effectiveness of the program. These requirements also ensure prudent institution management safety and soundness.

Suspicious Activity Report (SAR)

In 1992, the Department of the Treasury was granted broad authority to require suspicious transaction reporting under the Bank Secrecy Act (BSA). *See* 31 U.S.C. 5318(g). The Financial Crimes Enforcement Network (FinCEN), which has been delegated the authority to administer the BSA, joined with the bank regulators in 1996 in requiring, on a consolidated form (*i.e.,* SAR), reports of suspicious transactions. *See* 31 CFR 1020.320(a) (formerly 31 CFR 103.18(a)). The filing of SARs is necessary to prevent and detect crimes involving depository institution funds, institution insiders, criminal transactions, and money laundering. These requirements are necessary to ensure institution safety and soundness.

Banks and savings associations are required to maintain a copy of any SAR filed and the original or business record equivalent of any supporting documentation for a period of five years. The documents are necessary for criminal investigations and prosecutions.

FinCEN and the Federal financial institution supervisory agencies [2] adopted the SAR form to simplify the process through which depository institutions inform their regulators and law enforcement about suspected criminal activity. The SAR form was updated in 1998, 2000, 2003, 2006, 2011, 2012, 2015, and 2018.

Procedures for Monitoring Bank Secrecy Act Compliance

Under 12 CFR 21.21, national banks and savings associations are required to develop and provide for the continued administration of a program reasonably designed to assure and monitor their compliance with the BSA and applicable Treasury regulations. The compliance program must be in writing, approved by the board of directors, and reflected in the minutes of the national bank or savings association. These requirements are necessary to ensure institution compliance with the BSA and applicable Treasury regulations.

Type of Review: Regular.

Affected Public: Business, for-profit institutions, and non-profit.

Estimated Number of Respondents: 1,233.

Estimated Total Annual Burden: 615,130 hours.

The OCC issued a notice for 60 days of comment regarding this collection on May 6, 2019, 84 FR 19825. No comments were received. Comments continue to be invited on:

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

(b) The accuracy of the OCC's estimate 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 of information 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.

Dated: July 23, 2019.

Theodore J. Dowd,

Deputy Chief Counsel, Office of the Comptroller of the Currency.

[FR Doc. 2019–15959 Filed 7–26–19; 8:45 am]

BILLING CODE 4810–33–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, 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 their continuing effort to reduce paperwork and respondent burden, invite the general public and other federal agencies to take this opportunity 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 August 28, 2019.

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

- *Email: 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, email 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.

Additionally, please send a copy of your comments by mail to: OCC Desk Officer, 1557–0328, U.S. Office of Management and Budget, 725 17th Street NW, #10235, Washington, DC 20503 or by email to *oira_submission@omb.eop.gov.*

You may review comments and other related materials that pertain to this information collection [1] following the close of the 30-day comment period for this notice by any of the following methods:

- *Viewing Comments Electronically:* Go to *www.reginfo.gov.* Click on the ''Information Collection Review'' tab. Underneath the ''Currently under Review'' section heading, from the drop-down menu select ''Department of Treasury'' and then click ''submit.'' This information collection can be located by

---

[2] The Federal financial institution supervisory agencies are the Office of the Comptroller of the Currency (OCC), Board of Governors of the Federal Reserve System (Board), Federal Deposit Insurance Corporation (FDIC), and National Credit Union Administration (NCUA). The Office of Thrift Supervision, which was in existence at the time the SAR was adopted, was integrated into the OCC in 2011.

[1] On April 5, 2019, the OCC published a 60-day notice for this information collection, 84 FR 13786.

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.
- *Viewing Comments Personally:* You may personally inspect comments at the OCC, 400 7th Street SW, Washington, DC. For security reasons, the OCC requires that visitors make an appointment to inspect comments. You may do so by calling (202) 649–6700 or, for persons who are deaf or hearing impaired, TTY, (202) 649–5597. Upon arrival, visitors will be required to present valid government-issued photo identification and submit to security screening in order to inspect comments.

FOR FURTHER INFORMATION CONTACT: Shaquita Merritt, OCC Clearance Officer, Carl Kaminski, Special Counsel, or Priscilla Benner, Attorney (202) 649–5490, for persons who are deaf or hearing impaired, TTY, (202) 649–5597, Chief Counsel's Office, Office of the Comptroller of the Currency, 400 7th Street SW, Suite 3E–218, Washington, DC 20219.

SUPPLEMENTARY INFORMATION: Under the PRA (44 U.S.C. *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 OCC, on behalf of the Agencies, asks that OMB extend its approval of the information collection in this notice for three years.

Title: FFIEC Cybersecurity Assessment Tool.

OMB Number: 1557–0328.

Description: Cyber threats continue to evolve and increase exponentially with greater sophistication. Financial institutions [2] are exposed to cyber risks because they are dependent on information technology to deliver services to consumers and businesses every day. Cyber attacks 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, financial institutions and the financial sector as a whole 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 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 cyber attacks.

As part of these efforts, the Agencies 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 the technologies and connection types, delivery channels, online/mobile products and technology services that it offers to its customers, its organizational characteristics, and the cyber threats it is likely to face. Once a financial institution identifies its inherent cyber risk profile, it may use the Assessment's maturity matrix to evaluate its level of cybersecurity preparedness based on the financial institution's cyber risk management and oversight, threat intelligence capabilities, 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 the financial institution's 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 risk management and response programs, as appropriate. Use of the Assessment by financial institutions is voluntary.

Type of Review: Regular.

Frequency of Response: On occasion.

Affected Public: Businesses or other for-profit.

Burden Estimates: [3]

Assessment burden estimate	Estimated number of respondents less than $500 million @80 hours	Estimated number of respondents $500 million–$10 billion @120 hours	Estimated number of respondents $10 billion–; $50 billion @160 hours	Estimated number of respondents over $50 billion @180 hours	Estimated total respondents and total annual burden hours
OCC National Banks and Federal Savings Associations.	823 × 80 = 65,840 hours.	157 × 120 = 18,840 hours.	123 × 160 = 19,680 hours.	82 × 180 = 14,760 hours.	1,185 respondents, 119,120 hours.
FDIC State Non-Member Banks and State Savings Associations.	2,689 × 80 = 215,120 hours.	760 × 120 = 91,200 hours.	34 × 160 = 5,440 hours.	6 × 180 = 1,080 hours	3,489 respondents, 312,840 hours.
Board State Member Banks and Bank Holding Companies.	2,768 × 80 = 221,440 hours.	766 × 120 = 91,920 hours.	81 × 160 = 12,960 hours.	26 × 180 = 4,680 hours.	3,641 respondents, 331,000 hours.
NCUA Federally-Insured Credit Unions	4,830 × 80 = 386,400 hours.	536 × 120 = 64,320 hours.	8 × 160 = 1,280 hours	1 × 180 = 180 hours	5,375 respondents, 452,180 hours.
Total	11,110 × 80 = hours = 888,800.	2,219 × 120 hours = 266,280 hours.	246 hours × 160 = 39,360 hours.	115 hours × 180 = 20,700 hours.	13,690 Respondents, 1,215,140 hours.

On April 5, 2019, the OCC, on behalf of the Agencies published a 60-day notice requesting comment on this collection of information.[4]

The OCC received two comments from industry trade associations and

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

[3] Burden is estimated conservatively and assumes all institutions will complete the Assessment. Therefore, the estimated burden may exceed the actual burden because use of the Assessment by financial institutions is not mandatory. The burden estimates for financial institutions include technology service providers who may assist financial institutions in completing their Assessments.

[4] 84 FR 13786.

one comment from the Financial Services Sector Coordinating Council (FSSCC). The comments, described below, address concerns related to the collection of information.

Usability and Format of the Assessment

One industry group suggested changes to the format of the Assessment to increase usability. This industry group suggested that the FFIEC provide banks an automated or interactive document that banks can use to input information for the Assessment, as opposed to a static PDF document of questions and responses. The industry group added that many community banks are using the Financial Services Sector Coordinating Council's automated Assessment spreadsheet to complete the Assessment in advance of their examinations.

While this industry group asked the Agencies to provide the Assessment in a format that can be easily completed and provided to the examiner, if requested, the commenter also stated that none of the banks it represents reacted favorably to the questions in the notice inviting comment on the FFIEC agencies' potential use of automated collection techniques or other forms of information technology to collect Assessment information. This industry group stated that several banks were concerned that automated collection would lead to a greater need to provide defensible answers during the examination review of the Assessment. The industry group also stated, however, that many banks find it useful to discuss the Assessment with the examiner on-site.

The Agencies acknowledge the potential value of an automated or editable form of the Assessment for financial institutions that choose to use the Assessment. However, as the commenters noted, there are currently available a number of automated versions of the Assessment developed by financial institutions and industry groups. Automated versions are available publicly through trade associations, the Financial Services Information Sharing and Analysis Center, and the FSSCC. Accordingly, the Agencies do not intend to release an additional automated or editable version of the Assessment at this time.

Utility of the Assessment

One industry group commenter stated that the inherent risk review is very linear and could be better rooted in bank operations and market conditions. As an example, this commenter stated that many community banks engage cloud providers for data management, and while cloud computing is a standard term, not all cloud computing companies are equal. They do not all have the same risks or mitigating controls. The commenter stated that when a community bank checks the ''most'' risk level due to the sheer number of cloud providers, the Assessment should allow for an additional level of risk mitigation, such as vendor management and vendor type, which could significantly reduce the risk.

The Agencies appreciate the feedback and are continually seeking ways to update and improve the tools they use to assess cybersecurity. For example, in response to requests from financial institutions, the Agencies recently updated the Assessment to expand the response options for each declarative statement. With the additional response options, financial institutions' management may include supplementary or complementary behaviors, practices, and processes that represent current practices of the institution in assessing declarative statements.

Voluntary Nature of the Assessment

Both industry groups and the FSSCC stated that most financial institutions employ the Assessment as one of the tools they use to assess their cybersecurity risk and maturity. However, they do not use the Assessment exclusively. Most use the Assessment in conjunction with other recognized technology frameworks. As such, the commenters said that examiners should not require the use of the Assessment nor require a financial institution to translate any other risk framework they use into the Assessment format. The commenters stated that if a regulator requires an examiner to complete the Assessment, then the examiner should translate the framework used by the institution into the Assessment format.

The FSSCC and one industry group commenter stated that most of the financial institutions under the Agencies' respective jurisdictions do not perceive the Assessment to be voluntary. To clarify this misperception, these commenters asked the Agencies to make a clear statement that other methodologies, such as NIST Cybersecurity Framework and the FSSCC Cybersecurity Profile, are acceptable inputs into the examination process. The FSSCC also stated that the Agencies should more closely align the Assessment with the NIST Cybersecurity Framework or a NIST-based standard, like the FSSCC Cybersecurity Profile, because the NIST Cybersecurity Framework represents a leading approach to cybersecurity with an international community of users.

One industry group commenter stated that several of its members expressed concern that examiners sometimes provide only a cursory review of the Assessment, if at all, with financial institution staff. This industry group asked the Agencies to clarify that if an institution takes the time to complete the Assessment, examiners should spend time reviewing it with the institution, and that if examiners complete the Assessment as part of the examination process, then the examiner-completed Assessment should be reviewed with the institution during the exam.

The Agencies agree that the NIST Cybersecurity Framework is a valuable tool that provides a mechanism for cross-sector coordination. When developing the Assessment, the Agencies were informed by the NIST Cybersecurity Framework, the FFIEC Information Technology Examination Handbook, and industry accepted cybersecurity practices. In addition, Appendix B of the Assessment provides a mapping of the Assessment to the NIST Cybersecurity Framework. NIST reviewed and provided input on the mapping to ensure consistency with the NIST Cybersecurity Framework principles and to highlight the complementary nature of the two resources.

The NIST Cybersecurity Framework is intended to address cybersecurity across many different sectors. The Agencies determined that developing an assessment, informed by the NIST Cybersecurity Framework but tailored to the specific risks and risk management and controls expectations within the banking industry, could help financial institutions to effectively assess their cybersecurity preparedness. Additionally, we note that prior to the development of the Assessment, the Agencies received many requests from financial institutions, particularly smaller financial institutions, to provide them with a meaningful way to assess cyber risks themselves based on financial sector-specific risks and mitigation techniques. The Agencies developed the Assessment, in part, to address those requests and received several positive comments about how the Assessment met this need. Thus, the Agencies believe the Assessment supports financial institutions by giving them a systematic way to assess their cybersecurity preparedness and evaluate their progress.

Finally, as the Agencies stated when the Assessment was first published, use of the Assessment by financial institutions is voluntary. Therefore, financial institutions may choose to use the Assessment, the NIST Cybersecurity Framework, or any other risk assessment process or tool to assess cybersecurity risk. The Agencies' examiners will not require a financial institution to complete the Assessment, nor will they require financial institutions to translate other risk frameworks into the Assessment format. However, if a financial institution has completed the Assessment, examiners may ask the financial institution for a copy, as they would for any risk self-assessment performed by a financial institution.

Benchmarking

One industry group stated that an advantage to the broad collection of Assessment information across the entire financial services sector is the ability to compile information into useful benchmarking data for banks of comparable size and risk profiles so that peer institutions may become aware of their overall cybersecurity posture in the sector. The industry group stated that the information may be useful to an information security officer or board of directors, particularly when it comes time to discuss budget impacts of the financial institution's security posture. Additionally, benchmarking may allow the Agencies insight into broad categories of risk and exposure in the financial services sector.

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.

Accuracy of Burden Estimate

The Agencies estimated that, annually, it would take a financial institution between 80 and 180 burden hours, depending on the institution's size, to complete the Assessment.

All three commenters addressed the accuracy of the Agencies' burden estimates. The FSSCC letter stated that the Agencies' burden estimate understated the burden involved in completing the Assessment, and one of the industry groups referenced and endorsed the FSSCC's conclusions in its letter. The FSSCC advised that to be more accurate, the Agencies' burden hour estimates should include the time required to prepare for and complete the Assessment. The FSSCC stated that preparing to complete the Assessment includes the testing of controls and systems, gathering of materials as evidence, and the accompanying education of staff that are not familiar with the Assessment. The FSSCC stated that the time required to collect evidence and review systems before the Assessment can begin is significant, and the hours required to review the Assessment's more than 530 responses—usually by committee—is substantial. The FSSCC further stated that the hours required to complete responses to the Assessment, while concurrently completing assessments based on other industry-based standards (*e.g.,* NIST Cybersecurity Framework) for other regulatory agencies (such as state or market regulators), is significant. The FSSCC added that the amount of time spent training cybersecurity professionals on the Assessment is underestimated.

The other industry group stated that the Agencies overestimated the burden hours necessary for community banks to complete and subsequently update the Assessment. This industry group stated that its members reported the burden of completing an initial Assessment as being 40 hours or less. Members of this industry group reported that the burden of completing annual updates to the Assessment for subsequent evaluations could take between 15 and 20 hours.

The Agencies do not believe that commenters provided any additional information that would result in the Agencies changing their burden estimates at this time. The PRA defines burden to include the ''time, effort, or financial resources expended by persons to generate, maintain, or provide information to or for a federal agency.'' 44 U.S.C. 3502(2). The Agencies note that the burden estimates assume that the Assessment is completed by knowledgeable individuals at the financial institution who have readily-available information to complete the Assessment. Additionally, while the Assessment's User's Guide provides that institutions may use the Assessment to prioritize improvement of their cybersecurity posture, completing the Assessment does not include development or implementation of action plans. The Agencies further note that completion of the Assessment does not include internal reporting. Any internal reporting that financial institutions may choose to undertake is therefore outside of the scope of the Assessment. Because reporting to committees, developing and implementing internal action plans, and preparing for examinations are not part of completing the Assessment, these activities do not constitute burden under the PRA. In addition, for financial institutions, reporting to boards and management generally constitutes a usual and customary business practice. Usual and customary business practices are excluded from the definition of burden under OMB regulations.[5]

The Agencies recognize that the size and complexity of a financial institution impacts the amount of time and resources necessary to complete the Assessment and, for that reason, the Agencies' burden estimates vary based on financial institution asset size. The Agencies also appreciate that the time necessary for a particular financial institution to complete the Assessment can vary, potentially widely, based on whether the institution has readily available information to complete the Assessment. The Agencies will review their burden estimates from time to time and will update them in the future, if warranted.

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.

Dated: July 23, 2019.

Theodore J. Dowd,

Deputy Chief Counsel, Office of the Comptroller of the Currency.

[FR Doc. 2019–15964 Filed 7–26–19; 8:45 am]

BILLING CODE 4810–33–P

DEPARTMENT OF THE TREASURY

Office of the Comptroller of the Currency

Agency Information Collection Activities: Information Collection Revision; Submission for OMB Review; Municipal Securities Dealers and Government Securities Brokers and Dealers—Registration and Withdrawal

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

[5] 5 CFR 1320.3(b).