based on actual data from May 2022 - May 2024. During that 2-year period, 482 cyber incidents were identified, but only 200 of those incidents were identified as notification incidents that required reporting to the OCC, which is roughly 100 cyber incidents per year.
[6] Since cyber-incident disclosure activities required by the regulation are not reported to the OCC, this burden was

Assuming one response per respondent and 932 respondents, the OCC estimates a total of 932 responses and 2,796 burden hours annually. The OCC estimates the cost of the hour burden to respondents as follows:

2,796 hours x $129.40 = $ 361,802

To estimate wages the OCC reviewed May 2023 data for wages (by industry and occupation) from the U.S. Bureau of Labor Statistics (BLS) for credit intermediation and related activities (NAICS 5220A1). To estimate compensation costs associated with the rule, the OCC uses $129.40 per hour, which is based on the average of the 90th percentile for six occupations adjusted for inflation (4.3 percent as of Q1 2024), plus an additional 34.6 percent for benefits (based on the percent of total compensation allocated to benefits as of Q4 2023 for NAICS 522: credit intermediation and related activities).

13. Estimate of total annual cost to respondents (excluding cost of hour burden in Item #12):

Not applicable.

14. Estimates of annualized costs to the federal government:

Not applicable.

15. Change in burden:

Prior Burden: 2,472 Hours.
Current Burden: 2,796 Hours.
Difference: +324 Hours.

The slight increase in burden hours is attributed the OCC's use of actual incident data to determine the current burden. The prior burden was estimated before the effectiveness of incident notification rule and was based on projected (rather than actual) incidents.

16. Information regarding collections whose results are to be published for statistical use:

Not applicable.

17. Reasons for not displaying OMB expiration date:

Not applicable.

18. Exceptions to the certification statement:

Not applicable.

---

calculated based on the percentage of estimated firms that would be required to make disclosure. The burden estimate assumes that 124,779 firms would be subject to the disclosure requirements, which is the number of firms in the United States under NAICS code 5415 in 2021, the latest year for which such data is available. *See* U.S. Census Bureau, 2021 SUSB Annual Data Tables by Establishment Industry, https://www.census.gov/data/tables/2021/econ/susb/2021-susb-annual.html (page last revised July 22, 2024). Further, the estimate assumes that 2 percent of those 124,779 firms (approximately 2,496 firms) would be required to make disclosures each year. Dividing 2,496 firms equally among the three financial regulatory agencies (OCC, FDIC, and Board) allocates 832 firms to the OCC as disclosure respondents.

B. Collections of Information Employing Statistical Methods.

Not applicable.