Compiled Comments on *Consultation Document:*

Issues Paper on Cyber Risk to the Insurance Sector

14 April 2016 to 13 May 2016

Organisation	Jurisdiction	Comments	Resolution of comments
- General comment			
CRO Forum	EU	CRO Forum input to on IAIS Issues Paper on Cyber Risk The CRO Forum appreciates the opportunity to comment on the IAIS Issues Paper on cyber risk. As business and society becomes increasingly digitally dependent, cyber risk is becoming an increasingly important issue for the insurance industry. It is therefore appropriate that the IAIS looks to raise awareness of the challenges presented by cyber risk. In 2014, the CRO Forum established a dedicated working group on cyber risk to look at best practices for cyber resilience. The CRO Forum´s paper ´Cyber resilience: the cyber risk challenge and the role of insurance´ recognizes the important role that insurers play in: 1. Protecting the personal data that they hold from unauthorized access or improper use and ensuring the availability of IT services (information security, operational risk management); 2. Offering cyber risk insurance, which can help promote good cyber risk management (underwriting). It is recognized that the second point, cyber insurance, is out of scope of the Issues Paper. However, the CRO Forum would stress that for those insurers writing cyber cover, risk management of cyber risk naturally also extends to cyber insurance. Overall the CRO Forum agrees with the IAIS´s summation of the issues surrounding cyber risk. Below are three principles which the CRO Forum believes should guide the IAIS´s thinking as it finalizes the Issues Paper following the consultation and discusses next steps. The CRO Forum is continuing to work on cyber risk with a view to supporting improvements in the awareness, collection, analysis and sharing of cyber risk data and would welcome the opportunity to meet with the IAIS and share its thinking. A 1. Regulatory approaches to cybersecurity should be coordinated globally As the paper recognizes many different supervisory authorities and regulatory bodies are looking at cyber risk and a variety of different supervisory responses have emerged or are emerging.	Background comments noted. The Task Force appreciates the input from the CRO Forum. The three principles highlighted by CRO are generally consistent with points made in the Issues Paper and may be further taken into account in future IAIS work on cyber issues.

Organisation	Jurisdiction	Comments	Resolution of comments
		Given the borderless and increasingly interconnected digital environment, supervisory approaches to cybersecurity and data protection are only likely to be effective and efficient if they are well coordinated and implemented consistently across regions and sectors. Greater harmonisation of cybersecurity and data protection standards is needed to overcome the fragmented supervisory approach and avoid unnecessary overlaps or potential gaps in the promoting cyber security. Greater harmonisation would also allow the insurance industry to develop more holistic insurance solutions for cyber risk, thereby promoting a global cyber risk insurance market. 2. Cybersecurity standards should be principles-based and promote good cyber risk management The CRO Forum generally agrees with the five ICPs that the IAIS has identified as potentially being relevant to cyber risk and would see ICPs 7 and 8 which relate to good governance and risk management as being particularly important. The CRO Forum has chosen to define cyber risk in the broadest sense since a narrow definition could compromise effective risk management. Fraud is only one aspect of cyber risk which also covers cyber incidents that give rise to physical damage, business interruption or extortion. As a result, the CRO Forum would caution the IAIS against using ICP 21 ´Countering Fraud in Insurance´ to address cyber risk. If the IAIS considers that the ICPs need to be updated changes should be to the general risk management requirements in ICPs 7 and 8. The insurance industry has taken a proactive approach to managing cyber risk. The four pillar framework for cyber risk management set out in the CRO Forum´s 2014 paper encompassing preparation, protection, detection and improvement are largely aligned with the best practices set out by the IAIS in Chapter V of the Issues Paper and are core to the concept of Cyber resilience. As the IAIS has recognized it is not always possible to detect or prevent cyber incidents and therefore it is important that supervision promotes effective reaction and recover from potential failures and breaches. Any regulatory intervention needs to promote cyber risk management best practices. Cybersecurity standards should protect data confidentiality, integrity and availability without prescribing particular methods of protection. It is important that the IAIS refrains from promoting overly prescriptive requirements which risk quickly becoming obsolete due to changing technology and exposures (e.g. requirements for encryption). Such requirements could also impose ineffective, unnecessary or improper requirements that divert resources from Information Security.	The Task Force will consider this perspective during any future work on ICP 21. Presently, we do not expect that revisions to ICP 21 will cover cyber risk in detail. This may be dealt with through one or more Application Paper(s) that relates to more than one ICP.

Organisation	Jurisdiction	Comments	Resolution of comments
		3. Better cyber risk data collection and information sharing should be encouraged to increase cyber resilience Sharing of cyber threat intelligence and cyber incident information will increase resilience to cyber risk. Data sharing is only meaningful and effective if the data can be aggregated and analyzed. This necessitates a common methodology for categorising cyber incidents. The CRO Forum is currently developing such a categorisation methodology to help capture cyber risk data for the purposes of risk management, IT, information security and underwriting. The aim is to: - support informed discussions within companies on improving cyber defence mechanisms; - pave the way for more effective information sharing to promote cyber resilience. The CRO Forum expects to publish its methodology in the coming months. This will leverage existing loss databases (e.g., ORX for operational risk) and the experience of using these data bases. It is hoped that over time a common categorisation methodology will support the emergence of a more comprehensive cyber risk database. The CRO Forum looks forward to meeting with the IAIS to discuss its methodology.	The Task Force welcomes future interaction with CRO Forum.
AXA Group	France	The position paper provides a solid foundation of the cyber risks that are experienced. There were however certain aspects of the paper that perhaps could benefit from further clarification / adjustment to ensure the message reflects the situation experienced more precisely. There is reference in section 9 around the risks being primarily associated with systems connected to computer networks whereas certain non-connected infiltrations must also be recognised (such as those exploited by Stuxnet). The impact to brand / reputation of an organization should be considered with more prominence in the face of cyber risks. With regards to impacts overall, a significant percentage of the paper focuses on data availability and theft. However, data integrity and confidentiality are also areas of critical concern. Especially with regards to data confidentiality, insurers need to place strong emphasis on ensuring sensitive customer records are safeguarded in the face of cyber risks.	Background comments noted. The Task Force appreciates the input from AXA Group. Wording added to paragraph 4 to more clearly identify the need for data confidentiality.

Organisation	Jurisdiction	Comments	Resolution of comments
		There was mention on p32 "that most jurisdictions associate cybersecurity with standards compliance". However standards compliance should be seen as the minimum level. The nature of the threats may require scaling up the level of security to protect the assets in question due to the additional risks above "standards compliance". Relying on available data may also not entirely represent the cyber risk landscape accurately. There is a generally accepted position in the industry overall with regards to incomplete actuarial data on cyber incidents. Therefore, the conclusions drawn from available data should acknowledge the limitations of this extrapolation.	Future work may further address "minimum" standards compliance. Noted. The Task Force agrees with the comment about the implications of data limitations, but considered the issue to be implicitly addressed throughout the paper. May be further considered in subsequent work.
		The complexity of attacks appears to have been overlooked in some areas. Section 15 should note that where targeted computers are part of shared data storage systems, the ransomware has the capacity to also infiltrate enterprise storage environments and thereby amplifying the impact of the attack significantly. Section 16 references a group of technologies which indeed address common attacks but care should be taken to suggest that reliance on technology only will address the common causes. Proper system / application configuration and simple user education can be equally effective in counteracting these cyber risks.	Yes, but regarding Section 15 this point is too technical for this Issues Paper, which is intended primarily to raise awareness. May be further considered in subsequent work. The Task Force has added clarification of wording to paragraph 16.
		There is also an expectation on p14 "detection" section, that insurers "should include third party providers". However, pursuing this expectation negates the flexibility for the business to determine the nature of the monitoring service based on their internal capability and needs. The decision should be left completely to the entity based on an expected risk outcome rather than an expectation to use third parties. Participation in information sharing under "Situational Awareness" notes that "insurers should participate in established	Reworded - see ACPR comment to 39. The Task Force concurs and considers

Organisation	Jurisdiction	Comments	Resolution of comments
		information sharing initiatives". Whereas the position is accepted, the nature of this participation must be carefully defined in order to avoid exposure of sensitive commercial information or end customer details.	that this point is implicit.
Winquest Engineering Corporation	United States	Winquest Cybersecurity thanks IAIS for the opportunity to comment on the IAIS Issues Paper on Cyber Risk to the Insurance Sector. Winquest has experience with the types of cyber risks mentioned, concurs with the report's findings and looks forward to an opportunity to comment on future IAIS application papers.	Background comment noted. The Task Force appreciates the input from Winquest.
American Council of Life Insurers, American Insurance Association, National Association of Mutual Insurance Companies, Property Casualty Insurers Association of America, Reinsurance Association of America	United States of America	These comments reflect feedback from the following trade associations: American Council of Life Insurers, American Insurance Association, National Association of Mutual Insurance Companies, Property Casualty Insurers Association of America, Reinsurance Association of America Overall, this Issues Paper presents a general overview and compilation of cyber related news stories, cyber studies, and government approaches. It also generally meets the objective to raise the awareness for insurers and supervisors with the challenges manifested by cyber risks and the supervisory mitigants to those risks. Nonetheless, we do have a few suggestions to help strengthen the paper and generalize some of the statements to account for the evolving nature of the risk. We note that the importance of the IAIS' work, especially on an evolving issue such as cybersecurity, requires as much engagement and collaboration with its stakeholders as possible. The insurance industry has invested significant time and resources to risk management, including cyber risk, and we endeavor to contribute thoughtfully to the work of the IAIS. Accordingly, we urge that the IAIS solicit feedback from all interested stakeholders and further consider and analyze the feedback prior to moving forward with any next steps relating to cybersecurity. Adopting a collaborative approach will lead to informed discussion and to an appropriate determination as to whether any further steps by the IAIS are warranted. We also urge the IAIS to ensure that any new guidelines or standards proposed as part of any next steps are consistent with security standards already utilized by insurers and laws to which insurers are already subject. Further, and recognizing that the Issues Paper is directed towards insurance supervisors, it should acknowledge the "agnostic" nature of cyber risk - that is, that the risk is of concern to all forms of commerce, regardless of sector.	Background comments noted. The Task Force appreciates the input from ACLI, AIA, NAMIC, PCIAA, and RAA. The Task Force expects to interact with stakeholders respecting any future work. This point appears in the Issues Paper already.
- Comment on paragraph 1			

Organisation	Jurisdiction	Comments	Resolution of comments
American Council of Life Insurers, American Insurance Association, National Association of Mutual Insurance Companies, Property Casualty Insurers Association of America, Reinsurance Association of America	United States of America	We also think the paper would be well-balanced if it recognized that insurers are taking steps to protect insurer data. For example, paragraph one could be divided into two separate paragraphs as follows: "1. Concern over cybersecurity is growing across all sectors of the global economy, as cyber risks have grown and cyber criminals have become increasingly sophisticated. The cyber risk is agnostic in nature and no industry is immune from the possibility of an attack. In fact, insurers are keenly aware of the risks and have, on their own, taken many steps to help reduce and manage the risk in different ways based on corporate risk calculations. 2. For insurers . . ."	This point appears in the Issues Paper already (see first sentence). The Task Force does not have the basis to make this blanket statement but this is not intended to diminish the steps taken by insurers.
- Comment on paragraph 4			
American Council of Life Insurers, American Insurance Association, National Association of Mutual Insurance Companies, Property Casualty Insurers Association of America, Reinsurance Association of America	United States of America	As noted in our general comments and Paragraph 1, cybersecurity affects all sectors of the global economy and the composition of the insurance sector is continuously evolving. We would suggest revising this paragraph as follows: "All insurers, regardless of size, complexity, whether incumbent or Fintech, or lines of business, and intermediaries, thereafter collectively referred to as insurers, collect, store, and share with various third-parties (e.g. service providers, intermediaries, insurers, reinsurers) substantial amounts of private and confidential policyholder information, including in some instances sensitive health-related information. Information obtained from insurers and intermediaries through cyber-crime may be used…"	Added “intermediaries” as a third party.
- Comment on paragraph 6			
ACPR - Banque de France	ACPR (France)	Page 4 point 6 It might be useful to indicate that the Business aspect of cyber risk will be the subject of a separate analysis. Mitigation should still be envisaged. We propose to include this paragraph: "This paper focuses on cyber risk to the insurance sector and the mitigation of such risks, but does not cover IT security risks more broadly. It also does not specifically cyber insurance (insurers selling or underwriting that type of contract) which will be the subject of an analysis of OECD) or risks arising from cybersecurity incidents involving supervisors. IAIS underlines that mitigation should be envisaged in any case.	The Task Force appreciates the input from ACPR. The Task Force added clarifying wording on scope of the Issues Paper (see paragraph 6).
- Comment on paragraph 8			

Organisation	Jurisdiction	Comments	Resolution of comments
ACPR - Banque de France	ACPR (France)	Page 5 point 8-13 The cyber risk might be put into perspective with recent technological development. The frequency and the magnitude of the risk may vary a lot regarding technologic innovations (e.g. IoT), their democratization and the natural need of anticipation for an adequate supervision.	Noted - see paragraph 39.
- Comment on paragraph 17			
Winquest Engineering Corporation	United States	17. Winquest strongly agrees. Smaller firms have less resources to perform adequate cybersecurity practices. Also, based on our experience, many firms feel completely overwhelmed by the problem and/or have no idea where to begin in addressing the problem.	Noted.
- Comment on paragraph 21			
American Council of Life Insurers, American Insurance Association, National Association of Mutual Insurance Companies, Property Casualty Insurers Association of America, Reinsurance Association of America	United States of America	We request that this paragraph be amended to reflect the fact that Ponemon costs per record are only valid for breaches involving less than 100,000 records. The Issues Paper should mention this fact to provide further context and clarity.	Additional information regarding Ponemon work is included in footnote 20.
- Comment on paragraph 23			
Winquest Engineering Corporation	United States	23. Winquest findings are consistent with all three of the examples given.	Noted.
American Council of Life Insurers, American Insurance Association, National Association of Mutual Insurance Companies, Property Casualty Insurers Association of America, Reinsurance Association of America	United States of America	We request clarification of the last sentence of this paragraph. The sentence currently reads, "Insurers outsource a variety of services, which may increase exposure to cyber risk." We recommend modification to read as follows: "Insurers outsource a variety of services, which has the possibility of increasing exposure to cyber risk, absent appropriate and proper vetting by the insurer." This change would appropriately reflect the fact insurers undertake considerable efforts to ensure the security of the information transmitted to third party vendors.	Concur but consider the proposed wording overstated because vetting is a response to risk but does not eliminate the risk. Also, added language regarding the possibility of decreasing risk

Organisation	Jurisdiction	Comments	Resolution of comments
			through the use of outsourcing.
- Comment on paragraph 25			
ACPR - Banque de France	ACPR (France)	Page 5 point 8 and page 9-10 points 25-28 The definition of cyber risk seems consistent with the concept expected, using the source of the risk to define it. However it may be interesting to include also link the definition with a more complete list of potential losses or damages. We suggest enriching the list of damages caused by cyber-risk by adding at the beginning of the Chapter III pages 9 and 10, the following classification: 23. Classification of losses or damages may include notably: - loss of confidential data (personally identifiable information, intellectual property rights, non-compliance,…) - business interruption, - physical losses (e.g. machine, digital storage plateform…); - financial losses (e.g.: the potential loss of investors) - reputational damages (policyholders, rating agencies, business partner, sector) -potential loss of confidence of rating agencies and business partners in connection with the reputational loss -the regulatory breaches and non-compliance risk (e.g. data quality insufficiencies, IT and global governance inadequate and dysfunctional internal control system); 24. Some of these potential adverse consequences of insurance sector cybersecurity incidents are highlighted below.	Wording added to paragraph 24 to further expand on potential consequences. However, this list is not intended to be exhaustive.
- Comment on paragraph 26			
American Council of Life Insurers, American Insurance Association, National Association of Mutual Insurance Companies, Property Casualty Insurers Association of America, Reinsurance Association of America	United States of America	The second sentence in paragraph 26 should be eliminated to keep the paragraph more generic. The one line of insurance highlighted in the paper is cyber insurance and the possession of policyholder information related to "network security controls and other cyber resilience efforts." In actuality, the level of detail suggested in this sentence to be in the possession of the insurer may not be accurate. A generic approach is more appropriate for this Issues Paper.	Agreed to leave as a good example, but reworded in response to this point.
- Comment on paragraph 28			

Organisation	Jurisdiction	Comments	Resolution of comments
ACPR - Banque de France	ACPR (France)	Page 10 point 28 There is a typing error at the end of the first sentence (a point instead of a coma after "appropriate" and before "If". Page 10 point 28 Associated to the previous comment on the classification of damages, we propose to include the following sentence at the end of the point 28. "The reputational loss is non-negligible; indeed, it should be link to policyholders trust but also mainly to investors trust, rating agencies trust, business partners…"	Amended. Wording added in response to this comment.
American Council of Life Insurers, American Insurance Association, National Association of Mutual Insurance Companies, Property Casualty Insurers Association of America, Reinsurance Association of America	United States of America	We suggest that the paragraph be modified to read: "The foundation of the insurance business is policyholder trust that claims will be paid out in a timely way when appropriate. Policyholders also trust insurers to protect their personal and confidential information. If an insurer suffers a data breach, which exposes confidential policyholder information, that trust may be shaken. Similarly, if an insurer were to suffer a cybersecurity incident that rendered it unable to make timely claims payments or otherwise interrupted its operations, that trust may also be shaken. The reputational risk could extend to the sector as a whole."	Agreed to leave.
- Comment on paragraph 32			
American Council of Life Insurers, American Insurance Association, National Association of Mutual Insurance Companies, Property Casualty Insurers Association of America, Reinsurance Association of America	United States of America	We recommend that the last sentence should end after "serious." The phrase "if the attacks had concentrated on critical intra-company connections" could be seen as providing hackers insight into ways to attack companies.	Revised with more generic wording.
- Comment on paragraph 35			
American Council of Life Insurers, American Insurance Association, National Association of Mutual Insurance Companies, Property Casualty	United States of America	The example is described as a cyber-attack but this is more of a general fraud incident that often takes a non-electronic form.	Noted, but still considered to be a relevant and accessible example.

Organisation	Jurisdiction	Comments	Resolution of comments
Insurers Association of America, Reinsurance Association of America			
- Comment on paragraph 38			
American Council of Life Insurers, American Insurance Association, National Association of Mutual Insurance Companies, Property Casualty Insurers Association of America, Reinsurance Association of America	United States of America	"State of the art" should be eliminated as a qualifier in front of "network policies and procedures." It is not generally understood what "state of the art" would mean and what is considered "state of the art" today may not be "state of the art" tomorrow.	Changed to “appropriate” in response to this comment.
- Comment on paragraph 39			
ACPR - Banque de France	ACPR (France)	Page 13 point 39 Critical business function is a specific concept that deserves a specific definition due to the context. We suggest including a definition of critical business function: "Critical functions are those activities that are vital to an organization's survival and to the resumption of business operations. Typically, critical functions are the business functions that : - are most sensitive to downtime; - fulfill legal or financial obligations to maintain cash flow; - play a key role in maintaining your business' market share and reputation; and/or - safeguard an irreplaceable asset. (e.g. underwriting, pricing, actuarial function, claim management and risk management functions…) A reflection on the business context, the identification of critical functions and their resources, and the related security risks enables an insurer to focus and prioritize its efforts, consistent with its risk management strategy, its business needs and its business continuity management." Page 13 point 39 We offer a minor reorganization of the sentences in following paragraphs on protection and detection to limit redundancy and to facilitate the reading and understanding the two key definitions. - Protection	Reworded to avoid reference to “critical” in response to this comment.

Organisation	Jurisdiction	Comments	Resolution of comments
		Resilience can be provided by design. Comprehensive protection entails protecting interconnections and other means of access to insider and outsider threats to the institution and providers. When designing protection, the "human factor" should be taken into consideration. Therefore, training is also an essential part of the safety net against cyber risk. And controls should be in line with leading technical standards as strong IT controls contribute to protection. - Detection Continuous and comprehensive cybersecurity monitoring is essential for detection of potential cyber incidents that could impact the insurer directly or through third party providers. Performing security analytics also helps to detect and mitigate cyber incidents.	The idea of providers is included in paragraph 38. These sections reworded for additional clarity, but without removing content.
American Council of Life Insurers, American Insurance Association, National Association of Mutual Insurance Companies, Property Casualty Insurers Association of America, Reinsurance Association of America	United States of America	The tone of the described best practices should be modified to make it clear that they do not recommend or imply specific actions or that the use of a particular framework or standard is required. They should also take into account the need for flexibility to meet the challenges of this ever-evolving risk and corporate risk assessments. They should be principle-based and promote good cyber risk management. We do not take issue with the basic underlying objectives of the suggestions, but urge tone changes to make it clear that they only describe what is being done today and to incorporate a recognition that "best practices" will differ among companies. Specifically, under the "Governance" heading the second sentence could be edited to read: "For example, Senior Management increasingly includes an official with access to the Board, who is responsible for developing and implementing the cyber resiliency plan." It may also be useful to add a sentence to this paragraph highlighting the risk-based and evolutionary observations outlined above. Further, consistent with our comments for paragraph 38 and the need for flexibility and risk-based practices, we would recommend that the first sentence under "Protection" be eliminated. The concept of "leading technical standards" may fail to recognize that different standards may be appropriate for different businesses with different risk portfolios.	IAIS Issues Papers are not standards, and this paper is not intended as such. Paragraph 39 now framed as examples. The reference to CISO has been deleted. The concept of proportionality is included in the referenced cyber material and in the ICPs. This may be appropriate for further consideration in connection with future work of the Task Force.
- Comment on paragraph 40			
Winquest Engineering Corporation	United States	40. Winquest concurs the current ICPs cover cyber risk and does not believe a separate ICP for cyber risk is needed.	Noted.

Organisation	Jurisdiction	Comments	Resolution of comments
American Council of Life Insurers, American Insurance Association, National Association of Mutual Insurance Companies, Property Casualty Insurers Association of America, Reinsurance Association of America	United States of America	We appreciate the discussion of the ICPs as they may relate to cybersecurity, but respectfully acknowledge that some of the connections may not be consistent with their intended purpose.	Noted.
- Comment on paragraph 41			
ACPR - Banque de France	ACPR (France)	Page 15 point 41 The ICP 16 on ERM & Solvency may be a relevant principle to address this risk. As a reminder, the "ICP 16 Enterprise Risk Management for Solvency Purposes" specifies that: "The supervisor establishes enterprise risk management requirements for solvency purposes that require insurers to address all relevant and material risks." It seems clear that cyber-risk, in the frame of operational risk, is subject to enterprise risk management requirements. It has to be addressed properly by insurers. Identifying and addressing cyber risk should be an integral part of the ERM of a insurer. The ICP 18 on Intermediaries states: "The supervisor sets and enforces requirements for the conduct of insurance intermediaries, to ensure that they conduct business in a professional and transparent manner." These intermediaries are also concerned by the correct data management insuring confidentiality and transparency in a professional manner. That implies a correct management of cyber-risk.	ICPs 16 and 18 are now mentioned in footnote 31.
American Council of Life Insurers, American Insurance Association, National Association of Mutual Insurance Companies, Property Casualty Insurers Association of America, Reinsurance Association of America	United States of America	The role of intermediaries seems an omission given their function within the value chain and their susceptibility to cyber incidents and attacks. We would suggest including a reference to ICP 18 with a short description added to Section VI.	Intermediaries are included in ICP 19. In addition, reference to ICP 18 is now footnoted, as noted above.
- Comment on paragraph 42			

Organisation	Jurisdiction	Comments	Resolution of comments
American Council of Life Insurers, American Insurance Association, National Association of Mutual Insurance Companies, Property Casualty Insurers Association of America, Reinsurance Association of America	United States of America	We urge clarification to this paragraph to add the phrase "guidance to" prior to the reference to ICP 7. We also urge that the words "insurance sector" be substituted for the word "insurer." The paragraph should read as follows: "ICP 7 was revised in November 2015. Under this ICP, insurers are expected to be able to demonstrate the effectiveness of systems and controls and corporate governance framework. The guidance to ICP 7 states: "It is the Board's responsibility to ensure that the insurer has appropriate systems and functions for risk management and internal controls and to provide oversight to ensure that these systems and the functions that oversee them are operating effectively and as intended." Identifying and addressing cyber risk to the should be an integral part of the risk management of an insurer.	Reference to "guidance" added and reference to "insurance sector" deleted in response to this comment.
- Comment on paragraph 52			
Winquest Engineering Corporation	United States	52. Winquest concurs with an ICP 21 revision that addresses cyber risk more directly since a cyber incident could lead to identity theft and a related increase of insurance fraud.	Noted.
- Comment on paragraph 56			
American Council of Life Insurers, American Insurance Association, National Association of Mutual Insurance Companies, Property Casualty Insurers Association of America, Reinsurance Association of America	United States of America	We appreciate that the further materials are meant to help promote consistent outcomes and sound supervisory practices. We believe it is important for IAIS to promote consistency among international supervisors as it relates to guidance and applicable law. We again urge that prior to moving forward on any new guidance or proposed new standards that the IAIS work closely with all stakeholders to ensure that any new proposed guidance or standards are consistent and not duplicative of existing or proposed standards or laws.	Noted – will move forward, involving stakeholders as appropriate.
- Comment on paragraph 63			
American Council of Life Insurers, American Insurance Association, National Association of Mutual Insurance Companies, Property Casualty Insurers Association of America, Reinsurance Association of America	United States of America	It might be useful for the Issues Paper to articulate some of the expertise that is lacking among supervisory authorities.	Covered in paragraphs 92 and 93 for present purposes, but may be further considered in connection with future work in this area.
- Comment on paragraph 79			

Organisation	Jurisdiction	Comments	Resolution of comments
American Council of Life Insurers, American Insurance Association, National Association of Mutual Insurance Companies, Property Casualty Insurers Association of America, Reinsurance Association of America	United States of America	While the U.S. has done a great deal of work on the issue of cybersecurity, we do not see the need to reference which President signs the Executive Order. This observation is also noted in the block text for "Additional Supervisory and Cooperative Measures in the United States."	Changed to “the President.”
- Comment on paragraph 80			
American Council of Life Insurers, American Insurance Association, National Association of Mutual Insurance Companies, Property Casualty Insurers Association of America, Reinsurance Association of America	United States of America	Recognizing that insurers and banks have different regulatory structures and requirements, we would recommend the following edit: ". . . provides a logical approach to cyber risk management, aspects of which could be considered by other financial institutions. "	Added “aspects of which.”
- Comment on paragraph 81			
National Association of Insurance Commissioners (NAIC)	USA, NAIC	In box, insert "Federal" in heading after "Additional"	The Task Force appreciates the input from the NAIC. Revised accordingly.
- Comment on paragraph 82			
National Association of Insurance Commissioners (NAIC)	USA, NAIC	Sentence 8, edit to read as follows: "The Task Force is also working with the NAIC's Information Technology Examination Working Group and the Market Conduct Examination Standards Working Group to develop updated protocols for inclusion as guidance in the Financial Condition Examiners Handbook and the Market Regulation Handbook, respectively." Sentence 9, edit to read as follows: "Financial Examination revisions included in the 2016 Handbook are being used for examinations with an effective date of 31 December 2015."	Updated accordingly. Updated accordingly.

Organisation	Jurisdiction	Comments	Resolution of comments
		Insert additional sentence at the end: "Going forward, the Cybersecurity Task Force and the Working Groups will review use of their Handbook guidance to ensure it is continuously updated as cyber threats continue to evolve."	Wording added accordingly.
- Comment on paragraph 83			
American Council of Life Insurers, American Insurance Association, National Association of Mutual Insurance Companies, Property Casualty Insurers Association of America, Reinsurance Association of America	United States of America	As conversations of regulatory coordination and enforcement relating to cybersecurity continue to evolve, we would urge paragraph 83 to take a more general approach. We suggest the following language replace the first sentence in its entirety: "In general, in the event of a breach at a domestic insurer, the lead state may coordinate breach response activities including: coordinating status communications with the insurer and regulators; ensuring a coordinated approach to any regulatory requests; and a coordinated approach to any examinations that may be warranted."	This change is not considered necessary for the purposes of Issues Paper.
- Comment on paragraph 84			
American Council of Life Insurers, American Insurance Association, National Association of Mutual Insurance Companies, Property Casualty Insurers Association of America, Reinsurance Association of America	United States of America	We respectfully recommend that this paragraph be removed as it is premature and singles out one individual state's activity. It is true that New York has taken steps to initiate a dialogue among regulators regarding various cybersecurity oversight objectives, but the reader is left wondering whatever came from the November 2015 letter. In addition, the paragraph refers to the litany of actions as "potential regulations," however, the formal process for regulatory proposals in New York has not begun and the letter itself states it is an effort to "spark additional dialogue, collaboration and ultimately, regulatory convergence among our agencies on new, strong cyber security standards for financial institutions."	Agreed to retain but new wording added to reflect current status of the New York Department's work in this area.
- Comment on paragraph 87			
American Council of Life Insurers, American Insurance Association, National Association of Mutual Insurance Companies, Property Casualty Insurers Association of America, Reinsurance Association of America	United States of America	We believe that this paragraph is unclear. We would request the following modification, "Insurers face cyber threats from both internal and external actors, but focus considerable resources at mitigating that risk."	Revisions made, but without the reference to resources (which Task Force has not substantiated on a global basis).
- Comment on paragraph 94			

Organisation	Jurisdiction	Comments	Resolution of comments
American Council of Life Insurers, American Insurance Association, National Association of Mutual Insurance Companies, Property Casualty Insurers Association of America, Reinsurance Association of America	United States of America	We commend the IAIS for its commitment to monitor the evolution of issues and initiatives related to cyber risk. Again we urge the IAIS to engage in ongoing collaboration with interested stakeholders and to consistently gather input to ensure a transparent and ongoing dialogue about this evolving issue. If the IAIS decides to move forward with new guidance or standards, we again urge that interested stakeholders be given the opportunity to provide input on such issues. We urge that any new standards the IAIS considers not be prescriptive nor mandate a single uniform standard, but rather be principles based.	The comments will be considered in connection with future work in this area. The Task Force would expect to involve stakeholders as appropriate.
- Do you have any suggestions for specific measures, including supervisors' and the industry's capability to consider and address cyber risk that should be covered in IAIS supervisory material and/or followed up in future work on this subject?			
American Council of Life Insurers, American Insurance Association, National Association of Mutual Insurance Companies, Property Casualty Insurers Association of America, Reinsurance Association of America	United States of America	The Financial Crimes Task Force might consider adding a paragraph to highlight the benefits of mechanisms for private companies to share cyber threat information with law enforcement and each other where appropriate confidentiality guarantees and liability protections are in place. Sharing of cyber threat intelligence and cyber incident information will increase resilience to cyber risk. We note that a few survey responses highlighted existing sharing partnerships or the desire to improve on information sharing.	Wording added to paragraph 90 in response to this comment.