

June 18th, 2026

President Scott White; Commissioner, Virginia

Re: Recent NAIC Cybersecurity Incident – June 2026

President White:

On behalf of the National Association of Mutual Insurance Companies (NAMIC)¹, we write in response to the NAIC-reported cybersecurity incident from June 17, 2026, wherein the NAIC disclosed that an unauthorized third party gained access to a portion of NAIC IT systems.²

At the time of this writing, the NAIC is reportedly undergoing its investigation into the matter, but the mere occurrence of NAIC systems compromise, systems which house sensitive information on the whole of the industry, is evidence of a deepening problem of concentration risk and challenge to keep pace with the current cyber threat landscape.

To no fault of the NAIC, the current cyberthreat landscape is rapidly evolving and becoming more sophisticated, and the recent attack is evidence of an appetite toward insurance industry systems and data. Even with stringent controls and robust cybersecurity practices, cybercriminals continue to carry out more sophisticated attacks, and the financial services industry continues to be a prime target, given the sensitive information it holds and the role it plays in society. This fact has been confirmed by insurance industry-focused attacks like those by the cybercriminal group, Scattered Spider, where numerous insurance companies were targeted starting in June of 2025,³ and now most recently by this attack on the NAIC systems. What is incumbent upon NAIC is to recognize this moment's criticality and take a deep view of its own practices and risk mitigation. By centralizing sensitive information on the insurance industry, the NAIC has created a systemic vulnerability, providing a prime target for cyber criminals to obtain valuable information on a broad swath of the financial services industry.

¹ The National Association of Mutual Insurance Companies is the foremost trade association representing the property/casualty insurance industry. Serving more than 1,300 member companies, including local and regional insurers as well as some of the nation's largest carriers, NAMIC members collectively write \$492 billion in annual premiums, representing 62 percent of the homeowners and 56 percent of the automobile insurance markets. For more than 130 years, NAMIC has been the leading voice advancing public policy solutions and regulatory frameworks that promote a strong, competitive market and protect member companies and their policyholders.

² *An Important Update from the NAIC* (June 17, 2026), <https://content.naic.org/about/security-update>.

³ See, *Insurance Sector Should be on the Lookout for 'Scattered Spider' Hackers*, Insurance Journal, (June 23, 2025), <https://www.insurancejournal.com/news/national/2025/06/23/828749.htm> (detailing cybersecurity incidents at various insurance companies, and new industry focus, from cybercriminal group Scattered Spider).



The NAIC serves as a central repository for highly sensitive information, encompassing a wide range of regulatory, financial, market conduct, and emerging risk data. These systems include, but are not limited to, platforms and databases operated or support by the Center for Insurance Policy and Research (CIPR), the National Insurance Producer Registry (NIPR), the Systems for Electronic Rates and Forms Filings (SERFF), and State Based Systems (SBS), as well as financial examinations tools such as TeamMate+ and the suite of NAIC Market Information Systems. Collectively, these systems capture and store extensive data, including insurer financial filings, examination workpapers, company and licensing information, rate and form submissions, consumer complaints, Market Conduct Annual Statement filings, and data housed within the Regulatory Information Retrieval System (RIRS). In addition, the NAIC is in the process of developing a centralized cybersecurity event reporting portal that will further expand the scope of sensitive information maintained, including detailed incident and remediation data. While each of these systems independently contains information of significant value, in aggregate they represent a highly concentrated repository of regulatory and proprietary data, creating an increasingly attractive target for cybercriminal activity.

NAMIC has alerted the NAIC on multiple occasions of the risk of concentrating and then holding sensitive industry information by a private entity. Most recently, NAMIC raised alarm with the Cybersecurity (H) Working Group's proposed centralized cybersecurity event reporting portal.⁴ With respect to the recent PCMI data call, NAMIC has also stressed the importance of gathering data pursuant to confidentiality statutes by state, and having gathered data aggregated and anonymized. In communications issuing concern over the original PCMI's data anonymity and aggregation, NAMIC cautioned against storing the data in perpetuity and cited the dubious nature of transferring that data not only to FIO but to other segments of NAIC such as CIPR for its own use. Such troves of data are not only concerning from a statutory authority standpoint, but also clearly whet the appetite for willing bad actors.

In response to NAMIC's concerns, the NAIC has repeatedly stated that the organization has extensive experience in cybersecurity practices and housing sensitive information. Based on the breadth of the information that has been accessed in this event,⁵ it appears evident that the NAIC has not implemented proper cyber guardrails, including practices like segmenting sensitive information systems from one another.

Notwithstanding the substantive concerns of concentration risk above, NAMIC is also troubled with the lack of communication by the NAIC on this event. The NAIC did not seem to provide any type of directed alert other than what was posted on the NAIC website, did so nearly one full week after identifying the event

⁴ See, NAMIC Comments on the Centralized Cybersecurity Event Notification Portal Project v.3 (March 6, 2026); NAMIC Comments on the Proposed Cybersecurity Event Repository and Portal (November 15, 2025).

⁵ "The scope of the compromised data is extensive, including 2.1 million insurer regulatory filing PDFs and 40,000 quarterly statistical CSVs containing federal EINs and company data. Additionally, the breach includes over 45,000 licensed rating agency files from Moody's, Fitch, S&P, Kroll, DBRS, and AM Best, which contain CUSIP and ISIN identifiers. Other exposed information includes statutory annual and quarterly financial statements, premium and loss statistics, and HR Ratings master data." *Shinyhunters Claims Compromise of National Association of Insurance Commissioners (NAIC)* (June 18, 2026), <https://qpulse.quasarcybertech.com/news/4161/shinyhunters-claims-compromise-of-national-association-of-insurance-commissioners-naic-data>.

occurred, and did not follow similar standards imparted onto insurers for responding to cybersecurity events. The NAIC's Insurance Data Security Model Law (#668) alone requires insurers to notify the relevant commissioner – no later than 72 hours – with information including the description of how the information was breached, how the event was discovered, whether any information has been recovered, the identity of the source of the event, whether a report has been filed with law enforcement agencies, a description of the types of information acquired, the period of compromise, the total number of affected consumers, the identification of any lapsed controls, description of remediation efforts, a copy of the privacy policy, and a contact person. This lack of communication and information is especially concerning when licensed carriers may now have reporting requirements of their own due to the NAIC's experienced event. NAMIC requests that the NAIC provide full information on the event to carriers so that carriers may determine whether alerting their regulators is required or whether they might need to engage their own cyber insurers.

Given the foregoing, NAMIC strongly insists that the officers direct that the NAIC undergo a third-party evaluation of the concentration risk that NAIC data collection may pose to the industry, inclusive of all of their data and systems. Additionally, regulators should halt all industry data transmission to the NAIC and NAIC should halt workstream activity involving data until a full scope and strategy for resolution is established.

As part of an investigation, NAMIC also recommends the NAIC consider and seek counsel on whether some sections of the NAIC should dismantle in favor of the private market or other entities prescribed by state procurement laws. This evaluation should include currently proposed data projects the NAIC is undertaking or planning to undertake. The outcomes of such an investigation should be shared with stakeholders such as NAMIC, other industry trades, regulators, and regulated entities.

It is not our intent to criticize the NAIC in its administration of any of these functions but rather recognize that the coagulation of these systems and housing of sensitive data may in fact now represent a threat to state-based regulation and the industry as a whole. Mitigation strategies such as destruction of data after collection and dissemination to participating states may be a worthwhile exercise to address some, but not all, of these concerns.

We close by encouraging prompt attention to the growing risk we've noted here and the suggested actions that will additionally inform the impacted companies, who may have responsibilities to other parties now that their data has been compromised within the walls of the NAIC. This is representative of our initial reaction, and NAMIC looks forward to continuing to provide industry input as we learn more.

NAMIC is the largest vocal supporter of state-based regulation in the industry. We consider this situation a clear risk to that foundation, the market, and the consumers that our members serve. We will vigorously



defend the industry and the critical trade secret and policyholder data that it possesses, and we invite the NAIC to take a sober and open level of engagement with stakeholders to reduce this concentration risk in short order.

Sincerely,

Erin Collins, MPA, IOM, ARM
Senior Vice President – State and Policy Affairs