National Association of Secretaries of State

July 12, 2024

NASS Public Comment in Response to the Cybersecurity and Infrastructure Security Agency's Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA) Notice of Proposed Rulemaking (NPRM)

The following public comment is submitted on behalf of the Executive Board of the National Association of Secretaries of State (NASS):

NASS and its members appreciate the Cybersecurity and Infrastructure Security Agency's (CISA) ongoing coordination and communication with us, and we understand CISA's overarching goal of achieving a fuller understanding of the cyber threats impacting U.S. critical infrastructure. We also understand why CISA, in service of its critical mission, would want as much relevant information as it can obtain from election administrators about suspected cyber incidents. However, we have concerns about the resource and administrative burdens state, local, tribal, and territorial (SLTT) government entities would face from the requirements currently outlined in the proposed rule. Our questions, concerns, and suggestions are outlined below. Please note, this is not an exhaustive list. Furthermore, individual NASS members may also submit comments based on state-specific considerations.

- Since elections were designated a subsector of U.S. critical infrastructure in 2017, NASS and its members have worked with CISA to establish and maintain a voluntary partnership for information sharing and federal cybersecurity assistance for SLTT election entities. We are proud of our existing relationship that respects the independence and authority of state governments. NASS members are concerned the proposed cyber incident reporting requirements may disincentivize SLTT government entities from participating in this well-functioning voluntary partnership. CISA should prioritize continuing to maintain this voluntary partnership over imposing requirements on SLTT government entities.
    - Specifically, we ask CISA to consider making it voluntary for SLTT government entities to comply with the cyber incident reporting requirements. This would be consistent with our existing voluntary partnership and the statutory exemption from enforcement penalties for SLTT government entities.
- Through the Multi-State Information Sharing and Analysis Center (MS-ISAC) and the Election Infrastructure Information Sharing and Analysis Center (EI-ISAC), of which all states are members, NASS members have efficient means of reporting cyber threat information and potential cyber incidents to CISA. This is a testament to our positive coordination over the past several years. We ask CISA to utilize existing information-sharing avenues for SLTT government entities rather than requiring them to use a new, untested reporting structure.

  - We suggest SLTT government entities should be able to report cyber incidents to the MS/EI-ISAC and opt-in to having the report shared with CISA. This means of reporting is familiar and effective for SLTT government entities.
- As currently proposed, the required elements of a cyber incident report are overly broad and would strain the resources of SLTT government entities during a critical time for cyber incident response. Submitting an incident report would likely require numerous hours of work from multiple staff members, including those leading incident response in real-time. This is challenging for state government entities and potentially impossible for many small local jurisdictions.
  - Given these considerations, CISA should simplify the initial report to require only directly applicable and essential information pertinent to the cyber incident. Then in due course, request additional materials and details as needed at a later time.
    - As an example, "a description of the covered entity's security defenses in place" should be narrowed to reflect only those defenses relevant to the cyber incident, such as those bypassed by the attackers or used to detect the incident.
  - Additionally, overlapping authorities among SLTT government entities will often create the need for extensive coordination among multiple entities on reports.
    - For example, a cyber incident may impact multiple state agencies with different authorities to varying degrees. Alternatively, some incidents may impact overlapping jurisdictions such as a county and state.
  - Further, we are concerned about the potential of an inadvertent release of data associated with cyber incident reports through a data breach or other incident. There is substantial risk associated with CISA's collection and retention of detailed information on the cyber defenses and vulnerabilities for all critical infrastructure entities that experience cyber incidents.
- NASS requests CISA provide a more precise definition of "substantial cyber incident," and we urge the agency to focus only on truly substantial incidents. As currently proposed, we can imagine scenarios in which entities will need to spend a significant amount of time determining whether a cyber incident qualifies as "substantial."
  - The Cyber Incident Reporting for Critical Infrastructure Act of 2022 and proposed rule require reporting within 72 hours after the covered entity reasonably believes that the covered cyber incident has occurred. It may take a large portion of this time simply to determine the scope of a cyber incident and whether it meets the overly broad definition currently contained in this rule.
- We request clarification on the sector-based criteria for election entities in 226.10: "*Involved with information and communications technology to support elections processes. The entity manufactures, sells, or provides managed services for information and communications technology specifically used to support election processes or report and display results on behalf of State, Local, Tribal, or Territorial governments, including but not limited to: (i) Voter registration databases; (ii) Voting systems; and (iii) Information and communication technologies used to report, display, validate, or finalize election results.*"

- Does this only apply to third-party vendors in the non-profit or private sectors? If so, this should be explicitly stated.
- Could it be interpreted to apply to SLTT government entities that provide information and communications technology services to support elections? If so, could SLTT entities with a population under 50,000 be covered entities under this sector-based criteria?

State Chief Election Officials want to ensure the critical infrastructure designation continues to function in a productive way that respects state authority over elections. In this vein, NASS looks forward to working with CISA to achieve a more balanced approach to the proposed rule that optimizes cyber incident information sharing without diverting resources from cyber incident response or overburdening SLTT government entities with onerous administrative requirements.

The full NASS membership voted to approve the above public comment during the NASS 2024 Summer Conference Business Meeting in July. The comment was submitted during the comment period and can also be found in the Federal Register.