November 03, 2022

Submitted electronically to www.federalregister.gov/d/2022-19551

Re: **Request for Information (RFI) on Cyber Incident Reporting for Critical Infrastructure Act of 2022**

The National Rural Electric Cooperative Association (NRECA) respectfully submits the following comments in response to the U.S. Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA) Request for Information (RFI) on the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA).

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 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. NRECA's member cooperatives include 62 generation and transmission (G&T) cooperatives and 831 distribution cooperatives. The G&Ts generate and transmit power to distribution cooperatives that provide it to the end-of-line co-op consumer members. Collectively, cooperative G&Ts generate and transmit power to nearly 80 percent of the distribution cooperatives in the nation. The remaining distribution cooperatives receive power from other generation sources within the electric utility sector. Both distribution and G&T cooperatives share an obligation to serve their members by providing safe, reliable, and affordable electric service.

We appreciate the opportunity to provide NRECA's perspective in response to CISA's RFI.
Electric cooperatives agree, as stated in the RFI, "the growing number of cyber incidents, including ransomware attacks, is one of the most serious economic and national security threats our nation faces." Electric cooperatives also agree that reporting cyber incidents and ransom payments to the federal government is beneficial.

NERCA's membership, as part of the electricity subsector under the energy sector, has for decades participated in developing and using a robust mandatory and voluntary incident reporting structure. The structure, as described below, starts with recognizing the Department of Energy (DOE) as the Sector Risk Management Agency (SRMA) for the energy sector, which includes the electricity subsector, and its unique role in cybersecurity issues for the sector. The structure also includes mandatory reporting requirements to the Federal Energy Regulatory Commission (FERC), the North American Electric Reliability Corporation (NERC), the NERC-operated Electricity Information Sharing and Analysis Center (E-ISAC) CISA and DOE on cyber incidents depending on the criticality of an entity’s facilities to the electric grid and the severity and type of incident. Other important information, outside of mandatory requirements, can be and often is submitted to the E-ISAC which shares information with other entities in

the subsector.

Also, NRECA membership participates in voluntary information-sharing entities such as the Electricity Subsector Coordinating Council (ESCC) and the Multi-State Information and Sharing Analysis Center (MS-ISAC). The electric sector has also increased technology adoption to assist in the automated visibility and monitoring of its industrial control system and operational technology networks.

As CISA knows, not all critical infrastructure sectors are the same or have the same mandatory reporting structure. Therefore, when developing this rule, CISA must ensure a balanced reporting structure that does not harm the current flow of information between the federal government and critical infrastructure entities. If the rule is too broad, CISA will capture a high volume of unnecessary data and may miss national-level incidents. Too narrow, CISA might only see an incident when it has become too big to respond to or manage. The rule must focus on capturing the necessary national-level incidents at a point they are still manageable and actionable to prevent catastrophic consequences.

To this end, the DHS Secretary's report on duplicative Federal cyber incident reporting requirements and other related issues, developed in consultation with the Cyber Incident Reporting Council (CIRC), can provide helpful guidance to CISA before issuing its proposed rule in identifying and leveraging existing regulations and current pathways of reporting between the federal government and the critical infrastructure sectors to ensure they are not duplicated in new CISA regulations[1]. As directed in statute, CISA must establish an "agency agreement and sharing mechanism" with the respective federal agencies if the information provided by the industry to the agencies has "substantially similar information" and is "within a substantially similar timeframe."

Therefore, CISA's rule must accept current mandatory reporting pathways between entities and individual SRMA, federal partners, or regulatory authorities and only develop a rule to cover the cases of sectors without mandatory reporting pathways within the statute's limits.

We urge CISA to consider the following input to ensure timely and actionable reporting without burdening entities while dealing with live events. Below, we address specific issues raised in the RFI of particular interest to America's electric cooperatives.

1. **Definitions**
    a. **Defining “covered entity”**
    b. **Defining “covered cyber incident”**
    c. **Number of entities and incidents**
2. **Report Contents and Submission Procedures**
    a. **Balancing situational awareness and cyber incident response**
    b. **Submission and timing procedures**
    c. **Third-Party and Machine-to-Machine reporting**
3. **Other Incident Reporting Requirement and Security Vulnerability Information Sharing**
    a. **Current Reporting Structure for the Electricity Sector**

Definitions

[1] As described in the statute, the Cyber Incident Reporting Council will develop a report "in consultation with the Director of the Office of Management and Budget, the Attorney General, the National Cyber Director, Sector Risk Management Agencies, and other appropriate Federal agencies, to coordinate, deconflicted-conflict, and harmonize Federal incident reporting requirements, including those issued through regulations."

In developing the proposed rule, CISA must act consistent with statutory direction to limit the definitions of "covered entity" and "covered cyber incident." The statute restricts the rule to entities and incidents with national-level impact and not every cybersecurity incident within the country.

Defining “covered entity”

Section 2242 (c)(1) of the CIRCIA states that the definition of covered entities must be bounded by "(A) the consequences that disruption to or compromise of such an entity could cause to national security, economic security, or public health and safety; (B) the likelihood that such an entity may be targeted by a malicious cyber actor, including a foreign country; and (C) the extent to which damage, disruption, or unauthorized access to such an entity, including the accessing of sensitive cybersecurity vulnerability information or penetration testing tools or techniques, will likely enable the disruption of the reliable operation of critical infrastructure."

With these statutory limits in place, we suggest that CISA leverage pre-existing efforts to identify critical infrastructures that primarily address these elements. For example, CISA can start with the list of entities within the 16 critical infrastructures identified under Section 9 of Executive Order 13636 "Improving Critical Infrastructure Cybersecurity." This section mandated the DHS to identify owners and operators of "critical infrastructure where a cybersecurity incident could reasonably result in catastrophic regional or national effects on public health or safety, economic security, or national security." CISA can also use existing mandatory reporting standards, detailed below, that identify entities that "if destroyed, degraded, misused, or otherwise rendered unavailable, would affect the reliable operation of the Bulk Electric System" and categorizes them "based on the impact of their associated Facilities, systems, and equipment". (CIP-002)

Defining “covered cyber incident”

Section 2240(4) of the Homeland Security Act of 2002 defines a "covered cyber incident" as a substantial cyber incident experienced by a covered entity that satisfies the definition and criteria established by the Director in the final rule issued according to section 2242(b). Section 2240(6) then defines a "cyber incident" as "(A) has the meaning given the term "incident" in section 2209; and (B) does not include an occurrence that imminently, but not actually, jeopardizes: (i) information on information systems; or (ii) information systems". With these limits in place, a reportable "covered cyber incident" must only cover significant cyber incidents with the potential to cause national security, economic security, or public health and safety.

We suggest CISA leverage pre-existing directives to identify covered cyber incidents that address these elements. For example, DOE-417 Electric Emergency Incident and Disturbance Report collect information on electric incidents and emergencies.

Number of entities and incidents reports

The RFI further asks for comments on "The number of entities, either overall or in a specific industry or sector, likely to be "covered entities" and "The number of covered cyber incidents likely to occur on an annual basis either in total or within a specific industry or sector". It would be impossible to answer these questions since they depend on the final definitions of "covered entities" and "covered cyber incidents." Additionally, it is impossible to even estimate the number of covered cyber incidents likely to occur on

any basis. For this rule to add value, it must define covered entities and covered cyber incidents in a way that captures actual incidents of national-level impact without imposing unnecessary additional burdens on entities reporting and responding to incidents in real-time.

Report Contents and Submission Procedures

It is clear that Congress intended to limit what information the covered entities would need to report to CISA. However, the statute did not direct specific pathways of reporting. Therefore, the rule should be flexible on reporting methods, such as machine-to-machine reporting and other methods, to ensure minimal or no additional burden on the entities. Furthermore, as stated before, it would be beneficial to CISA to use the current structure of the electricity subsector regarding content and submission procedures.

Balancing situational awareness and cyber incident response

As described below, the electricity subsector already complies with federal reporting requirements for certain cyber incidents. The sector also has a robust voluntary component providing a pathway for the entities to report critical information for the benefit of the industry. These pathways have been refined to ensure situational awareness between industry and federal stakeholders without hindering active cyber incident response.

Submission and timing procedures

To ensure compliance concerns do not slow down response and recovery activities, it is crucial that the submission process and timing are straightforward. We recommend the proposed rule require reporting no sooner than 72 hours following entity confirmation of a covered cyber incident. As for reporting ransomware payments, while the statute calls for reporting no later than 24 hours, CISA should keep the contents of the report consistent with the statute to avoid it becoming an overly and unduly burdensome task in the wake of what is likely an ongoing recovery from the ransomware attack. CISA should also be mindful that victims will also be reporting to the FBI, and think about how to harmonize that reporting channel with what is required under CIRCIA. Introducing any complexity into the reporting requirements will detract from the important work of promptly responding to the incident itself.

Third-party and machine-to-machine reporting

As stated in the statute, "a covered entity that is required to submit a covered cyber incident report or a ransom payment report may use a third party, such as an incident response company, insurance provider, service provider, Information Sharing and Analysis Organization, or law firm, to submit the required report under subsection (a)." It also states that "third-party reporting under this subparagraph does not relieve a covered entity from the duty to comply with the requirements for covered cyber incident report or ransom payment report submission."

CISA must clarify that third-party reporting equals an entity's compliance with reporting. For example, the electric sector reports mandatory cyber incidents to DOE and the E-ISAC, a recognized third party in the statute. CISA receiving the information from the E-ISAC on behalf of the entity within the appropriate timeframe must be the same as accepting it directly from the entity.

Finally, CISA should also consider adding flexibility to the rule by leveraging current reporting structures and mechanisms and those that will be developed in the future. For example, the rule should accept

possible machine-to-machine options currently being explored within the sector. This type of reporting could provide rapid incident reporting and reduce the burden on the entity to report of amid an incident.

Other Incident Reporting Requirements and Security Vulnerability Information Sharing

The statute provides an exemption for a covered entity already required to report similar information to another federal agency within a similar timeframe if there is an agreement between CISA and the other federal agency. However, this only works if CISA proactively coordinates with its federal partners and removes the burden on the industry to do multiple reports.

As stated previously, electric utilities within the U.S. already report cyber security incidents to the federal government based on a structure enshrined in various statutes. Therefore, CISA should provide flexibility in the proposed rule and coordinate with DOE and FERC to ensure current information sharing at the federal level is maintained. Below is a detailed description of the current reporting structure used within the electricity subsector.

Current Reporting Structure for the Electricity Sector

Unique to the electricity sector, Section 61003 of the Fixing America's Surface Transportation Act (FAST Act) of 2015 states, "the Department of Energy shall be the lead Sector-Specific Agency for cybersecurity for the energy sector." DOE's responsibilities as the lead SRMA for cybersecurity include the day-to-day coordination with all federal stakeholders, including DHS, on prioritization and coordination of sector-specific activities, carrying out incident management responsibilities, providing, supporting, or facilitating technical assistance and consultations for the energy sector to identify and mitigate vulnerabilities and support the reporting requirements of the DHS under applicable law by providing, on an annual basis, sector-specific critical electric infrastructure information.

Therefore, the statutory obligation is on the federal government, not industry, to ensure DHS receives the information it needs from the sector.

To meet its overall national security and the DHS's National Response Framework responsibilities, the DOE has established mandatory reporting applicable to specific industry members when at least one of the qualifying criteria is met–pursuant to Section 13(b) of the Federal Energy Administration Act of 1974 (Public Law 93-275). This reporting is done through form DOE-417.

DOE-417 identifies the industry members responsible for completing the form, the associated timing of the report, and the event it must report. For example, if the incident is a cyber event that causes interruptions of electrical system operations, the member must notify within one hour. The member must report within six hours if the incident is a cyber event that could potentially impact electric power system adequacy or reliability. And finally, the specific industry member by the later of twenty-four hours after recognition of the incident or by the end of the next business day of the incident if either a complete loss of monitoring or control capability or a complete loss of Interpersonal Communication and Alternative Interpersonal Communication capability affecting its staffed Bulk Electric System control center for 30 continuous minutes or more. The DOE-417 also requires the entity to re-submit the form if significant information or changes become available after the initial report and a final report seventy-two hours after the incident. Since the criteria are agnostic to the type of attack, they can also be used to report ransomware attacks.

Another aspect of the reporting structure comes under the mandatory NERC Reliability Standards

applicable to all entities that are part of the Bulk Electric System. Specifically, Reliability Standards EOP-004, CIP-003, and CIP-008 require reporting by specific entities on various incidents, including cyber incidents.

Reliability standard EOP-004 - Event Reporting (EOP-004) requires each Responsible Entity to have an event reporting plan that includes the protocols for reporting to NERC and other organizations, such as FERC. It further requires each responsible entity to report specific incidents by the later of 24 hours or by the end of the next business day after recognition of the incident. Incidents needing a report are a complete loss of monitoring or control capability or a complete loss of Interpersonal Communication and Alternative Interpersonal Communication capability affecting its staffed Bulk Electric System control center for 30 continuous minutes or more. In addition, the standard lets responsible entities substitute the Attachment 1 form for a DOE-417 if the entity also needs to report to DOE. Finally, FERC receives a copy of the report at a later date from both DOE and NERC.

Reliability standards CIP-003-6 — Cyber Security — Security Management Controls (CIP-003) and CIP-008-6 — Cyber Security — Incident Reporting and Response Planning (CIP-008) both target incident reporting for cyber events. Specifically, CIP-008 requires responsible entities at the high and medium levels of the risk assessment to have a cyber security incident plan that includes mandatory notification to the E-ISAC and CISA of a cyber incident. Likewise, CIP-003 requires responsible entities at the low level of the risk assessment to also have a cyber security incident plan and to report incidents to the E-ISAC on a mandatory basis.

Finally, NRECA would like to highlight and lend support to the point made by the Chairman and Ranking Member of the House Committee on Energy and Commerce and the Senate Committee on Energy and Natural Resources in their April 8th letter to DOE Secretary Jennifer Granholm regarding the implementation of this statute in support of using the current reporting structure for this statute.

> "Prior to the passage of the Act, electric utilities and other energy companies were required to report certain cyber incidents to DOE, The Federal Energy Regulatory Commission (FERC), state and local agencies, and the North American Electric Reliability Corporation (NERC). As CISA develops a rulemaking for reporting requirements under the Act, we ask you to work to maintain DOE's roles as the SRMA for the energy sector, as required by law. Further, we ask that you urge the Secretary of Homeland Security and other federal agencies to harmonize existing cyber incident reporting requirements for the energy sector with CISA's forthcoming reporting requirements to provide clarity and consistency.
>
> Companies in the energy sector must focus their attention on maintaining cybersecurity and responding to cyber threats to critical infrastructure and avoid inconsistent and duplicative requirements."

In summary, it is vital to electric cooperatives that CISA looks at the current processes for required reporting to the federal government and uses all the tools at its disposal to ensure it receives the data needed without adding unnecessary burden to the industry. CISA must coordinate closely with DOE and other federal agencies with statutory missions that impact the energy sector to fully understand the existing robust reporting structure and how best to leverage it for the nation's security. The grid is expected to undergo significant change in the decades to come. Properly securing it will ensure electric

cooperatives can continue delivering affordable, reliable, safe, and secure power to their consumer-members.

Thank you for considering our comments. Please contact me at andres.lopez@nreca.coop or 703-907-5715 if you have any questions regarding these comments.

Sincerely,

Andres Lopez
Director Regulatory Affairs
National Rural Electric Cooperative Association