America's Credit Unions

Jim Nussle
President & CEO
202-508-6745
jnussle@americascreditunions.org

99 M Street SE
Suite 300
Washington, DC 20003

January 25, 2024

The Honorable Patrick McHenry
Chairman
Committee on Financial Services
U.S. House of Representatives
Washington, DC 20515

The Honorable Maxine Waters
Ranking Member
Committee on Financial Services
U.S. House of Representatives
Washington, DC 20515

RE: Opposition to H.R. 7036, the Strengthening Cybersecurity for the Financial Sector Act

Dear Chairman McHenry and Ranking Member Waters:

On behalf of America's Credit Unions, I am writing in opposition to H.R. 7036, the Strengthening Cybersecurity for the Financial Sector Act, as written in its current form. America's Credit Unions and our member credit unions believe that cybersecurity, including the security of vendors that credit unions do business with, is an important issue. However, we are opposed to granting additional authority to the National Credit Union Administration (NCUA) to examine third parties as proposed in this legislation. We believe in a strong NCUA, but we also believe that the NCUA should stay focused on where its expertise lies—regulating credit unions. Credit unions fund the NCUA budget. Implementing such new authority for the NCUA could result in the agency increasing its budget, due in part to hiring examiners with sufficient expertise, ultimately having credit unions and their members bear the cost.

There are other tools already in place for the NCUA to get access to information about credit union vendors. We believe the agency's time and resources are better focused on reducing regulatory burden by coordinating efforts among the financial regulators. The NCUA sits on the Federal Financial Institutions Examination Council (FFIEC) with the Federal Deposit Insurance Corporation (FDIC), the Office of the Comptroller of the Currency, and the Federal Reserve. The FFIEC was created to coordinate examination findings and approach in the name of consistency and to avoid duplication. This means that as a member of the FFIEC, the NCUA should be able to request the results of an examination of a core processor from the other regulators and not have to send another exam team from the NCUA into their business and duplicate an examination. This would seem to be an unnecessary burden on these small businesses. Additionally, if the NCUA did its own examination, the likelihood of finding anything the other regulators did not would seem low.

The NCUA is best positioned to act as an aggregator or amplifier of threat intelligence assembled by other private or government sources. Sharing relevant cybersecurity information with credit unions does not depend on gathering intelligence through a duplicative supervision program. An August 2023 report from the FDIC's Office of the Inspector General (OIG) states that "[a]ccording to FDIC officials, other U.S. government and private sector entities are proficient

at providing threat information to financial institutions," and further notes that "[h]istorically, the FDIC's Division of Risk Management Supervision (RMS) has shared relevant cyber threat and vulnerability information with financial institutions prepared by other sources, such as the DHS CISA, the Treasury Department, and the FBI."[1] While the FDIC does possess internally compiled threat and vulnerability information relevant to the banks it supervises, the agency's Inspector General has recommended that "the FDIC share FDIC-developed threat and vulnerability information with financial institutions or other financial sector entities."[2] Such information sharing, if extended to the NCUA, would offer a straightforward and effective pathway for enhancing the NCUA's early warning capabilities and protecting credit unions.

America's Credit Unions and our credit union members recognize the importance of mitigating vulnerabilities to the financial system. However, there are more efficient ways to proceed. Instead of granting the NCUA vendor examination authority, Congress should encourage the agency to use the FFIEC and gain access to the information on exam findings on companies that have already been examined by other regulators. If that option is not available for the NCUA due to the decisions of the other FFIEC regulators, Congress should consider compelling the other regulators to share such information with the NCUA. This would be a more preferable route than raising costs on credit unions and their 140 million members for the creation of a duplicative NCUA program with uncertain scope. Supervisory reports for core providers will likely have significant cross-applicability; according to the NCUA, approximately five core processor vendors control approximately 85 percent of credit union data.[3]

Furthermore, it is uncertain whether simply replicating the existing supervisory authorities of other federal banking regulators will reduce exploitation of third-party vulnerabilities. Recent trends suggest that a significant share of vulnerabilities lie dormant (i.e., zero-day vulnerabilities) until they are exploited for the first time.[4] Given the limited time and expertise available to probe the inner workings of proprietary vendor systems, a core component of service provider oversight is the sufficiency of risk and security controls documented in agreements between third parties and regulated institutions.[5] The NCUA has codified these principles in its regulations.[6] While federal financial regulators emphasize adoption of controls and appropriate governance over service providers, the role of detecting cybersecurity risks that exist outside of regulated institutions is more appropriately carried out by federal agencies with a cybersecurity

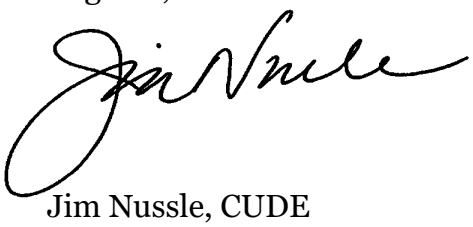
---

[1] Federal Deposit Insurance Corporation, Office of the Inspector General, Sharing of Threat and Vulnerability Information with Financial Institutions, 7-8 (August 2023), *available at* https://www.fdicoig.gov/sites/default/files/reports/2023-08/EVAL-23-002%20REDACTED%20FINAL_0.pdf.
[2] *Id.*
[3] NCUA OIG, Audit of the NCUA's Examination and Oversight Authority Over Credit Union Service Organizations at 3.
[4] *See* Mandiant, Analysis of Time-to-Exploit Trends: 2021-2022 (September 28, 2023), *available at* https://www.mandiant.com/resources/blog/time-to-exploit-trends-2021-2022 (Mandiant Intelligence analyzed 246 vulnerabilities that were exploited between 2021 and 2022. Sixty-two percent (153) of the vulnerabilities were first exploited as zero-day vulnerabilities.).
[5] *See* FFIEC, Information and Technology Handbook, 7 (2016).
[6] *See* NCUA, Appendix A to 12 CFR Part 748.

or law enforcement mandate. The NCUA can benefit from this distributed expertise by focusing its attention on improving information sharing with Treasury and other FFIEC agencies.

Use of existing reports for other technology service providers would also address the NCUA's concerns without creating additional costs to credit unions or increasing regulatory burdens on credit unions and small businesses. As such, we urge Congress to oppose granting the NCUA this new authority and urge you to oppose the Strengthening Cybersecurity for the Financial Sector Act in its current form.

Regards,



Jim Nussle, CUDE
President & CEO

cc: Members of the Committee on Financial Services