Financial Services Sector Coordinating Council
for Critical Infrastructure Protection and Homeland Security

12020 Sunrise Valley Drive
Suite 230
Reston, Virginia 20191

Thursday, June 6, 2019

Chief Counsel's Office
Office of the Comptroller of the Currency
400 7th Street SW
Suite 3E–218
Washington, DC 20219

Re: *Agency Information Collection Activities: Information Collection Renewal; Comment Request; FFIEC Cybersecurity Assessment Tool*
84 Fed. Reg 13786 (proposed April 4, 2019)
OCC 1557–0328

Submitted electronically to prainfo@occ.treas.gov

Dear Sir or Madam:

The Financial Services Sector Coordinating Council ("FSSCC")[1] appreciates the opportunity to respond to the Paperwork Reduction Act ("PRA") notice and request for comment by the Office of the Comptroller of the Currency ("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") with regard to the renewal of the information collection authored by the Federal Financial Institutions Examination Council ("FFIEC"), entitled the FFIEC Cybersecurity Assessment Tool ("CAT").

The FSSCC appreciates the time and effort the FFIEC and its member agencies devoted to developing the CAT. The financial services industry shares the FFIEC's goal to improve the cybersecurity posture of the sector and the nation as whole. We further recognize the FFIEC's continuing efforts to evolve and refine the CAT since its introduction in 2015, including ongoing dialogue with industry and expanding the number of diagnostic responses.

Summary of Recommendations

Similar to previous submissions to the Agencies in September 2015 and January 2016, the FSSCC offers the following recommendations to improve further cybersecurity risk assessments within individual institutions and across the sector.

[1] About FSSCC: Formed in 2002 as a public/private partnership with the support of the U.S. Department of Treasury, FSSCC collaborates with the Treasury and the financial regulatory agencies at the federal and state levels through the Financial and Banking Information Infrastructure Committee, which also formed in 2002 under Treasury's leadership. FSSCC members include 72 of the largest financial institutions and their industry associations representing banking, insurance, credit card networks, credit unions, exchanges, and financial utilities in payments, clearing and settlement.

12020 Sunrise Valley Drive
Suite 230
Reston, Virginia 20191

1. The Agencies should encourage firms to select the assessment approach most aligned with their risk, the CAT being just one of several voluntary assessment methodologies a firm's senior management may choose.

2. The Agencies should expand efforts to educate agency staff and supervised entities as to the acceptability of non-CAT assessment methods.

3. The Agencies should review and revise examination materials and processes that may create the perception of preference among assessment methodologies.

4. The Agencies should recalculate the PRA burden estimate to include implementation costs including compliance, risk management and other resource costs.

5. The Agencies should further align the CAT with the National Institute of Standards and Technology's Cybersecurity Framework ("NIST CSF") or NIST based frameworks, such as the Financial Services Sector Cybersecurity Profile ("FSSCC Cybersecurity Profile").

FSSCC Supports Voluntary Use of the FFIEC CAT

Despite supervisory statements that financial institutions may select the assessment method that best suits their needs, industry perception remains that use of the CAT is required in order to fulfill supervisory expectations. In June 2018, the American Bankers Association (ABA)[2] surveyed 122 banking institutions, 88% of which were under $10 billion in assets. With little variation across charter type or primary federal supervisor, 85% of the respondents reported that either use of the CAT was not voluntary or they were uncertain if CAT was voluntary.[3]

This survey, along with multiple individual firm references, indicates that the lack of clarity in the field and during examinations is creating a misconception about the voluntary nature of the CAT tool. A clear agency statement that other methodologies such as NIST CSF and the FSSCC Cybersecurity Profile are acceptable as input into the examination process would reinforce for examination staff, and the industry, both the voluntary nature of the CAT and the existence of

[2] The American Bankers Association is the voice of the nation's $17 trillion banking industry, which is composed of small, regional, and large banks that together employ more than 2 million people, safeguard $13 trillion in deposits, and extend more than $9 trillion in loans. www.aba.com

[3] The details and methodology of the June 2019 ABA survey of bank perceptions of CAT was part of a longer survey of IT and Cybersecurity Examinations. The survey is further detailed in ABA's response to the April 5, 2019 PRA request for comment (filed June 4, 2019).

12020 Sunrise Valley Drive
Suite 230
Reston, Virginia 20191

suitable frameworks and methodologies that could more effectively assist firms in identifying cybersecurity risks and programs.

Incorporate Implementation Cost and Review in the Calculation of Burden Estimates

The compliance and supervisory burden arising from the use of the CAT goes beyond the completion of the physical tool to include staff hours for research, documentation and training. The numerous hours required to complete responses to the CAT, while concurrently completing assessments based on other industry-based standards (e.g., NIST CSF) or for other regulatory agencies (e.g., state or market regulators) is significant. Additionally, the amount of time spent training cybersecurity professionals on the CAT is underestimated

Burden Related to Completion of the Assessment

As first mentioned in the FSSCC's 2015 and 2016 letters, firms of all sizes continue to report that the hours to comply with the CAT are underreported in the Agencies burden estimates. To be more accurate, the Agencies' estimates should include the time required to prepare for and complete the assessment. Preparing for a CAT 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 CAT. The time required to collect evidence and review systems before the CAT assessment can begin are significant, and the hours required to review the CAT's more than 530 responses—usually by committee—is substantial.

Burden Related to the Parallel Use of the CAT and Other Methods.

Due to each Agency's use of the CAT, there is confusion as to the voluntary nature of it. As a result, firm's burden is created from the ongoing use of the CAT within a firm's security and compliance procedures. Before the introduction of the CAT in 2014, many firms adopted a NIST CSF-based approach to cybersecurity. With the introduction of the CAT in 2015, some firms transitioned away from a NIST-based approach and adopted the CAT as their only cybersecurity assessment method. However, many firms have retained use of the NIST CSF, and now prefer using NIST-based (or other globally recognized) assessment methods, and run the CAT in parallel solely for examination purposes due to seeming supervisory preference. This duplicative effort has the effect of diverting critical cybersecurity personnel away from their core role protecting a firm and its clients.

Burden Related to Training experienced cybersecurity professionals on the CAT

Unlike the NIST CSF, which is globally recognized and based on a common approach to cybersecurity, use of the CAT is confined largely to financial services within the United States. This introduction added to an already complex and fragmented cybersecurity regulatory environment, particularly for firms operating in multiple markets or geographies.

12020 Sunrise Valley Drive
Suite 230
Reston, Virginia 20191

As institutions of all sizes hire cybersecurity expertise from across critical sectors, they are intimately familiar with NIST-based assessments (or other globally recognized approaches). It is inefficient and a strain on limited cybersecurity resources for highly-trained cybersecurity staff to be retrained on CAT when other methods are available, acceptable for examination purposes, and do not require retraining.

Further Align the CAT with the NIST CSF

Aligning the CAT with the NIST CSF or a NIST-based assessment such as the FSSCC Cybersecurity Profile would further enhance the cybersecurity and interconnectedness of the sector. This alignment would have three immediate benefits:

1. Serve as an introduction to globally recognized NIST CSF concepts and aid in bridging the frequent disconnect between financial services and security professionals among staff, senior executives, and directors;
2. Identify, prioritize, and alleviate the cybersecurity risks of greatest systemic concern for those institutions that have not yet adopted NIST or similar industry approaches; and
3. Guide the financial services sector into concurrence with globally-acknowledged industry standards for cybersecurity, including fostering a common understanding of risks and dependencies across critical sectors such as telecommunications and energy.

Following years of development, annual stakeholder meetings, and revision, the NIST CSF has evolved into a leading approach to cybersecurity with an international community of users.

In conclusion, we appreciate the opportunity to respond to the PRA request for comment. We commend the Agencies' foundational work on cybersecurity risk management for the financial services sector and invite further dialogue and collaboration with the shared goal of protecting our national critical infrastructure.

Sincerely,

Craig Froelich

Chair, Financial Services Sector Coordinating Council