SUPPORTING STATEMENT
Computer Security Incident Notification
(OMB Control No. 3064-214)

INTRODUCTION

The Federal Deposit Insurance Corporation (FDIC) is requesting OMB approval of a n extension, without change, of this information collection that requires a banking organization to provide its primary federal regulator with prompt notification of any "computer-security incident" that rises to the level of a "notification incident" as defined in the rule. The rule requires such notification upon the occurrence of a notification incident as soon as possible and no later than 36 hours after the banking organization has determined that the incident occurred. This notification requirement is intended to serve as an early alert to a banking organization's primary federal regulator and is not intended to provide an assessment of the incident. The rule allows a banking organization to authorize or contract with a bank service provider to allow the bank service provider to make the relevant notifications to the banking organization's primary federal regulator on the banking organization's behalf.

A. JUSTIFICATION

1. Circumstances that make the collection necessary:

Internet crime and cyberattacks reported to federal law enforcement have increased in frequency and severity in recent years.[1] These types of attacks may use destructive malware or other cybersecurity exploits to target weaknesses in the computers or networks of banking organizations supervised by the agencies.[2] Some exploits have the potential to alter, delete, or otherwise render a banking organization's data and systems unusable. Depending on the scope of an incident, a banking organization's data and system backups may also be affected, which can severely affect its ability to recover operations. In addition, banking organizations have become increasingly reliant on bank service providers to provide essential technology-related products and services. These bank service providers are also vulnerable to cyber threats.

The agencies believe that it is critically important that the primary federal regulator of a banking organization be notified as soon as possible of a significant "computer-security incident"[3] that could prevent the banking organization from carrying out banking

1 *See* Federal Bureau of Investigation, Internet Crime Complaint Center, *2019 Internet Crime Report* at 5 (last accessed Sept. 4, 2020), *available at https://pdf.ic3.gov/2019_IC3Report.pdf.*
2 *See Cybercriminals and Fraudsters: How Bad Actors Are Exploiting the Financial System During the COVID-19 Pandemic: Virtual Hearing Before the Subcommittee on National Security, International Development and Monetary Policy of the U.S. House Committee on Financial Services 116th Congress* (2020) *(*written statement of Tom Kellerman, Head of Cybersecurity Strategy, VMware, Inc.), *available at https://financialservices.house.gov/uploadedfiles/hhrg-116-ba10-wstate-kellermannt-20200616.pdf*.
3 As defined by the rule, a *computer-security incident* is an occurrence that results in actual or potential jeopardy to the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits; or constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies. To promote uniformity of terms, the agencies have sought to align this term to the fullest extent possible with an existing definition from the National Institute of Standards and Technology (NIST). *See*

operations, result in customers being unable to access their deposit and other accounts, or may jeopardize the viability of the operations of the individual banking organization or the stability of the financial sector.[4] The rule refers to these significant computer-security incidents as "notification incidents." The relevant agency receiving notice of notification incidents could assess the nature and severity of the incident, including whether it is isolated or widespread. The agency would then be in a position to take actions including, as appropriate, alerting other banking organizations and regulatory agencies, while protecting confidential supervisory information and facilitating requests for assistance. These actions could help to mitigate the impact of the incident, preserve the safe and sound operation of the banking organization, and reduce the risks to the financial sector.

This notification requirement is intended to serve as an early alert to a banking organization's primary federal regulator and is not intended to include an assessment of the incident. The rule allows a banking organization to authorize or contract with a bank service provider to allow the bank service provider to make the relevant notifications to the banking organization's primary federal regulator on the banking organization's behalf. Moreover, a bank service provider as defined herein and in accordance with the Bank Service Company Act (BSCA)[5] is required to notify affected banking organization customers within four hours of when it experiences a computer-security incident that it reasonably believes could disrupt, degrade, or impair services provided subject to the BSCA for four or more hours. "Bank service providers" would include both bank service companies and third-party service providers, under the BSCA.

2. Use of the information:

The notification requirement is intended to serve as an early alert to a banking organization's primary federal regulator and is not intended to include an assessment of the incident. Additionally, a bank service provider as defined in the rule and in accordance with the Bank Service Company Act (BSCA)[6] is required to notify affected banking organization customers within four hours of when it experiences a computer-security incident that it reasonably believes could disrupt, degrade, or impair services provided subject to the BSCA for four or more hours.

3. Consideration of the use of improved information technology:

Respondents may use any information technology that permits review by FDIC examiners.

4. Efforts to identify duplication:

Current reporting requirements do not sufficiently comprehend the risks posed by notification incidents. For example, under certain circumstances, a banking organization that has been a victim of a notification incident may have to file a Suspicious Activity

---

NIST, Computer Security Resource Center, *Glossary* (last accessed Sept. 20, 2020), *available at https://csrc.nist.gov/glossary/term/Dictionary*.

4 These computer-security incidents may include major computer-system failures, cyber-related interruptions, such as coordinated denial of service and ransomware attacks, or other types of significant operational interruptions.

5 12 U.S.C. § 1861–67.

6 12 U.S.C. § 1861–67.

Report (SAR) to identify suspicious activity that might signal criminal actions (*e.g.*, money laundering or tax evasion). However, information from SARs, when available, may not cover all computer-security incidents impacting operations, and those incidents that are reported are often not reported timely enough for the agencies to take steps to reduce risks to the banking organization or the financial sector, if necessary. The rule is narrowly focused to address the need for timely alerts of notification incidents without interfering with or expanding other applicable reporting requirements.

5. Methods used to minimize burden if the collection has a significant impact on a substantial number of small entities:

This information collection would not have a significant impact on a substantial number of small entities.

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

Less frequent collection could result in incidents not being reported in a timely manner and could hinder the agencies' ability to take steps to reduce risks to banking organizations or to the financial sector.

7. Special circumstances necessitating collection inconsistent with 5 CFR Part 1320.5(d)(2):

There are no special circumstances. This information collection is conducted in accordance with the guidelines in 5 CFR 1320.5(d)(2).

8. Efforts to consult with persons outside the agency:

On November 5, 2024, the agencies published a notice in the Federal Register (89 FR 87877) requesting comment for a period of 60 days on the proposed renewal of this information collection. No comments were received.

9. Payment or Gift to Respondents

None.

10. Any assurance of confidentiality:

Information will be kept private to the extent allowed by law.

11. Justification for questions of a sensitive nature:

No sensitive information is to be collected.

12. Estimate of hour burden including annualized hourly costs:

Estimated Number of Respondents and Responses per Respondent

Potential respondents to the ICs in this ICR include FDIC-supervised IDIs and third-party bank service providers. As of June 30, 2024, the FDIC supervised 2,902 IDIs. Of these,

2,173 are considered small for purposes of the Regulatory Flexibility Act (RFA).[7] The FDIC does not have data available to identify the total number of bank service providers that provide services to the IDIs that it supervises.

The first IC in this ICR is incurred when an IDI notifies its primary federal banking regulator within 36 hours after it has determined a "notification incident" has occurred (IC #1). To estimate the number of respondents to this IC, FDIC used supervisory data to identify instances where FDIC-supervised IDIs had notified the FDIC of cybersecurity-related incidents. Between April 1, 2022 – the effective date of the 2021 Final Rule – and August 31, 2024. The FDIC identified 206 records of relevant notifications. The 206 estimated notifications were submitted by 166 unique IDIs, 161 of which were supervised by the FDIC. Of these 161 IDIs, 79, or approximately 49 percent, are considered small for purposes of the RFA as of June 30, 2024.[8]

The period between April 1, 2022 through August 31, 2024 comprises 883 days, or approximately 2.419 years. Using the unique number of FDIC-supervised IDIs that submitted notifications identified by this analysis over this time period – 161 IDIs – results in an estimate of approximately 67 annual respondents (161 / 2.419 ≈ 67). Therefore, over a three-year PRA renewal period, FDIC estimates that approximately 67 FDIC-supervised IDIs will submit at least one notification annually. Taking the percentage of total respondents over this period that are small – 49 percent – IFDIC estimates that approximately 33 small FDIC-supervised IDIs will submit at least one notification annually.

The estimate of 67 annual respondents is a decrease from the previous estimate of 96 annual respondents in the 2022 ICR. This decrease is due to a change in estimation methodology from the 2022 ICR, which used an ex-ante estimation procedure to estimate "notification incidents" due to the nonexistence of Subpart C at the time.

FDIC-supervised IDIs submitted 201 notifications in the period from April 1, 2022, through August 31, 2024. To estimate the number of responses per respondent, FDIC divides the total number of notifications submitted by FDIC-supervised IDIs over this period – 201 – by the total number of FDIC-supervised IDIs that submitted at least one notification over this same period – 161. This results in an estimated number of responses per respondent for IC #1 of approximately 1.25. This is an increase from the previous estimate of one response per respondent in the 2022 ICR. This increase is due to a change in methodology from the 2022 ICR, which assumed a single annual response per respondent.

The second IC in this ICR is incurred when a bank service provider notifies each affected IDI 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"[9] services provided to such IDIs for four or more hours (IC

7 The SBA defines a small banking organization as having $850 million or less in assets, where an organization's "assets are determined by averaging the assets reported on its four quarterly financial statements for the preceding year." See 13 CFR 121.201 (as amended by 87 FR 69118, effective December 19, 2022). In its determination, the "SBA counts the receipts, employees, or other measure of size of the concern whose size is at issue and all of its domestic and foreign affiliates." See 13 CFR 121.103. Following these regulations, the FDIC uses an insured depository institution's affiliated and acquired assets, averaged over the preceding four quarters, to determine whether the insured depository institution is "small" for the purposes of RFA.

8 FDIC Call Report data for the four-quarter period ending on June 30, 2024, or ending in the most recent period for which the IDI submitted Call Report data.

9 See 12 C.F.R. §304.24

#2). The FDIC does not have the data necessary to estimate the total number of notifications issued by bank service providers of FDIC-supervised IDIs. Therefore, to estimate the number of respondents for this IC, we used the methodology used in the 2022 ICR. The methodology assumes a 2 percent per year frequency of such incidents from bank service providers. To estimate the number of bank service providers, the FDIC uses the number of firms classified as "Computer Systems Design and Related Services", as defined by the North American Industry Classification System (NAICS).[10] According to NAICS data as of 2021, the latest period for which data is available, there are 124,779 firms under this classification (NAICS code 5415). Using the assumption above, the FDIC estimates that there will be approximately 2,496 incidents annually.

There is no data available currently on the number of bank service providers that meet the definition of a small entity[11] for purposes of the RFA. Instead, FDIC used the Small Business Administration (SBA) Office of Advocacy's definition of a small business, which is an independent business with fewer than 500 employees.[12] Using this definition, FDIC calculated the fraction of all active bank service providers using the NAICS classification above with fewer than 500 employees. Of the 124,779 firms under this classification, 123,839, or approximately 99 percent, have fewer than 500 employees. To estimate the number of respondents that would be considered as small for IC #2, IFDIC multiplies the estimate of 2,496 annual respondents by the proportion of bank service providers that it estimates to be small – 99 percent. Thus, approximately 2,471 annual respondents (2,496 * 0.99 ≈ 2,471) to IC #2 would be considered small for purposes of the RFA.

Finally, the methodology apportions this estimated number of incidents equally across the three federal banking agencies – the FDIC, OCC, and Federal Reserve Board. Therefore, of the 2,496 incidents estimated using this methodology, the FDIC assumes the burden for 832 (2,496 * (1/3) = 832) of these. Using the estimated percentage of bank service providers that are small - 99 percent - FDIC estimates that approximately 824 (832 * 0.99 ≈ 824) of these incidents will come from small bank service providers.

The estimate of 832 annual respondents to IC #2 is an increase from the previous estimate of 802 annual respondents in the 2022 ICR. This increase is due to an increase in the number of firms classified as "Computer Systems Designed and Related services" in this ICR – at 124,779 firms using 2021 NAICS data - compared to the 2022 ICR – at 120,392 firms using 2018 NAICS data.

Respondents under IC #2 may be providing services to multiple IDIs. According to Subpart C, service providers are required to provide notifications to all IDIs that are affected by a computer security incident that meets the criteria described above. For purposes of this ICR, a response to IC #2 comprises all the activities that the bank service providers must perform to meet the requirements of subpart C if and when it experiences a computer-security incident that meets the conditions under 12 CFR 304.24. Given the

10 See U.S. Census Bureau, 2021 Statistics of U.S. Businesses (SUSB) Annual Data, Tables by Establishment Industry, https://www.census.gov/data/tables/2021/econ/susb/2021-susb-annual.html.

11 The SBA does not have an exact dollar or employment threshold to be considered as small for NAICS code 5415. However, the SBA defines a small office of "Computer Systems Design Services" (NAICS 541512) and "Custom Computer Programming Services" (NAICS 541511) as having $34 million or less in annual receipts. *See* 13 CFR 121.201.

12 U.S. SBA Office of Advocacy, "Frequently Asked Questions About Small Business, 2023," available at https://advocacy.sba.gov/2023/03/07/frequently-asked-questions-about-small-business-2023/ (accessed October 25, 2024).

methodology above that assumes that each of the 2,496 incidents per year are connected to a single respondent, FDIC uses a count of one annual response per respondent for this IC. This estimate remains unchanged from the estimate in the 2022 ICR.

Estimated Hourly Burden

The 2022 ICR estimated that, for both ICs in this ICR, respondents will incur approximately three hours of burden. For IC #1, this estimate pertains to all the activities conducted by an IDI to notify its primary federal regulator. For IC #2, this estimate pertains to all activities that a bank service provider conducts to notify bank-designated points-of-contact at each affected IDI after it has experienced a notification incident (IC #2). The FDIC has reviewed this estimate and the underlying regulatory requirements in Subpart C – which have not changed since the publication of the 2022 ICR – and confirms that, based on its supervisory experience, this estimate remains reasonable and appropriate.

The estimated annual burden for the ICs in this ICR, in hours, is the product of the estimated number of respondents, number of responses per respondent per year, and hours per response, as summarized in Table 1 below. The total estimated annual burden for this ICR is 2,748 hours, an increase of 54 hours from the 2022 ICR (2,694 hours). This increase is due to an increase in the estimated number of respondents in IC #2. This increase is attenuated by a decrease in the estimated annual burden for IC #1.

Table 1. Summary of Estimated Annual Burden (OMB No. 3064-0214)

Information Collection (IC) (Obligation to Respond)	Type of Burden (Frequency of Response)	Number of Respondents	Number of Responses per Respondent	Time per Response (HH:MM)	Annual Burden (Hours)
1. Notification Incident Reporting, 12 CFR 304.23 (Mandatory)	Reporting (On Occasion)	67	1.25	03:00	252
2. Service Provider Notification, 12 CFR 304.24 (Mandatory)	Third-Party Disclosure (On Occasion)	832	1	03:00	2,496
				Total Annual Burden (Hours):	***2,748***

Source: FDIC.

Note: The estimated annual IC time burden is the product, rounded to the nearest hour, of the estimated annual number of responses and the estimated time per response for a given IC. The estimated annual number of responses is the product, rounded to the nearest whole number, of the estimated annual number of respondents and the estimated annual number of responses per respondent. This methodology ensures the estimated annual burdens in the table are consistent with the values recorded in OMB's consolidated information system.

Total Estimated Hourly Labor Compensation Rates

To estimate the average cost of compensation per hour, FDIC uses the 75th percentile hourly wages reported by the Bureau of Labor Statistics (BLS) National Industry-Specific Occupational Employment and Wage Estimates (OEWS) for the relevant occupations in the Depository Credit Intermediation sector. However, the latest OEWS wage data are as of May 2023 and do not include non-wage compensation. To adjust these wages for use in the memo, FDIC multiplies the OEWS hourly wages by

approximately 1.53 to account for non-wage compensation, using the BLS Employer Cost of Employee Compensation (ECEC) data as of March 2023 (the latest published release prior to the OEWS wage data). It then multiplies the resulting compensation rates by approximately 1.05 to account for the change in the seasonally adjusted Employment Cost Index for the Credit Intermediation and Related Activities sector (NAICS Code 522) between March 2023 and June 2024.

After making these adjustments, FDIC weights the total hourly compensation by the relevant shares of the occupations shown in Table 2. After reviewing the two ICs in this ICR, as well as the associated requirements in Subpart C, the FDIC estimates that the labor allocated for both the ICs in this ICR would be allocated as follows: IT Specialists would perform 60 percent; Executives and Managers would perform 25 percent; Lawyers would perform 10 percent; and Clerical workers would perform five percent. FDIC weights the hourly compensation rate for each IC by its annual estimated burden hours and sum the resulting wage rates across the two ICs in this ICR to obtain an estimated weighted average hourly cost of $123.26 for this ICR.

Table 2. Summary of Hourly Burden Cost Estimate (OMB No. 3064-0214)

Information Collection (IC) (Obligation to Respond)	Hourly Weight (%)	Percentage Shares of Hours Spent by and Hourly Compensation Rates for each Occupation Group (by Collection)						Estimated Hourly Compensation Rate
		Exec. & Mgr. ($146.13)	Lawyer ($182.07)	Compl. Ofc. ($77.07)	IT ($110.91)	Fin. Anlst. ($100.28)	Clerical ($39.39)	
1. Notification Incident Reporting, 12 CFR 304.23 (Mandatory)	9.17	25	10	0	60	0	5	$123.26
2. Service Provider Notification, 12 CFR 304.24 (Mandatory)	90.83	25	10	0	60	0	5	$123.26
							Weighted Average Hourly Compensation Rate:	***$123.26***

Source: Bureau of Labor Statistics: 'National Industry-Specific Occupational Employment and Wage Estimates: Industry: Credit Intermediation and Related Activities (5221 And 5223 only)' (May 2023), Employer Cost of Employee Compensation (March 2023), and Employment Cost Index (March 2023 and June 2024). Standard Occupational Classification (SOC) Codes: Exec. And Mgr = 11-0000 Management Occupations; Lawyer = 23-0000 Legal Occupations; Compl. Ofc. = 13-1040 Compliance Officers; IT = 15-0000 Computer and Mathematical Occupations; Fin. Anlst. = 13-2051 Financial and Investment Analysts; Clerical = 43-0000 Office and Administrative Support Occupations.

Note: The estimated hourly compensation rate for a given IC is the average of the hourly compensation rates for the occupations used to comply with that IC, weighted by the estimated share of hours spent by each occupation. The weighted average hourly compensation rate for the entire ICR is the average of the estimated hourly compensation rates for all ICs, weighted by the share of hourly burden for IC. These hourly weights, as shown in the “Hourly Weight” column of this table, are the quotients of the estimated number of annual burden hours for each IC and the total estimated number of annual burden hours across all ICs.

Total **Estimated Compliance Cost**

Given the above analyses, and applying the estimates summarized in Tables 1 and 2, the estimated total annual cost of compliance for this ICR is **$338,718** (2,748 hours / year * $123.26 / hour = $338,718 a year), as shown in Table 3. This is an increase of $28,908 from the 2022 ICR ($309,810). This increase can be explained both by an increase in the total estimated annual burden of IC #2, as well as an increase in the estimated hourly compensation rate from $115 in the 2022 ICR to $123.26 in this ICR. This increase is attenuated by changes to the estimation methodology for IC #1, resulting in a lower total annual burden for that IC.

13. Estimate of start-up costs to respondents:

None.

14. Estimate of annualized costs to the government:

None.

15. Analysis of change in burden:

See section 12 above..

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

No publication will be made of this information.

17. Display of expiration date:

Not applicable.

18. Exceptions to Certification

None.

B. Collection of Information Employing Statistical Methods

Not Applicable.