NAFCU
3138 10th Street North
Arlington, VA 22201-2149
703.522.4770 | 800.336.4644
f: 703.524.1082
nafcu@nafcu.org | nafcu.org
National Association of Federally-Insured Credit Unions

November 14, 2022

Todd Klessman
CIRCIA Rulemaking Team Lead
Cybersecurity and Infrastructure Security Agency
Department of Homeland Security
245 Murray Lane
Washington, D.C. 20528-0380

Re: Request for Information on the Cyber Incident Reporting for Critical Infrastructure Act of 2022; Docket ID: CISA-2022-0010

Dear Mr. Klessman,

On behalf of the National Association of Federally-Insured Credit Unions (NAFCU), I am writing in response to the Cybersecurity and Infrastructure Security Agency's (CISA) request for information (RFI) regarding implementation of the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA). NAFCU advocates for all federally-insured not-for-profit credit unions that, in turn, serve 133 million consumers with personal and small business financial service products.

Credit unions are subject to rigorous cybersecurity and incident response standards promulgated by the National Credit Union Administration, which administers the technical safeguard requirements established under the Gramm-Leach Blilely Act (GLBA). Credit unions also undergo regular cybersecurity exams which incorporate guidance published by the Federal Financial Institutions Examination Council (FFIEC).[1] These exams place strong emphasis on the need for credit unions to develop and maintain risk-based information security programs, protect vital records, oversee service providers, and guard against unauthorized access to member information.[2]

As CISA considers whether cyber incident response standards for credit unions are substantially similar to the requirements set forth in the CIRCIA, it should recognize that the NCUA is already planning to align its rules closely with a 72-hour reporting period, and existing incident response rules for unauthorized access to member information already require credit unions to notify the NCUA as soon as possible.[3] Accordingly, CISA should ensure that a future rule to implement the CIRCIA does not create duplicate or conflicting standards or definitions for credit unions.

[1] *See* FFIEC, IT Examination Handbook Infobase, https://ithandbook.ffiec.gov/.
[2] *See* 12 CFR § 748(b); *see also* 12 CFR Part 748, Appendix A.
[3] *See* NCUA, "Cyber Incident Notification Requirements for Federally Insured Credit Unions," 87 Fed. Reg. 45029 (July 27, 2022); *see also* 12 CFR Part 748, Appendix B.

General Comments

Cybersecurity is a top priority for both the NCUA and the credit union industry itself. Surveys of NAFCU members reveal that credit union cybersecurity budgets have more than doubled over the past five years, and nearly all NAFCU members expect those same budgets to grow in the future. NAFCU's members also anticipate that cybersecurity risk will remain a top risk management concern in the coming years.

Alongside prudent investments in IT security, the resilience and safety of the credit union system also benefits from harmonization of cybersecurity standards, which ensures that credit unions can focus their attention on critical security functions without the added burden of reconciling potentially conflicting or duplicative incident reporting standards. To achieve such harmonization, future implementation of the CIRCIA should recognize that the NCUA's recently proposed cyber incident reporting standard already matches the 72-hour requirement for reporting substantial cyber incidents.[4] NAFCU's comments to the NCUA in response to its cyber incident proposal emphasized the need for harmonization with future CISA standards so that credit unions could take advantage of the "substantially similar" reporting exception included in the CIRCIA, as this would allow the industry to follow a single set of rules administered by the NCUA and report to a single agency.[5]

To establish a streamlined reporting framework for credit unions that reduces administrative burden while preserving the NCUA's role as the industry's prudential regulator, a future rulemaking by CISA should not create additional or parallel reporting standards for credit unions. Instead, CISA should leverage government communication channels within the financial sector to access substantially similar cyber incident reports already on file at respective federal banking agencies, including the NCUA.

Definition of Covered Entity

Under section 2240(5) of the Homeland Security Act of 2002 (as amended), a covered entity is defined as "an entity in a critical infrastructure sector, as defined in Presidential Policy Directive 21, that satisfies the definition established by the Director in the final rule." The RFI requests input on how CISA should define a "covered entity," recognizing that the CIRCIA accommodates some degree of regulatory tailoring based on factors listed in section 2242(c)(1). Those factors require CISA to consider, among other things, "the consequences that disruption to or compromise of such an entity could cause to national security, economic security, or public health and safety."[6]

[4] *See* 87 Fed. Reg. 45029.
[5] *See* NAFCU Letter to NCUA re: Cyber Incident Notification Requirements for Federally Insured Credit Unions; (RIN 3133-AF47) (September 26, 2022), *available at* https://www.nafcu.org/comment-letter-ncua-cyber-incident-notification-requirements-federally-insured-credit-unions-File
[6] 6 U.S.C. § 681(c)(1).

A credit union that experiences a temporary system outage caused by user error, for example, would seem an unlikely source of disruption to the nation's financial sector critical infrastructure. Furthermore, credit unions control only a small share of banking assets.[7] The median credit union holds just over $50 million in assets and operates with nine full-time employees. The median bank has over $320 million in assets and 50 employees. Each of the two largest banks manages more assets than the entire credit union industry combined.

To regard a small credit union with only a few employees as an operator of critical infrastructure would unreasonably stretch the bounds of the current definition of a covered entity.[8] Presidential Policy Directive 21 (PPD 21) defines critical infrastructure consistent with the meaning given in the USA PATRIOT Act of 2001 (42 U.S.C. 5195c(e)); namely, systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.

While it might be argued that the total and simultaneous incapacity of the credit union industry could result in a debilitating impact on national economic security, no such event has ever taken place, in part because of the rigorous cybersecurity supervision the credit union industry already receives. The credit union industry is largely comprised of smaller credit unions where the prospect of temporary system outages would not equate to something as severe as a "debilitating impact" and certainly not achieve harm on a national scale. Accordingly, CISA should recognize that most credit unions will not be critical infrastructure operators within the scope of the CIRCIA and thus not covered entities. Such an acknowledgment would not degrade CISA's ability to learn of cyber incidents that occur at smaller credit unions, since all federally-insured credit unions (regardless of their covered entity status) are subject to the NCUA's incident reporting standards, and reports filed with the NCUA would be accessible to CISA under the terms of the CIRCIA.[9]

Meaning of "Substantial Cyber Incident" and "Covered Cyber Incident"

The CIRCIA defines a covered cyber incident as a "substantial cyber incident experienced by a covered entity."[10] An interpretation of these terms that emphasizes both the "materiality" of an incident and an entity's certainty of substantial harm would help establish a clearer reporting standard that aligns with risk-focused cybersecurity principles.

By referencing an incident's material impact, CISA would better account for the scale and sophistication of individual entities subject to a future rule or entities already subject to

[7] As of March 31, 2022, credit unions maintained 10 percent of household deposits.
[8] *See* 6 U.S.C. § 681(5).
[9] *See* 6 U.S.C. § 681g ("[A]ny Federal agency, including any independent establishment (as defined in section 104 of title 5, United States Code), that receives a report from an entity of a cyber incident, including a ransomware attack, shall provide the report to the Agency as soon as possible.")
[10] 6 U.S.C. § 681(4).

substantially similar reporting standards (as is the case with credit unions and the NCUA). For example, a cyber incident, such as a service outage, when measured in terms of materiality might look different for a small credit union that serves several thousand members versus a credit union that serves several million. Likewise, by referencing an entity's reasonable belief in the certainty of material harm occurring, the trigger for a reportable cyber incident will be clearer and less subjective. Such an interpretation would also align with prevailing industry standards in the realm of enterprise risk management.

CISA might also clarify component terminology used to describe events that would trigger reporting. The elements of a substantial cyber incident incorporate the terms "disruption," "cyber incident," and "ransomware attack."[11] These terms can encompass overlapping concepts which might create confusion when attempting to discern how each delimits reporting under specific factual circumstances. Some causes of disruption—which may be natural, non-malicious, immaterial, or not directly targeting a credit union or its vendors—may not be clearly understood as a reportable event.

For example, it may not be clear whether a power outage that causes a disruption in credit union member service is a reportable event if the root cause is a ransomware attack targeting a utility company. While the definition of a substantial cyber incident includes a reference to supply chain compromise at third party data hosting providers, the ultimate cause of disruption may be attenuated beyond those listed entities.

Whether more attenuated forms of disruption are reportable may present an especially difficult question given the broad statutory definition for "supply chain compromise." Under the CIRCIA the term is defined as "an incident within the supply chain of an information system that an adversary can leverage or does leverage to jeopardize the confidentiality, integrity, or availability of the information system or the information the system processes, stores, or transmits, and can occur at any point during the life cycle."[12] NAFCU recommends CISA recognize reasonable limits on the breadth of a credit union's information system supply chain to reduce the administrative burden of investigating root causes of disruption that are far removed from the credit union's immediate IT infrastructure. Appropriate limits would reflect the likelihood that highly attenuated supply chain attacks will be reported to CISA separately by covered entities nearer to the original source of compromise.

Disruption caused by supply chain compromise could also be the result of an ongoing, but relatively low severity ransomware attack affecting other sectors of the economy. Yet the resolution of such an attack could be beyond the credit union's control and its length indeterminant, which would complicate initial assessments when reporting is required. Furthermore, the term ransomware attack is defined in a way that does not consider the actual success or failure of the attack, although it does consider the credibility of the ransom threat

[11] *See* 6 U.S.C. § 681b(c).
[12] 6 U.S.C. § 681(17).

itself.[13] Collectively, these ambiguities may result in a reporting framework where credit unions are not sure when to report certain incidents and how they should be described. As recommended previously, an emphasis on a covered entity's certainty of harm and the materiality of the cyber event (whether an incident, disruption, or compromise) in terms of its impact would establish clearer parameters for reporting.

Additionally, CISA should consider limiting formal reporting for non-malicious system outages—events that are neither cyberattacks nor compromises but could potentially be reportable. In these circumstances, an exclusion from formal reporting would help alleviate administrative burden when a credit union undergoes a technology transition or system upgrade that may correspond with increased likelihood of prolonged service outage. Given that the CIRCIA's underlying concern lies with cyberattacks and other malicious incidents, reporting exceptions for temporary outages that do not have these characteristics would constitute reasonable regulatory tailoring for credit unions already subject to NCUA supervision and incident reporting rules.[14]

Meaning of "Substantially Similar Information"

Under the CIRCIA, an exception to filing a cyber incident or ransomware report directly with CISA is available when CISA has an existing agreement in place with a covered entity's federal regulator and the covered entity is required by law, regulation, or contract to report substantially similar information to its federal regulator within a substantially similar timeframe.[15] The CIRCIA also establishes a Cyber Incident Reporting Council charged with reviewing "existing regulatory requirements, including the information required in such reports, to report incidents and ensure that any such reporting requirements and procedures avoid conflicting, duplicative, or burdensome requirements."[16]

In terms of CISA's implementation of rules governing the submission of supplemental reports, the CIRCIA provides that the agency, in a future rulemaking, shall "consider any existing regulatory reporting requirements similar in scope, purpose, and timing to the reporting requirements to which such a covered entity may also be subject, and make efforts to harmonize the timing and contents of any such reports to the maximum extent practicable."[17] Collectively, these provisions emphasize principles of cybersecurity harmonization that NAFCU has long promoted.

Credit unions currently file incident response reports with the NCUA that contain information substantially similar to what the CIRCIA demands.[18] Once the NCUA finalizes its proposed 2022

[13] *See* 6 U.SC. § 681(14).
[14] See e.g., 12 CFR 748.1(b).
[15] *See* 6 U.S.C. § 681b(a)(5)(B).
[16] 6 U.S.C. § 681g(b)(1)
[17] *See* 6 U.S.C. § 681b(c)(7)(B).
[18] See 12 CFR Part 748 B; § 748.1(b) (catastrophic act reporting); § 748.1(c) (suspicious activity reporting); Appendix B to Party 748 (describing incident reports for events involving access to sensitive member information).

Cyber Incident Notification Rule, there will be even greater alignment.[19] The 2022 Cyber Incident Notification Rule states that reports filed by federally-insured credit unions (FICUs) should include the following:

- A basic description of the reportable cyber incident, including what functions were, or are reasonably believed to have been, affected.
- The estimated date range during which the reportable cyber incident took place.
- Where applicable, a description of the exploited vulnerabilities and the techniques used to perpetrate the reportable cyber incident.
- Any identifying or contact information of the actor(s) reasonably believed to be responsible.
- The impact to the FICU's operations.

Each of these elements aligns closely with the contents described in section 2242(b)(4) and (5) of the CIRCIA.

To ensure that credit unions can fully benefit from the CIRCIA's provisions aimed at easing regulatory burden and avoiding duplication of effort, NAFCU encourages CISA to coordinate with both the NCUA and the Treasury Department to ensure that credit unions will only need to meet a single standard administered by the NCUA that satisfies all prongs of the CIRCIA's reporting regime: substantial cyber incident reporting, ransomware reporting, and supplemental reporting as applicable. NAFCU anticipates that once the NCUA finalizes its 2022 Cyber Incident Notification Rule, credit union reporting standards will be sufficiently aligned with the CIRCIA to accommodate such a framework.

Although the NCUA has not established a specific ransomware reporting requirement at this time, it is likely that material ransomware events that occur within the credit union industry will be reportable—at least initially—as substantial cyber incidents. The ransomware-specific information that would be required under section 2242(b)(5) of the CIRCIA, such as "identifying or contact information related to the actor or actors reasonably believed to be responsible for the ransomware attack" could be collected by the NCUA through existing supervisory processes and subsequently transmitted to CISA if the credit union is determined to be a covered entity.

Mechanisms for Information Sharing and Streamlining of Reporting

In general, CISA should accommodate a framework for credit unions where all required reports flow through the NCUA rather than insist on parallel mechanisms for direct transmission to CISA. In comments to the NCUA regarding the agency's 2022 Cyber Incident Notification Rule, NAFCU emphasized the need to accommodate a range of different notification channels to facilitate fluid

[19] 87 Fed. Reg. 45029 at 45032.

communication with supervisory contacts, as initial assessments of cyber incidents could change relatively quickly.[20]

To preserve this flexibility and close engagement between credit unions and their primary regulator, CISA should recognize that cyber incident reports submitted to the NCUA meet the definition of substantially similar information, and that the NCUA's existing and proposed mechanisms for collecting such information from credit unions are sufficiently aligned with the reporting timeframes included in the CIRCIA.[21] With respect to CISA's establishment of an agreement with the NCUA to coordinate sharing of incident reports, NAFCU recommends that the parameters governing such information sharing do not necessitate excessive follow-up with credit unions once an initial report has been filed with the NCUA.

To minimize the burden of filing supplemental reports, CISA should first engage with the NCUA to determine whether supervisory staff have already collected information that would be substantially similar to what is required under section 2242(a)(3) of the CIRCIA, since credit unions may also file—in the aftermath of a covered cyber incident—a catastrophic act report which may contain relevant information. A catastrophic act can include events that would also be covered cyber incidents if they result in disruption to vital member services (e.g., core services) projected to last more than two consecutive business days.[22]

As required under 12 CFR 748.1 of the NCUA's regulations, "within a reasonable time after a catastrophic act occurs, the credit union shall ensure that a record of the incident is prepared and filed at its main office" and "include information sufficient to indicate the office where the catastrophic act occurred; when it took place; the amount of the loss, if any; whether any operational or mechanical deficiency(ies) might have contributed to the catastrophic act; and what has been done or is planned to be done to correct the deficiency(ies)."[23] Given that NCUA examiners will have access to these records, CISA should not need to impose additional supplemental reporting requirements related to cyber incidents or ransomware payments—most of which would meet the definition of a catastrophic act—and instead could request copies of notice or records through the NCUA.

Confidentiality of Reports

[20] *See* NAFCU Letter to NCUA re: Cyber Incident Notification Requirements for Federally Insured Credit Unions; (RIN 3133-AF47) (September 26, 2022), *available at* https://www.nafcu.org/comment-letter-ncua-cyber-incident-notification-requirements-federally-insured-credit-unions-File.
[21] 87 Fed. Reg. 45029 at 45030 (requiring notification as soon as possible but no later than 72 hours after a FICU reasonably believes that a reportable cyber incident has occurred).
[22] *See* 12 CFR 748.1(b); § 749.1 (defining vital member services to include "informational account inquiries, share withdrawals and deposits, and loan payments and disbursements" – services that practically encompass the entirety of a credit unions' operations).
[23] 12 CFR 748.1(b).

NAFCU asks that CISA include a clear statement in any future rule that notices and reports transmitted either directly or indirectly to the agency which relate to cyber incidents are exempt from Freedom of Information Act (FOIA) requests. Such a statement would clearly communicate the applicability of relevant statutory FOIA exemption and give credit unions greater confidence that sensitive information about IT systems or operations will not be inadvertently disclosed to the public.[24]

Conclusion

CISA should aim to simplify cyber incident reporting as much as possible to ensure that credit unions are not burdened by excessive administrative compliance. CISA should recognize that most credit unions are not covered entities given their small size, limited share of financial sector assets, and very low probability of causing disruption on a national scale. Furthermore, CISA should not impose unrealistic forensic requirements on smaller covered entities as part of an overall reporting regime, as this would only serve to divert resources from practical cybersecurity functions.

Despite their small size, credit unions invest significantly in cybersecurity and are already subject to regular supervision by the NCUA. Implementation of the CIRCIA should reflect a risk-based approach for managing cybersecurity risk across critical infrastructure sectors, but this should not entail second-guessing or duplicating the existing supervision that credit unions already receive as highly regulated financial institutions.

For all reports mandated under the CIRCIA (covered cyber incident, ransomware payment, and supplemental), CISA should seek to collect required information from the NCUA by leveraging existing records and reports credit unions file instead of establishing parallel and duplicative reporting mechanisms directly with credit unions. The NCUA has already taken steps to align its cyber incident reporting standards closely with the CIRCIA's statutory requirements, and when proposed amendments are finalized, CISA will be able to access—through the NCUA—substantially similar information about covered cyber incidents or ransomware payments.

NAFCU and its members appreciate the opportunity to comment on CISA's request for information. Should you have any questions or require any additional information, please contact me at amorris@nafcu.org or (703) 842-2266.

Sincerely,

[24] *See* 5 U.S.C. § 552(b)(8) (2000) (describing FOIA exemption for records "contained in or related to examination, operating, or condition reports prepared by, on behalf of, or for the use of an agency responsible for the regulation or supervision of financial institutions")

Andrew Morris
Senior Counsel for Research and Policy