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)\(^1\) 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
Robert B. Meyer  
Vice President & Associate General Counsel

Lisa Tate  
Vice President & Associate General Counsel

For Electronic Delivery

April 10, 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 Proposed Principles for Effective Cybersecurity Insurance Regulatory Guidance

Dear Commissioner Hamm and Director Farmer:

ACLI appreciates the opportunity to submit additional comments on the proposed Principles for Effective Cybersecurity Insurance Regulatory Guidance (Principles). Most importantly, we again thank you for the opportunity to participate in this vitally important collaborative effort to enhance insurance sector cybersecurity to protect insurers and consumers.

In line with our earlier comments, ACLI supports, and stresses the overarching importance of, NAIC’s efforts to identify uniform standards and to develop a consistent, coordinated national approach to cybersecurity. Uniform national standards are critically important to life insurers that do business across the country, to avoid a patchwork of differing and possibly conflicting state cybersecurity laws, rules and regulations applicable only to insurers. Clear, uniform guidance will permit life insurers to better allocate resources to their highest and best use, geared toward managing a dynamic cyber security program to protect all of their constituents.
ACLI also appreciates the NAIC’s recognition of the importance of collaboration with industry and the federal government in the development of regulatory guidance relating to cybersecurity. We strongly support a collaborative approach that would join the insurance industry in a partnership with regulators and appropriate policymakers to focus efforts on ensuring a consistent, flexible risk-based approach. The nature and increasing number, sophistication, and intensity of cyber attacks targeting government, businesses and individuals in the United States requires nothing less than a collaborative, coordinated and consistent response.

As previously indicated, ACLI agrees with the NAIC that any effective cyber security guidance must be risk-based, flexible, scalable, and practical. Accordingly, while the Principles should provide for uniform national standards, ACLI urges that they also should be general, and allow an insurer the flexibility to most effectively protect its customer information in a manner appropriate to the size and complexity of the insurer and the nature and scope of its activities.

In contrast with the above, some of the proposed Principles, such as the following, appear to be overly specific and prescriptive and to prescribe mandatory controls:

- **Principle 15** appears to require that data be encrypted, regardless of whether it is inside the company “at rest” or being transferred, even though encryption may be neither the most recent nor the most effective protection for many types of data, and companies have many other safeguards in place to protect information, particularly information “at rest.”

  ACLI urges that Principle 15 be modified to provide that sensitive data should be protected by appropriate safeguards, such as encryption, multifactorial authentication, firewalls, intrusion detection controls, antivirus software, or other appropriate security controls or safeguards.

- **Principle 5** may be construed to require insurers’ security frameworks to be consistent with the National Institute of Standards and Technology (NIST) framework. However, the NIST framework may not represent an effective framework for all insurers, some of whom find other comparable standards, such as the International Organization for Standardization (ISO) standards to be more appropriate. Also, life insurers are subject to the Gramm Leach Bliley Act (GLBA) security standards reflected in the NAIC Standards for Safeguarding Customer Information Model Regulation (Safeguards Standards). These Safeguards Standards, adopted in 36 states, already require insurers to implement a comprehensive written information security program that includes administrative, technical and physical safeguards for the protection of customer information.

  ACLI urges that Principle 5 be modified to either eliminate the reference to NIST, or to make it clear that compliance with cybersecurity guidance should be consistent with NIST or other comparable standards or combination of comparable standards, appropriate to the size and complexity of the insurer and the nature and scope of its activities.

- **Principle 13** is overly specific in that it prescribes that all high-level internal IT audit findings be discussed with a Board of Directors, which may not always be warranted. Instead, Principle 13 should be modified to provide that IT internal audit findings that identify a material risk to the
company or other material matters relating to cybersecurity should be reviewed with the Board of Directors or an appropriate committee of the Board as necessary and appropriate.

- **Principle 14** is also overly specific and prescriptive in that it requires insurers to join the Financial Service Information Sharing and Analysis Center (FS-ISAC). Membership in a public-private sector threat intelligence analysis and sharing organization should not be limited to FS-ISAC. While FS-ISAC is a major, well-respected information analysis and information sharing organization, other information sharing groups may be as effective or more specifically focused on insurance. Accordingly, ACLI urges modification to **Principle 14** to either eliminate the reference to FS-ISAC or to also provide for insurers to join other appropriate information sharing programs.

ACLI appreciates that **Principles 3 and 11** provide for the protection of insurers’ sensitive information. However, given the significant adverse effect that could result from an inadvertent or public disclosure of such information, ACLI urges modification to the Principles, particularly to **Principles 3, 8, and 11**, to make it as clear as possible that the security and confidentiality of all sensitive information collected by, shared with, or housed at an insurance department, the NAIC, or a third party consultant will be protected from public and any other disclosure to the greatest extent possible under the law.

ACLI notes that **Principle 8** provides for “appropriate” regulatory oversight, that includes “risk-based, value added” examinations. Accordingly, we urge modification to clarify that “appropriate” oversight shall not include multiple, duplicative examinations of a single insurer by different states. We also request that this Principle be modified to provide for regulators to take into account validation of an insurer’s security framework performed internally by the insurer or by a third party at the request of the insurer.

In sum, ACLI appreciates and supports NAIC efforts to identify uniform national standards and to develop cybersecurity guidance that reflects a collaborative, coordinated and consistent national approach, which is risk-based, flexible, scalable, and practical.

Again, we thank you for the opportunity to participate in this important dialogue which we believe should be ongoing; and we would be glad to answer questions regarding any of the above.

Sincerely,

Roberta B. Meyer

Lisa Tate
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 insurers 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
Principles for Effective Cybersecurity Insurance Regulatory Guidance

Due to ever increasing cybersecurity threats, it has become clear that it is vital for insurance regulators and the insurance industry to work together to provide effective cybersecurity guidance regarding the protection of the insurance sector’s data security and infrastructure from unauthorized access to consumer information. 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 and the insurance regulators must collaborate with other stakeholders and recognized authorities 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 to curb the impact of cyber-attacks on the insurance industry and consumers.

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’ sensitive health and financial information from cybersecurity threats. In this role, regulators must collaborate with insurers, insurance producers, consumers, and state and federal governments to achieve the goal of a consistent, practical national approach.

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, risk-based, and consistent with national efforts and industry-specific standards. Furthermore, such guidance should respect the distinctions across different insurance lines and foster a measurement framework that aligns with standards and obligations of interest to specific industries, embodied in the National Institute of Standards and Technology (NIST) framework.

Principle 6: Regulatory guidance must be predicated upon an evaluation of, and take into consideration, a cost/benefit analysis for insurers, insurance producers, and consumers considering the resources of the insurer or insurance producer.

Principle 7: Effective cybersecurity guidance must be risk-based and threat-informed.
Principle 6: Insurance regulators should provide appropriate regulatory oversight, which includes but is not limited to, verification of an insurer’s risk assessment, program maturity, and operational alignment with a nationally- and industry-accepted cybersecurity standard assurance framework, conducting risk-based, value-added financial examinations and/or market conduct examinations regarding cybersecurity.

Principle 7: Planning for incident crisis response by insurance regulators, insurers, and insurance producers is an essential component to an effective cybersecurity program and should include incident coordination and preparedness exercises specific to the threats inherent in each specific insurance line.

Principle 8: The effective management of cybersecurity by third parties and service providers is essential for protection of consumer’s sensitive personal health and financial information.

Principle 9: Information sharing is important for cyber-security risk management purposes. It is essential that insurers take full advantage of available sources of relevant information such as active, engaged, proven and mature Information Sharing and Analysis Organizations (ISAOs), however, it must be limited to essential cybersecurity information and protect sensitive confidential information.

Principle 10: Cybersecurity risks should be included and addressed as part of an insurer’s and insurance producer’s Enterprise Risk Management processes, and should be included as appropriate in an insurer’s ORSA process and Board of Directors’ meetings.

Principle 11: High level information technology internal audit findings should be discussed at the insurers and insurance producers Board of Director meetings.

Principle 12: Periodic and timely training for employees of insurers and insurance producers regarding cybersecurity issues is essential.

Principle 13: Enhanced solvency oversight is needed for insurers selling cyber insurance to businesses and families.

Principle 14: Additional data on the sale of cyber insurance products should be collected to assist insurance regulators with oversight of financial and market regulation.
April 10, 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 - Supplemental Comments

Dear Mr. Nordman:

The American Insurance Association (AIA) and Property Casualty Insurers Association of America appreciate (PCI) the opportunity to provide additional comments on the draft “Principles for Effective Cybersecurity Insurance Regulatory Guidance” (Regulatory Guidance). As stated in our previous letters, cybersecurity is of critical importance to our members and to that effect we join other industry trades in expressing support for the NAIC’s work on the Regulatory Guidance and continued dialogue and collaboration on flexible, scalable, practical, risk-based guidance.

AIA and PCI’s March 23rd letters suggested edits and commentary on the March 12th draft Regulatory Guidance. This letter supplements and adds to the recommendations made in our prior comments. In addition to the points raised in our prior comments and the joint insurance trade association comments submitted today, we wish to draw additional attention to the following three principles:

Principle 3: Regulators and the NAIC have a responsibility to maintain the security and confidentiality of the information they receive from consumers and insurers. This should include considering security standards of state contractors and ensuring the protection of information shared with other regulatory agencies. Therefore, we have provided some suggested edits to Principle 3.

Principle 3: Insurance regulators and the NAIC have a significant role and responsibility in protecting sensitive customer and insurer information housed in provided or reported to state insurance departments and the NAIC.

---

1 AIA represents approximately 325 major U.S. insurance companies that provide all lines of property-casualty insurance to U.S. consumers and businesses, writing nearly $127 billion annually in premiums.

2 PCI represents nearly 1000 insurers and reinsurers that are over one third of the U.S. property and casualty insurance market.
Principle 17:
We appreciate that regulators have questions about the cyber insurance market; however, we continue to question why there is an emphasis on enhanced solvency oversight for these products.

Cyber coverage has been in existence in one form or another for approximately 15 years and insurers have responsibly developed and enhanced cyber coverage during this 15-year period. Insurers understand the complex and evolving nature of the risk and are exercising prudence when developing cyber insurance products. Furthermore, carriers are exercising careful underwriting strategies, including risk limits, reinsurance strategies that reduce primary insurer retentions and differentiation among various industries based on their varying exposures and any potential for risk aggregation.

In addition, with the NAIC’s adoption of the Own Risk and Solvency Assessment (ORSA) and with companies’ engagement in the ORSA process, we respectfully submit that there is no need for separate enhanced solvency oversight. As noted by the NAIC’s Center for Insurance Policy and Research, “ORSA is an internal process undertaken by an insurer or insurance group to assess the adequacy of its risk management and current and prospective solvency positions under normal and severe stress scenarios.” Under ORSA insurers manage their risks and analyze foreseeable and relevant material risks to include underwriting risks.

Further, we note that at least one nationally recognized financial regulator and some consumer advocates have also questioned the need for increased solvency oversight. To borrow from the regulator’s observation, why create an expectation of the need for additional solvency oversight when that is not needed.

For all of these reasons, we strongly believe that Principle 17 on cyber insurance does not belong in a document focused on corporate data security guidance for all lines of insurance business. Therefore, we urge that Principles 17 be removed from this document or at the very least be referred to the Financial Condition (E) Committee for further study prior to adoption as a Principle.

Principle 18:
We also do not believe that data collection related to cyber insurance belongs in a document focused on corporate security guidance for all lines of insurance business and respectfully urge that it be removed. While exploring data collection may be an appropriate charge for the Cybersecurity Task Force, data collection does not rise to the level of being a “Principle” for effective regulation. Perhaps a better way to state the Principle would be the following:

Principle 18: Insurance regulators should engage in a dialogue with insurers regarding the evolution of cyber insurance coverage in a manner that supports the continued responsible growth of this market while balancing confidentiality concerns.

---

3 NAIC’s Center for Insurance Policy and Research Key Issues Brief Abstract (02/27/2015),
http://www.naic.org/cipr_topics/topic_own_risk_solvency_assessment.htm


The E Committee has already engaged in the cyber insurance sphere through its work on a Blanks proposal. And, we have been engaged there too with a comment letter urging the preservation of proprietary data and the collection of data on an aggregated basis. We also intend to provide additional feedback during the Blanks Working Group exposure period. Therefore, the dialogue called for in the restated Principle is already happening.

Again, AIA and PCI appreciate the opportunity to provide additional comment and we look forward to a collaborative partnership on the issue of cybersecurity.

Respectfully submitted,

Angela Gleason
Associate Counsel
American Insurance Association

David Snyder, Vice President
Alex Hageli, Director
Thomas M. Glassic, Vice President
Policy Research and Development
Property Casualty Insurers Association of America
April 10, 2015

Commissioner Adam Hamm, Chair  
Cybersecurity (EX) Task Force  
National Association of Insurance Commissioners  
1100 Walnut Street, Suite 1500  
Kansas City, MO  64106

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 Blue Cross Blue Shield Association (BCBSA), we submitted a comment letter on this issue dated March 23, 2015, which included comments and recommendations on each of the March 12 Draft Principles. The reopening of the comment period announced during the Phoenix Spring National Meeting has allowed us additional time to seek further comments from our members and their information technology experts. The result of those comments is the attached redline proposal of the Draft Principles, which generally follow the recommendations in our earlier letter.

As noted in the Joint Trades comment letter submitted today, we trust these proposed revisions are useful as a starting point in an ongoing process and dialogue involving industry, regulators and other stakeholders. We look forward to discussing them further and working with you in this complex and dynamic arena.

Respectfully submitted,

America’s Health Insurance Plans  
Bob Ridgeway  
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.

We understand the NAIC’s interest in risk-based oversight and use of examinations as a tool, nonetheless, we would caution that any new examination requirements must include reasonable time for insurer’s to comply. In addition, instructive guidance around any new examination requirements should be provided by regulators as insurers work to fulfill new examination components.

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 and transferred 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 response 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
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.
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 insurers 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.

We propose 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 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 to protect 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** 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.
April 10, 2015

Commissioner Adam Hamm, Chair
Director Raymond Farmer, Vice Chair
Cybersecurity (EX) Task Force
National Association of Insurance Commissioners

Re: Cybersecurity Guiding Principles Draft

Dear Commissioner Hamm and Director Farmer:

Nine NAIC Consumer Representatives submit these comments on the Cybersecurity Task Force’s draft of “Principles for Effective Cybersecurity Insurance Regulatory Guidance. We focus primarily on questions and issues that arose during the March 29, 2015 Cybersecurity Task Force meeting in Phoenix, and draw upon the comments filed on March 12 by the Center for Economic Justice, Consumer Federation of America, United Policyholders and the National Consumer Law Center. Further, while issues of consumer and policyholder rights and protection are vital, we will address them in comments to the Task Force’s upcoming “Consumer Bill of Rights” project.

We understand that these draft principles are intended to provide a conceptual framework around which to organize the discussion and eventual implementation of the regulations necessary to bring these principles to life. We appreciate the recognition by the NAIC and state insurance regulators of the importance of this project, and commend the Task Force’s quick work in rapidly developing and opening for comment several draft documents, and holding an informative first open session in Phoenix.

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

Comment: We agree, but perhaps this first, general principle should note the urgency of regulatory action, as cyber breaches appear to be increasing in frequency and magnitude, and as several regulators have noted, “the bad guys are still way ahead of us.” This Task Force has set a useful example for regulatory action and should urge regulators and the industry to proceed with similar dispatch.

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

Comment: Even for a guiding principle, this strikes us as more of a truism than a helpful standard. And, while regulations should be realistic and not unduly
burdensome for the regulated entities (these statements are truisms as well), why shouldn’t regulators require insurers to have some minimum level of cybersecurity protocols in order to operate? Insurers have long been required to meet certain minimum standards to operate in a state, including capital requirements, loss reserves, and minimum experience levels for a corporate board. Another example is the NAIC’s aggressive push to ensure all insurers, regardless of size, were Y2K compliant at the turn of the millennium. In contrast, while the scope of the Y2K threat and the likelihood of its occurrence were uncertain; the continuing exposure to cyber attacks is a daily certainty for insurers and many other entities.

As insurers collect and utilize more and more consumer information, and do so in a world where cyber breaches are occurring at an alarming rate, minimum cybersecurity requirements will be a natural and appropriate regulatory tool (of course, what the minimum level should be is the real debate). Otherwise, their operations would be similar to allowing a bank to operate in a high crime area with its vaults unlocked; what is stolen due to its lack of care is the “property” (in some sense) of their customers.

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

We agree, but also suggest that mandatory periodic reporting requirements be included. Cyber threats and techniques change at a very rapid pace and therefore cybersecurity measures and standards must do so as well. Requiring regular updates not only provides insurers an additional incentive to keep current (and they have strong market-based incentives to do so already), but is also a way to inform regulators of how insurers are meeting these challenges and help them develop and update the most appropriate cybersecurity standards. This could be done at the NAIC level to avoid multiple, perhaps inconsistent reporting requirements by many states.

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

Comment: While there was some industry objection to the need for “enhanced” solvency oversight, we believe this principle is very important and thank the Task Force for including it. Here is what we know about cyber insurance:

- It is a “product in its infancy” (industry statements).
- Significant growth in the cyber insurance market is very likely (and desirable).
- As a new product, there are many underwriting, claim and legal uncertainties, included pricing, the frequency of loss, the extent of damages that can and should be covered, and the extent to which an insurer’s coverage intent in its policy will be similarly interpreted and enforced by the courts. This legal uncertainty could last for decades – for example, there is
still major litigation over the interpretation and application of the “absolute pollution exclusion” 30 years after its introduction.

- While there are uncertainties with any new insurance product, they are more acute here due to the speed by which the threats can mutate and multiply.
- Cybersecurity is also a national security issue and the federal government has identified the private cyber insurance market as one important tool to “harden” our country’s cyber exposure. Under-regulation and insurer market failures leading to a significant exit from or reduction of the cyber insurance market capacity would have consequences not found in other products.

For these reasons, and probably many others, “enhanced” regulatory understanding and oversight of the cyber insurance market strikes us as not only a good idea, but also a necessary one. The insurance market requires consumer (policyholder) confidence that insurers will be able and willing to pay covered claims well after the consumer has performed – paid the premium. As the NAIC and state regulators have repeatedly stressed, the major goal of insurance regulation in the U.S. is to make sure this promise is kept. Cyber insurance is a market of great promise, but it is also one of unusual uncertainty. Its development will be enhanced by effective market conduct and solvency regulation that is attune to the nuances of this insurance product and the risks it seeks to insure.

We have very recent examples where insurer underwriting and claim miscalculations, and/or the introduction of “faulty” insurance products, have led to the collapse or near collapse of major insurers. For example, in the 1990s and early 2000s, Lloyds was threatened with extinction due largely to the long-term tail exposures of U.S. asbestos and environmental claims that its syndicates had insured or reinsured dating back decades. The California workers’ compensation market similarly almost collapsed in the 1990s after deregulation due, very generally speaking, to inadequate pricing and intense competition and desire to maintain market share.

As Mr. Birnbaum and others have stated, insurer solvency and the containment of systemic risk to the financial system as a whole can be threatened by risky insurance products and underwriting miscalculations, and not only by inadequate capitalization, poor investment strategies and other financial risks that are a focus of traditional solvency regulation. Market regulation therefore is a necessary regulatory tool. The Task Force’s recognition of the importance of regulatory understanding and oversight of this market can lead to substantive regulatory approaches that bolster the cyber insurance market and give greater confidence to the policyholders who would benefit from it.

We appreciate the Task Force’s considerations of our comments and look forward to working with it in the coming months.
Sincerely,

Amy Bach  
United Policyholders

Brendan Bridgeland  
Center for Insurance Research

Bonnie Burns  
California Health Advocates

Marguerite Herman  
Consumer Advocates: Project Healthcare

Timothy Stoltzfus Jost  
Virginia Organizing

Karrol Kitt  
NAIC Consumer Representative

Peter Kochenburger  
NAIC Consumer Representative

Lincoln Nehring  
Voices for Utah Children

Annalise Mannix  
Fair Insurance Rates in Monroe
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 unrepaired.” 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.
The Council to Reduce Known Cyber Vulnerabilities
1747 Pennsylvania Ave. N.W., Suite 1000
Washington, D.C. 20006

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
Deeksha Gupta
March 13, 2015

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 in 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 insureds 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?
• TechArch: Inventory: What information protection-related inventory is kept and in what form(s)?
• Zones: How does the enterprise separate parts (zone) its network(s)?
• Zones: Placement: What systems, data, and people go in which zones and subzones?
• Zones: Connection controls: How are connections between devices controlled?
• Incidents: Detection: Are intrusions detected, and if so, how?
• Incidents: Malicious Alteration Detection: How is malicious alteration detected?
• Incidents: Response: Who controls and executes responses to information-related attacks?
• Incidents: Detection and response: What are the process requirements for detection and response?
• Content control: What mechanisms keep control over content with business utility?
• Content control: How is intelligence gathering countered?
• Content control: How is intellectual property protected?
• Redundancy: Fault model: What fault model is assumed for analysis of redundancy?
• Redundancy: Business continuity and disaster recovery: What information resources are where?
• Redundancy: Interdependencies: How is redundancy applied to interdependent mechanisms?

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?

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

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

Overarching: 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?
• Risk Management: How does the enterprise do risk management?
• 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: Costs: How is security budgeted?
• Management: How does the enterprise manage the information protection program?
• Management: CISO: Is there an enterprise information protection (IP) Lead, and where are they placed?
• Management: Duties: What duties does the information IP Lead have?
• Management: Influence: What power and influence does the IP Lead have?
• Management: Auditing: How are audits managed within information protection?
• Insurance: Audit findings: How are current audit findings treated?
• Management: Legal issues: How do legal issues interact with protection management?
• Incidents: Response: Who controls and executes responses to information-related attacks?
• Incidents: Detection and response: What are the process requirements for detection and response?

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 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 enacted 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
March 27, 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:

I am writing to share our concerns with regards to cyber threats and risks facing health insurers and highlight the progress made, as well as efforts currently underway to address the risks and implications of cyber threats and attacks on stakeholders within the healthcare industry. Collaboration with national organizations and across different sectors has been a critical component in the fight against cybercrime. Continued vigilance is required to protect sensitive healthcare data of American citizens and the Health Information Trust Alliance (HITRUST) looks forward to continued collaboration across different sectors to appropriately and effectively safeguard our nation’s health information.

HITRUST commends the National Association of Insurance Commissioners (NAIC) for establishing the Cybersecurity (EX) Task Force (“Task Force”) and support NAIC’s goal for collaboration among all stakeholders interest in achieving a consistent, coordinated national cyber security approach is essential.

As HITRUST considers how all industries must continue to respond to the increased threat landscape resulting from attacks on U.S. health insurance companies from Nation States and Criminal Enterprises, we seek a partnership with regulators around a security framework that is robust and comprehensive but also aligned to specific industry requirements. The approach that has been formed by leaders in the health industry incorporates the multiple obligations within a common framework that supports our industry and also co-exists with international and NIST security standards to provide a model aligned to the protections needed for consumers in the health industry.

I would welcome the opportunity to present to you how HITRUST can aid the Commission on the critically important issue of cyber security and data protection, and discuss opportunities for HITRUST to collaborate with you, State Commissioners, and your examination partners to address the current and on-going risks to industry and the consumers served by industry.
HITRUST Background

HITRUST was founded in 2007, after recognizing the need to formally and collaboratively address information security for healthcare stakeholders from all segments of industry, insurers, providers, pharmacies, PBMs and manufacturers. HITRUST endeavored to elevate the level of information protection in the healthcare industry—ensuring greater collaboration between industry and government, and raising the competency level of information security professionals.

With regards to aiding industry in cyber risk management, threat preparedness and response, HITRUST has implemented numerous programs in coordination with industry stakeholders. The cornerstone is the HITRUST CSF, a scalable, prescriptive and certifiable risk-based framework relating to information security tailored to the healthcare industry that incorporates US and International standards such as NIST and ISO, federal and state regulatory requirements, best practices and lessons learned from breach events. Over 84 percent of hospitals and health plans, as well as many other healthcare organizations and business associates, have adopted the CSF, making it the most widely adopted security framework in healthcare.

In 2008 and five years prior to the issuance of Executive Order (EO) 13636, “Improving Critical Infrastructure Cybersecurity” issued by the President on February 12, 2013 and before the National Institute for Standards and Technology (NIST) published its Cyber Security Framework, HITRUST published the first version of the CSF and had already identified information protection controls relating to cyber security and issued guidance to the healthcare industry. The CSF is continuously updated to ensure relevance, such as incorporating the NIST Cyber Security Framework and providing health industry implementation guidance as well as privacy controls. Now in its seventh year, the CSF has 135 individual security controls and 14 individual privacy controls and is influenced by the over 10,000 security assessments conducted by HITRUST in 2014 alone.

The HITRUST CSF Assurance Program delivers simplified compliance assessment and reporting for HIPAA, HITECH, state, and business associate requirements. Leveraging the CSF, the program provides healthcare organizations and their business associates with a common approach to manage security assessments that creates efficiencies and contains costs associated with multiple and varied assurance requirements. The CSF Assurance Program includes the risk management oversight and assessment methodology governed by HITRUST and designed for the unique regulatory and business needs of the healthcare industry.

In 2012, after identifying the need for coordination among stakeholders, particularly leveraging the expertise of more cyber-sophisticated organizations to assist less sophisticated players, HITRUST launched the Cyber Threat Intelligence and Incident Coordination Center (C^3) to provide threat intelligence, coordinated incident response and knowledge transfer specific to cyber threats pertinent to the healthcare industry. The C^3 facilitates the early identification of cyber-attacks and creation of best practices specific to the healthcare environment and maintains a conduit through the Department of Homeland Security (DHS) to the broader cyber-intelligence community for analysis support and exchange of threat intelligence. The Center was also the first to track vulnerabilities related to medical devices and electronic health record systems, which are both emerging areas of concern.
The HITRUST Cyber Threat XChange (CTX) was created to significantly accelerate the detection of and response to cyber threat indicators targeted at the healthcare industry. HITRUST CTX automates the process of collecting and analyzing cyber threats and distributing actionable indicators in electronically consumable formats (e.g. STIX, TAXII and proprietary SIEM formats) that organizations of almost all sizes and cyber security maturity can utilize to improve their cyber defenses. HITRUST CTX will act as an advanced early warning system as cyber threats are perpetrated on the industry. CTX is now offered free of charge to the public and has gained wide acceptance within healthcare.

Additionally, HITRUST developed CyberRX, now in its second year, which is a series of industry-wide exercises developed by HITRUST and the Department of Health and Human Services (HHS), to simulate cyber-attacks on healthcare organizations in order to evaluate the industry’s response and threat preparedness against attacks and attempts to disrupt U.S. healthcare industry operations. These exercises examine both broad and segment-specific scenarios targeting information systems, medical devices, and other essential technology resources of the Health and Public Health Sector. CyberRX findings are analyzed and used to identify areas for improvement for industry, government and HITRUST C³ and understand what improvements are needed to enhance information sharing between healthcare organizations, C³, and government agencies. HITRUST also recently announced a health plan specific CyberRX program, CyberRXHP, in partnership with HHS which will be conducted later this summer.

Finally, HITRUST and HHS coordinate a monthly Health Industry Monthly Cyber Threat Briefing – which is open to the public – that provides timely insights on emerging cyber threats and countermeasures. HITRUST is also an active participant on the Health Sector Coordinating Council (SCC) and provides a monthly cyber threat briefings to the SCC.

HITRUST is also a federally recognized information sharing and analysis organization (ISAO), has strong relationships with HHS, DHS and the Federal Bureau of Investigation (FBI) and considers them integral partners to elevate the threat landscape facing healthcare today and strengthen the continuum of care.

**Elevating the cyber awareness, preparedness and response of the healthcare industry**

Growing cyber threats are an increasing risk to not just all areas of critical infrastructure; but healthcare specifically. Increasingly, private sector networks are experiencing nation-state cyber activity similar to that seen on Federal networks. In addition to targeting government networks, there is a growing threat of nation-states targeting and compromising critical infrastructure networks and systems. Healthcare is no exception and is not immune from such threats.

Since 2007, HITRUST has endeavored to elevate the level of information protection by ensuring greater collaboration between industry and government, and raising the competency level of information security professionals across the healthcare industry. We have tremendous experience as a federally recognized ISAO and have many valuable lessons to share. In the past, there has been some confusion on who in the private sector companies can turn to in order to
work with their government partners. HITRUST is determined to be the focal link that will continue to provide value to strengthen our government, our economy, and our nation as a whole given the growing cyber threats the nation faces.

HITRUST, as the healthcare industry’s largest and leading ISAO, has taken a holistic approach to threat intelligence sharing and cybersecurity from the beginning with the HITRUST C3 program, the CTX, the Monthly Threat Briefings, and the CyberRX attack simulation exercises. HITRUST is also a leader in education and outreach. HITRUST’s CSF incorporates the NIST cyber security framework to ensure the CSF is the healthcare sector's premier framework and also an example for other sectors given its rigorous privacy controls.

**Streamlining the Risk Management Process**

Additionally, since July 2014, HITRUST has formally collaborated with the American Institute of CPAs (AICPA) to develop and publish a set of recommendations to streamline and simplify the process of leveraging the CSF and CSF Assurance programs for the AICPA’s Service Organization Control (SOC 2) reporting, the accounting standards for reporting service organization controls. This approach provides healthcare organizations that must comply with HIPAA or other regulatory requirements the ability to leverage one comprehensive, scalable and up-to-date framework relevant to their organization type. This means healthcare organizations can more easily meet the wide and varied array of information protection regulations, standards, best practices and other information protection requirements and streamline and support their SOC 2 reporting requirements.

**Partnership with State Regulators**

In October 2013, Texas Health Services Administration selected HITRUST to assist in development and maintenance of the SecureTexas Program. Texas is the first state to develop a formal approach to certification that incorporates state and federal privacy and security regulations. The Texas program leverages the HITRUST CSF and CSF Assurance programs.

The SecureTexas Program is designed to improve the protection of health information for Texas residents. Organizations participating in the program are able to show they have met state and federal privacy and security standards in order to manage risk and increase confidence in how they protect health information.

Thank you for your efforts and focus on consumer protection.

Very truly yours,

Daniel Nutkis
Chief Executive Officer
April 10, 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 the Health Information Trust Alliance (HITRUST), we thank you and the Cybersecurity (EX) Task Force (“the Task Force”) for the additional time and opportunity to comment on the draft “Principles for Effective Cybersecurity Insurance Regulatory Guidance” (“the Principles”).

We applaud the NAIC for establishing the Task Force and HITRUST believes that it is vitally important that we protect consumers, policyholders, employees, vendors, and others from cyber risks. As you go forward, we offer our cooperation, as well as our extensive experience on the Principles and the work of the Task Force.

Founded in 2007, the Health Information Trust Alliance (HITRUST) was born out of the belief that information protection should be a core pillar of, rather than an obstacle to, the broad adoption of health information systems and exchanges. HITRUST - in collaboration with public and private healthcare privacy and information security leaders - has championed programs instrumental in safeguarding health information, systems and exchanges while ensuring consumer confidence in their use.

HITRUST programs include the establishment of a common information risk and compliance management framework (HITRUST CSF); an assessment and assurance methodology; educational and career development; advocacy and awareness; and a federally recognized cyber Information Sharing and Analysis Organization (ISAO) and supporting initiatives. The HITRUST CSF is the most widely used information risk management framework adopted in the healthcare industry and has been leading the industry in cyber risk management, threat preparedness and response through initiatives such as the Cyber Threat Xchange – cyber threat
intelligence sharing platform and CyberRX – industry and segment specific threat preparedness and response exercises.

Based on our long experience in combatting cyber threats and framework development, we offer the following comments to the Task Force on the Guiding Principles document.

**Specific Comments on the 18 Principles for Effective Cybersecurity Insurance Regulatory Guidance**

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

HITRUST concurs with Principle 1 in that regulators play a significant role in cybersecurity; however, our experience in the healthcare industry has shown that regulators must take an active rather than a passive approach to this role if industry is to improve its state of cybersecurity preparedness. Although the HIPAA Security Rule became effective for most covered entities in April 2005 (April 2006 for small health plans), the industry didn’t begin to make real improvement in cybersecurity until after OCR began to enforce the Rule more vigorously in 2009. Yet despite these improvements, the lack of prescribed standards from federal regulators has demonstrably hampered real progress towards effective cybersecurity across the health industry. This is where industry regulators can play a significant role. As health insurers process and store a broad set of sensitive information, they are inherently a high value target for cyber criminals. As such, insurance regulators should focus on promoting the development and adoption of industry or sector-specific cybersecurity frameworks that align with industry-specific as well as the federal and state regulatory landscape. A focus at the state-level alone could prove problematic for multi-state entities as well as entities that provide provider and payer services through dilution of security efforts measuring against multiple standards and frameworks.

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

Principle 2 should be combined with Principle 1; same comments apply.

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

Principle 3 should be combined with Principle 1; same comments apply.

*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 4 should be combined with principle 5.
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.

While we agree with the premise, we suggest the principle be amended to include relevance to the organization’s business-lines and support an assessment methodology. We recommend updating the principle to read, “Compliance with cybersecurity regulatory guidance must be flexible, scalable, practical and consistent with national efforts embodied in the National Institute of Standards and Technology (NIST) Cyber Security Framework recommendations for industry, sector and organization-specific implementation.

The NIST Framework for Critical Infrastructure Cybersecurity is a broad, overarching framework that relies on existing standards, guidance, and best practices to achieve outcomes that can assist organizations in managing cybersecurity risk by providing a common language and mechanism to (1) describe their current and target states for cybersecurity, (2) identify and prioritize opportunities for improving the management of risk and assess progress toward the target state, and (3) foster communications among internal and external stakeholders. Organizations are expected to use its current processes and leverage the NIST Framework to identify opportunities to improve its management of cybersecurity risk. Alternatively, an organization without an existing cybersecurity program can use it as a reference to establish one. In other words, the NIST Framework provides an overarching set of guidelines for critical infrastructure industries to provide a minimal level of consistency as well as depth, breadth and rigor of industry’s cybersecurity programs.

By working with industry to leverage the NIST Cybersecurity Framework as it was intended, industry regulators can help realize its common goals by promoting the development and implementation of specific industry, sector or organizational-level information protection frameworks or programs that are (1) scalable to organizations or business units of various sizes, (2) tailorable to its unique business and threat environments, including incorporation of a broader risk management strategy to address non-cyber specific threats and multiple relevant regulatory compliance requirements, (3) prescriptive yet practical in its approach, and (4) consistent enough to provide standard, common assessments and meaningful assurances to internal and external stakeholders, such as its board of directors and industry regulators.

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

Principle 6 should be combined with Principle 7 as this is an essential if not critical part of risk-based information protection and must be included if regulatory guidance is to be successfully implemented by industry. Note the Department of Health and Human
Services (HHS) specifically addresses this flexibility of approach in the HIPAA Security Rule § 164.306(b).

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

Principle 7 should be combined with principles 5 and 6. The emphasis on a risk rather than a compliance-based approach to cybersecurity is absolutely necessary if organizations are to consider operational, financial and reputational impacts of a breach beyond the penalties associated with regulatory non-compliance. In fact, it is the risk analysis requirement in the HIPAA Security Rule that sets it apart from most other security-relevant legislation and regulation, as it ensures healthcare organizations—including insurers—implement an appropriate set of safeguards to protect against all reasonably anticipated threats to its information assets rather than simply rely on a necessarily limited set of safeguards specified in the Rule.

The term “threat-informed” is not widely used and could be deleted as a risk-based cybersecurity program necessarily considers all reasonably anticipated threats; however, it appears the term’s inclusion is meant to emphasize the need for organizations to continually assess and adapt to a constantly changing threat environment. Perhaps the language can be changed to read “… risk-based and threat-informed, making use of information sharing and threat analysis” or something similar. We also note the “threat-informed” requirement overlaps with Principle 11.

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.

We concur and HITRUST believes that multiple, independent regulatory examinations of an organization’s cybersecurity preparedness can easily become burdensome and counterproductive. Many organizations already struggle to manage their third party security and privacy assurance requirements, whether it’s the assurances they request or the requests they receive. So rather than implement yet another unique examination of an organization’s cybersecurity preparedness, regulatory oversight that includes a requirement for an industry standard independent review would provide tremendous value. By assessing once against a recognized set of comprehensive and prescriptive information safeguards scaled and tailored to its unique environment, organizations can satisfy multiple reporting requirements by providing specific, targeted views of its assessment. This “assess once, report many” approach ensures organizations can provide and receive necessary assurances that are accurate, timely, efficient and cost-effective.

For example, healthcare organizations could choose the industry-standard HITRUST CSF as a security and privacy best-practices reference or as a certifiable cybersecurity standard. Formal assessments against the CSF can be reported specifically for HITRUST validation or certification of an organization’s safeguards, or they can be leveraged to support external stakeholder requirements, such as AICPA SSAE-16 SOC2 reporting or
formal certification under the SecureTexas program, managed by the Texas Health Services Authority.

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

We concur. Given sufficient threat actor motivation, skills and resources, it’s not a question of if an organization will be breached, it’s a question of when and how often. By implementing traditional likelihood-reducing safeguards such as physical and logical perimeter security and data loss prevention, organizations can reduce the frequency of breaches, but by implementing impact-reducing safeguards such as monitoring and incident response, organizations can minimize the severity of its breaches.

Subsequently, regulators should emphasize the multiple components of an effective incident response program, which includes threat intelligence and incident response testing in addition to planning. The ability of organizations to consume threat intelligence varies greatly, as it requires not just an adequate source of intelligence but the necessary skilled resources and integrated incident management processes to help shape its incident response. Organizations should therefore routinely test their entire incident management capability to ensure effective and efficient detection, reaction, containment and remediation of potential intrusions when they occur. For example, HITRUST works with HHS on the CyberRX program, a series of progressive, no-cost local, regional and national-level incident response exercises to help improve the level of cyber preparedness in the healthcare industry.

**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 concur with Principle 10 as HHS data suggests that, although only about 20 percent of healthcare breaches involve a third party, these breaches account for more than half of the total number of records breached (for breaches over 500 records). What this tells us is that third parties have access to a significant amount of data and present a high risk to healthcare covered entities, and one can reasonably conclude this is true in many other industries. Regulators can and should emphasize the need for organizations to formally manage all their third-party risks—not just cyber-related risks—and leverage the “assess once, report many” approach outlined in our comments for Principle 8 to help provide assurances that are accurate, timely, efficient and cost-effective.

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

HITRUST recommends changing the term “important” to “critical” for the reasons cited in our comments on Principle 8. Through effective consumption of threat intelligence and timely information sharing, organizations can hope to keep pace with constant
changes in the cyber threat environment and efficiently respond to potential cyber breaches.

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

HITRUST concurs with Principle 12 and actively supports a growing consensus in government and industry on the utility of incorporating cyber risk in an organization’s enterprise risk management program. There are two reasons for this. First, cyber risks go well beyond IT as they can adversely impact an organization’s operational and financial viability. Limiting cyber risk management to the IT department can also inhibit the analysis and communication of cyber-related issues and hamper implementation of the cybersecurity program. And second, organizations generally operate in a competitive environment and are resource and budget-constrained. To effectively and efficiently manage risk, all risks to the organization must be identified and prioritized from a strategic, cross-departmental and economic perspective.

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

We concur, but suggest revising and broadening the language to include “as appropriate” since many of these findings may not be material or germane and include other relevant sources of information about an organization’s state of cyber preparedness. An organization’s Board of Directors has a fiduciary duty to provide risk oversight, i.e., to ensure the organization manages risk “consistent with its corporate strategy and risk appetite.” To do this the Board can leverage various documentation and evidence to (1) understand the organization’s approach to cyber risk management, (2) understand the legal implications of cyber risks, (3) have adequate access to cybersecurity expertise, (4) expect that cybersecurity risk will be addressed enterprise-wide, and (5) have regular and adequate time devoted to cybersecurity in board meetings to discuss cyber risk treatments as well as specific plans associated with each approach.

**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.**

We suggest principle 14 be changed as information-sharing and threat intelligence are essential components of cyber incident response; however, the requirement for insurers and insurance producers to join a specific ISAC is too specific and not consistent with the President’s Executive Order 13691 on Promoting Private Sector Cybersecurity Information Sharing, that promotes voluntary information sharing and collaboration amongst private and public organizations and encourages the development of Information Sharing and Analysis Organizations (ISAOs) that can “provide a broader and more flexible means of sharing information” than existing ISACs. For example, in the
healthcare industry the most active cyber threat information exchange is the HITRUST CTX.

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

While not a panacea, HITRUST concurs with the general requirement for the encryption of data-in-motion, as the traditional network perimeter no longer exists. However, even federal regulators recognize the encryption of data-at-rest can be problematic and should be evaluated on a case-by-case basis (reference CMS requirements for Stage 2 Meaningful Use of an Electronic Health Record system). We recommend deleting the data-at-rest encryption requirement or modifying the requirement to allow for selection when indicated by a valid and formally documented risk analysis.

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

Principle 16 should be expanded to address all insurer and insurance producer workforce members (e.g., consultants, interns and other non-traditional workforce members, not just employees) and place an emphasis on a continuous, timely information protection awareness campaign rather than on annual or other periodic training.

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

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.**

No comment.

I would welcome the opportunity to present to you how HITRUST can aid the Commission on the critically important issue of cyber security and data protection, and discuss opportunities for HITRUST to collaborate with you, State Commissioners, and your examination partners to address the current and on-going risks to industry and the consumers served by industry.

Thank you for your efforts and focus on consumer protection.

Very truly yours,

Daniel Nutkis
Chief Executive Officer
April 10, 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 the Health Information Trust Alliance (HITRUST), we thank you and the Cybersecurity (EX) Task Force (“the Task Force”) for the additional time and opportunity to comment on the draft “Principles for Effective Cybersecurity Insurance Regulatory Guidance” (“the Principles”).

We applaud the NAIC for establishing the Task Force and HITRUST believes that it is vitally important that we protect consumers, policyholders, employees, vendors, and others from cyber risks. As you go forward, we offer our cooperation, as well as our extensive experience on the Principles and the work of the Task Force.

Founded in 2007, the Health Information Trust Alliance (HITRUST) was born out of the belief that information protection should be a core pillar of, rather than an obstacle to, the broad adoption of health information systems and exchanges. HITRUST - in collaboration with public and private healthcare privacy and information security leaders - has championed programs instrumental in safeguarding health information, systems and exchanges while ensuring consumer confidence in their use.

HITRUST programs include the establishment of a common information risk and compliance management framework (HITRUST CSF); an assessment and assurance methodology; educational and career development; advocacy and awareness; and a federally recognized cyber Information Sharing and Analysis Organization (ISAO) and supporting initiatives. The HITRUST CSF is the most widely used information risk management framework adopted in the healthcare industry and has been leading the industry in cyber risk management, threat preparedness and response through initiatives such as the Cyber Threat Xchange – cyber threat intelligence sharing platform and CyberRX – industry and segment specific threat preparedness and response exercises.
Based on our long experience in combating cyber threats and framework development, we offer the following comments to the Task Force on the *Guiding Principles* document.

**Specific Comments on the 18 Principles for Effective Cybersecurity Insurance Regulatory Guidance**

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

HITRUST concurs with Principle 1 in that regulators play a significant role in cybersecurity; however, our experience in the healthcare industry has shown that regulators must take an active rather than a passive approach to this role if industry is to improve its state of cybersecurity preparedness. Although the HIPAA Security Rule became effective for most covered entities in April 2005 (April 2006 for small health plans), the industry didn’t begin to make real improvement in cybersecurity until after OCR began to enforce the Rule more vigorously in 2009. Yet despite these improvements, the lack of prescribed standards from federal regulators has demonstrably hampered real progress towards effective cybersecurity across the health industry. This is where industry regulators can play a significant role. As health insurers process and store a broad set of sensitive information, they are inherently a high value target for cyber criminals. As such, insurance regulators should focus on promoting the development and adoption of industry or sector-specific cybersecurity frameworks that align with industry-specific as well as the federal and state regulatory landscape. A focus at the state-level alone could prove problematic for multi-state entities as well as entities that provide provider and payer services through dilution of security efforts measuring against multiple standards and frameworks.

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

Principle 2 should be combined with Principle 1; same comments apply.

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

Principle 3 should be combined with Principle 1; same comments apply.

**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 4 should be combined with principle 5.
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.

While we agree with the premise, we suggest the principle be amended to include relevance to the organization’s business-lines and support an assessment methodology. We recommend updating the principle to read, “Compliance with cybersecurity regulatory guidance must be flexible, scalable, practical and consistent with national efforts embodied in the National Institute of Standards and Technology (NIST) Cyber Security Framework recommendations for industry, sector and organization-specific implementation.

The NIST Framework for Critical Infrastructure Cybersecurity is a broad, overarching framework that relies on existing standards, guidance, and best practices to achieve outcomes that can assist organizations in managing cybersecurity risk by providing a common language and mechanism to (1) describe their current and target states for cybersecurity, (2) identify and prioritize opportunities for improving the management of risk and assess progress toward the target state, and (3) foster communications among internal and external stakeholders. Organizations are expected to use its current processes and leverage the NIST Framework to identify opportunities to improve its management of cybersecurity risk. Alternatively, an organization without an existing cybersecurity program can use it as a reference to establish one. In other words, the NIST Framework provides an overarching set of guidelines for critical infrastructure industries to provide a minimal level of consistency as well as depth, breadth and rigor of industry’s cybersecurity programs.

By working with industry to leverage the NIST Cybersecurity Framework as it was intended, industry regulators can help realize its common goals by promoting the development and implementation of specific industry, sector or organizational-level information protection frameworks or programs that are (1) scalable to organizations or business units of various sizes, (2) tailorable to its unique business and threat environments, including incorporation of a broader risk management strategy to address non-cyber specific threats and multiple relevant regulatory compliance requirements, (3) prescriptive yet practical in its approach, and (4) consistent enough to provide standard, common assessments and meaningful assurances to internal and external stakeholders, such as its board of directors and industry regulators.

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

Principle 6 should be combined with Principle 7 as this is an essential if not critical part of risk-based information protection and must be included if regulatory guidance is to be successfully implemented by industry. Note the Department of Health and Human Services (HHS) specifically addresses this flexibility of approach in the HIPAA Security Rule § 164.306(b).
Principle 7: Effective cybersecurity guidance must be risk-based and threat-informed.

Principle 7 should be combined with principles 5 and 6. The emphasis on a risk rather than a compliance-based approach to cybersecurity is absolutely necessary if organizations are to consider operational, financial and reputational impacts of a breach beyond the penalties associated with regulatory non-compliance. In fact, it is the risk analysis requirement in the HIPAA Security Rule that sets it apart from most other security-relevant legislation and regulation, as it ensures healthcare organizations—including insurers—implement an appropriate set of safeguards to protect against all reasonably anticipated threats to its information assets rather than simply rely on a necessarily limited set of safeguards specified in the Rule.

The term “threat-informed” is not widely used and could be deleted as a risk-based cybersecurity program necessarily considers all reasonably anticipated threats; however, it appears the term’s inclusion is meant to emphasize the need for organizations to continually assess and adapt to a constantly changing threat environment. Perhaps the language can be changed to read “… risk-based and threat-informed, making use of information sharing and threat analysis” or something similar. We also note the “threat-informed” requirement overlaps with Principle 11.

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.

We concur and HITRUST believes that multiple, independent regulatory examinations of an organization’s cybersecurity preparedness can easily become burdensome and counterproductive. Many organizations already struggle to manage their third party security and privacy assurance requirements, whether it’s the assurances they request or the requests they receive. So rather than implement yet another unique examination of an organization’s cybersecurity preparedness, regulatory oversight that includes a requirement for an industry standard independent review would provide tremendous value. By assessing once against a recognized set of comprehensive and prescriptive information safeguards scaled and tailored to its unique environment, organizations can satisfy multiple reporting requirements by providing specific, targeted views of its assessment. This “assess once, report many” approach ensures organizations can provide and receive necessary assurances that are accurate, timely, efficient and cost-effective.

For example, healthcare organizations could choose the industry-standard HITRUST CSF as a security and privacy best-practices reference or as a certifiable cybersecurity standard. Formal assessments against the CSF can be reported specifically for HITRUST validation or certification of an organization’s safeguards, or they can be leveraged to support external stakeholder requirements, such as AICPA SSAE-16 SOC2 reporting or formal certification under the SecureTexas program, managed by the Texas Health Services Authority.
**Principle 9: Planning for crisis response for insurance regulators, insurers, and insurance producers is an essential component to an effective cybersecurity program.**

We concur. Given sufficient threat actor motivation, skills and resources, it’s not a question of if an organization will be breached, it’s a question of when and how often. By implementing traditional likelihood-reducing safeguards such as physical and logical perimeter security and data loss prevention, organizations can reduce the frequency of breaches, but by implementing impact-reducing safeguards such as monitoring and incident response, organizations can minimize the severity of its breaches.

Subsequently, regulators should emphasize the multiple components of an effective incident response program, which includes threat intelligence and incident response testing in addition to planning. The ability of organizations to consume threat intelligence varies greatly, as it requires not just an adequate source of intelligence but the necessary skilled resources and integrated incident management processes to help shape its incident response. Organizations should therefore routinely test their entire incident management capability to ensure effective and efficient detection, reaction, containment and remediation of potential intrusions when they occur. For example, HITRUST works with HHS on the CyberRX program, a series of progressive, no-cost local, regional and national-level incident response exercises to help improve the level of cyber preparedness in the healthcare industry.

**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 concur with Principle 10 as HHS data suggests that, although only about 20 percent of healthcare breaches involve a third party, these breaches account for more than half of the total number of records breached (for breaches over 500 records). What this tells us is that third parties have access to a significant amount of data and present a high risk to healthcare covered entities, and one can reasonably conclude this is true in many other industries. Regulators can and should emphasize the need for organizations to formally manage all their third-party risks—not just cyber-related risks—and leverage the “assess once, report many” approach outlined in our comments for Principle 8 to help provide assurances that are accurate, timely, efficient and cost-effective.

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

HITRUST recommends changing the term “important” to “critical” for the reasons cited in our comments on Principle 8. Through effective consumption of threat intelligence and timely information sharing, organizations can hope to keep pace with constant changes in the cyber threat environment and efficiently respond to potential cyber breaches.

**Principle 12: Cybersecurity risks should be included and addressed as part of an insurers and insurance producers Enterprise Risk Management processes.**
HITRUST concurs with Principle 12 and actively supports a growing consensus in government and industry on the utility of incorporating cyber risk in an organization’s enterprise risk management program. There are two reasons for this. First, cyber risks go well beyond IT as they can adversely impact an organization’s operational and financial viability. Limiting cyber risk management to the IT department can also inhibit the analysis and communication of cyber-related issues and hamper implementation of the cybersecurity program. And second, organizations generally operate in a competitive environment and are resource and budget-constrained. To effectively and efficiently manage risk, all risks to the organization must be identified and prioritized from a strategic, cross-departmental and economic perspective.

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

We concur, but suggest revising and broadening the language to include “as appropriate” since many of these findings may not be material or germane and include other relevant sources of information about an organization’s state of cyber preparedness. An organization’s Board of Directors has a fiduciary duty to provide risk oversight, i.e., to ensure the organization manages risk “consistent with its corporate strategy and risk appetite.” To do this the Board can leverage various documentation and evidence to (1) understand the organization’s approach to cyber risk management, (2) understand the legal implications of cyber risks, (3) have adequate access to cybersecurity expertise, (4) expect that cybersecurity risk will be addressed enterprise-wide, and (5) have regular and adequate time devoted to cybersecurity in board meetings to discuss cyber risk treatments as well as specific plans associated with each approach.

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.

We suggest principle 14 be changed as information-sharing and threat intelligence are essential components of cyber incident response; however, the requirement for insurers and insurance producers to join a specific ISAC is too specific and not consistent with the President’s Executive Order 13691 on Promoting Private Sector Cybersecurity Information Sharing, that promotes voluntary information sharing and collaboration amongst private and public organizations and encourages the development of Information Sharing and Analysis Organizations (ISAOs) that can “provide a broader and more flexible means of sharing information” than existing ISACs. For example, in the healthcare industry the most active cyber threat information exchange is the HITRUST CTX.

Principle 15: Sensitive data collected and stored and transferred inside or outside of an insurers or insurance producers network should be encrypted.
While not a panacea, HITRUST concurs with the general requirement for the encryption of data-in-motion, as the traditional network perimeter no longer exists. However, even federal regulators recognize the encryption of data-at-rest can be problematic and should be evaluated on a case-by-case basis (reference CMS requirements for Stage 2 Meaningful Use of an Electronic Health Record system). We recommend deleting the data-at-rest encryption requirement or modifying the requirement to allow for selection when indicated by a valid and formally documented risk analysis.

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

Principle 16 should be expanded to address all insurer and insurance producer workforce members (e.g., consultants, interns and other non-traditional workforce members, not just employees) and place an emphasis on a continuous, timely information protection awareness campaign rather than on annual or other periodic training.

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

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.**

No comment.

I would welcome the opportunity to present to you how HITRUST can aid the Commission on the critically important issue of cyber security and data protection, and discuss opportunities for HITRUST to collaborate with you, State Commissioners, and your examination partners to address the current and on-going risks to industry and the consumers served by industry.

Thank you for your efforts and focus on consumer protection.

Very truly yours,

Daniel Nutkis
Chief Executive Officer
To: Adam Hamm, Chair of the Cybersecurity (EX) Task Force

From: Patrick McNaughton, Chair of the IT Examination (E) Working Group

Date: April 6, 2015

Re: Cybersecurity Task Force Guiding Principles

The IT Examination (E) Working Group supports the adoption of the proposed guiding principles for effective cybersecurity insurance regulation. Cybersecurity risks represent a significant threat to insurance markets that demands an effective and comprehensive regulatory response. We commend the Task Force’s recognition of the significance of the issue especially in light of recent events in the industry.

As you know, risk-focused financial examinations will likely play a significant role in evaluating the insurance company responses to cybersecurity concerns. Based on the current structure of the guiding principles, we believe that financial examinations will be part of the regulatory response in applying principles 5 through 16.

Principle 5 specifically calls for consistency in cybersecurity guidance with “the national efforts embodied in the National Institutes of Standards and Technology (NIST) framework.” The IT Examination (E) Working Group is familiar with the NIST framework and believes that alignment with this framework will serve to enhance regulatory oversight over cybersecurity risks. Aligning with the NIST framework will help ensure that regulation of insurance companies stays consistent with current best practices which regulators will use to evaluate companies.

The Financial Condition Examiners Handbook (Handbook) already contains guidance to assist examiners in addressing cybersecurity risks during financial examinations. Our existing guidance is based on the Control Objectives for Information and Related Technology (COBIT) framework. The COBIT framework is one of the frameworks mapped within the NIST framework, and the Working Group is developing changes that will ensure existing Handbook guidance is also consistent with the NIST framework. We expect that the revised guidance will be more effective as a result of this comparison and the resulting changes to the Handbook.

While we believe that the NIST framework is a good reference point for evaluating guidance provided in the Handbook, we do believe that there should be a clarification made to allow some flexibility for companies in how they, themselves, respond to cybersecurity concerns. We know that many insurance companies already have an IT security framework based on an existing, widely recognized framework such as COBIT, NIST SP 800, or ISO/IEC 27001. Companies should not be expected to completely rewrite their existing IT security standards, but should instead use the NIST framework as an opportunity to re-evaluate their existing standards to ensure cybersecurity risks are sufficiently addressed. To that end, it may be useful to emphasize Principles 6 and 7 in discussions with those concerned with overregulation. These principles are already embedded within the concept of risk-focused examinations, but we believe this point may merit further discussion in any debates that ensue.

Our IT Examination (E) Working Group continues to consider cybersecurity as one of the most important issues that requires an efficient and effective regulatory response. We look forward to working with the Task Force in the implementation of these guiding principles.
April 10, 2015

Commissioner Adam Hamm, Chair  
Cybersecurity (EX) Task Force  
National Association of Insurance Commissioners  
1100 Walnut Street, Suite 1500  
Kansas City, MO  64106

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:

We, the undersigned, appreciate the additional time granted by the Cybersecurity (EX) Task Force to submit further comments on the proposed “Principles for Effective Cybersecurity Insurance Regulatory Guidance.” As you know, each of our associations submitted comments on the March 12 draft of the proposed Principles, and each of us affirms the comments we made in our respective letters. In this letter, we seek to identify areas of common agreement and of common concern to our associations.

Our respective letters naturally reflect the observations and experiences of insurers in various lines of business. However, we all agree the proposed Principles are a good starting place for further discussion and development. We also agree with comments of you and others that cybersecurity is an issue of paramount importance to government, the insurance industry, and our customers.

Consistent with those comments, we emphasize that cybersecurity regulatory guidance must be flexible, scalable, practical, risk-based, and consistent with nationally coordinated efforts. The Principles must be part of an ongoing process and dialogue involving industry, regulators, and other stakeholders in this dynamic environment, and they should be regularly reviewed and modified so they will not encumber good practices or give a false sense of security. Perhaps most importantly, we believe that guidance needs to be developed as part of a collaborative approach that avoids a patchwork of regulatory regimes, minimizes new administrative burdens, and yet remains risk-based and cost-effective.

We believe that draft Principles 5, 8, 13, 14 and 15 are prescriptive and conflict with the flexibility and resilience on which the Principles are founded. For example, Principles 5 and 14 should provide an insurer with the flexibility to structure its cybersecurity framework as best suited to its size, line(s) of business, particular risk exposure, and other factors unique to each
company and encourage engagement with entities that advance the goals of the Principles. Similarly, Principle 13 is overly specific and requires certain information to be discussed in insurance company board of directors’ meetings, when in fact such audits and risk assessments are already contemplated by most companies in their enterprise risk management processes, and ORSA Summary Reports are required to be delivered to the board or appropriate committee thereof. Principle 15 would require all “sensitive data” to be encrypted, yet information technology experts agree that encryption is not a panacea. We submit this Principle be modified to provide that sensitive data should be protected by appropriate measures, one of which may be encryption.

Again, we appreciate the opportunity to supplement the comments of our respective associations to assist the efforts of this Task Force, identifying the areas in which we share common agreement and concerns. We look forward to working with you on these Principles and other guidance to promote the goals of risk-based, flexible, cost-effective cybersecurity regulations for regulators, insurers, and their customers.

<table>
<thead>
<tr>
<th>Organization</th>
<th>Name</th>
<th>Phone Number</th>
<th>E-mail Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>American Council of Life Insurers</td>
<td>Robbie Meyer</td>
<td>202-624-218</td>
<td><a href="mailto:robbiemeyer@acli.com">robbiemeyer@acli.com</a></td>
</tr>
<tr>
<td></td>
<td>Lisa Tate</td>
<td>202-624-2153</td>
<td><a href="mailto:listate@acli.com">listate@acli.com</a></td>
</tr>
<tr>
<td>American Insurance Association</td>
<td>Angela Gleason</td>
<td>202-828-7181</td>
<td><a href="mailto:agleason@aiadc.org">agleason@aiadc.org</a></td>
</tr>
<tr>
<td>America's Health Insurance Plans</td>
<td>Bob Ridgeway</td>
<td>501-333-2621</td>
<td><a href="mailto:bridgeway@ahip.org">bridgeway@ahip.org</a></td>
</tr>
<tr>
<td>Blue Cross Blue Shield Association</td>
<td>Kim Holland</td>
<td>202-626-4810</td>
<td><a href="mailto:Kim.Holland@bcbsa.com">Kim.Holland@bcbsa.com</a></td>
</tr>
<tr>
<td>National Association of Mutual Insurance Companies</td>
<td>Paul Tetrault</td>
<td>978-969-1046</td>
<td><a href="mailto:PTetrault@namic.org">PTetrault@namic.org</a></td>
</tr>
<tr>
<td>Property Casualty Insurers Association of America (PCI)</td>
<td>David Snyder</td>
<td>202-349-7463</td>
<td><a href="mailto:David.Snyder@pciaa.net">David.Snyder@pciaa.net</a></td>
</tr>
<tr>
<td></td>
<td>Alex Hageli</td>
<td>847-553-3656</td>
<td><a href="mailto:Alex.Hageli@pciaa.net">Alex.Hageli@pciaa.net</a></td>
</tr>
<tr>
<td></td>
<td>Tom Glassic</td>
<td>202-349-7473</td>
<td><a href="mailto:Tom.Glassic@pciaa.net">Tom.Glassic@pciaa.net</a></td>
</tr>
<tr>
<td>Reinsurance Association of America</td>
<td>Karalee Morell</td>
<td>202-783-8380</td>
<td><a href="mailto:Morell@reinsurance.org">Morell@reinsurance.org</a></td>
</tr>
</tbody>
</table>
Dear Ms. Simpson:

As the Principal of i3nsight, an innovation company specializing in Semantic Web Technology and Artificial Intelligence, I count among my clients AIG Insurance, financial institutions and major federal governmental regulatory entities. I am also the developer of a Semantic Armature for regulatory compliance filings that was introduced to the market through the highly regulated insurance industry and is now ready for the adoption of any regulatory change, with the ability to surface conflicts and anomalies and be ready to be fully aligned with all statutory compliance requirements. My credits include the development of security-based systems on which I hold patents on security devices and methods. I also have authored extensive professional and academic papers on the subject of governance, risk and compliance.

Our comments in this paper outline a general prescription for cybersecurity based upon the concept that the facilitation of internal functional change is as important to cybersecurity as individual products and methods. Since many insurance applications are large, enterprise-wide systems, the value of these systems in the day-to-day operations is great, but the exposure to cyber-risk is high. Within these comments, we discuss a novel approach to security that leverages the current enterprise systems and facilitates operational integrity across all actors. We discuss how, through analysis of the “AS IS” state, a system of integrating new techniques can provide a multi-layered approach to security similar to those used by governments to secure their most fundamental data and processes. We make special reference to government-based initiatives throughout, inasmuch as we believe that inheriting such facilities in the commercial sector would help ameliorate risk for all stakeholders--internal and external.

We also believe that such methods would help facilitate meeting the increasingly onerous standards required by insurers that enable enterprises to acquire cyber security underwriting products, thus adding an extra layer of confidence for stakeholders.

The National Association of Insurance Commissioners (NAIC) should be aware that Semantic Modeling provides a powerful solution to cyber security threats because it adds a layer of intelligence into the security process. Semantic modeling speeds delivery of security integration features and solves for complexity that sometimes stultifies security integration efforts. In our comments here, we will discuss the ability to enhance current systems with a non-invasive and non-destructive method of updating legacy computer systems, so that the preservation of value is enhanced and system security is evergreen.
The Federal Identity and Credential Access Management (FICAM) standards provide a high standard of protection for any industry-based application. However, for the insurance industry, the following provides a delivery method based on ontological standards and knowledge based systems supported by Artificial Intelligence (AI) techniques that utilize these standards and enhance their performance.

These techniques provide a unique method of assuring information integrity for both the insurance industry and their clients/customers. The following outlines the adoption of the FICAM recommendations and the application of our specific recommendations utilizing our specialized techniques.

The solution we describe meets or exceeds the FICAM-stated business, data, service and technology goals. The fundamental architecture that we augment these recommendations with meets or exceeds the stated FICAM segmented architecture goals described in more detail below. The system inherits the HSPD-12 (Identity management) controls and standards, is fully FIPS (Federal Information Processing Standards) compliant and additionally, consistently monitors these standards during execution to assure the full integrity of the system.

This is particularly important for enabling the goals of interoperability across and between differing system architectures.

The fundamentals of our recommendations center around the following goals:
- Workflow Management
- Interoperability
- Flexibility/adaptability/agility
- Security

Security systems architectures should support differing workflows and contexts depending on whether it is a security management process serviced by a provider or access methods of a client/customer. These workflows can be many tiered to accommodate all operator levels from users to risk managers and security experts.

The technique we recommend is specifically geared toward enhanced workflow management. Supported by an environment that focuses on managing complexity in a fully segmented architecture that provides a holistic approach (FICAM-stated objective) in a proven architecture that separates concerns across system boundaries that provide intimate coupling to supporting systems such that management of the entire environment is comprehensive yet simplified in its execution.

Workflow management is supported by the development of workflows that can be created by subject matter experts in every domain of activity. At a technical level, the base platform allows graphical representation of the interaction between concepts, relationships (predicates) and subjects. These representations are converted into stable executable code segments that are executed within a stable inference engine that determines automatically goal execution pathways.
These pathways are executed on the satisfaction of pre-and post conditions that eliminate the need for costly design of every conceivable execution pathway. And this is key to managing complex security paradigms. It also enables multiple collaborative functions to interoperate across the business and technical boundaries in one seamlessly linked processing environment.

This eliminates bottlenecks and expedites the execution of processes. Further, the system specifies particular role based activities such that operators have specific boundaries of activities that they can execute, mapped to the best practices of governance, compliance, regulatory controls and training controls built in at the operational level. This too is key as many cyber attacks come from unattended workflows or breaks in security between workflows.

Separation of concerns also allows full interoperability between workgroups and collaboration between domains. For instance, the investigative process can be directly linked to the issuance rules where clearance is a function of a pre-condition for the issuance of a particular credential. These are described in detail section below.

**Increased Security.** By mapping discrete functions as taxonomically organized executable ontologies, functions such as authorization and authentication, encryption functions (including the redaction of PII (personal information identifiers) information, logging, journaling of transactions, audits, sensitive data management, database protection can be linked to create an holistic security function that has independent operators linked in routed workgroups of activity.

**Compliance.** Regulatory compliance is mapped directly from legislative descriptions, translated into - Subject – Predicate – Object frameworks that utilize state of the art standards in data storage and manipulation (RDF – triples), the addition of context is also supported. These may be interlinked to governance (internal policies), best practices at the role, responsibility and relationship level and to global, international, foreign sovereign, state, municipal or local compliance functions. Further, paradox and conflicts are exposed at runtime test to expose rules that may require legal or governance opinion.

**Futurecasting.** Is a technique to assure future compliance functions are implemented when regulation demands it and also allows early impact analysis to manage the effects of regulatory change. At runtime, impact analysis of rule changes can be ascertained in advance of execution and remedial steps taken in advance to assure system integrity.

**Improved interoperability.** This is supported by an open architecture that utilizes Service Oriented Architecture initiatives. Cross credential mapping can enable the requirements of the federal trust framework reducing the need for multiple credentials, improving access controls and reducing reporting overhead.

**Enhanced customer service.** The system enables user portals that are secure and inherit all the security, rule conditions and operator functions that enable self service functions to be as efficient as operator based intervention. In addition, dynamic system monitoring records every transaction, links to supporting servers, time analysis and efficiency monitoring to provide early feedback on customer interactions.
Elimination of redundancy. The interoperability standards, inherit cross domain rules so that replication of functions is removed where there is a common decision cycle or processing of transactions, access to common intermediary databases or persistent stores are synchronized for efficiencies. This is demonstrable in current applications where, for instance, an insurance form filing system can inherit the state by state regulatory rules promulgated by the NAIC so that they are synchronized with each states nuanced regulations; regulatory alignment.

Thus the above topics are amply covered by the recommended process including the implementation roadmap in accordance with security standards such as FICAM.

The proposed concept also takes into consideration inter-agency/ inter business collaboration (treated as a workgroup) and utilizes technology advances that will not impact the fundamental design. In fact, new or emerging technologies such as cloud computing (fedRAMP), identity as a service and SAS models are inherently accommodated by the fundamental architecture; future-proofing the solution. This enables the solution of providing a gateway between, procurement of credentials through collaborating businesses and interoperability between current systems (either by designated APIs or specified “handshakes”.)

Requirement standards:
- A framework for establishing unique digital identity credentials
- A knowledge model for monitoring, controlling and executing how identity data is used
- A rule-based method for protecting private data including redaction at the document level, tagging of protected data and rules associated to access to protected data by role, relationship and responsibility layers of security.
- A role based (rule-based) control in context of access to identity data
- Built in maps to governance and compliance controls of identity data management
- Rapid change capability for remediation of defects (90% documented improvement) and increased STP (Straight Thru Processing).
- Sharing and collaboration between interested parties, workgroups or collaborators including foreign entities, commercial and state regulators
- Revocation intervention either manual or through automated decision recommendations based on anomalous behavior detection
- Identity management across differing identity procurement, issuance and maintenance regimes.

The rules based knowledge models also support other goals:
- Authorization and Authentication assuring integrity of access control both physical and logical entities
- Protection from unauthorized creation, deletion, augmentation, modification or other infractions to credentials
- Provided information in context, reliably, and timely with full maintenance and assured availability under authentication rules.
- Full accountability and reporting of processes, accesses and changes (differential analysis and non repudiation.)

www.i3nsight.com
+1 917 216 3740 • jcoyne@i3nsight.com
The knowledge model, ontology and taxonomic execution platform assures the following for access management. These combine to provide the intersection of information to bind the digital representation of an entity to the credential for access privilege.

- **Reliable resource management:** Business and IT management for establishment and maintenance of identity data. This also allows process control at the transaction level.
- **Privilege management is maintained as a dynamic case.** Cases comprise dossier in electronic form that include privileges, multi-factor authentications, (by role or context) background information, supporting documentation. These can include both physical and logical access management, with separation of privileges at a term level, transaction level, local level, and global level thus managing privileges from a centrally managed case file.
- **Policy management through rules based knowledge models.** These incorporate the full level of compliance, governance, policy management, best practices or other user-defined controls at the role, responsibility, relationship, levels.

**Overcoming current roadblocks**

Complexity is a driving force of stultifying the implementation of cross-border systems. These recommendations overcomes these through a common platform that breaks down complexity into domain slices that allow separate development of differing worldviews with differing vocabularies into a cohesive executable framework.

Common terminology is facilitated by semantic bridges that allow independent groups to use specific terminology (that may have developed over decades) inculcated into current systems to develop their independent knowledge models. The semantic bridge maps terminology into a common ontology that executes independently developed models as a single processing unit.

Term inheritance allows independent groups to inherit rules for execution.Duplicates, paradox and conflicts are surfaces at runtime test. Management can make the best decisions to either support redundant rule execution or integrate them through inheritance.

**Increasing ROI.** Eliminating redundant processes, rules, and behavior models allows for improved use of shared resources and the increase of mutualization in shared services. Thus, reducing duplicate processes, data and maintenance.

**Rapid adaptation.** Emergency situations are anomalies that cannot be adequately programmed for in standard technologies. The proposed platform allows rapid change in use of the system across domain specific boundaries, to individual credentials. This is a function of the semantic taxonomic models that can inherit rules by the simple connection of a relationship from on rule set to another.

**Compliance maturity.** Where interoperating business units have differing maturity of executable policies, management can inherit rules (from common legislation for instance) and improve compliance at their local level while also improving compliance in the interoperating system.
Facilitating cross-disciplinary interaction. The domain slices allow rules and taxonomies to be created within specific disciplinary domains and interfaced to the common platform based on such factors as time, location, periodicity, function, or any rule property (including emergencies) without impacting the individual disciplines current systems environment.

Goal Achievement

The regulatory compliance functions built into the platform support: federal laws, compliance, standards, governance and best practices. It establishes accountability, reporting and audit capability at the role, relationship and responsibility levels. Thus, management hierarchies can have full transparency to decision support, processes and transaction histories.

This recommended approach also enables e-government. The proposed solution has been responsible for government to consumer, consumer to government applications that have established for instance the government of the Netherlands, to receive a United Nations survey analysis of best e-government countries of number 1 in Europe and number 2 in the world. This has the by-product of establishing the public trust and confidence in government systems.

Improving security. The proposed system also improves security because it utilizes multi discipline, agency, security, privacy, data and processing regimes in an integrated platform that acts like a multi-factor authentication at the gross level. These gross level (coarse grain) abstractions inherit the fine grain factors for security also making breaches more difficult, due to the complexity of the interactions. This is also a background protection for cyber security breaches.

Common risk management profile. The recommended approach facilitates a common risk profile for use of the system across credential types, agencies, participants and individuals. This also facilitates alignment with external partners. The common framework reduces administrative burdens by providing detailed audit and reporting through standard reports and automated dashboards.

Regulatory inheritance

Unlike competing alternatives, the recommended approach can interpret and inculcate a full range of legislative and regulatory initiatives. Such as the following: HSPD-12, PL 110-53 (9/11 commission) EO12977, 13467, OMB M-00-10 (paper elimination) M-04-04 recommendations for authentication, M-05-05 (digital signatures) M-05-24 common standards, M06-16 (protection of sensitive information) M-07-16 (PII safeguards)

These can be implemented as guidelines, rules of behavior, audit analysis for comparison to standards, or inculcated at the process level. The reasoning trace elements of the proposed solution provided by the AI functions can reveal the rule, its source and the map of decisions made during a transaction process. This also enables the audit to include “how was that decision made, what data was used, what rule was fired, and why)
The recommended approach also meets or exceeds the standard of the Federal Segment Architecture Methodology (FSAM) and its five-step architectural reference guide. Firstly, it meets the objective of a holistic approach.

Secondly, its domain slicing accommodates the separation of concerns into the five layer Federal Enterprise Architecture (FEA) recommendations: Business layer, data, service (SOA) and technology.

The special feature on supporting these is the ability to demonstrate the inter-relatedness between these layers, expose road blocks and redundancies and facilitate interoperability.

The performance architecture models the business goals, drivers and objectives into executable models for impact testing.

The proposed solution “Static Analysis” feature provides an exact “AS IS” state for setting baselines in architecture, system interactions and code execution from field, to term, to process, to rule, to application. This provides the starting point for the interaction and interoperability between and across existing system architectures.

Supports full use case enablement

<table>
<thead>
<tr>
<th>Use Case</th>
<th>Embodiment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create and maintain digital Identity record for user</td>
<td>Provides knowledge model to establish a digital identity and modification of the ID record over time as attributes change</td>
</tr>
<tr>
<td>Provide Background investigation for applicant</td>
<td>Provide multi-level process steps for conducting background investigation</td>
</tr>
<tr>
<td>Create issue and maintain PIV card</td>
<td>Provides multi-level process steps by role for issuing a PIV credential and maintaining same over lifecycle complying to FIPS 201</td>
</tr>
<tr>
<td>Create and Issue PKI credential</td>
<td>Creates multi-level process steps for creating PKI certificates over credential lifecycle</td>
</tr>
<tr>
<td>Create and issue passwords</td>
<td>Creates multi-level process steps for creation and comparison to standards of a password token for the lifecycle of the credential</td>
</tr>
<tr>
<td>Provision and de-provisioning of user account for an application</td>
<td>Provides multi-level authorization and authentication facilities for creating, maintaining and de provisioning of user accounts including particular access privileges by term of use or SLA</td>
</tr>
<tr>
<td>Grant physical access for employees, contractors or visitors</td>
<td>Creates multi-level facility to provide physical access to locations including multi-factor authentication where required</td>
</tr>
<tr>
<td><strong>Grant logical access</strong></td>
<td>Creates multi-layer/level access control by role, responsibility, relationship, context to systems, applications, processes data. System exceeds ICAM standards by providing alternate/multiple pathways, routing for authentication processes</td>
</tr>
<tr>
<td>------------------------</td>
<td>-------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Secure document or communication with PKI tokens</strong></td>
<td>Provides dossier, document, heading, word level tagging of documents in currently available document systems for encryption, redaction or removal of sensitive data to role level users.</td>
</tr>
<tr>
<td><strong>Enable Trigger events</strong></td>
<td>System enables triggering events that initiate processes, multiple triggers supported</td>
</tr>
<tr>
<td><strong>Actor Support</strong></td>
<td>Provides mult-level access to individuals, workgroups, collaborators by role, context responsibility</td>
</tr>
</tbody>
</table>

**Service-level Frameworks**

Provides a multi-level container that provides, categories and classifications of service components. A service container maintains the attributes for a business process or service with predetermined or well-formulated functionality operated across and between a well defined and documented technology interface.

Some service components include: Vetting, adjudication, lifecycle management, identity attribute discovery, linkages, attribute exchange, sponsorship, enrollment and registration issuance, privilege administration, self service, provisioning, attribute management, authentication and authorization, credential validation, session management, service federation, policy administration, enforcement, decision, digital signature, encryption services, key management, audit management, dashboards.

**AS IS architecture. Defining the AS IS state – tools for rapid identification of data and code provenance across heterogeneous environments**

The AS IS architecture provides the snapshot of existing systems and dependencies so that the target architecture is correctly conceived in the context of leveraging the current infrastructure, systems, applications and any code base. This means that the existing system value of the insurer is maintained and enhanced.

**Static Analysis of current systems to augment with security features**

This is a particularly thorough way of pinpointing security breach possibilities: intra-application – inter-application, network, third party connections and middleware. Through static analysis of code based systems the proposed system and tools successfully performed the following:
• Exposed the entire architecture of systems and interfaces with a full graphical taxonomy – facilitating forward and backward analysis
• Revealed the activities of applications and each and every transactional term within the program
• Created reports that expose the Name of the Application, the description of its activity, terms used, processes invoked and actual code with line numbers to confirm raw business rules.
• Created a full term and rule cross reference on all analyzed code
• Exposed all inter-program dependencies so that changes in one application can show propagation of effects across all linked programs and term usage
• Created “slices” which allow separation of computed items, business cases, and process cases – reducing complexity
• Created a full differential analysis of code so that anomalous functions can be identified – revealing dead code, spaghetti code and paradox
• Created a fully curated environment that allows check in and check out with full signature and recognition of the most minute changes in applications with time stamps and where necessary digital signatures
• Vendor integration analysis (greatest source of security breaches)

Process and operations analysis

In addition to the analysis of programs and data, it is necessary to review how applications are used by operators and the heterogeneous network of servers and client systems in, across and between systems.

With real-time analysis of personal usage of systems we can:

• Provide full analysis of what applications a user calls
• How long they remain in the application,
• The rate of response from servers,
• Analysis of anomalous behavior and,
• Comparative usage against best practices.

Every screen, decision and activity at the field level is exposed.

Migratory modernization

What this means is that if necessary, system modernization can be a migratory activity that allows insertion of repairs, augmentations or work-around alternatives at the line or term level within an application. This leverages the legacy while preparing for the future in a practice we describe as “above the line” programming.

From this fundamental approach it can be seen that a single term or field within a report can be traced all the way back to its original source with all the transformations and calculations revealed. In addition it can also be seen that any function can be followed to reveal its next transformation in the process flow. This forward and backward tracing provides exact transactional detail at the finest granularity.
Graphical Architecture Exposure

In this diagram of a real architecture a top down approach is revealed.

In this example, JCL running particular programs identifying the exact inputs and outputs (green boxes) of any program together with the conditional relationships between them. Furthermore, we can discovered where a particular input was created, and what were the inputs involved in its creation.

This is important for data provenance compliance and completeness. We may discover, for instance, that one of the inputs is insufficient (should have contained more data).

Figure 1. Coarse Grain Architecture Taxonomy

This is not all, each box contains within it expandable detail with all the information at the application level which in turn contain precision details of terms and computations.

Figure 2. Application level exposure from expansion of application content

After viewing the logical view of the application, individual terms can be exposed which is one of the most fine-grained of details.
These logical views are helpful for process discovery. However, it would be helpful to follow terms from the user’s viewpoint. So, for instance, if in a customer report, a particular field has an exposed balance transaction, the tool can expose the full provenance of the field, its calculation base at the term level, the rules as applied in the application and the sources of data and inter-dependent programs so that if the exposure is not compliant, the source of the problem is found.

In the illustration below, the tool, allows a user to view the actual screen presented as in for instance a report or an input system. This means for instance (in the example given) that a balance number can be researched from the report itself and traced all the way back to its origins in data, terms, computations, and transformations - from the architecture to the actual calculation and the line numbers where they occurred. The tool reveals the business term and translates it to the technical term, provides attribute data and any parent/child relationship.

We can see the screen as it is presented to the user, as well as the names and properties of all fields on the screen.

Since the tool reveals both the headers of the fields (which give their business meaning) and the technical names as they appear in the code, this information can be used to systematically build a Data Dictionary, which is an essential ingredient of any analysis.

This helps the pattern analysis build and spiral effect of efficiency in understanding the overall goals of the application.

This is also exposes how one can intervene in the application process. Now, knowledge of the data, data element, and line of code where the event takes place is revealed. This means we can automate the capture of anomalies and report them to the appropriate stakeholders.

Field or Term of interest in the project explorer
Revealed screen with fields and identifiers
Attributes – references – traces
Term

www.i3nsight.com
+1 917 216 3740 • jcoyne@i3nsight.com
The Discovery of Business Terms

The discovery of business terms is based on the ability to expose the raw rules as expressed by the code and a translation of those terms into business terms recognizable by any subject matter expert or experienced business user.

The tool allows you to perform an iterative process to build a complete dictionary that will be part of the reporting analysis. This allows the identification of terms and associated parent/child relationships between them. Also calculations associated with each are revealed. In addition, every predicate (backward trace) can be explored with the automated query facility.

Figure 5. Term searching with rules and attribute exposure

Discovery of business terms is the same as building a Data Dictionary, something that it is may be missing in some older systems. Unlike a Data Dictionary that sits in an outside document, our business terms have pointers to the code, indicating which fields implement them. This means that in future, the data dictionary will be part of the report and fully reference-able.

One can start with only SOME knowledge about the business terms (such as G-Total) in this case, and then identify all terms (and implicitly individual fields) of interest.

This process continues through an alternative/iterative process:

- find a term
- find a rule about the term
- see which fields participate in the rule
- make terms out of the important fields
- continue with the first step

The result is a complete Data Dictionary.

Discovery of Business Rules

Rules in undocumented (or poorly documented) systems can be hidden behind the code itself. Commentary in applications do not always document the variables and conditional effects of flags associated with data. Discovery of rules can be determined through the query tool that allows exposure of the terms, variables and expressly written code to add business language in the commentary.
In the illustration above, the user selects the term of interest, the term details are revealed and the code associated with it identified by application and line number.

**Discovery of computations and business cases**

When looking at particular cases of activity within a program, it is desirable to focus on certain terms and business cases to limit the breadth of activity to areas of particular interest. This means that investigations should be limited to particular computations (on actual data) or on terms within a program. Or, to particular domains of activity which are business related. These views are called “slices” as they allow the analyst to take a slice of activity and treat it as a particular case of interest within a complex program. This reduces complexity to the merely complicated.

Two types of “slicing” are supported:

- Computation attributes and parent child relationships
- Domain of interest
- Total complexity of application
- Domain slice in graphical form with conditional statements

A computation slice reveals how a term is computed
- A domain slice reveals operations in a particular business case

Sample computation slice:
- How is interest adjustment computed in all cases (all accounts, transactions, etc.)

Sample domain slice:
- What is done with transaction code #7, or accounts with a particular characteristic.

The two techniques may be combined to find, for instance, how the system computes adjustment for a particular transaction.

Since 64 account numbers for instance may not appear explicitly in the code, particular accounts are processed based on some of their attributes.

If these are known, domain slicing can limit the computations to these accounts.

To apply this technique we need to know accounts and transaction attributes, which are perhaps stored in some data files or tables.

Figure 6. Term extraction and detail – with code – line number – attributes

Figure 7. Reducing complexity through –term – domain – computation slicing
Making Sense of The Raw information

For engineers, the raw information may be meaningful but for business users and those that must corroborate the business rules, native language is more appropriate.

The stages in identifying terms move from: raw (as coded) to specified, when an SME reviews the raw term and gives it business meaning and can move to audited if the term needs additional review and approval.

Figure 8. Rule exposure – raw – specified and audited

Comprehensive Reporting

The extraction and analysis tools produce a fully searchable file that creates a report that can be used at any time when investigating: Fields, Terms, Rules, Processes, Data Flows, Data Transformations, Sources of processing, Sources of Data, calculations and computations. These reports become the foundation of comprehensive sourcing for all uses of terms across all applications. What this means is that a term used in one application can be queried to see every application that it is also used in. This reduces the need for individual reports that specify the usage of particular cases as a calculation made in one report will be propagated throughout all other reports using the same calculation base.
Locating business rules and their associated terms

Once terms and rules are established, a database of cross-references aids analysts in locating the term, its associated rule and its varied locations. This quick reference guide can accelerate term identification that can be used in comprehensive searches. It eliminates any vagaries and can help to establish single points of reference for terms that do the same process but use alternate naming conventions.

This cross-reference allows an analyst to quickly locate a business rule.

One may ask the question: what rules are concerning Year-To-Date Interest Accrual. The analyst may look up this business term, then see which rules apply.
Anomaly Detection – Differential Analysis

One of the benefits of fully understanding the architecture, code and data elements is that comparative analysis can be performed at any level to detect undocumented changes. This is also useful in cleaning code bases that may have redundant code, truncated strings and “spaghetti code”. For IT, this facilitates the basis for a "check in – check out" method that provides a stronger level of control and non-repudiation of changes. It can also be used to assure that recommended changes have been performed in a specified time frame.

Just as important, the system can support full cross dependency referencing. In other words the system automatically reports on all applications, terms and processes and their cross dependency with other applications, terms and processes across and between systems.

![Cross dependency matric at the architecture – application – program and term levels](image)

In the report above, application dependencies are clearly displayed so that IT managers can instantly see where changes in one application may affect multiple associated applications.

Figure 11. Cross dependency matric at the architecture – application – program and term levels

Statistical Metrics

A side benefit of the depth of analysis is the ability to forecast and analyze the complexity of particular applications. For instance, in one application with 50,000 lines of code the system detected 12,000 branches which is 12 times the norm. The number of data structures at the (01) level was nearly 350 and the number of fields was 16,500. This is an extremely complex application. However, identification of the data and structures moves the degree of difficulty in dealing with it from complex (meaning virtually unknowable in manual terms) to the merely complicated as each level of complexity can be identified and managed discretely.

In addition, the system can report on I/O complexity, business rule density and relative application layer sizes.
With these comprehensive tools, IT departments can document at the most detailed level, the fundamentals of their “as is” state within hours, days, or weeks depending on the complexity. Manual processes may be entirely unfeasible which is one reason that security breaches occur. The IT department simply doesn’t know what is happening with the internals of the compute environment.

The purpose of such tools is to establish, without armies of programmers and analysts the basic structure of those elements that can be augmented, repaired or discarded at a level of precision that has hitherto been impracticable. What this means to business users and IT executives is that “you can get there from here”.

Managing/ Embracing Complexity

These technologies enable agility in defining, building and deploying complex systems. Systems that are open ended with no pre-defined (closed world definitions) and can goal seek to achieve decisions and recommendations that would otherwise be too complex or infeasible to design for with traditional methods. The company routinely deals with the top three elements of complexity:

- Dynamic
- Social
- Emerging

**Dynamic complexity** comprises the activities, procedures and processes across the entire enterprise and incorporate the further complexities of business requirements and IT support of those requirements. The proposed case management system separates these responsibilities into a unified environment that enables rapid development and deployment of applications while adhering to the most stringent of SDLC standards.

**Social complexity** deals with the interactions between business activities in the context of their stakeholders (internal and external). The dynamic case management enables enterprise management to master value chain integration; creating complete value webs.

**Emerging complexity** is characterized by change and uncertainty and the ability of an organization to adapt. Case applications have increased the time to change by over 90% in documented cases and increased straight through processing to 98% (recorded as time to change, implementation reduction in exceptions and step execution reduction)
Semantic Executable Models

A semantic model describes business logic in such a way that it is openly accessible and readable for human beings, through the use of diagrams and near natural language.

At the same time providing the means for computers to interpret the logic and derive meaningful conclusions from it. This allows the ability derive decisions based on incomplete information, logical pathways and multiple (perhaps unknown) dependencies.

The recommendation of a case management system means that it is fully goal seeking. It separates the business logic from the execution by having models defined in an ontology that executes through an inference engine that finds the best path to achieving particular outcomes. An ontology is a way of describing relationships between objects for instance between various applicant characteristics as well as the dependencies between certain business activities and relations between business rules.

The system adheres to and employs open standards such as: Resource Definition Framework (RDF) and Web Ontology Language (OWL). The proposed dynamic case management comprises four main domains:

- Products and Decisions
- Cases, Activities and Artifacts
- Interaction and Services
- Registration and Objects

The goal of administrative functions is to arrive at a decision (sometimes with incomplete information). Built into the dynamic case management system are various pre-configured (modifiable) instruments for modeling decisions and making determinations, classifications and calculations.

A semantic system produces a complete decision trace (reasoning trace) of all decisions and pathways utilized for any conclusion. When highly complex interactions are taken into consideration, these reasoning chains can be analyzed in “domain slices” that reduce complexity to certain decision areas. This is enabled by the use of taxonomies of business structures that may be linked to a complex web of activities but analyzed independently. The design models also allow any level of abstraction to facilitate the analysis of interaction between taxonomies.
Cases - Activities and Artifacts

Typical business definitions are linear with particular lanes of activity and decision dependencies between lanes that become complex and near infeasible to design for every unforeseen requirement that becomes exposed at implementation time.

A semantic dynamic case management is goal seeking (backward chaining). It starts with a desired outcome of a process (typically a decision) and then determines for every single case or transaction which activities (including actors for routing) are necessary for that goal to be achieved; automatically. Because it is a completely dynamic process it can be unique to each and every case. Importantly, the case list of activities is automatically and immediately updated whenever there is relevant or new information relating to the case.

In a dynamic case management system, there is no predetermined sequence of operations. The semantic model contains the full range of defined business activities and their pre and post conditions for activation. This means a business activity can only start if its pre-conditions are met. This creates an environment in which every meaningful range and combination of activities is possible to execute in the least amount of steps. This enables improved straight through processing with a wide variety of case variations (known or unknown). Every case is unique by design, using only the rules and activities that are needed to complete it.

Interaction and Services

Management is also supported by standard functions that manage flexibility, such as imposed time limits between activities. This can be a monitor for best practices, governance, regulatory controls or simply internal strategies of operational and performance controls against a variety of measurement criteria. Since there is a direct correlation between such rules, a reasoning map would provide full audit reporting, that for instance stated, that a particular time limit had multiple dependencies (governance and regulatory for instance) with direct mapping to the actual text and rules of execution (enabling performance monitoring against actual goals) providing further analytics. Dashboards are also available for management control.

Further, when new legislation or rules are determined to be necessary in some future date, these can be pre loaded, tested for impact and fired on the day they are required with full trace of the impact on all cases.

Dynamic artifacts (emails, voicemails, spreadsheets, dockets, forms, Word documents etc.) can be controlled by and through the dynamic case management system. This provides auditors and security teams with the capability to review communications between internal and external users and have them associated directly with the case with full time stamp journaling provided, maps to regulations, governance, security, accuracy analysis etc.
Registrations and Objects

Throughout the course of dynamic case handling, a wide variety of information and data is collected to facilitate decisionmaking. This input can be made manually or collected from various data sources. The semantic structure contains all the functionality required to describe these properties.

A dynamic case model only contains business logic. This allows the models to remain stable and meaningful while underlying technical mappings to data models in other business applications and databases are stored separately in behavior profiles. This enables the separation of concerns allowing IT to configure the technical behavior of the case including integration with other systems. These definitions can include, data abstraction, access and type for that matter (replication services, warehousing, distributed, centralized, networked etc.), communication protocols, authentication and authorization (at the role level and the element level), infrastructure and integration with other systems that may be called or used from time to time.

Meta models for decisions, cases and registrations are large and sophisticated; enough to drive all user interaction in full role, responsibility and relationship context. To enable rapid adoption, templates can be utilized so that there is no need to specify screens. The dynamic case management system “knows” how to interpret Models and present the correct questions and options at the precise moment they are needed. These templates can be modified to meet specific corporate direction.

The dynamic activity plan is an important standard feature. It displays at all times a comprehensive list of activities whose pre-conditions have been met such that they can be started. There is no predetermined order. In addition, it displays all activities that have been met and dynamically determines all activities that can be performed now and in the future. After each activity (or actor, in collaboration or workgroup) completes a task, the activity list is recalculated automatically.

Registrations also provide the mechanisms of control for access such that for instance all access can be defined for internal or external users to use a particular portal. Roles, responsibilities, relationships can all be defined with controls to regulate what information can be viewed, used, updated or otherwise manipulated in the course of a case process.

Integration Services

In addition, the semantic platform integrates (interoperates) with other systems through registrations of service calls. The service structure allows IT to determine orthogonally the most appropriate service mechanisms to achieve user functionality. IT departments routinely use a Services Oriented Architecture with SOAP (simple object access protocol) and/or ReST together with XML handshakes. This means that services can be defined in containers of activities such as cases, users, roles, and the like. Containers or contained access may result in different services to be accessed within a case. For instance, registration of an insurance customer will go through a registration service, then on to product linkages. Brokers and staffers may utilize the services of specialists, lawyers, and adjudicators. Each role can be defined as a service and registered as such. This orthogonal approach enables complexity in execution while reducing design complexity.
As such, use-models as services, contain all the documentation relating to their design as an automatic link. The model of activity is defined not only by the taxonomy but the elements of the taxonomy are further defined by type with full-written descriptions of their processes and goals. This means it will have well known and published operational characteristics.

**Security as a service**

Security for user management can also be a service function. The semantics approach can accommodate single sign on, authentication and authorization at any registered level. An LDAP directory can be used to create the authentication and authorization layer and provide the first line permissions associated with role definitions at any level of granularity. Containerization can be a powerful mechanism to separate specialized authentication rules for particular cases. Equally, security can utilize “mutualization” [sic] to provide a common service layer. The dynamic case management accommodates any regime.

---

**About John R. Coyne**

A leading technologist and entrepreneur with expertise as a software C-Suite management executive, industry advisor, and developer of transformative business innovations, John R. Coyne is a published inventor with multiple patents issued and pending in advanced technology, devices, systems and methods.

With decades of experience, including the successful startup and development of several enterprises, Mr. Coyne has proven his executive prowess in developing thriving businesses from scratch. Particularly in financial services, media and defense industries, he has developed innovations to transform assets and performance for all stakeholders.

He was the senior lead in the development and sale of artificial intelligence-based mainframe systems developed in Europe. He has managed operations in the U.K., The Netherlands, Germany, France and Ireland for both public and privately traded businesses. Acting for Netscape, he was the principal architect of a strategic partnership with Citibank, an alliance that generated substantial revenue. Mr. Coyne also founded the Object Technology Group for SHL Systemshouse, which led to its acquisition by MCI. He was a principal in IPECO; an intellectual property company focused on invention and innovation technologies for e-commerce concerns.

As a technologist, Mr. Coyne was a founding member of the Rosetta Project; a privately funded research group that provided transportable software languages based on BCPL. He founded Base Technologies, which produced the world’s first windowing software for PCs and the world’s first multi-file access operating systems enhancements. Mr. Coyne also founded Cool Technologies, which provided the basis for multi-component object classes that could be re-combined to produce “applications-on-demand.”

Other past positions have included Director of Advanced Solutions for KPMG and Director of Strategic Consulting for Oracle, a division he founded.

www.i3nsight.com
+1 917 216 3740  •  jcoyne@i3nsight.com
April 10, 2015

General Commentary:

The term “Cybersecurity” is a misnomer in my opinion because it gives the impression that exposures in this area are to be addressed in the realm of Information Technology; nothing could be further from the truth, and I prefer the terms/phrases “Privacy and Network Security” or “Information and Information Systems Security” because I believe it speaks to the broader concerns rather than the subset of “cyber” issues. Certainly, Information Technology is a significant component in the overall information asset ecosystem and I’m not diminishing the importance of a strong IT security posture, but it is only a single component. Without a holistic approach to this space and these issues, starting at the Board and Senior Leadership levels, there is a high likelihood that any organization will fail to take the appropriate steps to materially insulate themselves against data breaches and other privacy or network security incidents. There needs to be an awareness and supporting effort at every level and within every department, because this space is a weakest link proposition; therefore, it requires senior leadership to properly develop and administer a meaningful privacy and network security program.

Commentary on various “Principles”:

Principle 6: While some controls and security tools are very expensive, as a privacy and network security insurance underwriter for 7+ years and through my review of thousands of risks from that perspective (including a fair number of insurance-related entities), I’d note that there are meaningful, low-cost strategies and solutions that are not being used by a vast majority of all companies. A significant amount of the “noise” in this space could be reduced if companies were simply addressing the “low-hanging fruit.”

These include (but are not limited to) things like:

- Creating a data asset classification program
- Addressing appropriate access to information
- Requirement of stronger passwords with longer strings of characters
- Robust training and awareness programs for all levels of employees
- Evaluation and triaging of data assets that may no longer be necessary for business operations

Principle 8: Evaluation is important, but in my opinion regulatory oversight often leads to a “checking-of-the-boxes” approach/mentality by organizations looking to comply. This space, and the malicious actors in it, are dynamic and anything that leads to a static cycle of review and compliance could ultimately be detrimental to the broader goal of enhanced privacy and network security controls for the insurance industry and for businesses in general. Companies are compelled to devote time and resources to “complying” which may not always be the same as devoting time and resources to the greatest areas of privacy/network security concern for that particular organization. Any oversight should look not only for the “checked boxes,” but also that an organization’s efforts are in the spirit of progress rather than compliance.

Principle 12: I agree with the sentiment of inclusion in organizational ERM, but believe that most insurers and insurance producers are not yet fully capable of accurately evaluating the exposure at the enterprise level. There is very little in the way of loss data, and the landscape is worsening/changing at a rapid pace, creating further difficulty in evaluating the exposure. Just noting as something that may need to be considered...

Principal 16: Education is critical. However, I personally believe the vast majority of training tools are insufficient. They do identify relevant issues generally, but fail to personalize the message... more specifically, people still don’t fully comprehend the potential implications of their actions and inactions, and the training materials that I
commonly see do not do a good job of bringing this critical area of concern to life. Education and awareness is a front line defense in the privacy and network security space, but the approach needs an overhaul.

If the above is not consistent with the type of feedback you were looking for, please let me know. I appreciate the opportunity to provide commentary - have a great weekend.

Sincerely,

Joshua M. Ladeau, CISSP
Practice Lead - Privacy & Network Security
Allied World Insurance Company
1690 New Britain Avenue Suite 101
Farmington, CT 06032
T: 860-284-1654
M: 860-713-3966
E: joshua.ladeau@awac.com
W: www.awac.com
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
April 10, 2015

The Honorable Adam Hamm
Chairman
NAIC Cybersecurity (EX) Task Force
North Dakota Insurance Department

The Honorable Raymond Farmer
Vice-Chairman
NAIC Cybersecurity (EX) Task Force
South Carolina Department of Insurance

Dear Commissioners Hamm and Farmer:

Marsh & McLennan Companies (MMC) appreciates the opportunity to submit comments pertaining to the National Association of Insurance Commissioners (NAIC) Draft Principles for Effective Cybersecurity Insurance Regulatory Guidance.

Marsh & McLennan operates through four market-leading brands — Marsh, Guy Carpenter, Mercer and Oliver Wyman. Our 57,000 employees provide advice to clients across an array of industries in the areas of risk, strategy and human capital. As the leading insurance broker in the world, Marsh has a unique perspective on the cyber insurance market.

In addition to providing these comments, MMC has been at the forefront of engagement with policymakers in the US and UK to assist them in better understanding this rapidly developing insurance sector. In January 2015, MMC testified before the US Senate Homeland Security and Government Affairs Committee and provided lawmakers with cyber insurance market data, including cyber take-up rates, pricing and limits available for purchase. Recently, Marsh in collaboration with the UK Government, produced a report entitled “UK Cyber Security: The Role of Insurance in Managing and Mitigating the Risk,” which highlights the role insurers and insurance can play in reducing cyber security risk.¹

We commend the NAIC for its diligent efforts in developing the Principles for Effective Cybersecurity Insurance Regulatory Guidance. As the Principles rightfully recognize, insurance regulators have a significant role in protecting customers from cyber

¹ A full copy of the report is available at:
risks, including the unauthorized disclosure of personal data. In addition, insurance regulators have a unique role in helping regulated entities share information and drive change across the industry.

However, cyber risk is an emerging problem with constantly evolving threats and attacks over which our understanding remains imperfect. Enhanced information sharing, regular assessments and training will serve to strengthen cyber preparedness. In contrast, setting static practice standards that use common denominators to address cyber risk could sap resources with little gain. Accordingly, the Principles should reflect risk-based priorities that are designed to counter evolving threats with finite resources.

**Avoid Technical Mandates**

It is important for the Principles to set a similar tone that avoids a mandate for efforts to empower cyber defense. For example, draft Principle 5 contemplates that “Compliance with cybersecurity regulatory guidance should be flexible, scalable, practical and consistent with the national efforts embodied in the National Institute of Standards and Technology (NIST) framework.” (Emphasis added.) However, the NIST Framework avoided any suggestion of a compliance regime and favored a voluntary, performance-based and cost-effective approach toward cybersecurity. Use of the word “compliance” in Principle 5 suggests replacing the voluntary approach with mandated actions.

Similarly, draft Principle 15 advises that “[s]ensitive data collected and stored and transferred inside or outside of an insurers or insurance producers network should be encrypted.” Encryption technologies are a vital component of security, but the draft Principles should refrain from technical recommendations given the industry use of diverse encryption technologies. The draft Principles should recognize that other controls, such as data minimization, can be as important as encryption in a robust data security program.

**Encourage the Growth of Cyber Insurance**

Moreover, draft Principle 8 recognizes the importance of regulatory oversight. However, it will be equally important to drive change through incentives and innovation. While regulated organizations incur threats to customer data and their own networks, the insurance market has also created resources for entities to address cyber threats. Today, cyber insurance is a growing component of strategic planning to mitigate, respond to and recover from cyber threats. Because the insurance market can drive broader change, insurance regulators should promote its potential.

Draft Principle 17, which mandates “[e]nhanced solvency oversight” of insurers selling cyber liability coverage, should be reconsidered. As cyber insurance develops in its nascent stage, enhanced solvency requirements could create a disincentive for selling cyber coverage. While cyber coverage is a relatively new product, it presents no unique risk to insurer solvency. Isolating cyber coverage for additional scrutiny has the potential
to stymie the growth of the cyber insurance marketplace at a time when consumers most need this protection.

Support the Three-Aspect Framework on Information Sharing

Recent federal legislative and executive proposals on information sharing encourage the development of a basic three-step approach for information sharing: (i) create vehicles for organizations to feed real-time cyber threat information to coordinating federal agencies and among peer organizations; (ii) require that the sharing organization undertake approved protocols for purging its data of personally identifiable information; and (iii) protect those organizations that properly implement privacy protocols with liability protections. We believe that this undertaking is as important as the assessment approach of the NIST Framework and should be supported by the NAIC and the Principles.

Address Cyber Vulnerabilities at the Source

Finally, it is worth noting that according to recent NIST data underlying software flaws are a major source of cyber vulnerabilities. The NAIC should encourage software providers to adopt higher security standards and more robust testing of software prior to release. Recent breaches in the health insurance industry confirm that weaknesses in software can expose the personal information of millions of policyholders. Any comprehensive approach to cybersecurity, therefore, requires working with software providers to mitigate flaws in the software powering the insurance industry.

Thank you very much for the opportunity to comment on these Principles. Should the Task Force have questions regarding Marsh’s perspective on these matters, we would be pleased to provide additional details and a broader overview of our experience in the cyber insurance market place.

Sincerely yours,

Erick R. Gustafson
April 10, 2015

Adam Hamm, Chair – Cybersecurity (EX) Task Force
Raymond G. Farmer, Vice Chair – Cybersecurity (EX) Task Force
c/o Pam Simpson
National Association of Insurance Commissioners
1100 Walnut Street, Suite 1500
Kansas City, MO 64108-2662
Via e-mail: psimpson@naic.org

Dear Messrs. Hamm & Farmer,

Principles for Effective Cybersecurity Insurance Regulatory Guidance Comment Submission

The North American CRO Council (“CRO Council” or “Council”) appreciates the opportunity to comment on the Principles for Effective Cybersecurity Insurance Regulatory Guidance which was released for public comment by the National Association of Insurance Commissioners (“NAIC”). Member CROs represent 29 of the largest Life and Property and Casualty insurers in North America. As a body formed to promote sound practices in risk management, the CRO Council would like to formally submit its comments and concerns regarding the most recent release of the Principles for Effective Cybersecurity, as well as offer assistance with the language contained therein.

The CRO Council appreciates and is supportive of the NAIC’s efforts towards a consistent and coordinated national approach to cybersecurity regulation in the insurance industry. The Council believes cybersecurity is an essential element of an insurance company’s enterprise risk management processes, as embodied in the NAIC’s Principle 12, and as a result is broadly supportive of many of the principles put forward by the NAIC.

Additionally, the Council believes insurers’ boards of directors should routinely discuss the company’s risk profile and the effectiveness of the company’s risk management framework specific to cybersecurity. Principle 13 addresses board level discussions, but as currently drafted is restricted to addressing internal audit findings. In order for the board of directors to engage meaningfully with management on this or other topics, prescribing the nature of the communication may limit a more robust discussion. Insurers’ Own Risk and Solvency Assessments, which are required to be submitted to a company’s board of directors, could also serve as a helpful avenue for addressing this within the current regulatory framework.

The Council believes it is important, given the evolving nature of this risk and how it is managed, that the NAIC avoid a highly prescriptive approach in developing regulations. As it is currently drafted, Principle 15, as an example, implies encryption of sensitive data should be required. However, encryption is but one means of protecting sensitive data, and it should not be perceived a panacea. Many forms of encryption have exploitable vulnerabilities, and sophisticated hackers have found alternative means around even advanced forms of encryption. Other means of protecting sensitive data may be more effective for an insurer to implement and the NAIC should avoid mandating a specific technological response.
The Council believes that the NAIC should not endorse explicit frameworks or information sharing venues. Principle 5 can be interpreted as encouraging insurers to adopt the National Institute of Standards and Technology (NIST) framework, and Principle 14 states that it is “essential” for insurers to join Financial Services Information Sharing and Analysis Center (FSISAC). The Council believes that both NIST and FSISAC serve valuable purposes and many insurers can benefit from both. However, alternative frameworks and information sharing venues are available, and an insurer may determine that those alternatives are more appropriate for its operations and risk profile. For example, many insurance company operations are multinational or global in scope. Implementing different frameworks or utilizing different information sharing venues country by country can increase complexity without increasing the protection of data.

The Council believes that insurance offerings protecting consumers and businesses in the event of a data breach can be an element of an effective cybersecurity risk management program. Principles 17 and 18 imply that this type of product is somehow riskier than other products insurers sell and warrants “enhanced solvency oversight” and disclosure. Insurers offering such products should manage this risk in line with their broader risk appetite framework with appropriate controls, limits, and monitors. But the Council is not aware of any analysis of this product suggesting it poses a heightened risk to an insurer’s solvency such that it would warrant “enhanced solvency oversight”. Imposing additional regulatory costs on this product may increase the cost insurers charge for it or otherwise reduce its availability to consumers and businesses. As with our comment on Principle 13, an insurer’s Own Risk and Solvency Assessment could serve as a helpful avenue for addressing any concerns within the current regulatory framework.

Lastly, the CRO Council appreciates and is supportive of the NAIC’s efforts towards a consistent and coordinated national approach to cybersecurity regulation in the insurance industry. We would ask that the NAIC consider whether existing regulations such as Health Insurance Portability and Accountability Act of 1996 or various data breach notification laws are sufficient before proposing additional regulations for insurers. To the extent that new regulations are warranted, we ask that the NAIC seek to minimize any inconsistencies these new regulations may have with existing regulations insurers are already subject to.

We appreciate the opportunity to provide our comments and concerns on the NAIC’s “Principles for Effective Cybersecurity Insurance Regulatory Guidance”, and would also appreciate any opportunity to work with the NAIC on this very important matter as it continues to evolve.

Sincerely,

Joseph Celentano, Chair
North American CRO Council

Mark Verheyen, Chair
Cyber Risk Working Group
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
Comments from Alan Seeley, New Mexico Office of the Superintendent of Insurance

Draft: March 12, 2015

**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.
Dear Messrs. Hamm & Farmer,

Principles for Effective Cybersecurity Insurance Regulatory Guidance Comment Submission

The North American CRO Council (“CRO Council” or “Council”) appreciates the opportunity to comment on the Principles for Effective Cybersecurity Insurance Regulatory Guidance which was released for public comment by the National Association of Insurance Commissioners (“NAIC”). Member CROs represent 29 of the largest Life and Property and Casualty insurers in North America. As a body formed to promote sound practices in risk management, the CRO Council would like to formally submit its comments and concerns regarding the most recent release of the Principles for Effective Cybersecurity, as well as offer assistance with the language contained therein.

The CRO Council appreciates and is supportive of the NAIC’s efforts towards a consistent and coordinated national approach to cybersecurity regulation in the insurance industry. The Council believes cybersecurity is an essential element of an insurance company’s enterprise risk management processes, as embodied in the NAIC’s Principle 12, and as a result is broadly supportive of many of the principles put forward by the NAIC.

Additionally, the Council believes insurers’ boards of directors should routinely discuss the company’s risk profile and the effectiveness of the company’s risk management framework specific to cybersecurity. Principle 13 addresses board level discussions, but as currently drafted is restricted to addressing internal audit findings. In order for the board of directors to engage meaningfully with management on this or other topics, prescribing the nature of the communication may limit a more robust discussion. Insurers’ Own Risk and Solvency Assessments, which are required to be submitted to a company’s board of directors, could also serve as a helpful avenue for addressing this within the current regulatory framework.

The Council believes it is important, given the evolving nature of this risk and how it is managed, that the NAIC avoid a highly prescriptive approach in developing regulations. As it is currently drafted, Principle 15, as an example, implies encryption of sensitive data should be required. However, encryption is but one means of protecting sensitive data, and it should not be perceived a panacea. Many forms of encryption have exploitable vulnerabilities, and sophisticated hackers have found alternative means around even advanced forms of encryption. Other means of protecting sensitive data may be more effective for an insurer to implement and the NAIC should avoid mandating a specific technological response.
The Council believes that the NAIC should not endorse explicit frameworks or information sharing venues. Principle 5 can be interpreted as encouraging insurers to adopt the National Institute of Standards and Technology (NIST) framework, and Principle 14 states that it is “essential” for insurers to join Financial Services Information Sharing and Analysis Center (FSISAC). The Council believes that both NIST and FSISAC serve valuable purposes and many insurers can benefit from both. However, alternative frameworks and information sharing venues are available, and an insurer may determine that those alternatives are more appropriate for its operations and risk profile. For example, many insurance company operations are multinational or global in scope. Implementing different frameworks or utilizing different information sharing venues country by country can increase complexity without increasing the protection of data.

The Council believes that insurance offerings protecting consumers and businesses in the event of a data breach can be an element of an effective cybersecurity risk management program. Principles 17 and 18 imply that this type of product is somehow riskier than other products insurers sell and warrants “enhanced solvency oversight” and disclosure. Insurers offering such products should manage this risk in line with their broader risk appetite framework with appropriate controls, limits, and monitors. But the Council is not aware of any analysis of this product suggesting it poses a heightened risk to an insurers’ solvency such that it would warrant “enhanced solvency oversight”. Imposing additional regulatory costs on this product may increase the cost insurers charge for it or otherwise reduce its availability to consumers and businesses. As with our comment on Principle 13, an insurer’s Own Risk and Solvency Assessment could serve as a helpful avenue for addressing any concerns within the current regulatory framework.

Lastly, the CRO Council appreciates and is supportive of the NAIC’s efforts towards a consistent and coordinated national approach to cybersecurity regulation in the insurance industry. We would ask that the NAIC consider whether existing regulations such as Health Insurance Portability and Accountability Act of 1996 or various data breach notification laws are sufficient before proposing additional regulations for insurers. To the extent that new regulations are warranted, we ask that the NAIC seek to minimize any inconsistencies these new regulations may have with existing regulations insurers are already subject to.

We appreciate the opportunity to provide our comments and concerns on the NAIC’s “Principles for Effective Cybersecurity Insurance Regulatory Guidance”, and would also appreciate any opportunity to work with the NAIC on this very important matter as it continues to evolve.

Sincerely,

Joseph Celentano, Chair  
North American CRO Council

Mark Verheyen, Chair  
Cyber Risk Working Group
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 inquires and also help foster the conditions where cybersecurity 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
Stephen Johnson  
Deputy Insurance Commissioner, Office of Corporate and Financial Regulation  
Pennsylvania Insurance Department  

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.
April 8, 2015

Commissioner Adam Hamm, Chair  
C/O Pam Simpson  
NAIC Cybersecurity (EX) Task Force  
444 N. Capitol Street NW, Suite 700  
Washington, DC 20001

VIA EMAIL: psimpson@naic.org

Dear Commissioner Hamm,

On behalf of National Association of Professional Insurance Agents (PIA), I would like to thank the NAIC for focusing on the important issues around managing cyber risk, cybersecurity, and associated insurance products and to offer comments on the proposed “Principles for Effective Cyber Security Insurance Regulatory Guidance” (Principles). PIA supports the efforts of the NAIC to ensure that insurers and insurance producers have robust cybersecurity and risk mitigation programs. In addition, PIA supports efforts by the NAIC to help foster a strong cyber insurance market; as we believe that cyber insurance products are integral to the economic security and stability of the U.S.

In general, PIA agrees that there must be a consistent and coordinated national approach to cybersecurity, highlighting cooperation between states and the federal government. PIA also appreciates the Principles’ recognition that any approach must be “flexible, scalable, practical, and consistent” and that a “one-size-fits-all” approach to cybersecurity will not be sufficiently effective. Finally, PIA believes that the Principles should be enduring and not overly rigid. Please see below PIA’s specific comments on Principles 5, 6, 12, 14, and 15.

Principle 5
Principle 5 references the National Institute of Standards and Technology (NIST) Cybersecurity Framework, which is an important standard for managing risk, but it is not the only standard. Many other standards and procedures, beyond NIST, may be more appropriate tools for insurance producers. Further, as technology changes, best practices for managing cyber risks are likely to evolve. PIA suggests language such as, “… and other similar, current, and future standards for managing cyber risks” be added to the end of Principle 5.

--

PIA is a national trade association founded in 1931 which represents member insurance agents in all 50 states, Puerto Rico, Guam, and the District of Columbia. PIA members are small business owners and insurance professionals who can be found across America. Furthermore, PIA members, in numerous states, currently sell cyber liability insurance products through a PIA sponsored program.
Principle 6
PIA supports Principle 6 and commends the NAIC for including it. PIA members are small and mid-sized business owners. As such, very different risk mitigation programs are necessarily utilized by PIA member agents and agencies than in large corporations. PIA believes that the resources, size, nature of business, and the risk-profile of insurance producers are all essential considerations when establishing regulatory guidance on cybersecurity.

Principle 12
PIA agrees that cybersecurity risks should be included and addressed as part of an insurance producer’s enterprise risk management processes. However, regulators should, in line with Principle 6, consider that internal risk management processes will vary based on the resources, size, nature of business, and the risk-profile of insurance producers in any oversight on this issue.

Principle 14
PIA agrees that sharing information and staying informed about cyber and physical threat intelligence is necessary. But, requiring membership in one specific group may actually undermine this goal. The FS-ISAC is an excellent organization, but it is specially tailored for financial services. There are other Information Sharing and Analysis Centers (ISACs) and methods that may be more appropriate for insurance producers. PIA asks for more flexibility in this principle and suggests language such as, “Insurers and insurance producers should stay informed about cyber and physical threat intelligence analysis and sharing, which may be accomplished by joining an ISAC.”

Principle 15
PIA agrees that sensitive data collected, stored, and transferred inside or outside of an insurance producer’s network should be protected, and encryption is one way to do that. However, encryption is only one way to protect data based on current technology. PIA recommends that this principle be less prescriptive as to the precise method to be used to achieve appropriate data protection. Instead, PIA suggests removing the word “encrypted” and inserting “appropriately safeguarded.”

PIA appreciates the considerable effort that has gone into drafting these principles, and we are grateful for the opportunity to provide the independent agent perspective on these important issues. Please contact me at jennwe@pianet.org or (703) 518-1344 with any questions or concerns. Thank you for your time and consideration.

Kind Regards,

Jennifer M. Webb, Esq.
Counsel & Director of Regulatory Affairs
National Association of Professional Insurance Agents
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
April 10, 2015

To: Pam Simpson, National Association of Insurance Commissioners         
   Cybersecurity (EX) Task Force

From: Don Estes, Chief Technology Officer
       REDpill Systems, Inc.

Re: Principles for Effective Cybersecurity Insurance Regulatory Guidance

Dear Ms. Simpson:

As the Chief Technology Officer of REDpill Systems Inc., a software development company that creates greenfield systems, as well as affords clients with a highly unique guarantee of 100 percent results in legacy modernization, I serve major insurance companies, financial institutions and major federal governmental regulatory entities.

Right now, insurers all over the world are grappling with modernizing their legacy systems, of which a sizable majority are sited on IBM mainframes. These systems were constructed prior to the existence of security “hacking” as we know it today, and the very foundations of their designs mistakenly assume either that there is no significant problem at all or the IBM mainframe platform is invulnerable.

In fact, these systems may be modernized onto platforms that are decidedly vulnerable. This means that security needs to be “baked” into the fundamental design of the systems, and not simply assumed to be present. To the extent that modernized replacement applications are influenced by the past designs, the application teams need to be on guard for this "we don't have to worry about it" mode of thinking.

We are on the eve of a new kind of software development—one based on Semantic Web standards augmented by artificial intelligence, not just the Java and Oracle thinking that is the de facto standard today.

It will be important for insurance regulators and executives to understand that it is not enough for modernized applications to be able to turn on a dime to meet changing business needs, but they need to have both reactive and proactive elements equally baked into the design to constantly look for security breaches that can only be recognized by the impact on the application systems and allow application level responses.

These reactive and proactive elements must be as responsive to changing conditions in the security space as in the business space, but operate both inside and outside of the functionality of the application systems.

www.REDpillSystems.com
www.REDpillSystems.com      don.estes@redpillsystems.com      +781-577-1556
About Don Estes

During his four-decade career in IT, Don Estes has devoted 25 years of that time to legacy modernization, working with six different legacy modernization vendors, among other projects that have included the Federal Reserve Bank of New York and the United States Patent Office.

A proven thought leader in the modernization space, Mr. Estes has focused on solving the technical and business problems in modernization projects, along with sales and marketing, product expansion and integration, and project delivery.

Among his accomplishments have been the development of the only software that could prove forensically that an application was Y2K compliant and, recently, REDpill's Synchronizer, which affords users with the guarantee of 100 percent methodology compliance.

An MIT graduate in physics, Mr. Estes also holds a Masters in Psychology from the University of Texas. He is a member of the Cutter Consortium and a Guest Editor of the Cutter IT Journal.

www.REDpillSystems.com
don.estes@redpillsystems.com  • +781-577-1556
Pamela,
RI has the following comments to be considered by the Task Force:

1. Guiding Principles 4, 6, 9, 12, 13, 14, 15 and 16:
The above Principles reference insurers and insurance producers. Should we expand such to include "other licensees" or "other regulated entities" (if appropriate) as many states issue other licensee types such as adjusters, appraisers, TPA's, MGA's, navigators, surplus line brokers etc.? While insurers are ultimately responsible the act(s) of its "agents", we think its appropriate to consider other regulated licensee types as well. Unless this was discussed and/or contemplated that these licensee types fall under Principle 10 that appears to be more vendor related than regulated entities?

2. Leveraging existing NAIC systems:
To the extent possible and where appropriate, insurance regulators should leverage SERFF and SBS to track filings, data breach notifications and/or complaint data relating to cybersecurity. These discussions may already be underway by various NAIC Working Groups. As an example, RI is adding "Cybersecurity" to our "State Keyword" options in SBS/Consumer Services Module. This will allow us to track and compile data for all consumer cases (assistance/inquiries/complaints) relating to cybersecurity. States can easily add this keyword to SBS by contacting SBS directly.

Thank you for the opportunity to comment. Happy to answer any questions.
Paula

Paula Pallozzi, SPIR
Associate Director
RI Insurance Division
1511 Pontiac Avenue, Bldg 69-2
Cranston, RI 02920
401-462-9616
Follow us on Twitter @RIDBRInsurance
LinkedIn Rhode Island Insurance Division
April 10, 2015

Commissioner Adam Hamm, Chair
Cybersecurity Task Force
National Association of Insurance Commissioners

Attn: Pamela Simpson, Senior Administrative Assistant

Re: Cybersecurity Task Force-Draft Cybersecurity Guiding Principles

Dear Commissioner Hamm:

On behalf of the Risk and Insurance Management Society, Inc. (RIMS), I want to thank you for the opportunity to comment on the task force’s recently released draft “Principles for Effective Cybersecurity Insurance Regulatory Guidance. We applaud the task force for committing to provide uniform guidance that will serve to protect consumers and the insurance industry as a whole.

We are pleased that the term “consumer” is mentioned several times within the draft; however, we want to stress that the protection of the commercial consumer is equally important as the protection of the individual insurance consumer. Insurers and insurance brokers possess a great deal of sensitive information regarding their commercial clients, including financial information, allocation of risks, concentration of employees, personal employee information, etc. A data breach of an insurer or broker could lead to a breach of their commercial clients thus increasing both the risk of loss of proprietary information and economic losses resulting therefrom exponentially.

We encourage the task force to make a concerted effort to ensure that any regulatory guidance is uniform and consistent across state lines. The more uniform guidelines or regulations are in this area, the more efficient the industry can be in ensuring their cyber security methods meet those standards. The task force should also be wary of implementing any guidance or regulations that overlap or cause repetition from guidance that may already exist from the federal government, the NAIC itself, or elsewhere.

RIMS considers Principle 17 to be one of the most important roles that the NAIC can play in this, or any, risk area. Being a relatively new risk that is only increasing in scope, it is critical that the insurers selling this insurance to commercial entities have the solvency to cover any losses in both the short and long term.
Once again, RIMS thanks the NAIC and the task force for taking an active role in this increasingly important issue area. We look forward to working with the NAIC and all interested parties to ensure that we achieve an effective and efficient way to regulate the cyber insurance marketplace while ensuring the commercial, and personal lines, consumer is adequately protected. If you have any questions or would like additional information, please contact Nathan Bacchus, RIMS Sr. Government Affairs Manager, at nbacchus@rims.org.

Sincerely,

Richard Roberts Jr.

Richard Roberts
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 Systems 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
Commissioner Hamm and Director Farmer:

We appreciate the NAIC's focus on cybersecurity matters and thank you for the opportunity to comment on the draft NAIC Principles for Effective Cybersecurity Insurance Regulatory Guidance.

As the NAIC is well aware, cybersecurity is a global issue. Cyber threat solutions for U.S. insurers are global and not national or local. Underlying our comments below is the expectation that NAIC regulatory guidance is intended to similarly reflect the global nature of cybersecurity policy.

We offer the following specific comments and suggestions regarding draft Principles 4, 5, 8, 14, and 15.

**Principle 4**

Regarding Principle 4, Swiss Re supports the goal of a consistent, coordinated national approach to cybersecurity regulatory guidance. In Swiss Re's view, that consistency and coordination should also exist at the global level. The principle could more appropriately read:

*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

Regarding Principle 5, Swiss Re agrees that cybersecurity regulatory guidance must be flexible, scalable, practical, and consistent with global best practices. Swiss Re supports the National Institute of Standards and Technology (NIST) framework, in addition to the International Organization for Standardization ISO 27002 standard, the Service Organisation Controls (SOC) assurance reports, and other global cybersecurity best practices.

The global insurance industry has also been proactive in developing cybersecurity best practices. For example, the CRO Forum's December 2014 Cyber Resilience paper offers related insights regarding cyber risk management and the role of insurance.¹

In Swiss Re's view, the Principle should not be specific to a single framework. The Principle could more appropriately read:

*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 global best practices.*

Principle 8

In response to Principle 8, Swiss Re notes only that regulators should also consider existing methods for examining an insurer's cybersecurity. For example, regulators could leverage SOC assurance reports, through which an insurer demonstrates the design and effectiveness of its cybersecurity framework.

Principle 14

Regarding Principle 14, Swiss Re recognizes the value of cyber threat information sharing among the public and private sectors. Swiss Re also supports the work of FS-ISAC. However, in Swiss Re's view, the Principle should focus on information sharing generally and not on a specific information sharing facility. For example, the Principle could more appropriately read:

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

Principle 15

Regarding Principle 15, Swiss Re agrees that sensitive data should be protected. Encryption of data sent over a public network is both appropriate and required by many U.S. laws. Similarly,

encryption of data stored on removable media and laptops could effectively protect the data in the event of a loss or theft. However, particularly for data stored on a data center server, encryption is not always the only or most effective protection measure. Encryption can even introduce new risks, for example regarding availability of the data for authorized users.

In Swiss Re's view, the matter of principle should be to effectively protect sensitive data, and not to mandate a specific protection measure for all circumstances. The Principle should, therefore, more appropriately read:

**Principle 15:** Sensitive data collected and stored and transferred inside or outside of an insurers or insurance producers network should be protected against unauthorized access using adequate controls.

***

Swiss Re would welcome the opportunity to further share its views with you regarding these Principles and other cybersecurity policy matters.

Regards,

Matthew McKenney
Senior Risk Officer P&C
Vice President

Swiss Re America Holding Corporation