July 11, 2022

The Honorable Bennie Thompson
Chairman
House Committee on Homeland Security
U.S. House of Representatives
H2-176 Ford House Office Building
Washington, DC 20515

The Honorable John Katko
Ranking Member
House Committee on Homeland Security
U.S. House of Representatives
H2-117 Ford House Office Building
Washington, DC 20515

Dear Chairman Thompson and Ranking Member Katko:

The undersigned insurance trade associations commend policymakers for their work on the National Defense Authorization Act (NDAA) for FY2023, and for exploring solutions to the growing threat of cyberattacks through public-private collaboration. Our collective members who offer cyber insurance products provide a valuable risk transfer mechanism for businesses of all sizes and work to enhance risk awareness, cyber hygiene, and planning and preparedness. As Congress considers various legislative proposals to better address the threat of cyber incidents and cybercrimes, we continue to engage constructively to share our unique perspective.

However, we urge opposition to language in the amendment filed by Rep. Langevin to the NDAA to establish an Office of Cyber Statistics within the Cybersecurity and Infrastructure Security Agency (CISA).

This amendment includes misguided provisions on the **'furnishment of data and information related to covered claims'** to require the Director of the OCS to request data and information from insurers about cyber incidents experienced by their customers that lead to a covered claim, including detailed data beyond the scope of information insurers currently collect or need to process claims. It also requires the Director to publish procedures for how data and information may be transmitted to the OCS and requires the Director recommend policy options to Congress to enhance the OCS' capacity to collect this data and information.

If passed, this language would be an unwarranted intrusion into the contractual relationship between insurance providers and their customers. It would also serve as a precursor to a reporting mandate that would present a host of challenges on businesses of all sizes due to significant costs, limits on the availability of information sought, and potential new enforcement issues. **This legislation has not been introduced or considered by the multiple committees with jurisdiction over CISA or over the business of insurance in the House or Senate. Therefore, we ask that it not be included as part of the NDAA bill due to our significant concerns, which include:**

Potential New Reporting Requirements/Big Costs
Insurers are not currently collecting the level of detailed information contained in the amendment to be collected by the OCS. Insurers would have to retool systems or expend additional resources to cull detailed granular information about a policyholder's cyber incident that may be buried in forensic or other IT reports outside the control of the insurer. This type of requirement would burden insurers and

victims such as small and medium-sized businesses with significant costs and would divert limited resources.

Lack of Access to/Availability of Required Information

A business who is victimized by a cyberattack and submits a claim to their insurer may not have definitive information about the event and may not be able to provide fulsome information to the insurer, even if requested or mandated. This detailed information about individual cyber incidents, including third party services such as forensics and IT reports, is not information insurance companies collect to process a policyholder's claim. Many policyholders also engage their own counsel during cyber incidents and their investigation documents are privileged and not provided to insurers. The proposal could lead to putting insurers in a difficult situation between promptly paying valid claims or failing to report information to the OCS.

Negative Impacts to Insurance Providers and Customers

An insurance provider should not be asked for or required to provide information about their customers' sensitive data to the federal government. We are concerned that this approach could establish an adversarial relationship with our customers and could discourage some from seeking appropriate coverage. Insurance providers have their own proprietary application and claims data to analyze and glean insights from as each insurer can link its claims data back to relevant terms and conditions of its insurance policies.

Victim Entity Should Report

As a threshold issue, any federal information requests or reporting requirement on cyber incidents should be for the victimized entity as they have first-hand information. Congress recognized this earlier this year with the passage of cyber incident reporting for critical infrastructure entities who are victims of cyber-attacks. CISA has not yet implemented these regulations, and these impacts should be understood before Congress considers additional reporting burdens on businesses.

Security of Information at Risk

Insurers are well known targets as financial institutions that already hold a great deal of sensitive data, and should this proposal be enacted hackers may be able to glean additional information on security controls and vulnerabilities in the industry. Pooling the data outlined in the amendment could make insurers even bigger targets. The federal government is not immune to cyber risks. An August 2021 report[1] by Chairman Peters and Ranking Member Portman revealed that data entrusted to eight key federal agencies remains at risk as the agencies had significant cybersecurity weaknesses. We have concerns with the level of security that will be employed to protect sensitive, lucrative data from hackers as well as leakers.

Potential New Regulatory Enforcement – Insurance is a state-regulated industry, and this proposal would add a potential new layer of federal regulatory enforcement from a new OCS. Insurance providers are subject to numerous state cyber incident reporting mandates. In addition to the upcoming CISA cyber incident reporting rulemaking, companies of all sizes are potentially facing new federal reporting

[1] https://www.hsgac.senate.gov/imo/media/doc/Federal%20Cybersecurity%20-%20America's%20Data%20Still%20at%20Risk%20(FINAL).pdf

requirements from the Securities and Exchange Commission (SEC).

For these reasons, we urge opposition to language in the amendment.

Sincerely,

Nathaniel F. Wienecke
Senior Vice President
American Property Casualty Insurance Association

Jimi Grande
SVP – Federal and Political Affairs
National Association of Mutual Insurance Companies

Charles E. Symington Jr.
Senior Vice President, External, Industry & Government Affairs
Independent Insurance Agents & Brokers of America, Inc.

Joel Wood
Senior Vice President of Government Affairs
Council of Insurance Agents and Brokers