4810-033-P

DEPARTMENT OF THE TREASURY

Office of the Comptroller of the Currency

Agency Information Collection Activities: Information Collection Renewal; Submission for OMB Review; FFIEC Cybersecurity Assessment Tool

AGENCY: Office of the Comptroller of the Currency (OCC), Treasury.

ACTION: Notice and request for comment.

SUMMARY: The OCC, on behalf of itself, the Board of Governors of the Federal Reserve System (Board), the Federal Deposit Insurance Corporation (FDIC), and the National Credit Union Administration (NCUA) (collectively, the Agencies), as part of its continuing effort to reduce paperwork and respondent burden, invites the general public and other Federal agencies to comment on a continuing information collection as required by the Paperwork Reduction Act of 1995 (PRA). In accordance with the requirements of the PRA, the Agencies may not conduct or sponsor, and the respondent is not required to respond to, an information collection unless it displays a currently valid Office of Management and Budget (OMB) control number. The OCC is soliciting comment on behalf of the Agencies concerning renewal of the information collection titled, "FFIEC Cybersecurity Assessment Tool" (Assessment). The OCC also is giving notice that it has sent the collection to OMB for review.

DATES: Comments must be submitted on or before [INSERT 30 DAYS FROM DATE OF PUBLICATION IN THE **FEDERAL REGISTER**].

ADDRESSES: Commenters are encouraged to submit comments by e-mail, if possible. You may submit comments by any of the following methods:

- *E-mail*: *prainfo@occ.treas.gov*.
- *Mail*: Chief Counsel's Office, Attention: Comment Processing, 1557-0328, Office of the Comptroller of the Currency, 400 7th Street, SW., suite 3E-218, Washington, DC 20219.
- *Hand Delivery/Courier*: 400 7th Street, SW., suite 3E-218, Washington, DC 20219.

- *Fax*: (571) 465-4326.

Instructions: You must include "OCC" as the agency name and "1557-0328" in your comment. In general, the OCC will publish comments on *www.reginfo.gov* without change, including any business or personal information provided, such as name and address information, e-mail addresses, or phone numbers. Comments received, including attachments and other supporting materials, are part of the public record and subject to public disclosure. Do not include any information in your comment or supporting materials that you consider confidential or inappropriate for public disclosure.

Written comments and recommendations for the proposed information collection should also be sent within 30 days of publication of this notice to *www.reginfo.gov/public/do/PRAMain*. Find this particular information collection by selecting "Currently under 30-day Review – Open for Public Comments" or by using the search function.

On May 31, 2022, the OCC published a 60-day notice for this information collection, 87 FR 32497. You may review comments and other related materials that pertain to this information collection following the close of the 30-day comment period for this notice by the method set forth in the next bullet.

- Viewing Comments Electronically: Go to *www.reginfo.gov*. Hover over the "Information Collection Review" tab and click on "Information Collection Review" from the drop-down menu. From the "Currently under Review" drop-down menu, select "Department of Treasury" and then click "submit." This information collection can be located by searching by OMB control number "1557-0328" or "FFIEC Cybersecurity Assessment Tool." Upon finding the appropriate information collection, click on the related "ICR Reference Number." On the next screen, select "View Supporting Statement and Other Documents" and then click on the link to any comment listed at the bottom of the screen.
- For assistance in navigating *www.reginfo.gov*, please contact the Regulatory Information Service Center at (202) 482-7340.

FOR FURTHER INFORMATION CONTACT: Shaquita Merritt, OCC Clearance Officer, Chief Counsel's Office, (202) 649-5490, Office of the Comptroller of the Currency, 400 7th Street, SW., suite 3E-218, Washington, DC 20219. If you are deaf, hard of hearing, or have a speech disability, please dial 7-1-1 to access telecommunications relay services.

SUPPLEMENTARY INFORMATION: Under the PRA (44 U.S.C. 3501 *et seq.*), Federal agencies must obtain approval from OMB for each collection of information they conduct or sponsor. "Collection of information" is defined in 44 U.S.C. 3502(3) and 5 CFR 1320.3(c) to include agency requests or requirements that members of the public submit reports, keep records, or provide information to a third party. The definition contained in 5 CFR 1320.3(c) also includes a voluntary collection. The OCC asks that OMB extend its approval of the collection in this notice.

Title: FFIEC Cybersecurity Assessment Tool.

OMB Number: 1557-0328.

Description: Cyber threats continue to evolve and increase in frequency and sophistication. Financial institutions[1] are exposed to cyber risks because they are dependent on information technology to deliver services to consumers and businesses every day. Cyberattacks on financial institutions may result in unauthorized access to, and the compromise of, confidential information, as well as the destruction of critical data and systems. Disruption, degradation, or unauthorized alteration of information and systems can affect a financial institution's operations and core processes and undermine confidence in the nation's financial services sector. Absent immediate attention to these rapidly increasing threats, individual financial institutions and the whole financial sector are at risk.

For this reason, the Agencies, under the auspices of the Federal Financial Institutions Examination Council (FFIEC), have worked diligently to assess and enhance the state of the

[1] For purposes of this information collection, the term "financial institution" includes banks, savings associations, credit unions, and bank holding companies.

financial industry's cyber preparedness and to improve the Agencies' examination procedures and training to strengthen the oversight of financial industry cybersecurity readiness. The Agencies also have focused on providing financial institutions with resources that can assist in protecting them and their customers from the growing risks posed by cyberattacks.

As part of these efforts, the Agencies, with the other FFIEC members, developed the Assessment to assist financial institutions of all sizes in assessing their inherent cyber risks and their risk management capabilities. The Assessment allows a financial institution to identify its inherent cyber risk profile based on technologies and connection types, delivery channels, online/mobile products and technology services, organizational characteristics, and cyber threats it is likely to face. Once a financial institution identifies its inherent cyber risk profile, it can use the Assessment's maturity matrix to evaluate its level of cybersecurity preparedness based on its cyber risk management and oversight, threat intelligence and collaboration, cybersecurity controls, external dependency management, and cyber incident management and resiliency planning. A financial institution may use the matrix's maturity levels to identify opportunities for improving its cyber risk management based on its inherent risk profile. The Assessment also enables a financial institution to rapidly identify areas that could improve the financial institution's cyber response programs, as appropriate. Use of the Assessment by financial institutions is voluntary.

Type of Review: Regular.

Affected Public: Businesses or other for-profit.

Burden Estimates:

Number of Respondents: 12,781.

Total Burden: 1,154,540 hours.

On May 31, 2022, the OCC published a notice for 60 days of comment concerning this collection, 87 FR 32497. The OCC received one comment from a trade association, which generally recognized that the Assessment may be a useful tool for community banks and included several recommendations for consideration. First, the commenter stated that use of the

Assessment should remain voluntary and that institutions should not be required to use a specific tool or to switch tools.

Financial institution's use of the Assessment is voluntary. While FFIEC members have emphasized the benefits of using a standardized approach to assess and improve cybersecurity preparedness, they have also recognized that institutions may choose from a variety of standardized tools aligned with industry standards and best practices to assess their cybersecurity preparedness.[2]

The commenter also suggested that the Agencies work with the trade association and community banks to update the Assessment, including to improve understanding by and education for senior leaders and boards of directors, who may not be information technology specialists.

The Agencies appreciate the commenter's feedback and are continually seeking ways to update and improve the tools they use to assess cybersecurity. For example, in response to requests, the Agencies, with the other members of the FFIEC, updated the Assessment to expand the response options for each declarative statement in the maturity matrix.[3] Similarly, feedback from commenters informed the development of frequently asked questions.[4] In addition, several other resources are available to assist financial institutions in using the Assessment efficiently, including an "Overview for Chief Executive Officers and Boards of Directors" that provides an executive summary of the Assessment and identifies questions that financial institution boards and senior management may ask.

---

[2] "FFIEC Encourages Standardized Approach to Assessing Cybersecurity Preparedness," FFIEC Press Release, August 28, 2019, *available at* https://www.ffiec.gov/press/pr082819.htm.

[3] "FFIEC Release Update to Cybersecurity Assessment Tool," FFIEC Press Release, May 31, 2017, *available at* https://www.ffiec.gov/press/pr053117.htm (explaining that the additional response options would allow "financial institution management to include supplementary or complementary behaviors, practices and processes that represent current practices of the institution in supporting its cybersecurity activity assessment").

[4] "FFIEC Cybersecurity Assessment Tool: Frequently Asked Questions," October 17, 2016, *available at* https://www.ffiec.gov/pdf/cybersecurity/FFIEC_CAT%20FAQs.pdf.

Finally, the commenter suggested that the Agencies provide non-attributable reports and statistical analysis based on information collected by the Agencies. Since use of the Assessment by financial institutions is voluntary and may vary across financial institutions, the Agencies do not to intend to publish or otherwise make publicly available the results of financial institutions' use of the Assessment. However, through the FFIEC, the Agencies regularly issue statements and alerts regarding threats and vulnerabilities and provide additional resources.[5]

Comments continue to be invited on:

(a) Whether the collection of information is necessary for the proper performance of the functions of the Agencies, including whether the information has practical utility;

(b) The accuracy of the Agencies' estimates of the burden of the collection of information;

(c) Ways to enhance the quality, utility, and clarity of the information to be collected;

(d) Ways to minimize the burden of the collection on respondents, including through the use of automated collection techniques or other forms of information technology; and

(e) Estimates of capital or start-up costs and costs of operation, maintenance, and purchase of services to provide information.

Theodore J. Dowd,
Deputy Chief Counsel,
Office of the Comptroller of the Currency.

[FR Doc. 2022-16872 Filed: 8/5/2022 8:45 am; Publication Date: 8/8/2022]

[5] Refer to the "Cybersecurity Awareness" page on the FFIEC's website, *available at* https://www.ffiec.gov/cybersecurity.htm.