Principles for Effective Cybersecurity Insurance
Regulatory Guidance
Comments Received
March 23, 2015

Pam Simpson
National Association of Insurance Commissioners
444 North Capitol Street NW,
Suite 700
Washington, DC 20001

By email to: psimpson@naic.org

Dear Ms. Simpson:

The American Bankers Association (ABA), and the American Bankers Insurance Association (ABIA), the ABA’s insurance subsidiary, strongly support adoption of the comprehensive cyber-security regulatory principles for insurance operations described in the NAIC’s March 12 press release. The obligation to manage insurance transactions within as secure an electronic environment as possible is vital to the integrity of insurance markets, insurance companies, insurance agencies and the consumers we serve.

The energy being expended to adopt frameworks for information sharing and system governance are fundamental to fulfilling this obligation. Accordingly, we applaud the NAIC’s call for insurers to participate in the Financial Services Information Sharing and Analysis Center (FSISAC) and to adopt the National Institute of Standards and Technology (NIST) framework.

The Federal Financial Institutions Examination Council (FFIEC) has long supported a similar approach but also agreed to several enhanced recommendations in their March 17 plan:

- **Cybersecurity Self-Assessment Tool**: The FFIEC plans to issue a self-assessment tool this year to assist institutions in evaluating their inherent cyber-security risk and their risk management capabilities.
- **Incident Analysis**: FFIEC members will enhance their processes for gathering, analyzing and sharing information with each other during cyber-incidents.
- **Crisis Management**: The FFIEC will align, update and test emergency protocols to respond to system-wide cyber-incidents in coordination with public-private partnerships.
- **Training**: The council will develop training programs for the staff of its members on evolving cyber-threats and vulnerabilities.
- **Technology Service Provider Strategy**: The FFIEC’s members will expand their focus on technology service providers' ability to respond to growing cyber-threats and vulnerabilities.
• **Collaboration with Law Enforcement and Intelligence Agencies:** The council will build upon existing relationships with law enforcement and intelligence agencies to share information on the growing cyber-security threats and response techniques.

The FFIEC recommendations make sense and offer enhanced response capabilities to counter threats and breaches. We urge the NAIC to adopt them.

We would also urge the NAIC to examine requirements being debated in Congress around establishing building codes and testing protocols. Most of the information sharing efforts currently underway are motivated by the statutory requirements around breach notice and remediation duties contained in various federal and state laws, not on how to build secure software. Cyber-insurance products are designed to compensate policyholders for the costs associated with fulfilling these notice duties. In our opinion, more energy needs to be expended on avoiding breaches in the first place instead of compensating policyholders for the costs of reporting them.

For example, more than a century ago, large portions of the city of Chicago burned down twice. The buildings were row houses, which were attached to each other, and made of wood. It became clear that the number of fire stations and firemen was not a relevant factor in stopping such city-sized fires.

The city of Chicago implemented building codes to create brick row houses – in fact – the original term ‘firewall’ comes from the brick walls between row houses. Risk management became defined by what is done to prevent fire, not what is done once a fire is discovered.

When electric appliances first made an appearance in America, accidents and poor design contributed to deaths and fires. In response, Underwriters Laboratory was set up to evaluate and approve these devices prior to being sold. And when air travel became common place, after a series of plane crashes, the National Transportation Safety Board was established to create a team capable of conducting independent forensic investigations to determine cause, so that steps could be taken to prevent similar events in the future.

Recently USA Today reported that the National Highway Traffic Safety Administration may begin giving automobiles five star cyber security ratings to help consumers in the near future. The logical question to apply to cyber policy, therefore, from the historical experience detailed above, is this: could software building-codes and a Cyber Underwriter Laboratory for software prevent breaches in the future?

Clearly, yes; given recent events, it’s hard to understand why we don’t have these facilities already.
Therefore, we recommend the NAIC adopt the principles detailed in your release but also consider a model law or protocol that urges insurance organizations to do the following:

1. Adopt a rigorous protocol for creating and maintaining cyber-hygiene: compel disclosure of known software vulnerabilities from all vendors.
2. Require software to be “patchable” and institute a mandate that once a vulnerability is discovered, the vulnerable component be replaced with the least vulnerable component available according to the NIST database.

If the various NIST, FS-ISAC and FFIEC protocols are adopted, and a serious effort is made to establish and maintain cyber-hygiene, breaches should become less frequent, which means that consumers’ information will be more protected. It should also mean that the insurance financial institutions purchase will be both less expensive and have a wider definition of covered perils.

One reason insuring breach is so difficult is that the underwriting metrics and the structures that make creating the metrics possible do not exist in the cyber world at present. This needs to change. One effort designed to prompt creation of sound cyber hygiene metrics was a bill introduced in the 113th congress, H.R. 5793, the Cyber Supply Chain Management and Transparency Act. It makes very useful recommendations for software makers.

We consider establishment and maintenance of secure electronic environments a national priority and look forward to working with the NAIC on this vital work.

Sincerely,

[Signature]

SVP & Director, ABA Office of Insurance Advocacy
March 23, 2015

Commissioner Adam Hamm, Chair
Cybersecurity (EX) Task Force
National Association of Insurance Commissioners
2301 McGee Street, Suite 800
Kansas City, MO 64108

Attn: Pamela Simpson, Senior Administrative Assistant
Via e-mail: psimpson@naic.org

Re: Cybersecurity (EX) Task Force – Draft Cybersecurity Guiding Principles

Dear Commissioner Hamm:

Thank you for the opportunity to comment on the Draft Principles for Effective Cybersecurity Insurance Regulatory Guidance ("Draft Principles") and the proposed Cybersecurity Insurance Coverage Supplement ("Supplement").

At the outset, ACE wishes to commend the NAIC for establishing the Cybersecurity Task Force. ACE is committed to safeguarding the sensitive personal and financial information of all of its customers as well as our own proprietary and confidential information and believes that meaningful regulatory guidance can play a vital role in helping us fulfill this commitment. To the extent that the Draft Principles focus on the systems that carriers, producers and service providers employ to protect against data breaches, we believe they represent a positive, if somewhat broad-based first step; we are confident that as the Task Force’s work proceeds with input from stakeholders that focus will sharpen.

We do, however, have concerns with the Draft Principles insofar as they address issues related to the regulation of cyber insurance. Principle 17, for example, calls for “enhanced solvency oversight” for insurers that sell cyber coverage. ACE believes that such oversight is unnecessary. As with all insurance products, issuing cyber coverage involves prudent underwriting and appropriate pricing using actuarially sound, adequate rates. Regulators already have myriad tools at their disposal that are sufficient to ensure that carriers writing cyber coverage do so in a manner that is fiscally prudent and appropriate for the marketplace. Adding additional layers of regulation aimed specifically at cyber insurance will merely add frictional cost and expense to the products with no greater protection for consumers. In our view the Draft Principles will be most effective if their focus remains on developing optimal procedures and systems to prevent cyber attacks.

We also have concerns with the proposed Supplement. While we appreciate the NAIC’s desire to understand the cyber security market, the Supplement does not sufficiently account for the variety of ways in which cyber coverage is issued. For example, the Supplement breaks cyber security coverage into
two main categories: "Standalone" and as a component of a Commercial Multi Peril Package. This approach, however, ignores other products in which cyber coverage might be available, as well as the types of cyber risks covered by each. As a result, carriers may have difficulty providing the type of consistent, accurate data that would give regulators a truer picture of the marketplace. As with the Draft Principles, we believe the focus of the Supplement needs to be refined. We offer the following additional comments on specific provisions of the Draft Principles.

- We presume the term "consumer" in Principle 1 is intended to refer to corporate entities as well as individuals. Indeed a wide variety of proprietary and confidential data is regularly exchanged between insurers and corporate commercial clients. Principle 1 should be clarified to include the sensitive information of both corporate and individual consumers.

- In this same vein, we recommend that the language "sensitive customer health and financial information" in the second line of the draft of Principle 2 be changed to "sensitive customer information, including health, financial and personal data."

- While the National Institute of Standards and Technology Cybersecurity Framework ("NIST") referenced in Principle 5 is one source of standards for managing critical cyber security infrastructure it is not the only one. The Principle should be clarified to state that other comparable or superior sources should be acceptable, or modified to reflect the mandate of Executive Order 13636. We would suggest the following language as one possible approach: "Principle 5: Compliance with cybersecurity regulatory guidance must be flexible, scalable, practical and consistent with the national efforts to reduce cyber risks to critical infrastructure."

- It is unclear whether Principle 8 is aimed at the financial impact of cyber security infrastructure and consumer data protection or the regulation of insurance products covering cyber security. As noted above, ACE believes that financial and market conduct issues related to the regulation of cyber insurance should be left to traditional systems of product/solvency regulation. Principle 8 should be revised accordingly.

- It is unclear what the term "essential cybersecurity information" refers to in Principle 11: The insurer's own corporate confidential information? Consumer information? This should be clarified.

- As with Principle 8, it is unclear if the focus in Principle 12 is the risks presented by the reporting entity's systems for managing its own internal cyber risks, the risks that it is assuming as a cyber insurer or both. This too, should be clarified.

- While ACE agrees that encryption can be an effective safeguard for protecting sensitive information, it is only one of the cyber protection tools available to carriers. Other tools such as masking and tokenization can also be effective and in some instances may be more appropriate than encryption. Principle 15 should recognize this.

- With respect to Principle 18, we again state our position that regulators currently have sufficient procedures and resources at their disposal to regulate the cyber insurance market without adding a further layer of regulation. Hence, we believe Principle 18 should be eliminated.

ACE appreciates the opportunity to comment on the Draft Principles and Supplement. As noted we remain committed to developing and implementing the strongest possible systems and procedures to protect our own sensitive data and that of our customers, and would be pleased to discuss our views further with members of the Task Force.

Very truly yours,
For Electronic Delivery

March 23, 2015

The Honorable Adam Hamm  
Chair, NAIC Cybersecurity (EX) Task Force  
North Dakota Insurance Department  
600 E. Boulevard Avenue  
Bismarck, North Dakota 58505-0320

The Honorable Raymond G. Farmer  
Vice Chair, NAIC Cybersecurity (EX) Task Force  
P.O. Box 100105  
Columbia, South Carolina 29202

Re: Comments on Draft Principles for Effective Cybersecurity Insurance Regulatory Guidance

Dear Commissioner Hamm and Director Farmer:

Cyberattacks targeting governments, businesses and individuals in the United States are increasing in sophistication and intensity. Our country has experienced well-orchestrated assaults aimed at stealing information and destabilizing the nation’s cybersecurity infrastructure. The American Council of Life Insurers (ACLI) commends the National Association of Insurance Commissioners (NAIC) for establishing the Cybersecurity (EX) Task Force and developing the draft Principles for Effective Cybersecurity Insurance Regulatory Guidance. We commit to joining you in your efforts to enhance insurance sector resiliency to cyber-attacks.

ACLI supports the focus of the Task Force on a “consistent, coordinated national approach” to cybersecurity regulation. In this instance, national security and industry oversight are intersecting which necessitates the coordinated efforts of the federal and state governments and of industry.

We concur with the NAIC that any regulatory guidance must be “flexible, scalable, practical and consistent”. A ‘check-the-box’ and ‘one-size-fits all’ approach will not yield needed results. Rather it is a risk-based approach to cybersecurity, where the greatest resources are directed toward the greatest risks, that will best enable insurers to address emerging threats.

Going forward, we believe that the final Principles should be broad and allow for flexibility in the ever changing landscape of digital dangers. The evolving nature of attacks and counter-measures is a vital ‘lesson learned’. Over-specificity in the Principles may not enhance the progress made to date in cybersecurity and may not adequately capture future threats. For example, the NAIC may want to consider crafting Principle 15 to ensure reasonable and appropriate safe guards and protections of data.

---

1 ACLI is a Washington, D.C.-based trade association with approximately 300 member companies operating in the United States and abroad representing more than 90 percent of industry assets and premiums. 75 million American families rely on life insurers’ products for financial and retirement security. Life insurers invest $5.6 trillion in the U.S. economy.
The principle should not be so narrow that it would eliminate other appropriate and effective data protection methods.

On the state level, the NAIC has developed regulatory approaches to risk management and corporate governance that give insurance regulators insight into how insurers are adapting to and addressing evolving cybersecurity threats.

The life insurance industry also has made strides in cybersecurity independent of, and often in conjunction with, government regulation. To support these efforts, ACLI is an inaugural member of the Financial Services Sector Coordinating Council (FSSCC) and a member of the Financial Services Information Sharing and Analysis Center (FS-ISAC) and participates in its Insurance Risk Council. FS-ISAC is among the leading resources for cyber threat intelligence, analysis and sharing within a large, national community of businesses, governmental entities, and other interests. These on-going national dialogues are, in our view, the most effective approach to combatting cyber threats.

We are committed to protecting the integrity of our systems against the growing threats from cyber-attacks. And we are dedicated to ensuring that sensitive consumer information is safeguarded from data hackers and threats from state-sponsored organizations. We again reiterate our pledge to work with the NAIC and all other stakeholders to isolate and protect against cybersecurity threats.

Sincerely,

J. Bruce Ferguson
March 23, 2015

Commissioner Adam Hamm, Chair
Cybersecurity (EX) Task Force
National Association of Insurance Commissioners
2301 McGee Street, Suite 800
Kansas City, MO  64108

Attn:    Pamela Simpson, Senior Administrative Assistant
Via e-mail:  psimpson@naic.org
Re:    Cybersecurity (EX) Task Force – “Principles for Effective Cybersecurity Insurance Regulatory Guidance”

Dear Commissioner Hamm:

On behalf of America’s Health Insurance Plans (AHIP) and the Blue Cross Blue Shield Association (BCBSA), we thank you and the Cybersecurity (EX) Task Force (“the Task Force”) for this opportunity to comment on the draft “Principles for Effective Cybersecurity Insurance Regulatory Guidance” (“the Principles”).

We commend the NAIC for establishing the Task Force and support the 2015 charges as adopted last November. Cyber terrorism is a national security issue that requires strong collaboration between both the public and private sectors to accurately assess emerging threats and prevent future breaches. Health plans are committed to working in partnership with government and other stakeholders to protect consumers, identify potential threats and secure member information. We also offer our thoughts, below, on the Principles and the work of the Task Force.

GENERAL COMMENTS

Below we offer our detailed comments on the Principles. As you consider them, there are several threshold issues to note. Most importantly, as indicated in Principle 4, we believe that collaboration among all stakeholders toward the goal of a consistent, coordinated national approach is essential. Cyberattacks, cyber threats, and cyber risks often involve extremely sophisticated and technologically advanced international operations, possibly including foreign nationals or state sponsors. These cyber threats pose risks to all sectors of our economy and our society. As such, cybersecurity is foremost a national security issue which suggests, almost by necessity, a primary role in such matters for the Federal government, including U.S. law enforcement, defense, and security agencies. However, we also support state-oriented solutions when appropriate.
It is also important to note that there are a number of Federal and state privacy and security laws and regulations that incorporate and relate to goals and guidance in the draft Principles. For health insurers, chief among these are the Federal Health Insurance Portability and Accountability Act of 1996 (HIPAA), the HIPAA privacy and security regulations, and related state requirements that build on this Federal construct. Since 2005, the HIPAA security regulations have provided the healthcare and health insurance industry with a flexible, scalable set of standards that enables a risk-based assessment approach to achieving the appropriate physical, technical, and administrative security protections for health insurers’ information technology capability.

On February 12, 2015, the President signed an Executive Order, “Promoting Private Sector Cybersecurity Information Sharing.” The Federal Bureau of Investigation is aggressively investigating recent breaches involving insurers and other private commercial entities, as well as Federal government databases. At the same time, various Congressional committees are considering legislative proposals addressing cybersecurity issues. The NAIC’s activities should be closely coordinated with federal authorities in order to avoid duplicative or conflicting objectives.

The insurance industry has been engaged in proactive measures designed to enhance its cybersecurity protections. As the Federal Executive Order recognizes, private sector information sharing is key to detecting and responding to threats, and the government can play a useful function by facilitating a private sector response. State regulators, like their Federal counterparts, can encourage insurer participation in appropriate industry cyber information-sharing relationships and organizations, such as the National Health Care Information Sharing and Analysis Center (NH-ISAC), and information sharing and analysis organizations (ISAOs) designated by the Executive Order.

The NAIC has been active in this area as well. For example, over a decade ago, the NAIC adopted the Standards for Safeguarding Customer Information Model Regulation #673, which requires licensees to implement a comprehensive information security program. The NAIC has also more recently adopted the Risk Management and Own Risk and Solvency Assessment (RMORSA, or ORSA) Model Act (#505), which requires insurers to report on their ongoing process of risk assessment, not only on current risks, but also to identify those future risks which are reasonably foreseeable. This reporting requirement supports effective and meaningful assessment of all risks, including cybersecurity, as well as the implementation of pragmatic methods to deal with those risks.

We believe that the efforts of industry and regulators could be not only ineffective but even counterproductive unless they are guided by input and information from qualified experts. Before state regulators or the NAIC proceed further to develop or promote guiding principles, we believe it would be prudent to seek information from such qualified experts in the fields of forensic information technology and risk management, and perhaps from ISAOs as well. It is only with such guidance that insurers and regulators will be able to adequately refine their objectives.
There are several principles articulated in the draft Principles that can serve as the basis for further positive engagement, as we outline in greater detail below. For example, Principles 4, 6, 7, 9 and 16 are compatible with federal efforts and industry initiatives, and work in this context because they articulate broad themes instead of narrow or prescriptive regulatory efforts. On the other hand, several principles would actually be mandates on the insurance industry. For example, we have significant concern about Principle 15 regarding encryption. While encryption is certainly appropriate in some circumstances, it is not appropriate in all circumstances, and has the potential to impose substantial costs and operational challenges with only speculative consumer benefits. We have similar concerns about Principle 14. A mandate to join an information sharing and analysis center (ISAC) is a requirement, not a principle, and is likely to have negative unintended consequences. Industry ISACs are voluntary organizations and function as such. If insurers are forced to join but do so without an insurer’s corresponding commitment to share information, it may not serve the interests of the ISAC, the insurer, or the consumer.

SPECIFIC COMMENTS

We offer the following general and specific comments on the draft Principles:

**Principle 1:** Insurance regulators have a significant role and responsibility regarding protecting consumers from cybersecurity risks. We believe this principle places too much responsibility upon insurance regulators. Ultimately, under federal law and policy it is the entity holding data that has the primary responsibility for defending against cybersecurity risks. The federal government encourages the sharing of threat information but also recognizes that the regulatory authority of the United States government is not the primary defense against cyber-threats. This is also true for state government and regulators. In the context of health insurance, that role and responsibility is actually in the hands of those government entities charged with the enforcement and compliance authority of the applicable security laws and regulations. For example, in the case of HIPAA security, that entity is the Office of Civil Rights in the U.S. Department of Health and Human Services. For years, health insurers, and other healthcare entities have complied with the HIPAA privacy and security requirements. To broaden the reach of HIPAA to business associates and related entities, the Federal government modified HIPAA with the Health Information Technology for Economic and Clinical Health (HITECH) Act. It should also be noted that any effort to assume those responsibilities by the NAIC or state regulators would likely entail responsibilities they would be unable to support. We recommend deletion of this Principle, and would suggest that Principle 2 (as modified as suggested below) is more in line with the potential role of states in supporting a national solution to cybersecurity threats. An alternative approach would be to merge Principle 1 with Principle 4, to emphasize the NAIC’s appropriate role and its recognition of the critical need to collaborate and coordinate its efforts with stakeholders, including but not limited to federal authorities, independent and industry experts (e.g., IT security advisors and risk managers), industry and consumers.

**Principle 2:** Insurance regulators have a significant role and responsibility regarding the insurer’s efforts to protect sensitive customer health and financial information. We are concerned with this Principle’s breadth. Insurance regulators may play a role here in overseeing the compliance activities of insurers, but we would suggest it not be misinterpreted to imply
regulators should establish and oversee detailed security standards, which are not primarily within the jurisdiction or area of expertise of state insurance departments.

Principle 3. Insurance regulators have a significant role and responsibility in protecting the sensitive information housed in insurance departments and at the NAIC. We agree with this principle and suggest strengthening it by stating that insurance regulators have the leading role in protecting information housed with them.

Principle 4. Insurance regulators recognize the value of collaboration in the development of regulatory guidance with insurers, insurance producers, consumers and the federal government with the goal of a consistent, coordinated national approach. As stated previously in our comments, we fully support this Principle and believe it is paramount. Coordination with all stakeholders in this arena is not only prudent, it is essential.

Principle 5. Compliance with cybersecurity regulatory guidance must be flexible, scalable, practical, and consistent with the national efforts embodied in the National Institute of Standards and Technology (NIST) framework. We support this Principle, in general terms. We note there are multiple security tools for information technology that should be considered to achieve “flexible, scalable, practical and consistent” results in an entity’s security application. Many health insurers incorporate the National Institute of Standards and Technology (NIST) framework as the backbone of their cybersecurity efforts, and map their processes through the Health Information Trust Alliance (HITRUST) Common Security Framework (CSF). In light of the Federal interest here, and the role played by the U.S. Congress, U.S. Department of Health and Human Services, and other Federal agencies, we once again highlight the need for broad coordination. Lastly, we note a significant overlap between Principles 5 and 7, and would suggest that they could be merged.

Principle 6. Regulatory guidance must consider the resources of the insurer or insurance producer. We support this principle. Further, we note Congress included this concept in HIPAA.

Principle 7. Effective cybersecurity guidance must be risk-based and threat-informed. We support this Principle. Current HIPAA security regulations are based on risk-based analysis. Additionally, the HITRUST CSF, which many healthcare and health insurance entities employ, currently incorporates risk-based, threat-informed processes. As noted above in our comments to Principle 5, it appears the concepts of Principles 5 and 7 involve significant overlap, and the two could be combined.

Principle 8. Insurance regulators should provide appropriate regulatory oversight, which includes but is not limited to, conducting risk-based, value-added financial examination and/or market conduct examinations regarding cybersecurity. Insurers are highly motivated to continually improve their cybersecurity to secure their customers’ information. The goals of this Principle, security and readiness, would be better served if the expectation were levied upon the insurer, not regulators. The regulators should not try and take on the examination of cybersecurity within an insurer, but instead expect and perhaps verify that the insurer has sought out external validation of their program. As previously noted, there is an extensive Federal
regulatory structure that clearly outlines the steps and standards to protect health care information. It is important to note that cybersecurity talent is very limited, due to the current demands of government and industry. This demand, and the corresponding resource drain, will continue into the near future. State insurance regulators will have a difficult time acquiring the talent or knowledge to enable each state to independently support this principle.

**Principle 9.** Planning for crisis response for insurance regulators, insurers, and insurance producers is an essential component to an effective cybersecurity program. We support this Principle. We suggest the replacement of the word “crisis” with “incident,” which is more of an industry standard term.

**Principle 10.** The effective management of cybersecurity by third parties and service providers is essential for protection of consumer’s sensitive personal health and financial information. We support this principle, and note that many health insurers already have a detailed third-party vendor assessment program to do just this. This arena is informed by HIPAA and some provisions of Gramm-Leach-Bliley.

**Principle 11.** Information sharing is important for risk management purposes; however, it must be limited to essential cybersecurity information and protect sensitive confidential information. While this principle is somewhat ambiguous because of the undefined phrase “essential cybersecurity information,” we believe that information sharing — for example, about possible threats, organized crime rings, scams, etc. — is highly appropriate, and health insurers do share such information with other companies, law enforcement, and regulators. We also see potential overlap between Principles 11 and 14, both of which speak to the importance of information sharing.

**Principle 12.** Cybersecurity risks should be included and addressed as part of an insurers and insurance producers Enterprise Risk Management processes. We do not believe that these principles should dictate to companies which particular risks, including cybersecurity, should be included in a company’s enterprise risk management process, and we would disagree with any principle or interpretation that would require reporting by insurers beyond that cybersecurity risk information which may already be included in an insurer’s ORSA Summary Report.

**Principle 13.** High level information technology internal audit findings should be discussed at the insurer’s and insurance producer’s Board of Director meetings. We suggest that this principle can be combined with Principle 12. Additionally, we reiterate that a "Principles" document is not the right vehicle for prescriptive requirements, including what should be discussed at Board meetings. In other contexts, we have supported the RMORSA Model Act calling for delivery of a copy of the ORSA Summary Report to the Board of Directors or appropriate committee thereof.

**Principle 14.** It is essential for insurers and insurance producers to join Financial Services Information Sharing and Analysis Center (FSISAC) to share information and stay informed about cyber and physical threat intelligence analysis and sharing. Although we support the concept that insurers take full advantage of available ISAOs, we strongly disagree with any requirement that an insurer must join FSISAC or any other specific ISAC. FSISAC in particular
is tailored to financial institutions, and has been found to be of limited value to many insurers. Health insurers are turning to the NH-ISAC because of its focus on healthcare or are already participating in the HITRUST CSF or other ISAOs. The President’s Executive Order is permissive in nature, and recommends use of an ISAO of the entity’s choosing. We urge that the principle be consistent with the national policy. As mentioned previously, we suggest merging this principle, as amended, with Principle 11.

Principle 15. Sensitive data collected and stored and transferred inside or outside of an insurer’s or insurance producers network should be encrypted. Encryption is a security tool and we caution that a security tool is not a principle. Security tools, such as encryption, can also be static, subject to the next technological development that renders them ineffective or obsolete. Insistence on solutions that are flexible, scalable, practical, and consistent is the correct approach and is not compatible with a requirement to use specifically mandated security tools. As we have learned from recent heavily publicized cybersecurity breaches, encryption will not always prevent the loss of sensitive consumer data. We strongly suggest that the word “encrypted” be changed to “protected.” This increases the flexibility needed by insurers to most effectively and efficiently protect various types of information in different locations and uses.

Principle 16. Periodic and timely training for employees of insurers and insurance producers regarding cybersecurity issues is essential. We support this principle, and note that the HIPAA Security Rules require such training.

Principle 17. Enhanced solvency oversight is needed for insurers selling cyber insurance to businesses and families. This principle is not applicable to the health insurance industry and we therefore have no comment.

Principle 18. Additional data on the sale of cyber insurance products should be collected to assist insurance regulators with oversight of financial and market regulation. This principle is not applicable to the health insurance industry and we therefore have no comment.

Again, we thank you for the opportunity to provide these comments, and we look forward to working with the Task Force and the NAIC on this important issue.

Respectfully submitted,

America’s Health Insurance Plans
Mark Pratt

Blue Cross Blue Shield Association
Kim Holland
March 23, 2015

VIA Electronic Mail: psimpson@naic.org

Eric Nordman, Director of Regulatory Services and CIPR
NAIC Central Office
1100 Walnut, Suite 1500
Kansas City, MO 64106-2197

RE: Draft Principles for Effective Cybersecurity Insurance Regulatory Guidance

Dear Mr. Nordman:

The American Insurance Association (AIA) appreciates the opportunity to provide comments on the draft “Principles for Effective Cybersecurity Insurance Regulatory Guidance” (Regulatory Guidance). AIA represents approximately 300 major U.S. insurance companies that provide all lines of property-casualty insurance to U.S. consumers and businesses, writing nearly $117 billion annually in premiums. Our membership includes U.S. insurers that write insurance only within the U.S., U.S. insurers that write insurance inside and outside the U.S., and the U.S. subsidiaries of multi-national insurers.

The draft Regulatory Guidance document evidences the importance that regulators and industry place on protecting customer data. Further, we believe that the Regulatory Guidance, particularly principles 5 and 6, recognizes that there is a balance between protecting customer information and avoiding overly burdensome regulations that can have the unintended consequence of preventing an insurer from adapting and protecting their systems consistent with the threat they face and nature and scope of the insurer’s activities. The insurance industry appreciates the significant responsibility we have to maintain the privacy and security of the data that are customers have entrusted us with. As such companies have developed internal cybersecurity best practices, which continue to evolve with the rapidly changing threat landscape. Therefore, consistent with the collaborative nature that Regulatory Guidance advances, we applaud the NAIC’s efforts and have provided a mark-up of the principles with explanatory material below.

Again, AIA appreciates the opportunity to comment and we look forward to a collaborative partnership on the issue of cybersecurity.

Respectfully submitted,

Angela Gleason
Associate Counsel
Principles for Effective Cybersecurity Insurance Regulatory Guidance

Due to ever increasing cybersecurity issues, it has become clear that it is vital for insurance regulators to provide effective cybersecurity guidance regarding the protection of the insurance sector’s data security and infrastructure. The insurance regulators commend insurance companies for conducting a review of their cybersecurity policies, regulations, and guidance with the goal of strengthening the insurance sector’s defense and response to cyber-attacks. The insurance industry looks to the insurance regulators to aid in the identification of uniform standards, promoting accountability across the entire insurance sector, and to provide access to essential information. The insurance regulators also depend upon the insurance industry to join forces in identifying risks and the offering of practical solutions. The guiding principles stated below are intended to establish insurance regulatory guidance that promotes these relationships and protects consumers and the insurance industry.

**Principle 1:** Insurance regulators have a significant role and responsibility regarding protecting consumers from cybersecurity risks.

**Principle 2** Insurance regulators have a significant role and responsibility regarding the insurers’ efforts to protect sensitive customer health and financial information.

**Principle 3:** Insurance regulators have a significant role and responsibility in protecting the sensitive information housed in insurance departments and at the NAIC.

**Principle 4:** Insurance regulators recognize the value of collaboration in the development of regulatory guidance with insurers, insurance producers, consumers and the federal government with the goal of a consistent, coordinated national approach.

**Principle 5:** Compliance with cybersecurity regulatory guidance must be flexible, scalable, and practical. We are very supportive of regulatory guidance that is flexible, scalable, and practical. AIA has a very positive reaction to the Framework and the process by which it was developed and we generally feel that it is a flexible tool that identifies general concepts in a common risk management process. However, we think specific reference to the NIST Cybersecurity Framework (Framework) is contrary the overall guiding principle. Specific reference to one document fails to recognize the many other standards and guidance that may be appropriate tools for a company’s cybersecurity posture. Hence, we recommend that this principle be amended to remove the NIST reference thereby truly reflecting flexibility.

**Principle 6:** Regulatory guidance must consider the resources of the insurer or insurance producer. We are very supportive of the consideration of resources available to insurers and insurance producers and thank the NAIC for their consideration of this factor.

**Principle 7:** Effective cybersecurity guidance must be risk-based and threat-informed. We are curious as to what is meant by threat-informed.

**Principle 8:** Insurance regulators should provide appropriate regulatory oversight, which includes but is not limited to, conducting risk-based, value-added financial examinations and/or market conduct examinations regarding cybersecurity.

**Principle 9:** Planning for crisis cyber-attack response for insurance regulators, insurers, and insurance producers is an essential component to an effective cybersecurity program. The purpose of this clarification is to provide consistency with the opening paragraph and alleviate confusion as to the type of crisis the principles are directed to address.
Principle 10: The effective management of cybersecurity by third parties and service providers is essential. As part of an insurance regulator, insurer, or insurance producer's exercise of due diligence they should take appropriate steps to confirm that third parties and service providers have controls in place for protection of consumer's sensitive personal health and financial information.

AIA agrees that regulators and industry have a responsibility to perform due diligence regarding third party and service provider security policies and procedures with respect to cybersecurity; however, the way that this principle is currently drafted suggests that regulators and industry would be expected to manage cybersecurity practices for these entities and in a sense be responsible for the practices of these outside providers. Our proposed edits will allow regulators and insurers to take a risk-based approach to this principle that is also consistent with Principle 5 and the current NAIC model, “Standards for Safeguarding Customer Information.”

Principle 11: Voluntary information sharing is important for risk management purposes; however, it must be limited to essential cybersecurity information and protect sensitive confidential information and must be accompanied with liability protections.

Principle 12: Cybersecurity risks should be included and addressed as part of an insurers and insurance producers Enterprise Risk Management processes.

Principle 13: High level Information technology internal audit findings presenting a material risk to the company should be discussed at the insurers and insurance producers reviewed with the Board of Director meetings or an appropriate committee thereof.

Sharing information with the Board or appropriate delegated committee can strengthen information risk management; however, even at a high level, not all IT internal audit filings may need to be shared at a Board of Director’s meeting. Information shared with the Board should be based on severity, impact and the risks the findings present.

Principle 14: It is essential for insurers and insurance producers to join Financial Services Information Sharing and Analysis Center (FS-ISAC) to share information and stay informed about cyber and physical threat intelligence analysis and sharing.

This principle is overly prescriptive for a principles document. AIA views the intent of this principle as promoting preparedness through information sharing and staying informed. FS-ISAC is a good organization and is one appropriate method for furthering preparedness. However, there are a number of threat intelligence solutions and data sharing organizations that may be a better option for insurers and insurance producers. We respectfully recommend that a specific reference to FS-ISAC be removed.

Principle 15: Sensitive data collected and stored inside or outside of an insurers or insurance producers network should be appropriately protected encrypted.

This principle addresses a specific technology control and reads like a de facto encryption requirement rather than a guiding principle. We respectfully recommend that principles 5 and 6 inform the development of this principle and allow for flexibility and consideration of insurer and insurance producer resources. Encryption is one method of securing data that may be effective in some cases but not in others and may be beyond what is needed, particularly data collected and stored and transferred inside an insurer or insurance producers’ network. Other system controls usually allow for adequate protection without significant cost, effort and complexities. In addition, there are often limitations to any one solution depending upon the systems environment. Further, there may be an equally effective alternative that is available or even new technologies developed that help keep data protected. There are also different types/strengths of encryption so one could be in compliance with the encryption requirement, but still not have adequately protected their data. Further, there may already be laws in place to address this requirement.

Principle 16: Periodic and applicable timely training for employees of insurers and insurance producers regarding protecting sensitive health and financial customer information cybersecurity issues is essential.

These amendments are meant to add flexibility and consistency with the remainder of the document.
Principle 17: Enhanced solvency oversight is needed for insurers selling cyber insurance to businesses and families.

Given the unique position of the insurance industry in the cybersecurity area, we understand why the NAIC has put in two principles related to cyber insurance. However, the majority of the Regulatory Guidance has been focused on the protection of customer data from an insurance company perspective. AIA believes that principle 17 and 18 are separate issues related to cybersecurity that are better addressed in a completely separate matter.

Specific to this principle we would note that we are concerned that it presupposes that this risk is more volatile than other existing or emerging risks. Insurance regulators already oversee solvency, regardless of these principles, and we are not aware of any data that would suggest that this line of business is potentially more volatile than other risks.

Principle 18: Additional data on the sale of cyber insurance products should be collected to assist insurance regulators with oversight of financial and market regulation.

Similar to Principle 17, we feel that this is an issue that is better addressed as a separate matter. Additionally, it is unclear what “additional data” is to be collected.
March 23, 2015

The Honorable Adam Hamm, Chairman
Commissioner, North Dakota Insurance Department
NAIC Cybersecurity Task Force

The Honorable Raymond G. Farmer, Vice Chairman
Commissioner, South Carolina Department of Insurance
NAIC Cybersecurity Task Force

Re: NAIC Request for Comment On Principles for Effective Insurance Regulatory Guidance

Commissioners Hamm and Farmer:

Thank you for the opportunity to comment on the recently exposed Principles for Effective Regulatory Guidance. Alvarez & Marsal is an international consulting firm with recognized expertise in insurance and insurance regulation, as well as cyber security, cyber risk mitigation strategies, and post-breach forensic analysis. Alvarez & Marsal is a global firm of over 2,500 professionals providing a wide range of sophisticated advisory services to commercial enterprises and governmental entities. Cyber Protection Services are a core offering of our Global Forensics Technology Services Practice, and we have extensive, direct experience conducting investigations into cyber breaches involving large commercial entities - including insurance companies. Alvarez & Marsal also runs an Insurance and Risk Advisory Services practice. These partners are former senior state insurance regulators that have first-hand experience with sensitive regulatory issues, and are intimately familiar with the regulatory processes.

We applaud the NAIC for its proactive stance on this increasing area of risk. As recent headlines demonstrate, every commercial enterprise, nonprofit, and government entity is a target for cyber criminals looking to steal confidential information housed on servers and databases. These criminals include foreign governments and their agents, organized crime syndicates, employees, and individuals working in small cells or even alone. While it is not possible to make one’s business or government agency completely impervious to cyber attack, there are steps that can be taken to provide additional layers of security and minimize the potential for harm to consumers, including the development of a rapid response capability in the event of an attempted or actual breach.

As we read the exposure draft, we offer our comments on the following Principles:

**Principle 5:** Compliance with cybersecurity regulatory guidance must be flexible, scalable, practical and consistent with the national efforts embodied in the National Institute of Standards and Technology (NIST) CyberSecurity framework.
A&M Comment: We wholeheartedly agree with the use of the NIST cybersecurity framework. In addition, we would recommend that the NAIC review guidance developed by other regulatory bodies (such as HIPAA, HITECH, and PCI), which may be adaptable for use by the NAIC.

**Principle 7:** Effective cybersecurity guidance must be risk-based and threat-informed.

A&M Comment: Again, we agree wholeheartedly. Guidance should include a requirement that an organization have an understanding of where their sensitive information is located. Many organizations currently do not know what systems are storing/transmitting sensitive information. As one would expect, this void makes developing a realistic risk profile all but impossible. In addition, vulnerability assessments and penetration testing are essential components of developing system level risks. Depending on the sensitivity of the information being protected, consideration should be given to standards for continuous monitoring.

**Principle 9:** Planning for crisis response for insurance regulators, insurers, and insurance producers is an essential component to an effective cybersecurity program.

A&M Comment: The most effective way to plan for crisis response is to first build a crisis response plan and then to conduct crisis simulation exercises to test the effectiveness of the plan. Crisis simulation exercises provide the best evaluation regarding whether the plan is effective as well as provide indicators as to whether companies are aware of and trained to respond to the plan. The most prepared organizations run these exercises on a yearly basis engaging their entire response teams in order to ensure effective and efficient reaction to any declared information security incidents.

**Principle 10:** The effective management of cybersecurity by third parties and service providers is essential for protection of consumer’s sensitive personal health and financial information.

A&M Comment: Risk Assessments must be conducted of all third parties and service providers that handle the consumer’s data. Without such a risk assessment, there is no way to effectively identify the risk profile and provide recommendations for improvement.

**Principle 13:** High-level information technology internal audit findings should be discussed at the insurers and insurance producers Board of Director meetings.

A&M Comment: Every successful cyber security program must include appropriate governance from the Board of Director level. This must not just be limited to a mere awareness or discussion, but should require an *active* engagement in cyber security issues.
Boards of Directors should be held responsible for the success or failures of their cybersecurity programs.

**Principle 15:** Sensitive data collected and stored and transferred inside or outside of an insurers or insurance producers network should be encrypted.

**A&M Comment:** This prescription should include encrypting servers, desktops, mobile devices, e-mail, instant messaging and other forms of communication. All locations that contain sensitive data should be identified and actively monitored to ensure the data is only being utilized for appropriate business requirements. For Highly Sensitive data, we recommend whitelisting and/or File Integrity Monitoring (FIM) be required in order to add further security to these critical systems.

We hope that Task Force members find our input informative and helpful. Thank you again for the opportunity to comment. Please do not hesitate to contact us directly should the Task Force desire additional information or wish to follow up on any of these items.

Regards,

[Signature]

Art Ehuan
Managing Director
March 20, 2015

Insurance Commissioner Adam Hamm, Chair
Cybersecurity (EX) Task Force
Attn: Pam Simpson - psimpson@naic.org

Dear Commissioner Hamm:

As the trade association for 68 fraternal benefit societies operating in the U.S., the American Fraternal Alliance (Alliance) would like to provide general comments for this task force as it begins the process of monitoring, reporting and making recommendations to the Executive (EX) Committee on cybersecurity issues that impact insurers.

The Alliance stands with other industry trade representatives in our desire to work with regulators to make sure that sensitive personal information of consumers in the possession of insurers is safeguarded to prevent cyber breaches from occurring. As in other areas, the insurance industry looks to state regulators to help develop uniform standards that can help insurers identify cybersecurity risks, develop appropriate responses to those cybersecurity risks, and help maintain the privacy of the personal data insurers maintain to protect consumers.

We look forward to partnering with other industry representatives and the NAIC to develop guidelines that will assist insurers and state regulators in achieving these goals.

Very truly yours,

Joseph J. Annotti
President and CEO
Comments of
the Center for Economic Justice
the Consumer Federation of America
United Policyholders and
the National Consumer Law Center (on behalf of its low-income clients)
on March 12, 2015

NAIC Draft Principles for Effective Cybersecurity Insurance Regulatory Guidance

CEJ, CFA, UP and NCLC offer the following comments on the March 12, 2015 draft “Principles for Effective Cybersecurity Regulatory Guidance.”

We commend state insurance regulators for addressing issues of cybersecurity of entities regulated by state insurance departments. The issue has grown in importance for both market regulation and financial oversight because insurers and producers are collecting far greater amounts of personal consumer information today than even ten years ago. Today, a data breach of an insurer puts huge amounts of personal, non-insurance consumer information at risk in addition to insurance information. This greater amount of data in the hands of fraudsters puts consumers at greater risk of identity theft as well as scams directed at consumers. In addition, greater amounts of personal consumer data collected by insurers means greater financial risks to insurers from data breaches, including the costs of responding to and addressing data breaches (such as contacting consumers whose personal information has been stolen, dealing with new information to protect consumer privacy and repairing and strengthening data systems). The financial risks go beyond the costs of dealing with a data breach and can include reputational risk and hacker fraud directed at the insurer. The challenge to state insurance regulators is great – in large part because insurance regulatory practices have not kept up with the increased data collection (big data and data mining) practices of insurers. Consequently, vital consumer protections are not in place.

A fundamental omission from the draft principles is that they never explicitly state the requirement for insurers and producers to comply with existing state data security and breach laws. While such a principle may be a given, it would be helpful to remind the insurance industry that complying with existing laws is a bare minimum, but that more may be expected from an industry that holds so much confidential, sensitive information of consumers.
We note that the draft principles were derived from “Principles for Effective Cybersecurity Regulatory Guidance” published by the Securities Industry and Financial Markets Association. SIFMA is an organization of broker-dealers, banks and asset managers. SIFA describes itself as the “voice of the nation’s securities industry.” Not surprisingly, the SIFMA principles reflect the perspective of businesses who collect and maintain personal consumer information related to the sale of financial products. The SIFMA principles do not reflect the views or needs of consumers whose personal information is collected and put at risk by these organizations. It is unclear why the SIFMA principles were chosen as the basis for cybersecurity policy of state insurance regulators.

We also note that the SIFMA document contains discussion of each principle. This discussion is essential to understand and interpret the terminology used in the principles. The draft NAIC principles copy terms from SIFMA like “guidance must be flexible, scalable and practical” and “guidance is risk-based and threat-informed.” While the SIFMA document attempts to explain these concepts, the draft NAIC document does not, with the result that the NAIC principles use vague terms with no explanation such that different stakeholders will read into the principles what the stakeholder wants.

Specific Comments

We copy the text of the draft and use redline to show our suggested edits, followed by comments to explain the edits.

Due to ever increasing cybersecurity issues, it has become clear that it is vital for insurance regulators to provide effective cybersecurity guidance regarding the protection of the insurance sector’s data security and infrastructure. The insurance regulators commend insurance companies for conducting a review of their cybersecurity policies, regulations, and guidance with the goal of strengthening the insurance sector’s defense and response to cyber attacks. The insurance industry looks to the insurance regulators to aid in the identification of uniform standards, promoting accountability across the entire insurance sector, and to provide access to essential information. The insurance regulators also depend upon the insurance industry and the consumers whose personal information is collected and at risk, to join forces in identifying risks and the offering of practical solutions. The guiding principles stated below are intended to establish insurance regulatory guidance that promotes these relationships and protects consumers and the insurance industry.
Comment: We suggest deletion of the second sentence. First, it is unclear what substantive efforts insurance companies have taken to prevent cyberattacks and protect personal consumer information and if the data protection efforts have matched insurer data collection activities. Second, even if such a commendation was warranted, it is out of place in a document outlining regulatory guidance principles.

We also suggest adding a phrase identifying consumers, whose personal information is collected and at risk, as a stakeholder.

Principle 1: Insurance regulators have a significant role and responsibility regarding to ensure personal consumer information held by insures and producers is protected from protecting consumers from cybersecurity risks and that systems are in place to quickly alert consumers when that personal information has been stolen from insurers and producers.

Comment: If regulators have a responsibility, then clearly regulators have a role. It is redundant to use both terms. The principle as drafted is quite vague. Our suggested edits make clear what the threat is and what the regulators’ responsibilities are. Our proposed edits capture the intent of both principles 1 and 2.

Principle 2 Insurance regulators have a significant role and responsibility regarding the insurers’ efforts to protect sensitive customer health and financial information. Insurers and producers have a responsibility to policyholders, applicants and claimants to inform these consumers of the specific personal information maintained by the insurer or producer on a periodic basis and in the event the personal information is stolen from the insurer or producer. The disclosure to consumers should itemize the personal information to enable the consumers to better respond to the theft of their personal information.

Comment: The original draft principle 2 is captured in our suggested edits to principle 1. We proposed a new principle because insurers and producers have a responsibility to policyholders, applicants and claimants to inform these consumers of the specific personal information maintained by the insurer or producer on a periodic basis and in the event the personal information is stolen from the insurer or producer. The disclosure to consumers should itemize the personal information to enable the consumers to better respond to the theft of their personal information. The addition of this principle is essential to presenting a balanced approach that considers the interests of all stakeholders – those whose personal information is collected and at risk and those responsible for protecting that information.
Principle 3: Insurance regulators have a significant role and responsibility in protecting the confidential sensitive information of insurers, producers and consumers maintained in insurance departments and at the NAIC and to quickly alert consumers, insurers and producers when that confidential information has been stolen from the insurance department or the NAIC.

Comment: We suggest replacing “sensitive” with “confidential” since there are statutory requirements regarding protection of confidential information and confidential information is the terminology used in state open records laws. We also suggest state regulators have a responsibility both to protect the confidential information and to alert entities in the event of a data breach.

Principle 4: Insurance regulators recognize the value of collaboration in the development of regulatory guidance with insurers, insurance producers, consumers and the federal government with the goal of a consistent, coordinated national approach.

Comment: “Recognizing the value” is not a principle. The recognition of the need for collaboration is reflected in action, such as exposing this document for comment as well as the other substantive principles requiring collaboration.

Principle 5: Compliance with cybersecurity regulatory guidance must be flexible, scalable, practical and consistent with the national efforts embodied in the National Institute of Standards and Technology (NIST) framework.

Comment: It is unclear what it means for compliance with regulatory guidance to be “flexible, scalable and practical.” If these terms have substantive meaning, then the document should provide some explanation of the terms. In any event, compliance should ensure reasonable protection of personal consumer information. If such efforts are not “practical” for the insurer or producer, then the insurer or producer should not be collecting and maintaining the information.

Principle 6: Regulatory guidance must consider the resources of the insurer or insurance producer.

Comment: This principle is taken from SIFMA and reflects the one-sided perspective of SIFMA. Regulatory guidance should consider the potential harm to consumers. If the insurer or producer does not have the resources to protect consumers’ personal financial information, the insurer or producer should not be holding that information.
**Principle 7:** Effective cybersecurity guidance must be risk-based and threat-informed.

Comment: This principle is taken from SIFMA. While the terms “risk-based and threat-informed” are catchy, it is unclear what they mean or how they would shape regulatory guidance. Unless these terms are defined or translated into meaningful language, the principle should be deleted.

**Principle 8:** Insurance regulators should provide appropriate regulatory oversight, by auditing insurer and producer cybersecurity capabilities that go beyond the use of checklists or other self-reporting mechanisms which includes but is not limited to, conducting risk-based, value-added financial examinations and/or market conduct examinations regarding cybersecurity.

Comment: The terms “risk-based” and “value-added” are taken from SIFMA. It is unclear what “value-added” means in terms of examinations or who would perform that calculation. The core concept of the SIFMA principle (upon which this language is based) refers to the use of audits instead of check lists. We agree.

**Principle 9:** Planning for crisis response for insurance regulators, insurers, and insurance producers is an essential component to an effective cybersecurity program.

**Principle 10:** The effective management of cybersecurity by third parties and service providers used by insurers and producers is essential for protection of consumer’s sensitive personal health and financial information.

**Principle 11** Information sharing is important for risk management purposes; however, it must be limited to essential cybersecurity information and protect sensitive confidential information. 

Comment: It is unclear what parties are included in the information sharing in this principle or what is means to limit sharing to “essential cybersecurity information.”

**Principle 12** Cybersecurity risks should be included and addressed as part of an insurers and insurance producers Enterprise Risk Management processes.

**Principle 13** High level information technology internal audit findings should be discussed at the insurers and insurance producers Board of Director meetings.

**Principle 14** It is essential for insurers and insurance producers to join Financial Services Information Sharing and Analysis Center (FSISAC) to share information and stay informed about cyber and physical threat intelligence analysis and sharing.

**Principle 15** Sensitive data collected, stored and transferred inside or outside of an insurer’s or insurance producer’s network should be encrypted.
Principle 16 Periodic and timely training for employees of insurers and insurance producers regarding cybersecurity issues is essential.

Principle 17 Enhanced market regulation/solvency oversight is needed for insurers selling cyber insurance to businesses and families.

Comment: As opposed to enhanced solvency oversight tools for cyberthreats, it is unclear why enhanced solvency oversight is needed for cyberinsurance, what makes cyberinsurance a unique threat to insurer solvency or why traditional solvency oversight tools are inadequate for cyberinsurance. On the other hand, since some existing commercial policies currently provide some coverage for cyberliabilities, and new products are emerging that are advertised to provide insurance specifically for data breaches, enhanced market regulation/product oversight seems imperative. We have seen the sale of useless “identify theft” products to vulnerable consumers barraged with warnings about the harms of identity theft. Our concern is as great or greater for small and medium-sized businesses purchasing new cyberinsurance coverage. The fact that cyberinsurance is a new product in an area with limited understanding by personal and commercial policyholders calls for enhanced market regulation, including careful review of policy contracts to ensure they provide substantive coverage, are not deceptive and are not duplicative of existing coverage from other commercial policies.

Principle 18 Insurance regulators should collect additional data related to on the sale of cyber insurance product sales, claims and reserving practices to ensure effective prudential and market conduct oversight should be collected to assist insurance regulators with oversight of financial and market regulation.

Comment: We suggest revised wording to make it clear that insurance regulators should be collecting information and that the data should cover more than sales.
Ms. Pam Simpson  
National Association of Insurance Commissioners  
444 North Capitol Street NW,  
Suite 700  
Washington, DC 20001

By email to: psimpson@naic.org

Dear Ms. Simpson:

Thank you for the opportunity to comment on the draft comprehensive cyber-security regulatory principles for insurance operations described in the NAIC’s recent press release.

In general, we believe that the current focus by policy makers on post-cyber breach policies, as well as on information sharing misses the broader historical lessons learned by the insurance industry and government when presented with new technology and devices that bring great advancements, but also the potential to cause great harm.

When faced with conflicting and confusing data, it may help put the current cyber breaches into historical context, to give policy makers such as yourselves a familiar framework.

We believe the historic role of the insurance industry in effecting change and safety regarding the widespread use of new technology must be considered when weighing options about how the insurance industry responds to the cyber safety crisis our nation now faces.

Firewalls came about after the second time most of Chicago burned to the ground. The prevalence of many more fire stations or fire alarms did not prevent the second burning of the city. It was only after brick walls between the buildings (firewalls) were mandated by building codes, that the row house fires were contained.

As you know, there are no software or firmware building codes. There have been detailed and successful drafts of such codes that could be adapted for all code, most recently by Dr. Carl Landwehr of George Washington University regarding medical devices, which is linked to here and on the last page of this letter.

Please find presentation titled “Supply Chain Security,” linked to here, with specific examples of hundreds of known security vulnerabilities in a networked medical device currently used in hundreds of hospitals now in the U.S.
When electric appliances first appeared, their safety problems were widely reported and the public demanded action. Thus, Underwriter Laboratories was created, located in Chicago. As standards were set and enforced, the safety of electric devices increased, and their safety is such that most now consumers do not even consider that such products could be unsafe.

There is no equivalent of a Cyber Underwriter Laboratories to set and promulgate standards for code or any accepted method or place to even test code for vulnerabilities, or approve it’s deployment.

When air travel began and passenger plane crashes increased in frequency and numbers, again, the public demanded action and the National Transportation Safety Board was born. Plane crashes dropped, and air travel has become a safe and trusted mode of travel.

The NTSB came about to understand why these crashes were happening and to create policies to prevent them in the future. It was clear to policymakers at that time that relying on information from the manufacturer or the owner of the planes that crashed was resulting in more plane crashes, not fewer. (Please find attached Chris Wysopal’s presentation of why a cyber version of the NTSB is here and link to the video of the same presentation: https://www.youtube.com/watch?v=glhagb68Sk.)

When automobile crashes began to take lives and a public debate about safety mechanisms and design of automobiles made it a priority for policy makers, The Insurance Institute for Highway Safety (IIHS) and The Highway Loss Data Institute (HLDI) were formed in response to demand by the public about the safety of every make and model of car sold in the United States. The fact that every vehicle sold has a safety test rating, which is based on repeated tests and scientific data, contributes greatly to the improving safety of every vehicle.

For a credible cyber security rating that is trusted by the public, an independent testing facility and rating system needs to be established.

The historic response to new technology and demands for safety, as well as the role of the insurance industry to set, maintain, promulgate and effectively enforce those standards has been a great historic success.

None of these mechanisms are in place in the software industry, and none of these mechanisms are the focus of policy makers.

Unfortunately, the historic role of preventing disasters and loss of life by the insurance industry has largely been ignored in the debate about cyber security.
Virtually all legislative and policy attention has been centered around what happens after a breach, not on preventing them in the first place.

The Single Greatest Factor in Preventing Cyber Breaches

The Massachusetts Institute of Technology recently concluded that eighty percent of the cyber breaches in 2014 were caused by published, known vulnerabilities in code that were not patched.

Other estimates put the breaches because of already known vulnerabilities at forty-four percent, or ninety-nine point nine percent.

No one really knows whether the number is half, eighty percent or virtually all of the recent breaches were because of known vulnerabilities that were not patched. This lack of precision on this point is an indication of exactly how nascent we are in addressing the expensive problem of cyber breaches (one recent industry estimate put the annual cost of cyber breaches at nearly half a trillion dollars.)

We are aware that the lack of specific data means that meaningful policies to insure against breaches are impossible to underwrite. This lack of analysis and data regarding breaches argues, in our view, for a review of the policy options we have outlined above.

The First Cornerstone Building Code: Reduce Known Vulnerabilities

Outside of the historic policy options that could be modified to help prevent cyber breaches, we believe that MIT is correct in their assessment that the number one cause of breaches is known vulnerable code that is not patched.

From the perspective of a hacker, why not try all the known vulnerabilities, before having to reinvent the wheel and start from scratch to find a completely new, and unknown vulnerability?

In the article titled “Almost to Big to Fail,” by Dan Geer, CISO at In-Q-Tel and Joshua Corman, CTO of Sonatype (linked to here) they found that “more than half (59%) of the vulnerable base [open source] components remain unrepaid.” Of the 41% that were repaired, the Mean Time To Repair (MTTR) was 390 days. This finding is as stunning as it is disturbing.

There is a movement within highly regulated financial and aerospace industries to no longer tolerate known vulnerabilities in any code they purchase.

Further, with many of these companies in the financial industry leading the way, they are forcing their own software supply chain to comply with this no known vulnerabilities standard.
To illustrate the pervasiveness of just how many known vulnerabilities can exist in either software or firmware -- from which hackers can exploit and launch all manner of attacks such as denial of service, malware injection, ransom ware, data exfiltration or any of the other well known attacks -- please find linked to here and at the end of this letter, a second Codenomicon presentation on the number of known vulnerabilities in various devices.

**The Second Cornerstone Building Code: Patchability**

In addition to illustrating the widespread nature of these known vulnerabilities, pay close attention to the Codenomicon graph that shows devices become more infected with vulnerable code over time, and what happens if they are not patched, or are not designed to be patchable.

Code with no known vulnerabilities when it is deployed will soon become vulnerable as components or binaries of open source code that was used, become known to contain newly discovered vulnerabilities.

Thus, making all software or firmware patchable is the second key software building code. This will allow software with no known vulnerabilities remain so over time. For example, today there are still 300,000 Internet facing devices with the vulnerable Heartbleed software component. It is likely that these devices cannot be patched, because the Heartbleed component is in firmware. These devices will remain Heartbleed infected until the device is replaced.

**The Third Cornerstone Building Code: Consistent Patching of Software as Vulnerabilities become Known**

For organizations with hundreds of thousands or millions of lines of code in their business operations, it is essential that they keep a bill of materials of all the binaries, including their version number, so that every binary can be catalogued and checked as new vulnerabilities are announced daily by the National Institute for Standards and Technology’s National Vulnerability Database.

Safercar.gov is a website that allows consumers to be informed and track a car part that has become known to be defective. (These parts are recalled so the car can be fitted with a non-defective, safe part.) Software programmers regularly use components built by someone else in their software. But consumers have no visibility into what those third party binary software parts are, or which parts have become known to be defective since the software was published and purchased.

It is important that a process be encouraged to replace defective software components discovered after the software is purchased or published. This way,
consumers, businesses and governments can be protected from breaches based on known vulnerabilities that are discovered after the software is published.

There is no “auto update” process, like exists for your laptop or phone, for a third party or open source binary component that has become known to be defective to be replaced. Only by checking new announcements of components that have become known to be vulnerable, and comparing those announcements against the bill of materials of components used, will consumers, business or the government know they have a component that has become known to be vulnerable, which they must patch with the non-vulnerable version. Software operators have a need to know when their software or devices become vulnerable to being breached.

Federal legislation was introduced in the U.S. House December 2014, which can be easily adopted by states to effect these three key building codes of no known vulnerabilities and Patchability – H.R. 5793, The Cyber Supply Chain Management and Transparency Act (attached).

We urge NAIC to consider these policy and software building code suggestions, as you work to broaden the positive impact of the insurance industry on preventing future cyber breaches.

The current situation when insurance policies focus on payouts associated with events after the breach – such as notification costs, credit card replacement costs – must give way to insurance policies that insure against the billions of dollars lost from cyber breaches. This means that meaningful data about how to underwrite policies for specific businesses must be in hand, and trusted neutral entities must exist to gather and analyze such data, as well as to make their findings public through ratings or a Cyber Labs seal of approval.

Sincerely,

Wayne Jackson, CEO, Sonatype
David Chartier, President, Codenomicon
Chris Wysopal, Co-Founder and CTO, Veracode
Mike Ahmadi, Global Director, Critical Systems Security, Codenomicon
Joshua Corman, CTO, Sonatype
Dan Perrin, Executive Director, The Council to Reduce Known Cyber Vulnerabilities
The Council to Reduce Known Cyber Vulnerabilities is applying for its 501 (c) 4 status.

Links to Attachments:

*Building Codes for Medical Devices*

*Supply Chain Security*

*NTSB for Cyber*

*Geer and Corman on Known Open Source Vulnerabilities*

*Codenomicon Briefing on Known Vulnerabilities in Medical Devices, Federal Government Workstations and Routers*
March 16, 2015

Thanks for the opportunity to comment.

I would like to see Principle 5 changed to allow for more than one framework to be used or identified.

Principle 5: Compliance with cybersecurity regulatory guidance must be flexible, scalable, and practical. Usage and compliance with a framework such as NIST, ISO 27001, CoBIT, etc. should be utilized to ensure controls are in-place and effective.

Thanks,

Mark
I agree with Insurance regulator and Insurance company jointly owning responsibility to protect sensitive data.

I also think we should also have mechanisms that older insurance data is removed from storage spaces after it has lost its utility. It should be insurance company and their vendors responsibility that older insurance data (maybe > 5 years or > 10 years) must be removed and permanently destroyed. To this effect this language should be added in the legal contracts signed between insurance company and its vendors. Not doing this could unnecessarily lead to following

1) Data could be prone for more cyber attacks as most of this data would be secured on various formats (tapes, servers, FTP) and will mostly be un-encrypted

2) 5 year back dated data might not be too useful to assess current risks

3) Will not be compatible with Solvency II rule

4) Unnecessarily expense (storage space, IT maintenance cost) for insurance company and the vendors

Regards,
Deeksha Gupta
Response to NAIC Draft
“Principles for Effective Cybersecurity Insurance Regulatory Guidance”

2015-03-22
by

Fearless Security

Table of Contents
Response to NAIC’s Draft.................................................................2
NAIC’s Principles for Effective Cybersecurity Insurance Regulatory Guidance........3
How Fearless Security helps realize these principles.................................10
The insurance industry is uniquely positioned to positively influence the cyber security deployed by US enterprises, and therefore the overall security of the nation.

Fearless Security, LLC (“Fearless”) currently provides assessment, actuarial, and other services associated with Cyber Security Insurance. Fearless provides these services in association with Ridge Global Insurance Solutions, backed by Lloyds of London consortium members, and through other means. Our executives are involved with many public and private sector efforts in this area.

This document is presented in two parts.

- In the first part we have provided commentary on each of the 18 Principles laid out in “Principles for Effective Cybersecurity Insurance Regulatory Guidance”.
- In the second part, we map the 18 principles to the processes Fearless Security currently uses.

The NAIC has an important role is guiding developments in this area. We welcome the opportunity to provide further assistance to the NAIC in these efforts.

A note on regulatory vs. business risk

Businesses respond to risks based, among other things, on management perceptions of urgency and importance. Tactical business risks are dealt with every day, and executives generally understand them. Regulatory risks are an artifice created by government and, from the perspective of most business executives, alter the natural risk conditions of the business. As such, regulations perform a public policy function. They benefit businesses and the public only to the extent that they alter the risks perceived by management in ways that benefit the public and the business. However, in artificially changing the risk management process, they sometimes favor things that harm businesses and the public.

- **Example:** A seemingly sensible regulation requiring the use of antivirus software and up-to-date patching may cause increased failure rates and very high costs in manufacturing systems, which are often not susceptible to the same weaknesses as more common computers, and which require recertification before continuity of operations when such changes are made.

The problem is that regulations often fail to account for such subtleties. It is necessary that regulations be prescriptive in order to have effect, and yet regulatory risks often end up prioritized over other business risks. This causes increased business and operational failures and does not benefit the public or the business. The strategic value of regulation must be understood in context to gain its rewards while not increasing other risks.
NAIC’s Principles for Effective Cybersecurity Insurance Regulatory Guidance

The National Association of Insurance Commissioners (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 five U.S. territories. Through the NAIC, state insurance regulators establish standards and best practices, conduct peer review, and coordinate their regulatory oversight. NAIC members form the national system of state-based insurance regulation in the U.S.

NAIC has coordinated two drafts which will provide comprehensive policy for oversight of insurance regarding cybersecurity:

The first is a draft of **Principles for Effective Cybersecurity Insurance Regulatory Guidance**, developed by the Cybersecurity (EX) Task Force. This document will help state insurance departments identify uniform standards, promote accountability, and provide access to essential information. It also outlines the process for working with the insurance industry to identify risks and offer practical solutions.

The second draft document: **Annual Statement Supplement for Cybersecurity policies**, comes from the NAIC’s Property and Casualty Insurance Committee.

There are 18 draft principles in the first document. Here they are along with details on how Fearless Security assessment processes help address these principles.

**Principle 1. Insurance regulators have a significant role and responsibility regarding protecting consumers from cybersecurity risks.**

Risk to consumers stem primarily from:

- Malicious actors acting directly against them (e.g., from malware on their PCs, scams coming over the Internet, etc.) and
- Malicious actors acting against businesses they deal with directly or indirectly.

Insurance can act to support both:

- Effective protection of the individuals (e.g., by requiring controls in the end-user systems) and
- Effective protection of individuals by the businesses they deal with.

Insurance does these things by identifying risks and insuring consumers directly against them. However, this can only be effectively done for consumers if the systems they use and the businesses they directly and indirectly depend on act for instead of against the interest of the consumer. These businesses are the ones who gather, retain, act upon, and intermediate almost all of the content and mechanisms that have effects on consumers. It is by leveraging insurance rates, retentions, exclusions, and insurability that insurance causes the costs and consequences to consumers to be laid at the feet of the responsible businesses.

An entire ecosystem must be built in which all businesses are insured and insurers use rates and insurability to mitigate harm to consumers. To do this effectively, risks must be
understood and correlated to business behaviors with mandatory reporting and accurate actuarial systems.

**Principle 2. Insurance regulators have a significant role and responsibility regarding the insurers’ efforts to protect sensitive customer health and financial information.**

The role of insurance regulators is to create conditions in which consumers, businesses, and insurers each play a part in the overall process by which insurance effects a social contract beneficial to all. This is done largely by placing liability on the party responsible for the harm. Rather than assessing individual liability for individual acts, insurance does this by charging all parties a premium related to their contribution to the overall risk. Rates change based on behavior and historical facts.

Insurance companies have a dual role in this. They have to evaluate companies and individuals for risks and determine appropriate rates in the competitive insurance environment, create pools for sharing these risks, and write policies with meaningful coverage. But they should also apply the same rigors to themselves as they do to those they insure.

**Principle 3. Insurance regulators have a significant role and responsibility in protecting the sensitive information housed in insurance departments and at the NAIC.**

The same rigors applied by insurance companies for information protection should be applied to the insurers and regulators.

- Regulators should require those in the insurance industry to undergo the same processes for determining insurability, rates, and retentions for themselves as they apply to their customers. Like their customers, there is no one-size fits all approach, and thus insurers must develop approaches to risk measurement and management suited to the size and nature of the insurance business just as they must do this for their customers in order to have an effective insurance program.

- Regulators should undertake the same processes with regard to their own protective programs that they apply to the insurers and the insured. Just as the same fire regulations for state building apply as those for private structures, the same cyber-security requirements should be applied.

**Principle 4. Insurance regulators recognize the value of collaboration in the development of regulatory guidance with insurers, insurance producers, consumers and the federal government with the goal of a consistent, coordinated national approach.**

No comment here
Principle 5. Compliance with cybersecurity regulatory guidance must be flexible, scalable, practical and consistent with the national efforts embodied in the National Institute of Standards and Technology (NIST) framework.

The NIST framework is a large complex methodology and it has great value in understanding issues. This framework is largely consistent with essentially all other cyber-security frameworks today, including ISO standards covering many related areas. Attaining and demonstrating consistency with this framework, however, holds two major challenges:

• The framework is not prescriptive in identifying areas to be addressed. It does not indicate how areas are to be addressed at a level of specificity allowing decision-makers to make good decisions for their situation.

• The level of complexity of the framework is far beyond that which is readily attainable at large scale today. This is because cybersecurity is a complex subject with many intertwined facets.

The requirement for flexibility and scalability is the key here. The lack of expertise in this field in general is a national-level problem, and in order to meet the needs of millions of business and hundreds of millions of individuals, the only path forward today appears to be the creation of intermediate providers who specialize in this area and develop processes to allow such complex frameworks to be effectively applied by those without the detailed knowledge required to apply them.

This is similar to the area of building codes, wherein the complexities of engineering are met by creating standard approaches and codifying them in a regulatory framework. Some amount of engineering is required, plans have to be submitted, inspections done throughout the process, and so forth. However, the current system of building codes and their application has taken a long time to create and required creating the various levels of expertise over a substantial time frame.

An intermediate process seems appropriate. Insurance companies should be allowed to create such approaches for the near-term and apply them consistent with the NIST or any other similar framework, demonstrating this to the regulatory bodies, but not requiring the whole process be applied to every consumer and business under insurance. A certification process of some sort should allow the insurers to gain approval for processes at different risk levels and the insurers should be required to apply those processes at the appropriate level of detail and scale to the individual business or consumer as and if appropriate.

Principle 6. Regulatory guidance must consider the resources of the insurer or insurance producer.

Any scalable process must address the needs of different sized entities by providing risk-appropriate levels of coverage with resource (time, money, business disruption, etc.) taken into account if that process is to be effective. Processes already exist today for risk assessment and tracking processes for the largest enterprises, mid-cap companies, and small businesses. Resources range from hundreds of thousands of dollars over months of effort with scores of people involved for large enterprises, to tens of thousands of
dollars over a period of 10 days involving 3-5 people for mid-cap companies, to one-hour a month sustained effort over a year for one or two people at small entities at a cost of hundreds of dollars a month. Individuals are currently being addressed with policies through their credit unions or other similar entities based on a minimal checklist and insurance in place for the entities they deal with. If regulations are consistent with the recently developed practices, resources should be within the reach of any and all concerned.

Principle 7. Effective cybersecurity guidance must be risk-based and threat-informed.

Currently available processes used for cyber-insurance have these properties. Insurance guidance merely needs to require their use in order to achieve this objective. However, this is an area where regulatory mandates have historically failed to support adequate flexibility and attempted to apply too much standardization.

- Specific risk assessment and management methodologies have long resulted in fictitious applications of probabilistic risk assessment, often characterized as “a guess multiplied by an estimate taken to the power of an expert opinion”. Insurance companies are experts in the area of risk and recognize that without good data to support processes and the proper surrogates for the actual causes of risks, this approach cannot succeed. This is largely responsible for the failings of current cyber insurance. Unless and until a viable framework for this approach is available, other surrogates will be required, and the actuarial process which is still in its infancy in this arena, will have to be developed and perfected over time.

- Threat information is another area of widespread confusion, as threat actors are often conflated with exploitation of vulnerabilities and consequences to produce scenario-based approaches to threat information. A different approach is needed in order to build a systematic understanding and approach to mitigation of risk based partially on threat. There are also a variety of different threat assessment approached based on resources, situation, and other related factors. While threats should be taken into account, excessive regulatory restrictions would likely do more harm than good.

Principle 8. Insurance regulators should provide appropriate regulatory oversight, which includes but is not limited to, conducting risk-based, value-added financial examinations and/or market conduct examinations regarding cybersecurity.

Having detailed examinations seems highly problematic for regulators. Consider the scale of the potential need. The most appropriate approach in this arena appears to be a combination of random verifications, periodic requirements to provide assessments, ongoing reporting of changes, consumer and customer complaints and reporting processes, survey methodologies, and similar sorts of efforts. The periodicity of these audits should be determined by value at risk and magnitude of potential consequences.
Principle 9. Planning for crisis response for insurance regulators, insurers, and insurance producers is an essential component to an effective cybersecurity program.

While crisis response is certainly an issue to be addressed, perhaps more effort might be reasonable spent in crisis avoidance. This is typically done by reducing common mode failures, disaggregating risks, using risk-appropriate protective approaches, and requiring assessments and similar methodologies appropriate to the risks from individuals, businesses based on size and type, having requirements for insurance similar to those of the automotive industry (where all parties must be insured in order to allow liability to be properly shared and pools are used to disaggregate risks), and other similar methods. Crisis response planning is normally included in effective protection assessments and should be integrated into the overall planning associated with cyber-related risks as part and parcel of the assessment and risk management process.

Principle 10. The effective management of cybersecurity by third parties and service providers is essential for protection of consumer's sensitive personal health and financial information.

While this is the ideal situation, historically it has proven to be ineffective. Rather, an approach based on requiring insurance for 3rd party providers might reasonably be used to help manage those risks. In addition, regulatory mandates regarding outsourcing and data location are reasonable in many cases, and a variety of relevant controls might reasonably be applied. However, in many cases, outsourcing is more effective from a protection standpoint than internal approaches, particularly for organizations that do not have the internal capabilities and expertise for effective protection suitable to the needs of their situation. The limited total pool of experts in this arena drive a need to gain economies of scale in the use of expertise.

Principle 11. Information sharing is important for risk management purposes; however, it must be limited to essential cybersecurity information and protect sensitive confidential information.

Nobody knows what is essential, nor should it be limited in this way if we wish to make progress. It is up to each enterprise to determine what to share with whom and under what circumstances. Furthermore, information sharing is largely about receiving information from outside sources rather than transmitting such information outbound. This is a process being undertaken on a national basis and national or global level sharing is necessary to meet the realities of the information age.

Principle 12. Cybersecurity risks should be included and addressed as part of an insurers and insurance producers Enterprise Risk Management processes.

It is obvious that enterprise risk management must include all risks. If and to the extent there are information-related risks, these must be taken into account.
Principle 13. High level information technology internal audit findings should be discussed at the insurers and insurance producers Board of Director meetings.

This is entirely correct for insurers, insurance producers, and insured enterprises, both public and private. The identification, mitigation, and where appropriate transfer of risk to willing third parties by Boards of Directors is an essential part of responsible organizational operation. For insured enterprises, the requirements of insurers for risk transfer are a key factor in quantifying cyber risks for their boards in that insurance rates imply the utility of mitigation as opposed to transfer and the average cost of acceptance. Risks are typically transferred because they are too large to accept or too expensive to mitigate. Insurers and insurance producers should use the same methods to quantify their own risks as they apply to potentially insured clients.

Principle 14. It is essential for insurers and insurance producers to join Financial Services Information Sharing and Analysis Center (FSISAC) to share information and stay informed about cyber and physical threat intelligence analysis and sharing.

While the FS-ISAC is a useful node in the broader Information Sharing network, and one such node that insurers and insurance producers should reasonably consider having direct and/or indirect involvement with, Information Sharing is a topic with wide implications which should be considered at appropriate depth by insurers and insurance producers.

In order to be properly informed for the purposes of actuarial decisions, to provide for organizational self protection, as well as for the purpose of guiding organizational and industry-wide planning, insurers and insurance producers should take an active role in:

- Determining appropriate sources of external intelligence.
- Creating and maintaining policies for acquisition of external intelligence.
- Developing and maintaining appropriate analytic capabilities for managing external and internal intelligence.
- Developing and maintaining appropriate capabilities to apply external intelligence for protective purposes.

In some cases some insurers and insurance producers may choose to share some direct or derived internal information with external parties, which parties may include:

- Other insurers or insurance providers.
- FS-ISAC or other ISACs/ISAOs.
- Public sector entities.
- Other third parties.

Insurers and insurance providers should establish and maintain processes to determine whether and to what extent any direct or derived internal intelligence is to be shared with external parties, and develop and maintain appropriate policies to enable that internal-to-external Information Sharing to occur in an appropriate fashion.
Principle 15. Sensitive data collected and stored and transferred inside or outside of an insurers or insurance producers network should be encrypted.

Unfortunately, the encryption of all data in motion goes against other US government equities, tends to defeat the intelligence processes in widespread use today, and makes resilience less effective in recovery and forensics processes. Such a requirement may well produce substantial negative unintended consequences and should not be adopted in the present situation. Rather, different combinations of architectural protection are required for different situations.

Principle 16. Periodic and timely training for employees of insurers and insurance producers regarding cybersecurity issues is essential.

Education, training, and awareness programs are all necessary in order to have effective protection. But a mere mandate does not address the specific requirements associated with a particular industry or enterprise. Without additional guidance, this is an open-ended mandate without any teeth or ability to meaningfully perform.

Principle 17. Enhanced solvency oversight is needed for insurers selling cyber insurance to businesses and families.

Without a basis for making such determinations, it is hard to tell whether this is so. If inadequate oversight is in place today there must be a basis for this assertion and none is provided in the NAIC documents to enable an effective response.

Principle 18. Additional data on the sale of cyber insurance products should be collected to assist insurance regulators with oversight of financial and market regulation.

To the extent that inadequate data is now available, regulators should seek to attain it. However, it is unclear what data of use to regulators insurance companies have or could readily produce. In addition, various regulatory mandates and contractual limitations on such data may exist.
How Fearless Security helps realize these principles

Fearless Security provides specification and verification of information protection. This capability is currently used by insurance providers to determine insurability, retentions, premium rates, and exclusions.

Commentary on the principles

Principle 1. Insurance regulators have a significant role and responsibility regarding protecting consumers from cybersecurity risks.

The key to meeting the need to identify risks and insure against them is to mitigate the interdependent risk associated with the businesses and organizations they deal with. This means that effective protection depends on creating an ecosystem of adequately protected businesses and spreading insurance risk across that ecosystem. This in turn implies the need to insure a large number of entities per state. Scalability then becomes a major limitation to assessing and mitigating risks.

- Fearless has the only scalable process known to be available today that can bring mid-cap companies assessments necessary to support cyber insurance at a reasonable level of fidelity and scale to very large volumes for small and medium business.

Determining insurance rates, retentions, exclusions, and insurability requires an actuarial process that doesn't exist yet today.

- Fearless has the capacity to collect information on events as they transpire, associate those events to protection architecture at the individual entities undergoing those events, and relate insurance outcomes to rates, protective measures, and outcomes over time. While this does not instantly translate into actuarial quality decision-making data, over time, the collection of this data will enable such determinations.

Principle 2. Insurance regulators have a significant role and responsibility regarding the insurers’ efforts to protect sensitive customer health and financial information.

Fearless provides assessments to enterprises of all sizes. Thus, for small and medium insurers, Fearless is an ideal candidate to provide scalable assessments. For larger entities, Fearless works with firms that undertake larger-scale assessments to meet the needs of that segment of the industry.

Standard assessments include coverage of a wide range of issues that relate to the protection of sensitive customer health and financial information, but there are many other protection objectives and consequences that also have to be dealt with and that insurance must cover to effectively protect businesses against malicious acts. A wide range of these are addressed in protection assessments required for and undertaken on behalf of insurers by Fearless.

Principle 3. Insurance regulators have a significant role and responsibility in protecting the sensitive information housed in insurance departments and at the NAIC.
Fearless and our partners can offer similar services to regulators and other government agencies, however, many of the requirements of government differ significantly from business and, as such, many areas of assessments will produce different outcomes.

**Principle 4. Insurance regulators recognize the value of collaboration in the development of regulatory guidance with insurers, insurance producers, consumers and the federal government with the goal of a consistent, coordinated national approach.**

We believe that Fearless can help develop and promote meaningful approaches and frameworks and that a standard of practice approach is the best current approach to meet these needs. However, if government regulations mandate frameworks, as they historically have done in other areas, the results are likely to be less effective protection of the public welfare. This is because there is a lack of consensus today as to the most effective protective measures, and the unpredicted side effects of premature, excessive, or politically driven guidance are most often to delay rather than assist in moving industry forward. Furthermore, unless and until adequate actuarial data is available, the consequence of such guidance may be to make poor decisions about risk and put entire risk pools at higher risk.

**Principle 5. Compliance with cybersecurity regulatory guidance must be flexible, scalable, practical and consistent with the national efforts embodied in the National Institute of Standards and Technology (NIST) framework.**

The Fearless approach is consistent with NIST guidelines in many ways, however there are substantial variances form NIST frameworks associated with specifics which do not apply in specific circumstances. “One-size-fits-all” approaches are not suitable to the wide range of industries and business models in the marketplace today, and seeking to force commonality has a tendency to create common mode failures of protection rather than a resilient protection program and approach. The Fearless approach takes into account individual businesses and situations and uses expert judgment combined with methodologies that adapt over time. This is something government frameworks are historically poor at doing.

**Principle 6. Regulatory guidance must consider the resources of the insurer or insurance producer.**

The Fearless approach is scalable to handle all sizes of enterprises and produce meaningful results for individual enterprises or risk pools. In the case of risk pools, groups of 100 businesses are handled together, allowing more cost-effective approaches that assess and adapt over longer time frames and limit risk aggregation while providing rate reductions for those with fewer negative outcomes and better protective schemes in place. These processes also help to educate and train business leaders on the issues they need to address to reduce risks and insurance rates while gathering information needed for actuarial calculations. This service also provides updates to help businesses and consumers meet the changing landscape of malicious cyber-related activity.

**Principle 7. Effective cybersecurity guidance must be risk-based and threat-informed.**

The Fearless assessment approach includes identifying consequences, vulnerabilities, and threats, and puts this in the context of the market and situation at large as well as in the context of the specific business. Effective protection should also inform businesses
and consumers of threats and how to deal with them, and the support services offered by Fearless provide just such value.

**Principle 8. Insurance regulators should provide appropriate regulatory oversight, which includes but is not limited to, conducting risk-based, value-added financial examinations and/or market conduct examinations regarding cybersecurity.**

Fearless can provide a framework for such assessments, however, we work for clients having assessments undertaken and not for 3rd parties. While we can work through 3rd parties, we maintain independence from products, vendors, and all other parties who are not our clients.

**Principle 9. Planning for crisis response for insurance regulators, insurers, and insurance producers is an essential component to an effective cybersecurity program.**

Fearless includes such issues in its standard assessment approach, along with many other issues that are also important. Unless and until we, as a national insurance industry, make progress on actuarial data and related feedback mechanisms, choosing what to emphasize seems premature. Historical data suggests that crises are fairly rare in the cyber-arena while day-to-day activities have higher aggregate consequences.

**Principle 10. The effective management of cybersecurity by third parties and service providers is essential for protection of consumer’s sensitive personal health and financial information.**

This is why an entire ecosystem must be created and insurance used across the a wide range of activities and business types. Uninsured risks related to 3rd party liability should be allowed as exclusions in order to assure that 3rd parties either gain insurance and join risk pools or take responsibility for the acts they undertake. But in order to accomplish this, it is necessary to have a scalable process, which Fearless offers.

**Principle 11. Information sharing is important for risk management purposes; however, it must be limited to essential cybersecurity information and protect sensitive confidential information.**

The insurance industry offers a unique opportunity for information sharing. Insurers have a requirement to gain information on events that take place and their customers have a requirement to provide such information (1) to provide adequate notice to insures who have right to act to mitigate risks in a timely fashion, and (2) to provide details on protective measures in place and allow insurers to make decisions about retentions, rates, and insurability. The combination of motivation to report events (in order to assure coverage) and the requirement to provide protective measures (as a condition of insurance in order to truthfully provide information necessary to make determinations) leads to a unique trusted position in assessing the utility of protective mechanisms and architectures not available elsewhere. Neither of these typically involve providing sensitive details such as identifying information, but all require reporting on incidents and protective measures, which are generally considered sensitive.

The Fearless approach combines assessment with reporting and actuarial analysis to provide for this information collection. Sharing outbound from businesses happens when Fearless provides aggregated information and advice to clients and as rates become dependent on outcomes and protective measures. Insurers in general, and those who
work with Fearless in particular, gain the advantages of these methods and fused information.

**Principle 12. Cybersecurity risks should be included and addressed as part of an insurers and insurance producers Enterprise Risk Management processes.**

The Fearless approach does just this by putting information-related protective decisions in the context of the enterprise. This is necessary both to support the enterprise risk management process as a whole and to inform the information protection function, which must link to the business objectives in order to be meaningful within the context.

**Principle 13. High level information technology internal audit findings should be discussed at the insurers and insurance producers Board of Director meetings.**

Fearless assessments are developed with the objective of providing meaningful information to executive management. Our assessments also evaluate the management process, which includes requirements for the position, influence, and observability of the protection management function and the integration of enterprise duties into the protection functions. Thus it both considers reporting to the board and executive management, and it requires top management participation in controlling and managing the protection program and mandates proper separation of duties to mitigate intentional subversion by management.

**Principle 14. It is essential for insurers and insurance producers to join Financial Services Information Sharing and Analysis Center (FSISAC) to share information and stay informed about cyber and physical threat intelligence analysis and sharing.**

Fearless gains information from many sources, and this particular source is not the only one appropriate for insurers. We also provide information to clients and insurers as part of the aggregation and analysis process associated with actuarial data collection and analysis.

**Principle 15. Sensitive data collected and stored and transferred inside or outside of an insurers or insurance producers network should be encrypted.**

Fearless has policies driven by our standard of practice approach that deal with encryption. Sensitive data is normally encrypted in motion, however, encryption in use and storage is often problematic as it limits recovery from common failures such as partial disk outages, increases dependencies on systems that are not as trustworthy as the mechanisms used to protect unencrypted data, creates unnecessary and potentially harmful interdependencies on 3rd party providers who have proven unreliable in the past, and produces many other undesired effects. In addition, some data paths do not have adequate protection but must be used by government mandate, and our standard of practice, which we follow, includes other methods more suitable to specific situations.

**Principle 16. Periodic and timely training for employees of insurers and insurance producers regarding cybersecurity issues is essential.**

The Fearless assessment approaches help to define proper training, awareness, and educational programs and the management of these programs in the context of use.

**Principle 17. Enhanced solvency oversight is needed for insurers selling cyber insurance to businesses and families.**
The question of what those requirements should be must reasonably be determined by information not yet available. Fearless is in the process of collecting such information as it works with insurers to allow them to identify specific solvency requirements associated with reasonable expectations of potential outcomes.

**Principle 18. Additional data on the sale of cyber insurance products should be collected to assist insurance regulators with oversight of financial and market regulation.**

Fearless supports mandatory reporting requirements associated with insurance providers so long as these do not violate client confidentiality, contractual, or other legal obligations.

**Mapping the Fearless Standard of Practice to the Principles**

To get a sense of the nature and complexity of these issues and how the Fearless assessment processes currently employed by insurers supports these, the following approximate mapping of elements of the Fearless SoP to the principles is provided. Note that this mapping takes a minimalist approach in that it identifies the direct links between elements of assessments to the principles. In many cases the entire Standard of Practice applies indirectly to the issues.

**Principle 1. Insurance regulators have a significant role and responsibility regarding protecting consumers from cybersecurity risks.**

Interdependencies and related risks include, without limit:

- Overarching: Location: Where are content and work located?
- Overarching: Security consultants: When are information security consultants used?
- Overarching: Mobility: What part and portion of the workforce is mobile?
- Overarching: Outsourcing people: What part and portion of the workforce is outsourced?
- Overarching: Outsourcing things: When is information technology outsourced?
- Business modeling: What are the business functions and what information do they depend on for what?
- Risk Management: Threats: What threats have been identified, what are their characteristics and relevant history?
- Risk Management: Vulnerabilities: How and when are information-related vulnerabilities assessed?
- Risk Management: Risk aggregation: What process is used to identify and control the aggregation of risks?
- Risk Management: Separation of Duties: How should duties be separated?
- Risk Management: Interdependencies: How are supply chain risks managed?
- Risk Management: Interdependencies: How are real-time interdependency risks managed?
- Risk Management: Changing systemic risks: How is changing systemic risks managed?
- Risk Management: Changing subsystem risk and surety: How are risk and surety changes of a subsystem handled?
- Control Architecture: Trust model: How is trust assessed and managed?
Fearless has the capacity to collect and analyze data from businesses and produce actuarial quality decision-making data. This is done through a process involving training businesses in what to report and how to report it, and acting to assist them in such collection through the assessment and ongoing support process.

**Principle 2. Insurance regulators have a significant role and responsibility regarding the insurers’ efforts to protect sensitive customer health and financial information.**

The Fearless approach covers a wide range of issues within an overarching model of the enterprise and protection-related issues. This is represented at a high level by the following diagram:
Protection objectives typically identified include:

- Integrity
- Availability
- Confidentiality
- Accountability
- Use controlled Transparency
- Custody

There are also many consequences identified with protection-related failures affecting these objectives, many of which are covered in different ways under different insurance policies. These are identified and supported, in part, through the following elements of the assessment process:

- Overarching: Business: What is the nature of the business?
- Overarching: Promises: What promises does the business make, to whom, and why? How do they relate to information?
- Overarching: Content: What content does the enterprise have and what are the consequences of protection failures?
- Overarching: Insurance: What coverage does the enterprise have/want and what are the consequences of protection failures (Brit)?
• Business modeling: What are the business functions and what information do they depend on for what?
• Oversight: What does enterprise oversight provide to the protection program to define duties to protect?
• Oversight: How are different sorts of duties prioritized in determining what to protect and how well?
• Risk Management: Risk management process: What risk assessment processes are used?
• Risk Management: Risk definition: How are risk levels for the protection program defined?
• Risk Management: Risks: When does the enterprise avoid, accept, transfer, and mitigate information-related risks?
• Risk Management: Risk aggregation: What process is used to identify and control the aggregation of risks?
• Risk Management: Interdependencies: How are supply chain risks managed?
• Risk Management: Interdependencies: How are real-time interdependency risks managed?
• Risk Management: Failsafes: When failsafes are required and how are they determined?
• Management: Incident handling: How are incidents managed?
• Management: Legal issues: How do legal issues interact with protection management?
• Control Architecture: Objectives: What are the protection objectives and how are they applied??
• Control Architecture: Change management: How are changes to information technology managed?
• TechArch: Inventory: What information protection-related inventory is kept and in what form(s)?
• TechArch: Metadata: What Metadata should be ingested, created, retained, and presented?
• TechArch: Lifecycles: What aspects of lifecycles are considered in the protection program and its processes?
• Incidents: Detection: Are intrusions detected, and if so, how?
• Incidents: Malicious Alteration Detection: How is malicious alteration detected?
• Incidents: Detection and response: What are the process requirements for detection and response?
• Content control: How is harmful and useless content controlled in my computing environments?
• Content control: What mechanisms keep control over content with business utility?
• Content control: Version control: How are versions of data over time protected?
• Content control: How is intelligence gathering countered?
• Content control: How is intellectual property protected?
• Redundancy: Business continuity and disaster recovery: What information resources are where?
• Redundancy: Interdependencies: How is redundancy applied to interdependent mechanisms?
• Redundancy: Data history redundancy: How many copies of data history should be retained, where, and for how long?

Principle 3. Insurance regulators have a significant role and responsibility in protecting the sensitive information housed in insurance departments and at the NAIC.

Fearless processes apply writ large to this area.

Principle 4. Insurance regulators recognize the value of collaboration in the development of regulatory guidance with insurers, insurance producers, consumers and the federal government with the goal of a consistent, coordinated national approach.

Fearless is highly supportive of developing and promoting meaningful approaches and frameworks. Today, we believe that the standard of practice approach is the best way forward, and that is works well with existing regulatory and national approaches. However, if and to the extent regulation comes too quickly or fails to take the factors identified in this document into account, there is a chance that such regulations will make effective approaches moot. We urge regulators to consider these approaches and issues in their considerations.

Principle 5. Compliance with cybersecurity regulatory guidance must be flexible, scalable, practical and consistent with the national efforts embodied in the National Institute of Standards and Technology (NIST) framework.

The Fearless approach takes into account individual businesses and situations and uses expert judgment combines with methodologies that adapt over time. Specific areas addressing such standards include, without limit:

• Overarching: Business: What is the nature of the business?
• Overarching: Content: What content does the enterprise have and what are the consequences of protection failures?
• Oversight: What does enterprise oversight provide to the protection program to define duties to protect?
• Oversight: Duties analysis: How is duty to protect analyzed?
• Risk Management: Risk management process: What risk assessment processes are used?
• Management: Policy: What information security policies are needed and used?
• Management: Standards: Which widely used control standards are best suited to the enterprise?
• Management: Legal issues: How do legal issues interact with protection management?

The Fearless process also addresses areas that existing standards do not address but that have substantial relevance to risks and insurance decisions.

Principle 6. Regulatory guidance must consider the resources of the insurer or insurance producer.

Service offerings and their scalability constraints are as follows as of this writing:

• Mid-cap initial assessment capabilities readily are scalable by end of 2015 to thousands of assessments per year and to tens of thousands the following year.
• Small-entity risk pools of 100 businesses assessed over longer time frames are scalable to tens of thousands of entities in 2015 and hundreds of thousands the following year.

Resource limitations associated with costs are also quite low relative to alternatives. Small entity pools are typically covered for less than $350/mo/entity, while mid-cap entities are covered at less than $50,000 per entity and $60,000/year for ongoing support. This is well within the budget of almost all entities of these sorts.

**Principle 7. Effective cybersecurity guidance must be risk-based and threat-informed.**

Consequences, vulnerabilities, and threats, in the context of the market and situation at large as well as in the context of the specific business are covered in the following assessment elements as well as by the overall assessment process:

• Overarching: Business: What is the nature of the business?
• Overarching: Promises: What promises does the business make, to whom, and why? How do they relate to information?
• Overarching: Content: What content does the enterprise have and what are the consequences of protection failures?
• Overarching: Insurance: What coverage does the enterprise have/want and what are the consequences of protection failures?
• Risk Management: How does the enterprise do risk management?
• Risk Management: Risk management process: What risk assessment processes are used?
• RM0 Risk Management: ICS Risk management process: What risk assessment processes should be used?
• Risk Management: Risk definition: How are risk levels for the protection program defined?
• Risk Management: Threats: How are information-related threats assessed?
• Risk Management: Threats: What threats have been identified, what are their characteristics and relevant history?
• Risk Management: Threats: What design basis threat is used?
• Risk Management: Threats: What attack mechanisms are considered?
• Risk Management: Vulnerabilities: How and when are information-related vulnerabilities assessed?
• Risk Management: Risks: When does the enterprise avoid, accept, transfer, and mitigate information-related risks?
• Risk Management: Risk aggregation: What process is used to identify and control the aggregation of risks?
• Risk Management: Separation of Duties: How should duties be separated?
• Risk Management: Interdependencies: How are supply chain risks managed?
• Risk Management: Interdependencies: How are real-time interdependency risks managed?
• Risk Management: Costs: How is security budgeted?
• Risk Management: Surety matching: How is surety matched with risk?
• Risk Management: Failsafes: When failsafes are required and how are they determined?
• Risk Management: Changing systemic risks: How is changing systemic risks managed?
• Risk Management: Changing subsystem risk and surety: How are risk and surety changes of a subsystem handled?

Many of the other elements of the standards of practice include decisions driven by risk-related issues including consequences and threats.

Principle 8. Insurance regulators should provide appropriate regulatory oversight, which includes but is not limited to, conducting risk-based, value-added financial examinations and/or market conduct examinations regarding cybersecurity.

Fearless open source standards of practice can be used by anyone wishing to do so.

Principle 9. Planning for crisis response for insurance regulators, insurers, and insurance producers is an essential component to an effective cybersecurity program.

Fearless includes such issues in its standard assessment approach including, without limit:

• Overarching: Promises: What promises does the business make, to whom, and why? How do they relate to information?
• Overarching: Content: What content does the enterprise have and what are the consequences of protection failures?
• Oversight: What does enterprise oversight provide to the protection program to define duties to protect?
• Risk Management: Surety matching: How is surety matched with risk?
• Risk Management: Failsafes: When failsafes are required and how are they determined?
• Management: Testing: What does the testing function do and cover?
• Management: Incident handling: How are incidents managed?
• Incidents: Detection: Are intrusions detected, and if so, how?
• Incidents: Response: Who controls and executes responses to information-related attacks?
• Incidents: Detection and response: What are the process requirements for detection and response?
• Redundancy: Fault model: What fault model is assumed for analysis of redundancy?
• Redundancy: Backups: What is backed up and how often?
• Redundancy: Storage location: Where and in what sort of containers are backups stored?
• Redundancy: Data center redundancy: How many data centers are required?
• Redundancy: Redundant facility distance: How far apart are redundant data centers and people to assure continuity?
• Redundancy: Business continuity and disaster recovery: What information resources are where?
• Redundancy: Interdependencies: How is redundancy applied to interdependent mechanisms?
• Redundancy: ICS Backups: What should be backed up and how often?
• Redundancy: Data history redundancy: How many copies of data history should be retained, where, and for how long?
• Redundancy: ICS control room redundancy: How many ICS control rooms are needed?
• Redundancy: ICS Redundant facility distance: How far should redundant data centers and people be to assure continuity?

Principle 10. The effective management of cybersecurity by third parties and service providers is essential for protection of consumer’s sensitive personal health and financial information.

Third-party and interdependencies are addressed in at least the following elements of the Fearless approach:

• Overarching: Location: Where are content and work located?
• Overarching: Security consultants: When are information security consultants used?
• Overarching: Mobility: What part and portion of the workforce is mobile?
• Overarching: Outsourcing people: What part and portion of the workforce is outsourced?
• Overarching: Outsourcing things: When is information technology outsourced?
• Risk Management: Interdependencies: How are supply chain risks managed?
• Risk Management: Interdependencies: How are real-time interdependency risks managed?
• Control Architecture: Trust model: How is trust assessed and managed?

Many 3rd party factors are also considered in other elements of the Fearless Approach.

Principle 11. Information sharing is important for risk management purposes; however, it must be limited to essential cybersecurity information and protect sensitive confidential information.

Fearless combines assessment with reporting and actuarial analysis to provide for confidential information collection. Dissemination of aggregated information occurs through risk evaluations, ongoing support for business decision-making, and providing alerts and similar information to businesses and their customers. This has long been the approach of using a trusted 3rd party to intermediate in the information protection space.

Principle 12. Cybersecurity risks should be included and addressed as part of an insurers and insurance producers Enterprise Risk Management processes.

The Fearless approach puts information-related protective decisions in the context of the enterprise including through the following elements of the Standards of Practice:

• Overarching: How does the enterprise describe itself and why this effort is being undertaken?
• Overarching: Protection model: What model is used to understand information protection issues?
• Overarching: Business: What is the nature of the business?
• Overarching: Promises: What promises does the business make, to whom, and why? How do they relate to information?
• Overarching: Maturity level: What maturity level does the information protection program have?
Overarching: Content: What content does the enterprise have and what are the consequences of protection failures?

Overarching: Insurance: What coverage does the enterprise have/want and what are the consequences of protection failures (Brit)?

Overarching: Location: Where are content and work located?

Overarching: Organization: What is the structure of the organization?

Overarching: Mobility: What part and portion of the workforce is mobile?

Business modeling: How does the enterprise model itself and its business?

Business modeling: What are the business functions and what information do they depend on for what?

Oversight: What does enterprise oversight provide to the protection program to define duties to protect?

Oversight: How are different sorts of duties prioritized in determining what to protect and how well?

Oversight: Duties analysis: How is duty to protect analyzed?

Risk Management: How does the enterprise do risk management?

Risk Management: Risk management process: What risk assessment processes are used?

Risk Management: Risk definition: How are risk levels for the protection program defined?

Risk Management: Separation of Duties: How should duties be separated?

Risk Management: Surety matching: How is surety matched with risk?

Risk Management: Changing systemic risks: How is changing systemic risks managed?

Management: How does the enterprise manage the information protection program?

Management: Influence: What power and influence does the IP Lead have?

Management: Personnel: How are personnel issues with information protection managed?

Management: Legal issues: How do legal issues interact with protection management?

Management: Physical security: How is physical security integrated with information protection?

Management: Knowledge: How is the knowledge program integrated with information protection?

Principle 13. High level information technology internal audit findings should be discussed at the insurers and insurance producers Board of Director meetings.

Fearless assessments include explicit requirements associated with reporting and positioning of information protection in the context of the enterprise. Relevant elements include, without limit:

- Oversight: What does enterprise oversight provide to the protection program to define duties to protect?
- Oversight: How are different sorts of duties prioritized in determining what to protect and how well?
- Oversight: Form of duties: What form are duties defined in?
- Oversight: Duties analysis: How is duty to protect analyzed?
Principle 14. It is essential for insurers and insurance producers to join Financial Services Information Sharing and Analysis Center (FSISAC) to share information and stay informed about cyber and physical threat intelligence analysis and sharing.

Threat-, vulnerability-, and incident-related information and intelligence issues are addressed in the Fearless approach, including without limit in:

- Risk Management: Threats: How are information-related threats assessed?
- Risk Management: Threats: What threats have been identified, what are their characteristics and relevant history?
- Risk Management: Threats: What design basis threat is used?
- Risk Management: Threats: What attack mechanisms are considered?
- Risk Management: Vulnerabilities: How and when are information-related vulnerabilities assessed?
- Risk Management: Changing systemic risks: How is changing systemic risks managed?
- Management: Incident handling: How are incidents managed?
- Management: Knowledge: How is the knowledge program integrated with information protection?
- Management: Security awareness: What sort of enterprise security awareness program does the enterprise have?
- Incidents: Detection: Are intrusions detected, and if so, how?
- Incidents: Detection and response: What are the process requirements for detection and response?
These include detailed decisions involving threat intelligence, information sharing and sources, and interdiction models such as those afforded by the FSISAC processes and other related processes.

**Principle 15. Sensitive data collected and stored and transferred inside or outside of an insurers or insurance producers network should be encrypted.**

Fearless has explicit decisions related to encryption, including without limit:

- Content control: What mechanisms keep control over content with business utility?
- Content control: Data in use: How is data in use protected?
- Content control: Data in motion: When is content in transit encrypted?
- Content control: Data at rest: What is stored encrypted?

These also have strong interactions with other related issues, such as maturity level, backup and recovery requirements, location, regulatory constraints, and so forth.

**Principle 16. Periodic and timely training for employees of insurers and insurance producers regarding cybersecurity issues is essential.**

The Fearless assessment approaches includes the following elements directly related to training, awareness, and education levels and requirements:

- Management: Personnel: How are personnel issues with information protection managed?
- Management: Knowledge: How is the knowledge program integrated with information protection?
- Management: Security awareness: What sort of enterprise security awareness program does the enterprise have?
- TechArch: Inventory: What information protection-related inventory is kept and in what form(s)?
- TechArch: Lifecycles: What aspects of lifecycles are considered in the protection program and its processes?
- Human factors: User decision-making: What decisions do users make and how do they make them?

**Principle 17. Enhanced solvency oversight is needed for insurers selling cyber insurance to businesses and families.**

Fearless works to develop metrics over time that allow clarity surrounding risk profiles, maximum and expected losses, however, this depends on getting information through the actuarial process. In order for this to work properly, the methodologies used for assessing risk must be aligned to evaluations of losses and their causes. Otherwise, surrogates for risk cannot be reliable related to outcomes for predictive value.

**Principle 18. Additional data on the sale of cyber insurance products should be collected to assist insurance regulators with oversight of financial and market regulation.**

Fearless supports reporting requirements through its actuarial and ongoing support functions as well as through select elements of the initial assessment process. Specific elements producing relevant data include:
Overarching: Content: What content does the enterprise have and what are the consequences of protection failures?

Overarching: Insurance: What coverage does the enterprise have/want and what are the consequences of protection failures?

Risk Management: Threats: What threats have been identified, what are their characteristics and relevant history?

Risk Management: Threats: What attack mechanisms are considered?

Incidents: Detection and response: What are the process requirements for detection and response?

While this information is not available to those not performing actuarial assessment for insurers relative to the specific business and those on the assessment team, statistical results and analysis of reporting from multiple businesses are used as part of Fearless analysis processes and form the basis for reporting and providing warnings and awareness information to clients.
March 13, 2015

Pamela Simpson,
Senior Administrative Assistant
National Association of Insurance Commissioners
1100 Walnut Street, Suite 1500
Kansas City, MO 64106

RE:

Dear Ms. Simpson:

I recommend that the NAIC support state or federal legislation the enact a legal privilege that permits private sector entities to perform certain risk assessments of their networks and physical information security environments; the results of which would remain privileged and confidential.

Such a legal privilege exists for hospitals and medical facilities on the state level. In Illinois, the legal privilege was enacted under the Medical Studies Act. For example, see 210 ILCS 85/10.2 "Participation in peer review; immunity from liability." Under this privilege, a hospital is empowered to perform an investigation to improve the health care of its patients. Most importantly, hospital management is allowed to keep the results confidential. Confidentiality promotes frankness and candor.

The attention of Congress, at present, is focused on "Information Sharing." Steps should also taken to implement other aspects of CyberSecurity.

In your document, “Principles for Effective Cybersecurity Insurance Regulatory Guidance” they are several Principles that would be enhanced by this legislation. Specifically:

Principle 8: Insurance regulators should provide appropriate regulatory oversight, which includes but is not limited to, conducting risk-based, value-added financial examinations and/or market conduct examinations regarding cybersecurity.

Principle 9: Planning for crisis response for insurance regulators, insurers, and insurance producers is an essential component to an effective cybersecurity program.

Principle 10: The effective management of cybersecurity by third parties and service providers is essential for protection of consumer’s sensitive personal health and financial information.

Learn about the various forms of Illinois Medical Studies Act that have been enact in all 50 states and then consider: What Congress should ask itself is: If a legal privilege has been so effective as an incentive for a hospital to investigate a rampaging virus among its patients, why shouldn't an IT manager have the same promise of legal confidentiality to launch an investigation to assess the risks of a rampaging virus in a company network?

The analogy is simple and compelling.

In addition, some of the legal privilege concepts already offered in the PCII, Critical Infrastructure Information Act of 2002.

See DHS explanation at: http://www.dhs.gov/pcii-protections-disclosure
Background

I discuss the concept applying the legal privileges of the Medical Studies Act to risk analysis of company networks in the materials I submitted in April 2013 to the Dept. of Commerce for NIST. See submission at:


Given my work on this issue over the past decade, I appreciated that my proposal was identified in the White House Release, 8/6/13, which specifically mentions "creation of a Federal legal privilege" in the list of incentives.

Liability Limitation — Agencies pointed to a range of areas where more information is necessary to determine if legislation to reduce liability on Program participants may appropriately encourage a broader range of critical infrastructure companies to implement the Framework. These areas include reduced tort liability, limited indemnity, lower burdens of proof, or the creation of a Federal legal privilege that preempts State disclosure requirements. As the Framework is developed, agencies will continue to gather information about the specific areas identified in the reports related to liability limitation.

Thanks, Gary
Sonja Larkin-Thorne, NAIC Funded Consumer Representative offers the following comments on the March 12, 2015 draft "Principles for Effective Cyber Security Insurance Regulatory Guidance."

The opening comments of the cybersecurity guidance states the following, "it is vital for insurance regulators to provide effective cybersecurity guidance regarding the protection of the insurance sectors' data security and infrastructure." The real issue is not just guidance, regulators should demand that insurance company's, affiliates and all business partners, and sources of personal consumer data be required to take all steps necessary to protect consumer information. Insurance carriers must be required to provide every consumer impacted by their data collection practices, detailed information with the type of information collected and retained in a company or business partners records.

The days of providing weak statements regarding the "type of information we collect or accessed" with the recent cyber-attacks is not acceptable. The insurance industry's dependance on personal consumer data to determine who will and will not have access to insurance, determine rates, and rates increases has become the back-bone of the industry's business practices. To allow these weak statements when access to the best products, policies, and rates increases are impacted by individual consumer credit scores, profiles, and other undisclosed data files built by insurance carriers and their business partners is just not acceptable.

How is the consumer to protect themselves and family from the impact of identity theft when the collector (insurance companies) refuses or fails to provide complete and accurate detailed information on what their data files contain? The backdoor gathering of a consumers personal information by insurers and their business partners, includes but is not limited to credit information, personal health data, (yes, one personal lines auto carrier said this on a disclosure insert), town building permits and records, photos of homes and vehicles, employment information, dates of birth and driving records of the named insured and family members, bank accounts and credit card numbers for online internet payments are just a few examples.

Recent cyber-attacks, J.P. Morgan's 76 million households, Walmart, Home Depot 60 million card numbers, Target up to 110 million customers, Neiman Marcus 1.1 million customer cards, Anthem 90 million customers and now Premera Blue Cross with 11 million consumers impacted are clear examples of the risk to consumers.

In April 2014 Federal auditors (OPM) warned Premera Blue Cross that its network security procedures were inadequate and provided 10 recommendations to fix the problems. Premera didn't disclose until January 2015 that in May 2014 hackers had broken into their system. Why did it take a Federal agency to tell a major insurance company that their system was broken and consumers personal information was at risk, why wasn't all sensitive data encrypted and why did it take 6 months for impacted policyholders to learn of the problems?

The NAIC Principles for Effective Cybersecurity Insurance Regulatory Guidance must be more than a document of statements. Consumer protection, privacy, security, complete transparency of what data is contained in the data files and access by individual consumers to their records is critical if individuals are to understand and protect their personal information.

Businesses will be able to purchase and more importantly afford the cost of cybersecurity endorsements or insurance policies. The individual consumer impacted by cyber-security attacks and stolen personal information is less likely to understand, have the personal or financial resources to rapidly response and repair the damage caused by an insurance company's failure to protect policyholder data. Let's not forget the impact stolen credit information will have on a consumers access to affordable insurance products and rates.

I encourage the NAIC's Cyber Security committee to start fresh and rewrite the opening statement to acknowledge the impact on individual consumers, their families and business owners. The principles are too general, lack serious direction, encryption requirements, notice timelines when attacks occur or accountability for insurers to their policyholders. I will continue to review, provide comments and support to the committee in your efforts in this area.

Sincerely,

Sonja Larkin-Thorne
NAIC Funded Consumer Representative
March 23, 2015

Commissioner Adam Hamm
Chair, Cybersecurity (EX) Task Force
NAIC Central Office
1100 Walnut Street, Suite 1500
Kansas City, MO 64106-2197

Attn: Pamela Simpson
Via E-mail: psimpson@naic.org

Re: Principles for Effective Cybersecurity Insurance Regulatory Guidance and the Annual Statement Supplement for Cybersecurity

Dear Commissioner Hamm:

The National Association of Mutual Insurance Companies (NAMIC) appreciates the opportunity to comment on the recently exposed Principles for Effective Cybersecurity Insurance Regulatory Guidance and the Annual Statement Supplement for Cybersecurity.

NAMIC is the largest property/casualty insurance trade association in the country, serving regional and local mutual insurance companies on main streets across America as well as many of the country’s largest national insurers. NAMIC consists of more than 1,300 property/casualty insurance companies serving more than 135 million auto, home, and business policyholders, with more than $208 billion in premiums accounting for 48 percent of the automobile/homeowners market and 33 percent of the business insurance market. More than 200,000 people are employed by NAMIC member companies.

**Process and Timing**

Before addressing the substance of the exposures we would like to offer some general thoughts about process and timing. As a general matter it is certainly not inappropriate for the NAIC to explore what it could be doing to support states’ efforts to protect regulated entities and ultimately consumers from cyber threats. And given the recent well-publicized breaches experienced by large companies including insurers it is not surprising to see the NAIC moving assertively in this area. However, the degree to which the NAIC seems to be accelerating efforts to quickly get something done is notable and potentially of concern.
When the Cybersecurity (EX) Task Force was created in November of last year, its adopted charges focused on monitoring and coordination and did not indicate plans to develop regulatory measures. The first indication that such was contemplated seems to have come in the NAIC’s National Meeting Preview which states, “Task Force will review comments received on its proposed cybersecurity guiding principles and will perhaps consider adoption of the guiding principles.” The Preview is dated February 20, 2015 yet the principles were not exposed until March 12. Meanwhile, there is no record of the Task Force ever meeting until March 12 when it did so in a regulator-only session starting at 3 p.m. Eastern so it is hard to understand when the principles were even developed. We would note that the cited reason for the session to be closed, “Consideration of strategic planning issues relating to federal legislative and regulatory matters or international regulatory matters,” does not seem applicable to the development of the proposed principles since they are clearly meant to guide state regulatory activity.

Finally, when the documents were exposed, a mere seven business days were provided for submitting interested party comments. While we understand there is a sense of urgency surrounding cyber security issues we nevertheless feel is appropriate to make these observations and ask whether a rushed process could result in faulty policy. And given the extremely short exposure period we would characterize these comments as preliminary impressions and thoughts responsive to the exposures and subject to expansion in and modification as work on this issue develops.

**Proposed Regulatory Guidelines**

We appreciate the values expressed particularly in Principles 5 and 6, that any regulatory guidance should be flexible, scalable and practical, and that the guidance must consider the resources of the regulated entity. And while reference to the National Institute of Standards and Technology (NIST) is appropriate we would note that there are other standards that may be appropriate as well and the guidance should allow for consideration of them as well.

In Principle 7, we agree that guidance should be risk-based but it is not clear what it means for guidance to be “threat-informed.”

We have some concern about Principle 8, referring to regulatory oversight including financial and/or market conduct examinations could translate into a call for more exams or more extensive exams and that such activity could be expensive while of questionable utility. While cyber security should certainly be a part of an insurer’s Enterprise Risk Management processes as noted in Principle 12 it is not clear that it needs to be the subject of specialized exam processes.

One proposed principle that seemed inconsistent with the aforementioned flexibility is Principle 14, stating that it is “essential” regulated entities to join Financial Services Information Sharing and Analysis Center (FSISAC). We believe that regulatory guidance could encourage consideration of the value of joining such an organization but that stating it is essential may be premature or off the mark.
Some NAMIC members expressed concern with the breadth of Principle 15 calling for encryption of “Sensitive data collected and stored and transferred inside or outside of an insurers or insurance producers network.” There seems to be a view that encryption is one of a number of tools that can be utilized to protect sensitive data but that there are others that can be more cost-effective depending on the circumstances. There was also an observation that “sensitive data” can be defined in different ways and that it may be preferable to change that word to “Personally Identifiable Information” consistent with NIST terminology throughout the principles document.

There is a sentiment among some NAMIC members that Principles 17 and 18, calling for enhanced solvency oversight for insurers selling cyber insurance and the collection of additional data on the sale of cyber insurance are out of place in the regulatory guidance document and should be removed. Certainly, insurance regulators currently have all the regulatory tools they need to monitor insurers for solvency as they already do. While cyber insurance is a new and developing product it is not distinct from other new and developing products such that different regulatory practices are necessary.

**Proposed Annual Statement Supplement**

In general there were few concerns identified by NAMIC members with respect to the proposed annual statement supplement compared to the proposed regulatory principles. One concern noted that the level of detail called for in the supplement may be excessive and could undermine the competitive position of an insurer writing cyber insurance. There was also a suggestion that the supplement should include a means to provide information about reinsurance since that could significantly impact a company’s actual exposure to risk from cyber threats.

Thank you for your consideration of these comments on this matter of importance to NAMIC members and their policyholders.

Sincerely,

Paul Tetrault, JD, CPCU, ARM, AIM
State & Policy Affairs Counsel
(978) 969-1046
ptetrault@namic.org
Attached are proposed (primarily grammatical) edits to the draft Principles for Effective Cybersecurity Insurance Regulatory Guidance. On Principle 6, I propose that the verb “should” be used instead of “must” since “must” is too strong and may pander to decisions by some insurers not to devote adequate resources to cybersecurity. Also, on Principle 14, I know nothing about FSIFAC but would want to be sure that the drafters have examined the appropriateness of this Principle and are not simply parroting the inherited language and decisions of SIFMA.

Thanks,
Alan
Principles for Effective Cybersecurity Insurance Regulatory Guidance

Due to ever increasing cybersecurity issues, it has become clear that it is vital for insurance regulators to provide effective cybersecurity guidance regarding the protection of the insurance sector’s data security and infrastructure. The insurance regulators commend insurance companies for conducting a review of their cybersecurity policies, regulations, and guidance with the goal of strengthening the insurance sector’s defense and response to cyber-attacks. The insurance industry looks to the insurance regulators to aid in the identification of uniform standards, promoting accountability across the entire insurance sector, and to provide access to essential information. The insurance regulators also depend upon the insurance industry to join forces in identifying risks and the offering of practical solutions. The guiding principles stated below are intended to establish insurance regulatory guidance that promotes these relationships and protects consumers and the insurance industry.

Principle 1: Insurance regulators have a significant role and responsibility regarding protecting consumers from cybersecurity risks.

Principle 2: Insurance regulators have a significant role and responsibility regarding the insurers’ efforts to protect sensitive customer health and financial information.

Principle 3: Insurance regulators have a significant role and responsibility in protecting the sensitive information housed in insurance departments and at the NAIC.

Principle 4: Insurance regulators recognize the value of collaboration in the development of regulatory guidance with insurers, insurance producers, consumers and the federal government with the goal of a consistent, coordinated national approach.

Principle 5: Compliance with cybersecurity regulatory guidance must be flexible, scalable, practical and consistent with the national efforts embodied in the National Institute of Standards and Technology (NIST) framework.

Principle 6: Regulatory guidance must consider the resources of the insurer or insurance producer.

Principle 7: Effective cybersecurity guidance must be risk-based and threat-informed.

Principle 8: Insurance regulators should provide appropriate regulatory oversight, which includes but is not limited to, conducting risk-based, value-added financial examinations and/or market conduct examinations regarding cybersecurity.

Principle 9: Planning for crisis response for insurance regulators, insurers, and insurance producers is an essential component to an effective cybersecurity program.

Principle 10: The effective management of cybersecurity by third parties and service providers is essential for protection of consumer’s sensitive personal health and financial information.

---

1 These principles have been derived from SIFMAs (Securities Industry and Financial Markets Association) “Principles for Effective Cybersecurity Regulatory Guidance”

© 2015 National Association of Insurance Commissioners
Principle 11  Information sharing is important for risk management purposes; however, it must be limited to essential cybersecurity information and protect sensitive confidential information.

Principle 12  Cybersecurity risks should be included and addressed as part of an insurer's and insurance producer's Enterprise Risk Management processes.

Principle 13  High level information technology internal audit findings should be discussed at the insurer's and insurance producer's Board of Director meetings.

Principle 14  It is essential for insurers and insurance producers to join Financial Services Information Sharing and Analysis Center (FSISAC) to share information and stay informed about cyber and physical threat intelligence analysis and sharing.

Principle 15  Sensitive data collected and stored and transferred inside or outside of an insurer's or insurance producer's network should be encrypted.

Principle 16  Periodic and timely training for employees of insurers and insurance producers regarding cybersecurity issues is essential.

Principle 17  Enhanced solvency oversight is needed for insurers selling cyber insurance to businesses and families.

Principle 18  Additional data on the sale of cyber insurance products should be collected to assist insurance regulators with oversight of financial and market regulation.
VIA EMAIL

March 23, 2015

Mr. Adam Hamm, Chair
Cybersecurity (EX) Task Force
National Association of Insurance Commissioners
2301 McGee Street, Suite 800
Kansas City, MO  64108

Dear Mr. Hamm:

On behalf of PCI’s nearly one thousand members, we are pleased to submit these initial comments on the NAIC’s draft Principles for Effective Cybersecurity Insurance Regulatory Guidance and Blanks cybersecurity insurance coverage supplement. While cybersecurity is certainly receiving a great deal of scrutiny as of late, it’s important to remember that both regulators and property and casualty insurers have been effectively managing their own cyber risk for quite a long time. What is needed now is not increased oversight of insurers’ own cybersecurity but rather measures designed to facilitate the ability of insurers to satisfy a rapidly increasing demand for cybersecurity insurance. With that said, we offer the following specific comments on the two proposals.

Principles for Effective Cybersecurity Insurance Regulatory Guidance

While many of the concepts and ideas encapsulated by the principles are relatively benign, we are concerned with the publication of new principles, other than those already effectively practiced by regulators and insurers, in that such publication suggests that cybersecurity is either new or that the property and casualty insurance industry is not properly managing their cybersecurity. Property and casualty insurers have long been subject to rigorous state and federal privacy and information protection laws, and the track record of both regulators and the industry is excellent in this regard. Rather than adopt a list of principles, a much better approach is to issue a general policy statement to the effect that any new regulatory requirements with regards to insurers’ cybersecurity should be based only upon an objective finding of gaps and should recommend the least burdensome method of compliance.

With respect to specific principles, we offer the following observations:

- Principle 8 – as previously mentioned, insurers are already subject to regulatory oversight and required to file detailed reports with regards to enterprise risk and solvency. We are concerned that this principle seeks to impose yet another reporting requirement on insurers with respect to cybersecurity. Every effort should be made to limit duplicative requirements on insurers.
- Principle 11 - who exactly is sharing information with whom? Insurers with government agencies? Insurers with other insurers? Both? Additional clarity regarding this principle is needed.
• Principle 14 – there are numerous public and private sector entities that are focused on cybersecurity. Why identify a specific group to join rather than encourage insurers to investigate and consider joining any one of the many such type of groups? We also wonder, again, with whom are insurers to share what kind of information? Additional clarity is required here.

• Principle 15 – we suggest that this principle focus on the protection of data generally, rather than mandating the use of any one particular means of doing so. To the extent the term “encryption” is used, it’s not clear what is meant by the term given that there are currently many standards of encryption currently available.

Blanks

We support adoption of the NAIC cybersecurity insurance coverage supplement form. The collection of information that the NAIC already collects with regards to other lines of insurance should also be collected with regards to cybersecurity insurance and will help inform public policy discussions.

Supporting the Growth of a Cyber Insurance Market

The greatest contribution the NAIC and state regulators could make is to work with the industry to identify where hurdles may exist to the offering of cybersecurity insurance. In addition, it would be beneficial if regulators could work in tandem with the industry to respond to federal inquiries and also help foster the conditions where cyber security insurance can grow, consistent with sound financial management.

Based on the property and casualty insurer record in this area, there simply is no need for additional, intrusive regulation. Rather, we respectfully submit to you that a simple policy statement is better than any lengthy set of principles, many of which may very well cause needless complications. A much better approach to cybersecurity insurance is for the NAIC to work together with industry to help facilitate the continued development of the cybersecurity insurance market.

Sincerely,

Thomas M. Glassic
Vice President, Policy and Government Affairs
thomas.glassic@pciaa.net

Alex Hageli
Director, Personal Lines Policy
alex.hageli@pciaa.net

David Snyder
Vice President, International Policy
david.snyder@pciaa.net

Cc: Aaron Brandenburg
    Eric Nordman
March 18, 2015

Generally I believe the document is well done. I do have an issue and a comment in regards to Principle 17. My overall comment is that this Principle should be deleted from the document. My rational around this is that, first, it is not well define, what is meant by “Enhanced solvency oversight”. Second, is why do we need such additional solvency oversight of an insurer writing such business. I would argue an insurer selling a general liability policy to a Fortune 100 company is exposed to much greater risk then a sell of a cyber policy where policy limits and exclusions limits the future exposure of a company. By having such a principle within the document will create an expectation that is not needed. Our solvency oversight has been greatly enhanced overall since the turn of the century like no other time in our history.

Thank you for the opportunity to comment.
Thank you for including Prometric as an interested party to give feedback to Eric Nordman and the Cybersecurity Task Force regarding the Principles.

I think the Principles cover all critical aspects of the mission however I recommend an edit to Principle #16. My feedback would be to extend Principle #16 beyond training by including a Cybersecurity Assessment. From our extensive experience in the testing and assessment field, Prometric would advise the Cybersecurity Task Force that training on its own will not assess if the knowledge is truly learned by the employees. Only an assessment can ascertain that.

Therefore, I recommend a change to Principle #16 to read:

Principle 16 Periodic and timely training paired with an assessment for employees of insurers and insurance producers regarding cybersecurity issues is essential.

As an attendee of the NAIC Spring National Meeting in Phoenix, would it be possible for me to receive an invite to any sessions or meetings conducted by the Cybersecurity Task Force?

Please let me know if you have any questions.

Best regards,
Holly

Holly Dance | Vice President, Global Account Management

Prometric
443 455 6128 OFFICE
410 949 7318 MOBILE
March 23, 2015

Pam Simpson
NAIC, Cybersecurity (EX) Task Force
(psimpson@naic.org)

RE: Comments Regarding Principles for Effective Cybersecurity Insurance Regulatory Guidance

Dear Ms. Simpson:

The Reinsurance Association of America (“RAA”) appreciates the opportunity to provide input regarding the Cybersecurity Task Force’s draft Principles for Effective Cybersecurity Insurance Regulatory Guidance, which were released on March 12, 2015.

The RAA is a national trade association representing reinsurance companies doing business in the United States. RAA membership is diverse, including reinsurance underwriters and intermediaries licensed in the U.S. and those that conduct business on a cross border basis. The RAA also has life reinsurance company affiliates.

Given the rapidly developing cybersecurity environment, we appreciate the importance of the NAIC and state regulators’ consideration of effective cybersecurity guidance regarding the protection of the insurance sector’s data security and infrastructure. We welcome the opportunity to work with you with the goal of strengthening the insurance sector’s defense and response to cyber-attacks and to identify risks and develop practical solutions. The draft guiding principles are an important initial step in this process and we agree with many of the concepts captured by the draft.

We caution the NAIC to carefully consider an appropriate balance with respect to regulatory requirements in this area to avoid unnecessarily onerous burdens and to reflect the fact that practices may differ in companies of different sizes, structures and cross-border activity. For example, the reference in Principle 17 to “enhanced solvency oversight” for companies offering cyber products is vague, potentially redundant to other solvency initiatives, and could suggest an unnecessary additional layer of regulation. Similarly, with respect to Principle 8, we assume that the intention would be to incorporate an analysis of cybersecurity issues into the existing examination process, rather than conducting separate examinations on this topic.

Given the speed with which the cybersecurity environment is changing, the NAIC principles should be structured in a way that allows for flexibility and adaptability in this evolving landscape. For example, while we agree with the concept in Principle 15 that sensitive data must be protected, we would recommend not specifying the method by which that protection should be achieved.
Moreover, we urge the NAIC to avoid concepts that go beyond broad principles to impose specific requirements or mandates. For example, Principle 14 mandates that insurers and insurance producers join a specific organization (the Financial Services Information Sharing and Analysis Center) to share information and stay informed about cyber and physical threat intelligence analysis and sharing. In our view, the principles of sharing information and staying informed are the key concepts, without the need to mandate the mechanism for accomplishing that goal.

Finding an appropriate regulatory balance is particularly important with respect to the development of cyber insurance products, a market that is evolving in parallel with the rapidly growing need for cybersecurity protection. While such products should be subject to appropriate and necessary regulation, such regulation should not inhibit the development of new and innovative products in this arena. Given the importance of this issue, it also may be appropriate to address necessary oversight for insurers and insurance producers selling cyber insurance separately from principles relating to addressing cybersecurity risks faced by the insurance industry.

Lastly, while we believe the draft principles are a productive starting point for the NAIC and industry to begin discussing these critical issues, we urge the Task Force to expose these principles for a second round of public comments prior to adoption. Given the highly technical nature of cybersecurity issues – both with respect to technology and IT issues and with respect to the nature and variety of cyberattacks – we also urge the Task Force to consider opportunities for both the NAIC and industry to enhance their expertise on these issues, whether through seminars, webinars or other means before finalizing the principles and as part of the ongoing consideration of these complex issues.

**Conclusion**

We appreciate the opportunity to provide input to the Task Force’s analysis of these issues. We look forward to continuing to work with the Task Force as these and other important issues relating to cybersecurity regulation continue to be discussed.

Sincerely,

Tracey W. Laws
Senior Vice President and General Counsel
Memo

To: Adam Hamm, Chair, NAIC Cybersecurity (EX) Task Force
cc: Patrick McNaughton, Chair, NAIC IT Examination Working Group
From: LeeAnne Creevy and Philip McMurray, RRC
Date: March 23, 2015
Subject: RRC Response to the NAIC Cybersecurity (EX) Task Force Regarding the Draft List of “Principles for Effective Cybersecurity Insurance Regulatory Guidance”

Background

On March 12, 2015, the National Association of Insurance Commissioners ("NAIC") exposed two cybersecurity-related exposure drafts for comment. The first of these exposure drafts included a set of 18 principles designed to "help state insurance departments identify uniform standards, promote accountability, and provide access to essential information". As an interested party, Risk & Regulatory Consulting LLC ("RRC") offers comments related to several of the principles included in the exposure draft, with the full scope of our response aligned with the principles referenced below.

In parallel with this response, RRC has also actively supported the NAIC's IT Examination Working Group ("ITEWG"), including recent efforts focused on enhancing the assessment of cybersecurity risks during the financial examination process. RRC provided a response to the ITEWG's request for input regarding cybersecurity risks and examination testing in February of this year, and we are currently volunteering to help align the NAIC IT review guidance with cybersecurity standards published by the National Institute of Standards and Technology ("NIST"). We fully support the efforts of the NAIC Cybersecurity Task Force and the ITEWG to enhance regulatory guidance regarding cybersecurity risks.

We appreciate the opportunity to offer our comments. Please note that we have elected to not comment on the exposure draft principles that are not referenced below as we concur with their content.

Comments Regarding Specific Principles

RRC's comments appear below, referencing specific principles both individually and grouped where appropriate.

Principles 5 and 6 – Recognizing the need for a scalable approach for performing regulatory examinations, RRC concurs with these principles with the caveat that a minimum set of cybersecurity standards be in place for all insurers that are physically connected to the Internet or other public data networks, regardless of size and scope of operations. Given the current ITEWG initiative to align the IT review process with existing NIST guidance, the practical definition of what constitutes this minimum standard can, and should, be included in the ITEWG’s efforts. However, because the Cybersecurity Task Force’s principles will serve to help guide those efforts, Principle 5 and/or Principle 6 should include language stating that a minimum set of cybersecurity standards should be defined for all insurers that make use of public data networks.
Principles 8, 12 and 13 – Transcending the IT review process, these three principles focus on the need for a holistic, top-down view of cybersecurity risks. While RRC fully agrees with these principles, it is also imperative that the financial examination process be extended beyond current ITEWG-based initiatives to include expanded procedures regarding executive-level cybersecurity awareness, inclusion of cybersecurity risks within the insurer’s ERM process and integration of cybersecurity into organizational strategic planning efforts. As a result, these principles should either be expanded, or they should be directly supported by extensions to the current financial examination guidance (for example, expanding guidance in Exhibit Y of the Examiners’ Handbook related to C-level management interviews), thereby mirroring the current ITEWG initiatives that are focused on IT-related controls and processes.

Principles 11 and 14 – RRC fully agrees with these principles, with the understanding that active information sharing among insurers and other financial services entities can significantly improve a shared understanding of cyber threats, and an enhanced ability to respond in a timely and effective manner. RRC also recommends that current wording of these principles be extended to encourage participation in other current and future information sharing forums. For example, Principle 14 references a significant information sharing group (FSISAC). However, a number of other cyber-threat sharing forums exist or are planned, including the one proposed at the White House Summit on Cybersecurity and Consumer Protection in February, 2015. As such, we recommend that consideration be given to broadening Principle 14 to include more than just the FSISAC.

Principle 15 – This principle addresses an important consideration relative to protection of insurer data, both in-transit and at-rest. However, RRC recommends that additional specificity be added relative to the definition of “sensitive”. The wording of the currently-drafted principle is somewhat ambiguous, allowing for interpretation of this term by insurers and entities that provide services to the industry. RRC recommends that existing data classification methods be referenced by this principle, with possible choices including the current NIST 800-60 and FIPS 199 guidance. It was also noted that this term is used in Principles 2, 3, 10 and 11, and RRC encourages a clearer definition of this term to help ensure consistent and appropriate data protection efforts are undertaken.
To: psimpson@naic.org  
Re: Comments on NAIC Draft Principles for Effective Cybersecurity Insurance Regulatory Guidance  
From: Mark Simon, Simon Cyber Group

The Simon Cyber Group is an affiliation of professionals who provide cyber security consulting services to owners and operators of critical infrastructures. Its principal member is Mark Simon. Mr. Simon holds Juris Doctor and Master of Science degrees, and holds certifications as a Certified Information Security Professional (CISSP) and Global Industrial Cyber Security Professional (GICSP).

The following comments from the Simon Cyber Group are intended to help make more effective the NAIC draft (March 12, 2015) Principles for Effective Cybersecurity Insurance Regulatory Guidance.

**Principle 6: “Regulatory guidance must consider the resources of the insurer or insurance producer.”**

Principle 6 places unwarranted emphasis on resources of the insurer or insurance producer. Consequently, Principle 6 can be too easily construed as justification for regulators, insurers and insurer producers to ignore risk management principles and the proper selection of privacy and security cyber controls.

Resource constraints are but one aspect of a risk management strategy and should not be singled out as an over-arching factor for establishing regulatory requirements or guidance. The U.S. banking and finance sector includes more than 7,000 domestic U.S. insurers. Collectively, the organizations that comprise this sector form the backbone of the U.S. economy and a vital component of the global economy. They are tied together through a network of electronic systems with innumerable entry points. A successful attack on these systems would have detrimental effects on the entire economy.

Accordingly, insurance regulators should not hesitate to establish minimum, risk-based privacy and cyber security measures applicable to insurers and insurance producers in order to ensure the reliability of the U.S. banking and finance sector, just as regulators do in the case of establishing minimum reliability measures for cars and licensed drivers, planes and the pilots who fly them, electric grid equipment and grid operators, etc.

Principle 6 is also inconsistent with the approach taken in the NIST security framework. Under the NIST framework, cyber security and privacy controls are selected in accordance with a multitude of factors that comprise a risk management strategy, including risk management processes, legal/regulatory requirements, business/mission objectives, and organizational constraints. Regulators should not and must not single out organizational constraints as an excuse for failing to protect consumer data or ensure the reliability of critical systems in the U.S. banking and finance sector. Since resource constraints are not singled out as a basis for selection of cyber security and privacy controls under the NIST security

---

1 Framework for Improving Critical Infrastructure Cybersecurity Version 1.0, National Institute of Standards and Technology, February 12, 2014 (pp. 5, 9, 18 and 23).
framework, Principle 6 is inconsistent with Principle 5 which states in pertinent part, “Compliance with cybersecurity regulatory guidance must be ... consistent with the national efforts embodied in the National Institute of Standards and Technology (NIST) framework.”

Principle 8: “Insurance regulators should provide appropriate regulatory oversight, which includes but is not limited to, conducting risk-based, value-added financial examinations and/or market conduct examinations regarding cybersecurity.”

Insurance regulators must be vigilant about the potential conflict between indemnification obligations of insurers and incident response service providers. Effective incident response services require collaboration between the service provider and the insured in order to address containment, eradication and recovery from a cyber security incident. These objectives could be comprised if incident response services are used as a pretext to collect evidence to support denial of an insured’s claim for indemnification. Thus, Principle 8 should be expanded to provide regulator oversight of relationships between insurers and third parties who provide remediation services in response to a cyber security incident.

Principle 9: “Planning for crisis response for insurance regulators, insurers, and insurance producers is an essential component to an effective cybersecurity program.”

Principle 9 ignores there are many “essential components” of an effective cybersecurity program. For example, supply chain risk should be addressed in an effective cybersecurity program. Threat agents (individuals, organizations, or nation-states) may directly or indirectly affect the management or operations of insureds, insurers and insurance producers by embedding vulnerabilities in IT hardware and software. A threat agent may have the power to coerce a manufacturer to hand over the manufacturing specifications of a sensitive system or to insert malicious capability into a product. Similarly, the rapid adoption of open source software, most commonly in binary form, extends supply chain risk scenarios to the libraries, frameworks, and toolkits on which so much of modern software relies. Threats and vulnerabilities created in this way are often extremely sophisticated and difficult to detect and thus provide a significant risk to the U.S. banking and finance sector.

Principle 12: “Cybersecurity risks should be included and addressed as part of an insurers and insurance producers Enterprise Risk Management processes.”

Cyber risk has the potential to cause significant losses due to substantial aggregation risk and the increasing sophistication of cyber attacks. Accordingly, regulators need to provide oversight of the industry's ability to monitor and model cyber risks, including but not limited to aggregation risk. Principle 12 should be strengthened by adding mention of the role of the regulator in providing oversight of insurers and insurer producers with respect to “Enterprise Risk Management processes.”
Principle 17: “Enhanced solvency oversight is needed for insurers selling cyber insurance to businesses and families.”

Principle 17 should be expanded to include the role of regulators in providing oversight as to scope or clarity of coverage. Some cyber attacks are simply too difficult to discover in their early stages, and may occur over a period of years. This raises complicated issues regarding discovery and scope of coverage under cyber risk policies. Also, reinsurers are not yet fully engaged in providing their capacity to cyber risk coverage. Although they continue to provide coverage for portfolios through CGL and first party/property coverage, these products may or may not respond to cyber-linked losses. These are but a few of the multitude of coverage questions integral to the determination of loss due to cyber risk and, ultimately, pose risk to the solvency of insurers selling cyber insurance.

For example, McAfee (an Intel company) published a report on this subject in an online article entitled, “The Security Industry’s Dirty Little Secret The debate over advanced evasion techniques (AETs).” The article discusses the difficulties in discovering an attack, such as in the following passage.

AETs are used by well-resourced, motivated hackers to execute [advanced persistent threat] APT attacks. While the AET is not an attack by itself, as the bits of code in the AET are not necessarily malicious, they are used to disguise an attack. The danger lies in that AETs provide the attacker with undetectable access to the network. By developing a set of dynamic AETs, the hacker creates a “master key” to penetrate any locked-down network to exploit and compromise their vulnerable target victims. AETs use a combination of evasion techniques, such as fragmentation and obfuscation, to bypass network security controls like firewalls and intrusion prevention systems (IPSs). AETs work by splitting up malicious payloads into smaller pieces, disguising them, and delivering them simultaneously across multiple and rarely used protocols. Once inside, AETs reassemble to unleash malware and continue an APT attack.

Conclusion

The Simon Cyber Group supports the NAIC initiative to address cyber risk. However, the proposed Draft Principles for Effective Cybersecurity Insurance Regulatory Guidance need further development or detail in order to provide meaningful and effective guidance to regulators, insurers and insurance producers.

Mark Simon, JD, CISSP, GICSP
+1 (312) 985-7346
+44 (0) 20 3287 0964
mark@simoncybergroup.com
www.simoncybergroup.com