America's Credit Unions

July 3, 2024

Todd Klessman
CIRCIA Rulemaking Team Lead
Cybersecurity and Infrastructure Security Agency
20th Street and Constitution Avenue, NW
Washington, DC 20551

RE: Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) Reporting Requirements; Docket No. CISA-2022-0010

Dear Mr. Klessman:

On behalf of America's Credit Unions, we are writing in response to the notice of proposed rulemaking (NPRM) issued by the Cybersecurity and Infrastructure Security Agency (CISA) regarding implementation of the Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) reporting requirements. America's Credit Unions is the voice of consumers' best option for financial services: credit unions. We advocate for policies that allow the industry to effectively meet the needs of their over 140 million members nationwide.

America's Credit Unions supports effective and appropriately tailored cybersecurity standards to protect Americans from the loss, abuse or theft of personal data. As highly regulated financial institutions, credit unions have long been subject to regular supervision and examination covering the adequacy of security controls and response plans for incidents involving unauthorized access to credit union member information.

The National Credit Union Administration (NCUA) implements the technical safeguards requirements of the Gramm-Leach Bliley Act (GBLA) and requires all federally insured credit unions to report "substantial" cyber incidents within 72 hours after a credit union reasonably believes that it has experienced such an incident. Given the close similarity that exists between the NCUA's cyber incident reporting standard and CISA's proposed rule, we ask that an exception be granted to allow credit unions to report incidents directly to the NCUA under the "substantially similar reporting" exception provided in 6 U.S.C. § 681b(a)(5)(B) of the CIRCIA.

General Comments

The CIRCIA requires CISA to implement by 2025 a cyber incident reporting framework for critical infrastructure owners (covered entities). The statutory parameters for this framework require covered entities to report "substantial" cyberattacks to CISA within 72 hours after forming a "reasonable belief" that a covered incident has occurred, and supplemental reports as new information becomes available. In addition, covered entities must report any ransomware payments to CISA within 24 hours of payment.

In September 2023, the NCUA adopted a new cyber incent notification standard under Part 748 of its regulations in response to CIRCIA's enactment and in anticipation of a future CISA rulemaking.[1] Under the NCUA's rule, a credit union that experiences a reportable cyber incident must report the incident to the NCUA as soon as possible and no later than 72 hours after the credit union reasonably believes that it has experienced such an incident. In general, the NCUA's rule is closely aligned with the CIRCIA's standard for what qualifies as a "substantial" and therefore reportable. However, the NCUA's rules do not adopt a separate ransom payment reporting requirement, which is a distinct component of the CIRCIA.

The addition of a specific ransom payment reporting component to NCUA's regulations could alleviate concern to the extent that it is regarded as a barrier to streamlined reporting. America's Credit Unions would urge the NCUA to make conforming amendments to its regulations well before 2025 to ensure that credit unions can avail themselves of the CIRCIA's substantially similar reporting exception. Furthermore, credit unions are currently subject to FinCEN rules that require the filing of a Suspicious Activity Report (SAR) in the event of a suspected ransom payment, and it is likely that CISA could obtain relevant ransom payment information directly from Treasury.[2]

Duplicate reporting to both the NCUA and CISA would impose significant administrative burdens on credit unions, diverting valuable resources from the immediate task of mitigating cyber threats. When a cyber incident occurs, the primary focus of credit union IT and cybersecurity teams should be on containment, eradication, and recovery efforts. The added burden of preparing and submitting multiple reports to different agencies detracts from these critical activities and could jeopardize the overall efficacy of incident response efforts. The cost and time burden of reporting to separate federal entities may be even greater for credit unions who must also notify their state regulators of cybersecurity incidents.[3]

Definition of Covered Entity

The proposed rule designates all federally insured credit unions, regardless of size, as covered entities subject to all reporting requirements. The NCUA's cyber incident notification standard in 12 CFR Part 748 adopts a similar approach and applies to all federally insured credit unions regardless of size. Such an approach reflects an intent to ensure that supervised credit unions provide timely notification in the event of a substantial cyber incident and to ensure the NCUA receives early warning of security vulnerabilities, third party compromise, or other forms of disruption. With respect to credit unions that are not federally insured, CISA should clarify

[1] *See* NCUA, Cyber Incident Notification Requirements for Federally Insured Credit Unions, 88 Fed. Reg. 12811 (March 1, 2023).
[2] *See* FinCEN, Advisory on Ransomware and the Use of the Financial System to Facilitate Ransom Payments FIN-2021-A004 (November 8, 2021).
[3] *See* GAO, Cybersecurity - Efforts Initiated to Harmonize Regulations, but Significant Work Remains, GAO-24-107602, 7 (June 5, 2024), available at https://www.gao.gov/assets/gao-24-107602.pdf.

whether these institutions are covered entities and treated as owners and operators of "financial services sector infrastructure."

To the extent credit union reports filed with the NCUA qualify for the substantially similar reporting exception, covered entity status should not present a challenge. However, if CISA does not adopt such an exception, we recommend consideration of a more tailored definition which takes into consideration the size of a credit union, similar to the way the proposed rule exempts certain small businesses concerns based on Small Business Administration (SBA) size standards.

While CISA's correctly observes that "an entity's size does not necessarily reflect its criticality," it is worth noting that most credit unions are very small, with a median asset size of approximately $57 million. For the sake of comparison, current SBA size standards based on the North American Industry Classification System (NAICS) identify a credit union as a small business concern if it has less than $850 million in total assets. The smallest credit unions today may have less than a dozen employees but would—in any event—have a duty to report cyber incidents to the NCUA and would inevitably have supervisory contact in the event of a reportable cyber incident occurring.

Under the CIRCIA, CISA may tailor the scope and applicability of its proposal by considering "the consequences that disruption to or compromise of such an entity could cause to national security, economic security, or public health and safety."[4] A small credit union that experiences a temporary system outage caused by user error, for example, would be an unlikely source of significant disruption to the nation's financial sector critical infrastructure.

Considering the close supervisory oversight already applied to small credit unions and the NCUA's existing reporting framework, CISA should consider adopting a small business exclusion for credit unions if it does not adopt an exception for substantially similar reporting to the NCUA. The exclusion should be based on an SBA size standard determination. Tailoring the definition of covered entity to exclude small credit unions would not impede CISA's ability to access reports filed by these institutions with the NCUA, nor would it correspond with disproportionate risk to the financial sector given that the smallest credit unions account for only a small fraction of total financial sector assets.

Substantially Similar Reporting

CISA interprets the statutory language in 6 U.S.C. § 681b(a)(5)(B) of the CIRCIA to require five criteria for the substantially similar reporting exception to apply. In practice, this exception should allow credit unions to file a single report with the NCUA to satisfy all CISA requirements.

In general, credit union covered cyber incident reports under 12 CFR § 748.1(c) are defined using the same statutory criteria and terms (derived from the CIRCIA) that CISA has relied upon in its proposal. However, as discussed below, the NCUA has not yet adopted a separate ransom *payment* reporting requirement—although it has expressed an intention to align with CISA

[4] 6 U.S.C. § 681(c)(1).

regulations in the future.[5] Although the NCUA's current notification standard does not include a distinct ransom payment reporting component, close interagency coordination can easily bridge the gap in terms of achieving substantially similar reporting. For covered cyber incidents involving ransomware, the incidents themselves are fully reportable to the NCUA today.

CISA's first condition for invoking the substantially similar reporting exception is that a report must be required to contain substantially similar information to that required to be included in the applicable CIRCIA report. With respect to a covered cyber incident report, the NCUA's rule adopts relevant definitions which closely match the terminology used in CISA's proposal. NCUA regulations provide that a reportable cyber incident is any substantial cyber incident that leads to one or more of the following:

> "(A) A substantial loss of confidentiality, integrity, or availability of a network or member information system as defined in appendix A, section I.B.2. e., of this part that results from the unauthorized access to or exposure of sensitive data, disrupts vital member services as defined in § 749.1 of this chapter, or has a serious impact on the safety and resiliency of operational systems and processes.
>
> (B) A disruption of business operations, vital member services, or a member information system resulting from a cyberattack or exploitation of vulnerabilities.
>
> (C) A disruption of business operations or unauthorized access to sensitive data facilitated through, or caused by, a compromise of a credit union service organization, cloud service provider, or other third-party data hosting provider or by a supply chain compromise."[6]

Each prong of the NCUA definition aligns with both the CIRCIA and the proposed rule's definition of a substantial cyber incident.[7]

With respect to the actual contents of filed reports, NCUA's rule is also similar. While CISA's proposal does offer more descriptive clarity around the types of information that might be shared in a report—specific categories of information need only be provided to the extent they are *available and applicable* to the type of cyber incident being reported.[8] This approach is substantially similar to the reporting guidance published by the NCUA.[9] Credit unions are specifically advised to include the following information, among other elements, in their cyber incident reports:

- Credit union name;
- Credit union charter number;
- Name and title of individual reporting the incident;

---

[5] *See* 88 Fed. Reg. 12811, 12812 ("It is the intention of the Board for the NCUA to coordinate with CISA on any future credit union cyber incident reporting to avoid duplicate reporting to both the NCUA and CISA.").
[6] 12 CFR 748.1(c).
[7] See 88 Fed. Reg. 12811, proposed §226.1 (definition of substantial cyber incident).
[8] *See* 88 Fed. Reg. 12811, proposed § 226.7.
[9] *See* NCUA, Letter to Credit Unions 23-CU-07, Cyber Incident Notification Requirements (advising credit unions to "provide as much [...] information as is known at the time of reporting.").

- Telephone number and email address;
- When the credit union reasonably believed a reportable cyber incident took place;
- A basic description of the reportable cyber incident, including what functions were, or are reasonably believed to have been affected or if sensitive information was compromised.
- Indicators of compromise;
- Network information or traffic regarding the attack;
- The attack vector;
- Information on any exfiltrated data; and
- Any forensic or other reports about the reportable cyber incident.[10]

These elements encapsulate the same core elements of information CISA is seeking in its proposal. More importantly, these elements generally reflect what the NCUA considers to be reasonably acquirable pieces of forensic data that are actionable for the purpose of preventing further harm to credit union members and other institutions. Decades of experience examining credit union cybersecurity practices has informed the NCUA's assessment of what can realistically be acquired in a 72-hour timeframe, and CISA should generally defer to this limit for the purposes of recognizing a substantially similar reporting exception.

A second condition relevant to the exception requires that a report filed at another federal agency (i.e., the NCUA) be provided in a timeframe substantially similar to the timeframe to which the covered entity would otherwise have been obligated to provide the report to CISA pursuant to CIRCIA. As described above, the NCUA's current 72-hour standard in Part 748 is identical with respect to covered cyber incident reports. However, the NCUA may need to amend its regulations to obtain ransom payment reports within 24 hours of a credit union making a payment to match CISA's proposal. America's Credit Unions will encourage NCUA to coordinate with CISA to ensure that substantial similarity exists before 2025. Given the NCUA's desire to prevent duplicative reporting and reduce administrative burdens for credit unions, we are optimistic that close coordination with CISA can facilitate interagency agreement on the use of the substantially similar reporting exception before any final compliance date.

With respect to supplemental reporting, the NCUA achieves equivalent follow-up with credit unions experiencing a covered cyber incident through its supervisory process, which may involve written information requests or other communications with credit union officials. In this regard, the supervisory process achieves the same practical results as supplemental reports under CISA's proposal, and may even offer superior intelligence to the extent that the NCUA faces no limits on how often it can contact regulated institutions regarding the progression of cyber incidents. Accordingly, we urge CISA to recognize the NCUA's use of follow-up supervisory processes as substantially similar to supplemental reporting.

For companies lacking a functional regulator, separate supplemental reports may serve as an important source of cyber intelligence; however, credit unions and other depository institutions are scrutinized to a much closer degree on an ongoing basis. CISA should recognize this

[10] *Id.*

fundamental difference and the rigor of existing examination procedures for credit unions when considering the applicability of an exception as it pertains to supplemental reports.

A third condition for the exception requires CISA and a federal agency to have an information sharing agreement in place that satisfies the requirements of 6 U.S.C. § 681g(a) (i.e., a CIRCIA Agreement). We strongly support the formation of such an agreement before the effective date of any final rule. In the event such an agreement cannot be practically formed until the NCUA has made adjustments to its own cyber incident reporting standard under Part 748 (i.e., adopting a ransom payment reporting component), CISA should seek to convene the NCUA and credit union industry stakeholders to facilitate reasonable adjustments to Part 748 for the purpose of reducing reporting overlap and duplication. An industry roundtable or working group could be used to fast-track development of ransom payment related amendments to 12 CFR Part 748 while further informing CISA about how existing credit union regulation is substantially similar to what is sought under the proposed rule.

The exception's final two criteria would require CISA and the NCUA to have an enforceable mechanism in place to ensure that reports are actually filed with CISA within the required timeframe. As noted above, the NCUA has already expressed a desire to closely coordinate with CISA to avoid future overlap and duplication. We encourage CISA to match this spirit of cooperation by establishing an enforceable CIRCIA Agreement well before the effective date of a final rule.

In the unlikely event that potential legal obstacles to information sharing impede the formation of such an agreement with respect to all types of CIRCIA Reports, CISA should publicly disclose what those impediments are and their legal basis. However, the broad federal information sharing authority granted under 6 U.S.C. § 681g(a) should generally accommodate all information sharing needs between the NCUA and CISA for the purpose of executing a CIRCIA Agreement.[11]

With respect to credit unions that are not federally insured, and to the extent these institutions are deemed covered entities, CISA should allow the substantially similar reporting exception to operate if relevant state financial institution regulators have executed an agreement with CISA to share reports.

Conclusion

America's Credit Unions supports the objective of timely and accurate cyber incident reporting; however, we urge CISA to recognize the reporting standards already applicable to credit unions and coordinate with the NCUA to ensure that the substantially similar reporting exception is something the industry can use to reduce administrative burden. A streamlined reporting process that avoids redundancy will allow credit unions to focus their resources on mitigation and response activities rather than on duplicative compliance tasks. We urge you to consider our

[11] *See* 6 U.S.C. § 681g(a) (requiring federal agency transmission of CIRCIA reports to CISA "Notwithstanding any other provision of law or regulation").

recommendations to ensure that CISA's future regulatory framework enhances cybersecurity without imposing unnecessary burdens on credit unions.

Thank you for considering this request. If you have any questions, please do not hesitate to contact me at 703-842-2266 or amorris@americascreditunions.org.

Sincerely,

Andrew Morris
Director, Innovation and Technology