July 3, 2024

Mr. Todd Klessman
CIRCIA Rulemaking Team Lead
Cybersecurity and Infrastructure Security Agency
1110 N. Glebe Rd
Arlington, VA 20598

Submitted to the Federal eRulemaking Portal, www.regulations.gov

Proposed Rule: Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) Reporting Requirements
Federal Register Number: 2024-06526
Docket Number: CISA-2022-0010
RIN: 1670-AA04

Dear Mr. Klessman,

NRECA is the national trade association representing nearly 900 local electric cooperatives and other rural electric utilities. America's electric cooperatives are owned by the people that they serve and comprise a unique sector of the electric industry. From growing regions to remote farming communities, electric cooperatives power 1 in 8 Americans and serve as engines of economic development for 42 million Americans across 56 percent of the nation's landscape.

Electric cooperatives operate at cost and without a profit incentive. Each cooperative is governed by a board of directors elected from its membership. NRECA's member cooperatives include 64 generation and transmission (G&T) cooperatives and 832 distribution cooperatives. The G&Ts generate and transmit power to distribution cooperatives that provide it to the end of line cooperative consumer-members. Collectively, G&T cooperatives generate and transmit power to nearly 80% of distribution cooperatives, which in turn provide power directly to consumer-members at the end of the line. The remaining distribution cooperatives receive power directly from other generation sources within the electric utility sector. Both distribution and G&T cooperatives share an obligation to serve their consumer-members by providing affordable, reliable, and safe electric service.

NRECA is a valuable contributor to cooperatives' cybersecurity efforts by improving access to the knowledge and tools they need to protect their systems. NRECA's Cybersecurity Program is founded on the concept of mutual assistance and service. By strengthening the cyber defenses of one cooperative, we improve the collective strength of all cooperatives. The Department of Energy (DOE) recognizes the role NRECA plays in advancing cybersecurity for our members and has awarded NRECA nearly $20 million since 2022 to support cyber monitoring, mentoring, technical assistance, and improvements to response capabilities. Some of NRECA's efforts include:

- NRECA established its Cooperative Cyber Goals Program in 2023 to help cooperatives work toward achieving high priority security measures and create a benchmark to help establish basic cybersecurity fundamentals.
- In 2024, NRECA stood up Project Guardian, which will provide an array of education, training, and workforce development programs for our members and establish a network of cyber "champions" across our membership to serve as resources for cooperatives for everything from incident response support to identifying and sharing effective cyber practices.
- NRECA is building a Threat Analysis Center (TAC) to synthesize and direct relevant cybersecurity information and alerts to members, help electric cooperatives detect and respond to potential hacks in their operating systems, and alert federal agencies in real time to credible threats.

Our members leverage these resources, along with federal, state, and cooperative-led efforts, and work collaboratively in the spirit of mutual assistance and "cooperatives helping cooperatives" to drive cyber preparedness. Cooperative cybersecurity personnel are proactive, capable, and excel at making the most efficient use of limited resources. Across NRECA's membership, cooperatives support their neighbor cooperatives by providing support for incident response, facilitating self-assessments, educating staff on security imperatives, coordinating group purchasing discounts, and forming cooperative cyber mutual aid groups. Some examples of this include:

- The Vice President of Information Security at New Horizon Electric Cooperative, a G&T based in Laurens, South Carolina, teaches a cyber course for cooperative staff and visits cooperatives to build relationships for strong collaboration on cybersecurity and evaluates their technologies, processes, and procedures to guard against cyber-threats.
- Associated Electric Cooperative Inc., the Springfield, Missouri-based G&T, created "Cyber Dome" in 2021 to provide round-the-clock service, including system monitoring and support for incident response, which allows it to centralize the majority of the costs and talent.
- Rappahannock Electric Cooperative, a distribution system based in Fredericksburg, Virginia, formed an IT & cybersecurity subsidiary in 2022 after a significant investment in bolstering the cooperative's own cybersecurity posture. The subsidiary has 40 employees with eight dedicated cybersecurity professionals and three certified ethical hackers to provide assessments, strategies, data analytics and technologies.

These examples demonstrate that cooperatives of all sizes are proactively responding to cyber challenges by nurturing a culture of cybersecurity and deploying risk-management strategies that are right-sized to meet the security needs of their specific cooperative and the communities they serve. Cybersecurity is a reoccurring topic at cooperative board meetings, NRECA conferences, and within the broader cooperative community. Cooperatives also actively participate in training and exercises, including the Electricity Information Sharing and Analysis Center (E-ISAC) biannual GridEx exercise, which is the largest grid security exercise in the country. Collectively, these efforts are demonstrating that, regardless of size and resources, electric cooperatives recognize the growing cyber threat and are employing effective, industry-leading practices to ensure the security and reliability of the systems they operate.

NRECA appreciates the opportunity to provide comments on the Cybersecurity and Infrastructure Security's (CISA) April 4, 2024, Notice of Proposed Rulemaking (NPRM) to implement the Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) cyber incident reporting requirements. In addition to the comments

provided below, NRECA associates itself with comments submitted on June 28, 2024 by a diverse coalition of industry stakeholders including the communications sector, financial services sector, and electricity sector. These comments focus specifically on a shared desire for CISA to raise the threshold for incident reporting by amending the definition of a substantial cyber incident in the final rule.

Reduce the Number of Entities Subject to Reporting Requirements

CISA's proposed criteria for identifying the "covered entities" that must report incidents are overly broad and would apply to all electric utilities regardless of size, location, or resources. This includes hundreds of small distribution cooperatives that serve a relatively small number of meters and are not part of the bulk electric system. NRECA believes that requiring all electric utilities to report incidents under the NPRM exceeds Congress's intent in the CIRCIA legislation, would create significant new costs for cooperatives and the communities they serve, and could potentially increase cyber risk to cooperatives by stretching limited cyber resources to focus on compliance activities, rather than incident response. CISA should revise its criteria to be risk-based, rather than all-inclusive, to ensure that it is identifying a subset of covered entities that can provide the most relevant and actionable information, in line with Congress's intent.

Congressional Intent when Drafting CIRCIA

Congress established clear statutory guidelines in the plain text of the CIRCIA law detailing which entities should be subject to reporting requirements. Specifically, the law includes four criteria that CISA was directed to consider when identifying covered entities:

1. The consequences that disruption to or compromise of such an entity could cause to national security, economic security, or public health and safety;
2. The likelihood that such an entity may be targeted by a malicious cyber actor, including a foreign country;
3. The extent to which damage, disruption, or unauthorized access to such an entity will disrupt the reliable operation of other critical infrastructure assets; and
4. The extent to which an entity or sector is subject to existing regulatory requirements to report cybersecurity incidents, and the possibility of coordination and sharing of reports between the Office and the regulatory authority to which such entity submits such other reports[1].

Congress further clarified its intent during the House Committee on Homeland Security Subcommittee on Cybersecurity and Infrastructure Protection's May 1, 2024, hearing entitled Surveying CIRCIA: Sector Perspectives on the Notice of Proposed Rulemaking. During the hearing, Rep. Yvette Clarke, the principal sponsor of CIRCIA, noted that while "the federal government would benefit from a well-scoped incident reporting framework…we do not expect all critical infrastructure owners and operators to be subject to this reporting requirement. Rather, we expect it to apply only to a subset." These criteria outlined in the law and the statements during Congressional hearings demonstrate Congress' intent to focus on the most-critical infrastructure operators whose disruption would result in significant, national-level consequences and to avoid an overly broad application of the reporting requirements. This is also consistent with the statutory definition of "critical infrastructure," outlined in the Critical Infrastructure Protection Act of 2002 (i.e., "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or

[1] H.R.5440 - Cyber Incident Reporting for Critical Infrastructure Act of 2021, SEC. 2220A(d)2(A)

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.")[2]

CISA's Criteria in the NPRM

In its NPRM, CISA outlined which critical infrastructure operators would be subject to cyber reporting requirements in the NPRM. Specifically, CISA included two criteria in the NPRM to identify covered entities, one is size-based and the other is sector-based. Meeting either criterion would qualify a cooperative as a covered entity.

CISA's sector-based criteria specify that bulk electric and distribution system entities that are required to "file an Electric Emergency Incident and Disturbance Report OE-417 form, or any successor form, to the Department of Energy" are subject to the NPRM's reporting requirements. Because DOE requires all electric utilities, including all rural electric cooperatives, to complete OE-417 reports,[3] all electric utilities would therefore be subject to CIRCIA reporting requirements. Absent the OE-417 criteria, only a small subset of cooperatives would be subject to the CIRCIA reporting requirements because most cooperatives are not large enough to meet the other criteria CISA provided outlined in the NPRM.

By including OE-417 as a part of the sector-based criterion, CISA is adopting an all-inclusive, rather than risk-based, approach to identifying covered entities that ignores key guidelines Congress established in the CIRCIA law, such as size, consequence of disruption, likelihood of being targeted, potential for disruption to other critical assets, or existing regulatory requirements.

Recommendation to Reduce Number of Entities Subject to Reporting Requirements

NRECA believes that, by including all electric utilities in the mandatory reporting requirements, CISA is exceeding Congress's intent in the CIRCIA law and, therefore, we recommend that CISA remove the OE-417 language from the sector-based criteria and replace it with a risk-based approach. This would reduce financial costs for cooperatives and their communities, ensure that limited cyber staff are able to focus on response activities rather than compliance, and enable CISA to focus its resources on cyber incidents that are most likely to have national-level impacts.

Raise Reporting Thresholds to Reduce Burden

Cyber incident reporting can help government and industry identify trends and systemic risk across sectors, but it also has the potential to divert resources away from improving cybersecurity outcomes to compliance. Congress left many of the definitions to the rulemaking process to allow for industry input, including the definition of a "substantial cyber incident." NRECA believes the definition of a substantial cyber incident included in the NPRM should be revised to raise the threshold for reporting to enhance reporting efficiency and security outcomes. CISA should narrow the scope of reporting requirements to truly impactful incidents so that we can separate signal from noise and glean meaningful insights that

[2] *Critical Infrastructure Protection Act of 2001*, govinfo.gov, https://www.govinfo.gov/content/pkg/USCODE-2010-title42/pdf/USCODE-2010-title42-chap68-subchapIV-B-sec5195c.pdf (January 2023)
[3] *DOE-417 Electric Emergency Incident and Disturbance Report*, DOE.gov, https://www.oe.netl.doe.gov/docs/OE417_Form_Instructions_05312024.pdf (May 2018)

address real risks. This may help CISA prioritize resources and mitigations for those incidents meeting that higher threshold.

Challenges with "Substantial Cyber Incident" Definition

In the NPRM, CISA defines a substantial cyber incident to include events that meet one of four criteria. The criteria included in the definition leverage terms that are broad and may result in ineffective and burdensome overreporting by impacted entities. The four criteria are:

1) A substantial loss of confidentiality, integrity or availability (CIA) of a covered entity's information system or network;
2) A serious impact on the safety and resiliency of a covered entity's operational systems and processes;
3) A disruption of a covered entity's ability to engage in business or industrial operations, or deliver goods or services;
4) Unauthorized access to a covered entity's information system or network, or any nonpublic information contained therein, that is facilitated through or caused by a compromise of a cloud service provider, managed service provider, or other third-party data hosting provider; or supply chain compromise.

The first two criteria include terms that are ambiguous and not defined within the NPRM (i.e., "substantial loss," "serious impact"). As such, much of the reporting will be dependent on whether an impacted entity believes CISA would interpret an event to include a "substantial loss" of CIA or a "serious impact" to safety. Moreover, CISA's definition of "information systems" includes any and all information technology and operational technology systems that the entity manages, including those that are not related to the delivery of the essential services that qualify the entity as critical infrastructure. Because CISA has not clarified these definitions, many cooperatives will likely choose to over report, in order to avoid CISA enforcement.

The third criterion is similarly broad. Electric cooperatives are not only responsible for the core functions of generation, transmission, and distribution of electricity, but they also operate nonessential business systems and provide a wide range of other services that, while important, are not critical to the reliability of electric grids. A disruption to "business operations" or an ability to "deliver goods and services" is sufficiently broad to include even minor cyber incidents to systems that have no connection to the critical infrastructure CISA is tasked with protecting and could lead to a large number of less significant incidents being reported.

Finally, the fourth criterion includes a provision where unauthorized access to any nonpublic information through a third party would also constitute a reportable event. Compromises resulting in the access of nonpublic information are, unfortunately, incredibly common in the United States. Since 2005, the Identify Theft Resource Center has tracked nearly 19,000 known data compromises, including more than 3,200 in 2023 – a 78% increase over 2022. Collectively, these incidents have impacted more than 12 billion victims and exposed nearly 20 billion records. By making incidents that impact the supply chain and other third-party vendors reportable events, CISA will further increase the number of incidents and reports that must be submitted.

Many cooperatives contract with the same third-party vendors, and an incident impacting one of those vendors would result in an untold amount of duplicative reporting to CISA under the proposed third-party

reporting rules. Furthermore, in some instances, cooperatives may not have the necessary information from their vendors to provide a report, which would further complicate the reporting requirements. For example, in 2023, a software and technology services vendor used by electric utilities suffered a data breach. The vendor's cooperative customers were aware that there had been a breach and that there had been data exfiltration, so many could assume that their information had been impacted. However, the vendor required time to manage the incident and determine the extent of the breach, so many of its customers were not notified that they had been impacted for several weeks. In this example, a cooperative could reasonably have assumed their information was compromised shortly after the incident occurred but would have been unable to provide CISA with the details needed for a report until long after the reporting deadline had passed.

Excessive Resource Requirements for CISA

As the scope and scale of data compromises increase, reporting all incidents will not only create reporting burdens for critical infrastructure operators but may also challenge CISA's ability to process the amount of information it receives. The NPRM estimates that CISA will receive more than 200,000 CIRCIA reports through 2033. However, a March 2024 GAO report noted that "CISA officials identified concerns with insufficient CISA staff with the requisite OT skills as a challenge…Consequently, CISA may not effectively deliver services needed to address OT risks facing critical infrastructure owners and operators.[4]"

In its 2024 budget request, CISA included nearly $100 million to support the staffing and implementation needs for CIRCIA. However, Congress's final award was more than $23 million below CISA's request for CIRCIA and $83.5 million below the agency's total requested budget. CISA's Executive Direct Brandon Wales noted the challenges with funding, stating that "The funding constraints are primarily impacting in our ability to begin to hire personnel that we believe will be [needed] for full implementation of [CIRCIA] and it has forced us to slow down some of the technology development that we believe is important for the implementation of CIRCIA.[5]" The need for personnel is further reflected in CISA's 2025 budget request of $115 million for CIRCIA implementation with the Department of Homeland Security's (DHS) noting that "To effectively meet CIRCIA's requirements, CISA must add new staff, update existing programs, and implement new processes and technologies, including…expanding staffing to enable CISA to receive, analyze, and action report.[6]"

Recommendation to Raise Reporting Thresholds to Reduce Burden

To address these issues, NRECA recommends that CISA revise the definition for substantial cyber incident to include only those incidents directly impacting the operational capabilities of the critical infrastructure entity, as determined by the owners and operators, and only where such operational capabilities fall within congressional intent. By focusing only on systems related to operational capabilities, CISA would reduce the burden on critical infrastructure operators to report incidents that did not have operational impacts to their systems and subsequently reduce the number of reports that CISA's analysts would have to review and process, allowing them to focus only on reports that have a direct threat to national security, economic

[4] https://www.gao.gov/assets/d24106576.pdf

[5] https://insidecybersecurity.com/daily-news/wales-cisa-budget-shortfall-could-impact-hiring-needs-implement-mandatory-cyber-incident

[6] https://www.dhs.gov/sites/default/files/2024-03/2024_0311_fy_2025_budget_in_brief.pdf

security, public health, and safety. Furthermore, NRECA also recommends that CISA revise the criteria for incidents originating from third-party vendors. Rather than expecting the customers of vendors to report cyber incidents that impact information held by their vendors, CISA should only require vendors that experience a substantial cyber incident to submit reports and notify their customers of the incident.

Limit the Workforce and Resource Burden on Cooperatives

Covered entities that experience a substantial cyber incident are expected to take several actions outlined in the NPRM. They must report the cyber incident within 72 hours after they reasonably believe the event to have occurred or, in the case of a ransom payment, within 24 hours after the payment has been disbursed. The report that the entity submits to CISA must include demographic information about the impacted entity, including relevant points of contact, as well as a detailed description of the incident, exploited systems, the entity's security defenses, mitigation actions, information about the perpetrator, etc. Once the entity has submitted the report, it must also submit supplemental reports promptly when substantial new or different information becomes available until the incident is resolved. Finally, the entity is responsible for preserving data from the incident for at least two years, including communications with the threat actor, indicators of compromise, log entries, forensic artifacts, and more. The amount of information requested in the initial and subsequent reports, along with the data preservation requirements, will present a significant burden to cybersecurity personnel who are actively responding to an incident, as well as new financial costs that must be passed on to consumer-members.

Cyber Workforce Shortage

Collecting data for and developing and submitting CIRICA reports for all cyber incidents included in the NPRM will be a time and resource-intensive process that would create a significant burden for the energy sector's cybersecurity workforce. The United States already experiences a shortage of trained cybersecurity personnel. Currently, the US is estimated to have almost 500,000 cybersecurity job openings across industries,[7] and, in 2023, only 20% of business leaders at energy utilities reported felt confident that they had the cyber talent they needed.[8]

Electric cooperatives are not immune from these hiring challenges and, by virtue of their size and available resources, will be disproportionately burdened by excessive reporting requirements. Many smaller cooperatives do not have dedicated cyber teams and opt to outsource cybersecurity programs due to workforce and resource restrictions. The work associated with excessive reporting could represent significant new costs for not-for-profit cooperatives that must be passed along directly to their consumer-members. This does not even consider other expenses, such as the burden on legal staff (which also may be outsourced) that will review submissions or the cost associated with data preservation requirements, which would put a significant burden on the finances of cooperatives that use a third party for their cybersecurity resources.

---

[7] *Total Cybersecurity Job Openings,* cyberseek.org, https://www.cyberseek.org/index.html (June 2024)
[8] *Cybersecurity Workforce Demand,* NIST.gov, https://www.nist.gov/system/files/documents/2023/06/05/NICE%20FactSheet_Workforce%20Demand_Final_20211202.pdf (June 2023)

Potential Impacts to Existing Cyber Workforce

Given the cyber workforce shortage, CISA should also consider the impacts that over reporting could have on cyber workers that already face high rates of burnout and attrition. Responding to even minor cyber incidents is a demanding and stressful activity. According to CISA's own materials, in the first days of an incident response, cyber staff often suffer from a lack of resources, and communication between decision-makers and responders may be impacted, leading to low morale among staff. Additionally, incidents taking more than 48 hours to resolve may lead to personnel becoming fatigued and further resource strained, especially if staff are not available to relieve responders.[9]

CIRICA reporting could distract cybersecurity staff from critical incident response activities necessary to secure a network, which would be especially impactful for cooperatives that do not have a deep bench of cyber personnel to draw from. Cooperatives have a responsibility to protect their workforce from burnout, both for the employee's sake and for the security of their systems, especially during incident response activities. Extreme burnout could lead to attrition and contribute to the growing number of cybersecurity vacancies. According to one study by Gartner, by 2025, nearly half of cybersecurity leaders will change jobs, with 25% moving to different roles entirely, due to work-related stressors.[10] Compounding this issue, cyber positions require more time than other fields to fill job postings and experience an attrition rate nearly 8 percentage points higher.[11]

Recommendation to Limit the Workforce and Resource Burden on Cooperatives

To limit the workforce and resource burden on cooperatives, NRECA recommends that CISA revise the definition for "substantial cyber incident" to raise the threshold for reporting, as outlined in the previous section (Raise Reporting Thresholds to Reduce Burden). This would reduce the overall costs in time and resources for cooperatives by decreasing the number of reports that cooperatives are required to submit and mitigate the additional burden placed on a cyber workforce that is already experiencing elevated levels of stress and attrition.

Protect Sensitive Information

NRECA is concerned with the lack of information and certainty regarding how CISA, other federal agencies, contract support, and others with access to CIRICA reporting will protect sensitive cooperative information. CISA's archive of CIRICA reports will present an attractive target for threat actors due to its accumulation of details regarding some of the nation's most critical infrastructure. CIRCIA reports will include highly sensitive information about cooperative systems, including technical details of networks and devices, security defenses, incident response procedures and mitigations, and other sensitive data. If compromised by a threat actor, access to cooperative system details would provide valuable details that could aid in new cyber

[9] *First 48: What to Expect When a Cyber Incident Occurs,* CISA.gov, https://www.cisa.gov/sites/default/files/video/safecom_first_48_22_1109_final_508c.pdf (November 2022)
[10] *Gartner Predicts Nearly Half of Cybersecurity Leaders will Change Jobs by 2025*, gartner.com, https://www.gartner.com/en/newsroom/press-releases/2023-02-22-gartner-predicts-nearly-half-of-cybersecurity-leaders-will-change-jobs-by-2025 (February 2023)
[11] *The State of US Cybersecurity Employment: Analyzing Growth, Demand, and Retention Challenges,* STIG.net, https://stig.net/the-state-of-us-cybersecurity-employment-analyzing-growth-demand-and-retention-challenges/ (April 2024)

attacks or lead to reputational loss if information about previously submitted incidents were released publicly.

Federal agencies have been shown to be major targets for threat actors, and some agencies have been the victim of significant cyber incidents over the years. Sophisticated attacks such as the SolarWinds in 2020 and Hafnium in 2021 leveraged IT products to breach the defenses of federal agencies and compromise sensitive government data. Similarly, the 2015 Office of Personnel Management Breach resulted in the loss of personally identifiable information, including fingerprint data, Social Security Numbers, financial records, and IT system credentials, for 21.5 million individuals, including 4.2 million current and former federal employees. As stated by the Congressional Research Service, "The government's inability to detect or prevent these attacks highlights the difficulty in curbing advanced, persistent threat (APTs) actors who are technically capable and motivated to conduct computer network operations (CNOs)." [12]

Recommendation to Protect Sensitive Information

CISA must ensure that any critical infrastructure data held by federal agencies or their partners is carefully secured to prevent unauthorized access. NRECA recommends that CISA prioritize the security of CIRCIA reports and provide transparency for how the information will be protected prior to the issuing of the final CIRCIA rule.

Avoid Duplicative Reporting

Across the Federal government, there are more than 50 in-effect or proposed cyber incident reporting requirements. Two of these requirements, NERC CIP and DOE OE-417, specifically impact electric utilities. In the NPRM, CISA outlines a process to harmonize these reporting requirements through the use of memorandums of understanding (MOU) signed between CISA and other Federal Agencies. Once in place, the MOUs would allow a report submitted to a partner agency to be shared with CISA and accepted as a CIRCIA report. Importantly, the information provided in the report to the other Federal agency must be substantially similar to the information required by CIRCIA and must be submitted in a similar timeframe.

In order to harmonize reporting between DOE OE-417, NERC CIP, and CIRCIA, CISA must first address discrepancies between the different reporting requirements. The North American Electric Reliability Corporation (NERC) already accepts submission of DOE-417 to fulfill reporting requirements for NERC CIP-008-6 and, in its comments to a CISA Request for Information (RFI) on CIRCIA, NERC acknowledged that "The incident reporting requirements that CISA is developing under CIRCIA could potentially overlap with the requirements in NERC Reliability Standards CIP-008-6 and CIP-003-8. Given the likely overlap, CISA should consider whether to classify the NERC reports as "substantially similar" under CIRCIA.[13]" While the information included in OE-417 and NERC CIP reports may be considered "substantially similar," CISA will need to address key differences between the requirements including the timeframes for reporting, reporting triggers, descriptions of reportable events, and thresholds for reporting. For example, thresholds

[12] *Federal Cybersecurity: Background and Issues for Congress*, CRSReports.Congress.gov, https://crsreports.congress.gov/product/pdf/R/R46926 (September 2021)

[13] *Request for Information on the Cyber Incident Reporting for Critical Infrastructure Act of 2022: Joint Comments of the North American Electric Reliability Corporation and the Regional Entities,* Regulations.gov, https://downloads.regulations.gov/CISA-2022-0010-0049/attachment_1.pdf (November 2022)

for reporting an incident to DOE under OE-417 require impacts to operational technology, a disruption in the delivery of electricity, or real or potential safety considerations, and the reports must be submitted within 24 hours or less. Whereas CIRCIA requires reports within 72 hours and has a much lower threshold for reporting that does not necessitate a disruption to critical services or a threat to safety. Under the CIRCIA law, Congress established a Cyber Incident Reporting Council (CIRC) within DHS that has explored these harmonization challenges in detail. In 2023, the CIRC produced a recent report on the "Harmonization of Cyber Incident Reporting to the Federal Government"[14] that provides a detailed list of challenges that should be addressed before MOUs or other agreements between agencies can be completed. Resolving these discrepancies will require negotiations between NERC, the Federal Energy Regulatory Commission (FERC), DOE, and CISA, which could potentially impact the timeline for establishing MOUs between the agencies and CISA. If these MOUs are not in place before the final CIRCIA rule is approved, it will result in duplicative reporting requirements and additional burdens on cooperatives.

Recommendation to Avoid Duplicative Reporting

NRECA recommends that CISA consider the findings and recommendations included in the CIRC report, resolve key discrepancies between the timelines, thresholds, and definitions included in NERC CIP 008-6, DOE OE-417, and CIRCIA, and establish MOUs with NERC, FERC, and DOE before a final rule is implemented. If MOUs are not in place at the time the final rule is approved, NRECA recommends that CISA delay implementation of the rule until such time as the MOUs are finalized.

Conclusion

NRECA supports CISA's goal of improving the nation's cybersecurity posture. Electric cooperatives are dedicated cybersecurity partners and take pride in the service they provide to their communities and the nation. As CISA works toward developing a final rule for CIRCIA, it is important that they adhere to congressional intent, consider the potential impacts on electric cooperatives, and avoid requirements that are overly broad and will strain our cyber workforce. Specifically, NRECA recommends that CISA make the following changes:

1. Reduce the number of entities subject to reporting requirements by removing the OE-417 language from the sector-based criteria and replacing it with a risk-based approach.
2. Raise reporting thresholds by revising the definition for substantial cyber incident to only include incidents directly impacting the operational capabilities of the critical infrastructure entity, as determined by the owners and operators, and only where such operational capabilities fall within congressional intent.
3. Limit the workforce and resource burden on cooperatives by reducing the number of entities subject to reporting requirements and raising the reporting thresholds.
4. Protect sensitive information by prioritizing the security of CIRCIA reports and providing transparency for how the information will be protected, prior to the issuing of the final CIRCIA rule.

[14] *Harmonization of Cyber Incident Reporting to the Federal Government,* DHS.gov, https://www.dhs.gov/sites/default/files/2023-09/DHS%20Congressional%20Report%20-%20Harmonization%20of%20Cyber%20Incident%20Reporting%20to%20the%20Federal%20Government.pdf (September 2023)

5. Avoid duplicative reporting requirements by considering the findings and recommendations included in the CIRC report; resolving key discrepancies between the timelines, thresholds, and definitions included in NERC CIP 008-6, DOE OE-417, and CIRCIA; and establishing MOUs with NERC, FERC, and DOE before a final rule is implemented.

Cost-effective federal regulations that minimize unnecessary burdens are critically important to cooperatives' ability to provide affordable, reliable, and safe electric power to their consumer-members. NRECA and its member electric cooperatives look forward to CISA's response to the issues highlighted in these comments and the development of critical information and resources that will guide the implementation of the CIRCIA Program.

NRECA appreciates the opportunity to comment on the NPRM. Should you have any questions, please contact John Ransom, regulatory affairs director, at john.ransom@nreca.coop.

Submitted on July 3, 2024, by:

John Ransom
Director, Regulatory Affairs
National Rural Electric Cooperative Association
4301 Wilson Blvd
Arlington, VA 22203
571.565.6509
john.ransom@nreca.coop