



September 7, 2022

Via Electronic Mail to prainfo@occ.treas.gov

Re: OCC 1557-0328 (PRA Request on FFIEC Cybersecurity Assessment Tool)

Dear Sir/Madam:

The American Bankers Association (ABA) and Bank Policy Institute (BPI)¹ appreciate the opportunity to comment on the Paperwork Reduction Act (PRA) request concerning renewal of the information collection titled, “FFIEC Cybersecurity Assessment Tool” (CAT)².

The Agencies developed and released the CAT in 2015 as a voluntary tool to assist financial institutions of all sizes in assessing their inherent cyber risks and their risk management capabilities. The CAT was designed to allow a financial institution to identify its inherent cyber risk profile based on technologies and connection types, deliver channels, online/mobile products and technology services, organizational characteristics and cyber threat it is likely to face. Then, a financial institution can use the CAT’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. ABA and BPI members welcome

¹The American Bankers Association (ABA) is the voice of the nation’s \$24 trillion banking industry, which is composed of small, regional and large banks that together employ more than 2 million people, safeguard nearly \$19.9 trillion in deposits and extend \$11.4 trillion in loans. The Bank Policy Institute (BPI) is a nonpartisan public policy, research and advocacy group, representing the nation’s leading banks and their customers. Our members include universal banks, regional banks and the major foreign banks doing business in the United States. Collectively, they employ almost 2 million Americans, make nearly half of the nation’s small business loans and are an engine for financial innovation and economic growth.

² See <https://www.govinfo.gov/content/pkg/FR-2022-08-08/pdf/2022-16872.pdf>.

voluntary tools and resources provided by the FFIEC agencies that help banks in enhancing their cybersecurity programs.

In 2015 and 2016, the ABA and BPI contributed to comment letters prepared by the Financial Services Sector Coordinating Council (FSSCC) in which the financial services sector encouraged the FFIEC agencies to update the CAT to better align with the NIST Cybersecurity Framework (CSF) and to do so in a collaborative manner with the Financial Services Sector Coordinating Council (FSSCC) given the voluntary nature of the CAT. To facilitate this process, the FSSCC developed the Profile.

Financial institutions have observed several issues with the CAT. First, the FFIEC agencies did not update the CAT and because of this, its usefulness and applicability has declined over time. Second, examiners request the CAT specifically but may not be trained on other frameworks or standards, such as the NIST CSF. This can cause unnecessary burden to industry by requiring institutions to cross walk global standards to bespoke assessments. Additionally, it undermines the FFIEC's stated intention of the CAT being a voluntary tool because it elevates one framework above all others during examinations.

Since the release of the CAT, the FSSCC (with participation by the ABA and BPI) launched a project to develop a comprehensive, NIST CSF-based assessment tool called the Financial Sector Profile (now the Cyber Risk Institute (CRI) Profile), and also worked to launch CRI as a non-profit standards development organization to continuously update the Profile. The CRI Profile integrates the CAT, as well as other regulatory requirements and expectations. Through this integration, the CRI Profile has also been helpful to financial institutions and examiners by streamlining the assessment process and enabling more risk-focused conversations within firms and their external parties, including examiners. For example, the CRI Profile has been cited as an effective approach by the FFIEC in August 2019 and in the more recent OCC Sound Practices document.

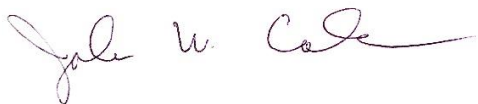
The CRI Profile also advances an important effort to converge and harmonize regulatory requirements and standards in response to the burdens numerous regulatory requirements and standards impose on bank management. Additionally, the CRI Profile is updated regularly to keep pace with evolving regulatory requirements and expectations, as well as changing technological advancements, such as cloud implementation through the Cloud Profile. In contrast, several of the FFIEC agencies have stated that the CAT will not be updated (nor are we advocating for such updates). As a result, leveraging the CRI Profile would provide greater opportunity for financial institutions to minimize the burden to responding to numerous bespoke exams, as well as provide regulators with greater (1) visibility into systemic risk by using a widely adopted cyber control assessment and (2) assurance that examiners and financial institutions are speaking the same language. By basing examinations on existing and widely-recognized standards, government agencies would be better positioned to hire examiners because a larger pool of potential candidates are familiar with the baseline examination expectations.

In light of advances in the development of the Profile, the ABA and BPI encourages the FFIEC to:

- Continue to treat the CAT as a “voluntary” tool that banks can continue to utilize
- Encourage examiner training on global standards and frameworks, such as the NIST CSF and by extension, the CRI Profile
- Leverage the Profile as a more robust and comprehensive assessment tool that is aligned with the NIST Cybersecurity Framework and aids in regulatory harmonization.

Thank you for the opportunity to comment on this Paperwork Reduction Act notice. If you have any questions, please contact John Carlson at (202) 663-5589 (jcarlson@aba.com) and Brian Anderson at (202) 589-2444 (Brian.Anderson@bpi.com).

Respectfully submitted,



John W. Carlson

Vice President, Cybersecurity Regulation and Resilience

American Bankers Association

1120 Connecticut Avenue, NW, Washington, DC 20036



Brian Anderson

Senior Vice President, Technology Regulation

Bank Policy Institute | BITS

1300 I St NW, Washington, DC 20005