Testimony of

Adam W. Hamm

Commissioner

North Dakota Department of Insurance

On Behalf of the National Association of Insurance Commissioners

Before the

Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies

Committee on Homeland Security

United States House of Representatives

Regarding:

The Role of Cyber Insurance in Risk Management

March 22, 2016

Introduction

Chairman Ratcliffe, Ranking Member Richmond, and members of the Subcommittee, thank you for the invitation to testify today. My name is Adam Hamm. I am the Commissioner of the Insurance Department for the state of North Dakota and I present today's testimony on behalf of the National Association of Insurance Commissioners (NAIC).[1] I am a Past President of the NAIC, and I have served as the Chair of the NAIC's Cybersecurity Task Force[2] since its formation in 2014. On behalf of my fellow state insurance regulators, I appreciate the opportunity to offer our views and perspective on cybersecurity challenges facing our nation and the role cyber insurance can play in risk management.

The Cyber Threat Landscape Creates Demand for Coverage

On one hand, threats to data privacy are not new for businesses, regulators, or the consumers we protect. Regulators and legislatures have required businesses to protect consumer data for

reputational damage, theft of digital assets, customer notifications, regulatory compliance costs, and many more liabilities that may arise from doing business in the modern connected universe.

Most businesses carry and are familiar with their commercial insurance policies providing general liability coverage to protect the business from injury or property damage. What they may not realize is that most standard commercial lines policies do not cover many of the cyber risks mentioned above. To cover these unique cyber risks through insurance, businesses need to purchase a special cybersecurity policy.

I want to urge some caution regarding the term "cybersecurity policy" because it can mean so many different things – while it is a useful short-hand for purposes of today's conversation, I want to remind the Committee that until we see more standardization in the marketplace, a "cybersecurity policy" will really be defined by what triggers the particular policy and what types of coverage may or may not be included depending on the purchaser and insurer. Commercial insurance policies are contracts between two or more parties, subject to a certain amount of customization, so if you've seen one cybersecurity policy, you've seen exactly one cybersecurity policy.

All these nuances mean securing a cybersecurity policy is not as simple as pulling something off the shelf and walking to the cash register. Insurers writing this coverage are justifiably interested in the risk-management techniques applied by the policyholder to protect its network and its assets. The more an insurer knows about a business's operations, structures, risks, history of cyber-attacks, and security culture, the better it will be able to design a product that meets the client's need and satisfies regulators.

Insurance Regulation in the U.S. – "Cops on the Beat"

The U.S. insurance industry has been well-regulated at the state level for nearly 150 years. Every state has an insurance commissioner responsible for regulating that state's insurance market, and commissioners have been coming together to coordinate and streamline their activities through the NAIC since 1871 . The North Dakota Insurance Department, which I lead, was established in 1889 and employs approximately 50 full-time staff members to serve policyholders across our state. It is our job to license companies and agents that sell products in our state, as well as to

relies on an extensive system of peer review, communication, and collaboration to produce

flow testing. Laws also restrict insurers' investments and impose capital and reserving requirements.

The monitoring of insurers is done through both on-site examinations and analysis of detailed periodic insurer reporting and disclosures. Insurers are required to prepare comprehensive financial statements using the NAIC's Statutory Accounting Principles (SAP). SAP utilizes the framework established by Generally Accepted Accounting Principles (GAAP), but unlike GAAP which is primarily designed to provide key information to investors of public companies and uses a going-concern concept, SAP is specifically designed to assist regulators in monitoring the solvency of an insurer. The NAIC's *Accounting Practices and Procedures Manual* includes the entire codification of SAP and serves as the consistent baseline accounting requirement for all states. Each insurer's statutory financial statements are filed with the NAIC on a quarterly and annual basis and include a balance sheet, an income statement, and numerous required schedules and exhibits of additional detailed information.

The NAIC serves as the central repository for an insurer's financial statement data, including

the U.S. may apply for inclusion in the NAIC's Quarterly Listing of Alien Insurers. The carriers listed on the NAIC Quarterly Listing of Alien Insurers are subject to capital and surplus requirements, a requirement to maintain U.S. trust accounts, and character, trustworthiness and integrity requirements.

In addition, the insurance regulator of the state where the policyholder resides (the home state of the insured) has authority over the placement of the insurance by a surplus lines broker and enforces the requirements relating to the eligibility of the surplus lines carrier to write policies in that state. The insurance regulator can also potentially sanction the surplus lines broker, revoke their license, and hold them liable for the full amount of the policy.

Like any other insurance market, as the cybersecurity market grows and more companies offer coverage, we anticipate the regulation will continue to evolve to meet the size and breadth of the market as well as the needs of consumers. State insurance regulators have a long history of carefully monitoring the emergence and innovation of new products and coverages, and tailoring regulation over time to ensure consumers are appropriately protected and policies are available.

Cybersecurity Insurance Market – New Reporting Requirements

As a still nascent market for coverage, accurately assessing exposure or the size of the

NAIC Efforts Beyond Cybersecurity Insurance

The NAIC and state insurance regulators are also ramping up our efforts to tackle cybersecurity issues in the insurance sector well beyond cybersecurity insurance. We understand that the insurance industry is a particularly attractive target for hackers given the kind of data insurers and producers hold, and to that end we are engaged on a number of initiatives to reduce these risks.

The NAIC adopted twelve *Principles for Effective Cybersecurity: Insurance Regulatory Guidance* in April 2015.[4] The principles set forth the framework through which regulators will evaluate efforts by insurers, producers, and other regulated entities to protect consumer information entrusted to them.

We also adopted an NAIC *Roadmap for Consumer Cybersecurity Protections* in December 2015 to describe protections the NAIC believes consumers should be entitled to from insurance companies and agents when these entities collect, maintain, and use personal information and to guide our ongoing efforts in developing formal regulatory guidance for insurance sector participants.[5]

Most recently, on March 3rd, the Cybersecurity Task Force exposed its new *Insurance Data Security Model Law* for public comment – written comments should be submitted by Wednesday,

these bills, including S.961/HR 2205, the Data Security Act, would lessen existing consumer protections in the insurance sector and could undermine our ongoing and future efforts to respond to this very serious issue.

Coordinating with our Federal Colleagues

Lastly, we understand that state insurance regulators are not alone in any of our efforts. We work