NAIC NATIONAL ASSOCIATION OF INSURANCE COMMISSIONERS

June 28, 2024

Cybersecurity and Infrastructure Security Agency
1110 N. Glebe Road
Arlington, VA 20598-0630

Via Regulations.gov

Re: Cyber Incident Reporting for Critical Infrastructure Act Reporting Requirements
89 FR 23644; 6 CFR 226; CISA-2022-0010; 1670-AA04; 2024-06526

To Whom it May Concern:

We write on behalf of the National Association of Insurance Commissioners (NAIC) regarding the Department of Homeland Security's (DHS) Cybersecurity and Infrastructure Security Agency's (CISA) proposed rulemaking on "Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) Reporting Requirements" (the "Proposed Rule").

Founded in 1871, the NAIC is the U.S. standard-setting and regulatory support organization created and governed by the chief insurance regulators from the 50 states, the District of Columbia, and the five U.S. territories. Through the NAIC, state insurance regulators establish standards and best practices, conduct peer review, and coordinate their regulatory oversight. We are tasked with protecting the public interest, promoting competitive markets, ensuring the fair and equitable treatment of insurance consumers, and supporting the financial stability of insurance markets. NAIC members, together with the central resources of the NAIC, form the national system of state-based insurance regulation in the U.S.

The NAIC respectfully submits the following comments to the Notice of Proposed Rulemaking (NPRM) and Request for Comment published in the April 4, 2024 issue of the Federal Register.

As a threshold matter, and for the purposes of this Comment Letter, we understand that the Proposed Rule includes our regulated entities—the insurance market—in the definition of "Covered Entities." The comments we provide in this letter proceed on that assumption and on the understanding that the Proposed Rule has significant implications for our regulated entities.

First, we recognize the importance of the Proposed Rule's objectives, as stated in the NPRM. Namely, that "information sharing will lead to Federal and non-Federal stakeholders having

the ability to adopt an enhanced overall level of cybersecurity and resiliency, resulting in direct, tangible benefits to the nation."

Second, we appreciate CISA's efforts to reduce duplicative reporting of covered cyber incidents through a substantially similar reporting exception. However, there is room to improve. We would urge CISA to expand the exception beyond other Federal departments and agencies to include substantially similar state-based reporting regimes.

In this vein, we would draw your attention to the NAIC's Insurance Data Security Model Law (#668). Model #668 establishes risk-based data security standards and standards for the investigation and notification to the state insurance commissioner of a cybersecurity event. It applies to any individual or non-governmental entity licensed, authorized to operate, or registered under state insurance laws, making it highly relevant to the discussion at hand. By recognizing state-based cybersecurity event reporting regimes, such as Model #668, CISA could further reduce duplication and streamline the reporting process, which would undoubtedly redound to the cybersecurity benefit of all.

Third, we advocate for the reduction of duplication and the synchronization of regulatory efforts. In that light, we encourage CISA to utilize the established work products in the field and to depend on predefined definitions, such as those established by the National Institute of Standards and Technology (NIST).

Fourth, and finally, it is imperative that CISA share the work product of this cyber reporting scheme with the NAIC and state insurance regulators in both the public and more detailed public/private partnership sharing forum formats. This collaboration is essential for maintaining a comprehensive view of the cybersecurity landscape and for enabling proactive responses to threats.

In closing, we remind CISA that insurance is regulated by the states, and as such, it is crucial to work in tandem with state regulators and the NAIC to effectively address cybersecurity risks within the insurance sector.

We appreciate the opportunity to comment and look forward to engaging further on this critical issue.

Sincerely,

Andrew N. Mais *(He/Him/His)*
NAIC President
Commissioner
Connecticut Insurance Department

Jon Godfread
NAIC President-Elect
Commissioner
North Dakota Insurance Department

Scott White
NAIC Vice President
Commissioner
Virginia Insurance Department

Elizabeth Kelleher Dwyer
NAIC Secretary-Treasurer
Director
Rhode Island Department of Business Regulation

Gary D. Anderson *(He/Him/His)*
Chief Executive Officer
National Association of Insurance Commissioners