NASS
National Association of Secretaries of State

February 2023

NASS Public Comment in Response to the Cybersecurity and Infrastructure Security Agency's Request for Information on the Cyber Incident Reporting for Critical Infrastructure Act of 2022

The following feedback was submitted on November 14, 2022 as a public comment on behalf of the Executive Board of the National Association of Secretaries of State (NASS):

We thank the Cybersecurity and Infrastructure Security Agency (CISA) for its ongoing coordination with NASS. We request that CISA considers existing cyber incident reporting structures and protocols for state, local, tribal, and territorial (SLTT) governments when drafting its final rule for cyber incident reporting requirements. Through membership in the Multi-State Information Sharing and Analysis Center (MS-ISAC), the Election Infrastructure Information Sharing and Analysis Center (EI-ISAC), and the Election Infrastructure Subsector Government Coordinating Council (EIS-GCC), NASS members have sufficient and effective means of reporting cyber threat information and potential incidents to CISA.

In 2018, the EIS-GCC established voluntary Threat Information and Incident Reporting Protocols for the Election Infrastructure Subsector. The protocols were created by CISA, the U.S. Election Assistance Commission (EAC), and SLTT election entities, through the EIS-GCC. The goal was to achieve optimal information sharing across the Subsector and with the federal government, while not overburdening SLTT jurisdictions with onerous requirements. The Subsector has exercised and refined these protocols over the past five years.

SLTT election entities have embedded the protocols into their standard operating procedures and incident response plans. Our federal partners, including CISA and the Federal Bureau of Investigation (FBI), have also incorporated the protocols into their incident notification policies. As CISA drafts any section of the final rule that applies to offices of Secretaries of State and/or other SLTT election entities, we request that CISA:

- Seeks ongoing input from the EIS-GCC and NASS related to the implementation of cyber incident reporting as it applies to the Election Infrastructure Subsector and/or Secretaries of State;
- Grants maximum flexibility to SLTT entities;
- Includes a reasonable timeframe for implementation of the new rule;
- Utilizes existing reporting structures including the MS-ISAC and the EI-ISAC;
- Follows the EIS-GCC's Threat Information and Incident Reporting Protocols;
- Avoids exceeding the reporting practices outlined in the Protocols and further avoids requiring reporting through additional avenues or to additional entities;
- Exercises caution in defining "covered cyber incident," "substantial cyber incident," and "reasonable belief" including ensuring reporting requirements do not apply to routine cyber activities we experience daily, such as scanning;

- Continues to respect our country's legal and historical distinctions and avoids overreach upon state authority; and
- Avoids costly requirements that would equate to an unfunded mandate on SLTT entities.

The full NASS membership voted to approve the above public comment on February 18, 2023, during the NASS 2023 Winter Conference Business Meeting.