DCUC
DEFENSE CREDIT UNION COUNCIL

1627 Eye St, NW
Suite 935
Washington, DC 20006

202.734.5007
www.dcuc.org

Jason Stverak
Chief Advocacy Officer

September 3, 2026

The Honorable Bill Foster
U.S. House of Representatives
2366 Rayburn House Office Building
Washington, DC 20515

Re: Strengthening Oversight for the Financial Sector Act of 2026

Dear Congressman Foster:

On behalf of the Defense Credit Union Council, I write to express our strong opposition to **H.R.10230** **the Strengthening Oversight for the Financial Sector Act of 2026 in its current form**.

DCUC has consistently opposed granting the National Credit Union Administration broad and unrestricted authority to regulate and examine credit union third-party vendors. We have done so for many good reasons, including concerns about duplicative examinations, escalating regulatory costs, reduced vendor competition, expanded agency jurisdiction, and the absence of meaningful statutory limits on how such authority could be exercised.

Our objection is not to cybersecurity as an objective. Cybersecurity, data protection, operational resilience, and the security of the financial system are critical responsibilities. Credit unions serving servicemembers, veterans, and military families have an especially strong interest in protecting member information and maintaining secure, uninterrupted access to financial services around the world.

Our concern is that the legislation is **far more sweeping than the cybersecurity problem it is purportedly designed to address**.

Your announcement focuses on artificial intelligence, cyberattacks, technology service providers, and the risk that third-party vendors could become a weak link in the financial system. However, the operative text of the bill is not limited to artificial intelligence, cybersecurity, data security, critical infrastructure, core processors, or material technology providers. Instead, Section 2 would reactivate the full scope of Section 206A of the Federal Credit Union Act by eliminating its expiration provision. The underlying authority applies broadly to services performed by contract and would subject those activities to NCUA regulation and examination to the same extent as if they were performed by a credit union itself.

The legislation does not establish a meaningful materiality threshold. It does not differentiate between a core processor with access to sensitive member data and a routine, low-risk service provider. It does not limit examinations to vendors that perform essential technology functions, present a documented systemic risk, or are otherwise beyond the reach of an existing regulator. It also does not expressly prevent NCUA from expanding its examinations into matters unrelated to cybersecurity.

That mismatch between the stated objective and the statutory language is the central problem with the bill. **If the problem Congress seeks to address is cybersecurity, then any authority granted by Congress should be limited to cybersecurity.** A legitimate concern about cyber threats should not become the basis for open-ended federal jurisdiction over virtually every company that provides a service to a credit union.

It is also unclear how the broad authority provided by this legislation would have prevented previous cyber breaches or would prevent future ones. Regulatory authority is not, by itself, a cybersecurity control. Federal agencies possess substantial regulatory, supervisory, enforcement, and technical authority, yet federal systems continue to experience significant cybersecurity incidents. The Government Accountability Office reports that federal agencies disclosed 32,211 information-security incidents in fiscal year 2023 and that, as of February 2026, more than 730 GAO cybersecurity recommendations remained not fully implemented.

This is not an argument against effective oversight. It demonstrates why Congress should require a clear explanation of the specific regulatory gap being addressed, the vendors and activities that create that gap, and how the proposed authority would prevent or materially mitigate a cyber incident. More authority does not necessarily produce more security. The authority must be connected to specific risks, controls, expertise, accountability, and measurable outcomes.

Credit unions also do not operate in a vendor-management vacuum. NCUA already holds credit unions accountable for the third-party relationships they establish. Credit unions are expected to conduct risk assessments and due diligence, evaluate a provider's financial condition and internal controls, negotiate appropriate contractual protections, monitor vendor performance, protect member information, and maintain controls proportionate to the risks presented by the relationship. NCUA examiners already evaluate whether credit unions are meeting those responsibilities.

NCUA's current artificial-intelligence guidance similarly states that a credit union using an AI vendor must understand how the product functions, the risks introduced by the technology, how it fits within the credit union's business model, and the adequacy of the vendor's safeguards, controls, and reliability. The credit union's board and management remain responsible for appropriate oversight and safe and sound operations.

Congress should examine whether these existing requirements are being implemented effectively before creating an expansive new regulatory structure. It should also determine whether relevant information is already available through another federal or state regulator. NCUA is a member of the Federal Financial Institutions Examination Council alongside the Federal Reserve, Federal Deposit Insurance Corporation, and Office of the Comptroller of the Currency. Before authorizing overlapping examinations, Congress should strengthen the mechanisms through which those regulators share findings about service providers that have already been examined.

DCUC previously urged Congress to pursue that approach. In 2022, DCUC opposed granting NCUA broad third-party examination authority through the National Defense Authorization Act and recommended that Congress instead facilitate access to examination information already held by other financial regulators. We warned that duplicative examinations would impose unnecessary costs on credit unions and their members while being unlikely to uncover issues that existing joint examinations had not already identified.

We remain concerned that unrestricted vendor authority could require NCUA to establish a substantial new examination program and hire personnel with specialized expertise in cloud computing, cybersecurity, artificial intelligence, payment systems, data architecture, and other rapidly evolving technologies. Because credit unions fund NCUA's operations, the costs of that expansion would ultimately be borne by credit unions and their member-owners.

Smaller credit unions and smaller technology providers could be disproportionately affected. Additional examinations, inconsistent regulatory demands, and compliance expenses could discourage emerging providers from serving the credit union market. That could reduce competition, slow responsible innovation, increase contracting costs, and further concentrate essential credit union services among a small number of dominant providers.

For defense credit unions, this is an operational concern as well as a regulatory one. Defense credit unions depend on secure relationships with core processors, payment networks, cloud-service providers, telecommunications companies, fraud-prevention firms, and other specialized partners to serve members stationed throughout the United States and overseas. Any legislative proposal must account for the need to maintain continuous service across military installations, deployments, permanent changes of station, and multiple time zones.

Nevertheless, DCUC is prepared to participate constructively in a discussion about whether a **narrowly tailored grant of authority** could address a demonstrated cybersecurity gap. Any consideration of such authority, however, must begin with meaningful consultation with the credit unions that would finance, implement, and be affected by it.

Congress should not legislate first and consult later.

Before moving forward, Congress and NCUA should engage directly with credit unions of different sizes and charter types, credit union service organizations, state credit union supervisors, cybersecurity professionals, core processors, technology vendors, and other affected stakeholders. That consultation should identify the precise risks that cannot be addressed through existing credit union examinations, contractual rights, independent audits, interagency coordination, or the examination authority of other regulators.

A limited cybersecurity framework developed through consultation would be fundamentally different from the sweeping authority contemplated by the current bill. It would focus NCUA's resources on providers that present genuine and material cyber risks rather than giving the agency potential jurisdiction over the full universe of credit union service relationships.

Accordingly, DCUC respectfully urges you not to advance the **Strengthening Oversight for the Financial Sector Act of 2026 in its current form**. We encourage you instead to begin a structured dialogue with credit unions and other affected stakeholders about whether a narrower, risk-based, cybersecurity-specific proposal is necessary and how it could be designed without creating duplicative, costly, and open-ended regulatory authority.

DCUC would welcome the opportunity to meet with you and your staff before any committee consideration of the legislation. We would be pleased to include executives and cybersecurity professionals from our member credit unions who can provide an operational perspective on third-party risk, vendor contracting, incident response, information sharing, and the potential consequences of the bill's current language.

We share your goal of protecting consumers and strengthening the resilience of the financial system. We believe that goal will be best achieved through targeted authority, meaningful consultation, interagency coordination, and clearly defined cybersecurity outcomes—not through an unrestricted expansion of regulatory jurisdiction.

Thank you for your consideration. We look forward to discussing this important issue with you and your staff.

Sincerely,

Jason Stverak
Chief Advocacy Officer
DCUC
Serving ALL Who Serve