31 October 2018

EU-U.S. INSURANCE DIALOGUE PROJECT

INSURANCE INDUSTRY CYBERSECURITY ISSUES PAPER

The EU-U.S. Insurance Dialogue Project (EU-U.S. Project) began in early 2012, as an initiative by the European Commission, the European Insurance and Occupational Pensions Authority (EIOPA), the Federal Insurance Office of the U.S. Department of Treasury (FIO), and the National Association of Insurance Commissioners (NAIC) to enhance mutual understanding and cooperation between the European Union (EU) and the United States for the benefit of insurance consumers, business opportunity, and effective supervision. In 2018, the EU-U.S. Project's members continued the work focusing on cybersecurity risk besides the other focus areas relating to the cyber insurance market, the use of big data and intra-group transactions.

I. Introduction

Recognizing that cyber risk is growing and evolving, both for the insurance sector itself and for those whom it serves, the EU-U.S. Insurance Project is pursuing a bilateral dialogue to share knowledge and information with respect to this dynamic area.[1] While cyber incidents are not unique to the insurance industry, insurers may be attractive targets because they collect and manage large amounts of personally identifiable information and private health information from individual consumers, as well as a variety of data from numerous businesses around the world.[2] Publicly reported examples of cyber incidents involving insurers include the theft of personal information for over 78 million current and former members and employees of Anthem in 2015, and the theft of data from CareFirst BlueCross Blue Shield, also reported in 2015.[3] EU and U.S. insurance regulators have prioritized improving insurance industry cybersecurity.[4] This paper outlines existing legislative and supervisory frameworks in the EU and the U.S., and describes selected initiatives and resources addressing insurance industry cybersecurity risk. The objective is to improve the mutual understanding of the EU and U.S. cybersecurity regimes, and to enhance supervisory cooperation.[5]

---

[1] *EU-US Insurance Dialogue Project: New Initiatives for 2017-2019*, https://www.treasury.gov/initiatives/fio/EU-US%20Insurance%20Project/Documents/EU-US_Initiatives_2017-2019.pdf.

[2] The Financial Stability Board (FSB) has proposed defining "cyber incidents" as an observable occurrence in an information system that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores or transmits; or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies, whether or not resulting from malicious activities. *See, e.g.*, FSB, *Cyber Lexicon – Consultative Document* (2018), http://www.fsb.org/wp-content/uploads/P020718.pdf.

[3] Bill McGuire, "Insurer Anthem Reveals Hack of 80 Million Customer, Employee Accounts," *ABC News* (February 4, 2015), https://abcnews.go.com/Business/insurer-anthem-reveals-hack-80-million-customer-accounts/story?id=28737506; Kate Vinton, "Data Belonging to 1.1 Million CareFirst Customers Stolen in Cyber Attack," *Forbes* (May 20, 2015), https://www.forbes.com/sites/katevinton/2015/05/20/data-belonging-to-1-1-million-carefirst-customers-stolen-in-cyber-attack/#2f7841bb3984.

[4] "Regulators," as used in this paper, includes supervisory authorities. The term "insurance regulators" is intended to be synonymous with the term "insurance supervisors" used in other Project issues papers.

[5] The Project's intent is to understand and build upon prior analyses, not to duplicate them. The attached Appendix includes a non-exhaustive list of instructive resources from Project members and others examining insurance industry cybersecurity, as well as cybersecurity for the financial sector more broadly.

II. Legislative and Supervisory Frameworks

While supervisory frameworks addressing insurer cybersecurity vary, EU and U.S. insurance regulators agree that, because of the potential severity of cyber incidents, all insurers must aspire to cyber resilience. The frameworks described below address issues such as cybersecurity, data privacy, and breach notification requirements. EU and U.S. regulators agree that it is important to be aware of material cyber incidents in order to understand the cybersecurity challenges facing insurers and to protect policyholders in their jurisdictions.

A. EU Frameworks

The Directive on the security of network and information systems (NIS Directive) is the first piece of EU-wide legislation on cybersecurity.[6] It provides legal measures to boost the overall level of cybersecurity in the EU. The NIS Directive applies across multiple sectors. The NIS Directive seeks to promote cybersecurity resilience and cooperation in the EU through three main objectives: (1) improving national cybersecurity capabilities; (2) building cooperation across the EU; and (3) promoting a culture of risk management and incident reporting among key economic actors, notably operators providing essential services and digital service providers.

Individual EU member states may enact sector-specific requirements. For example, the German supervisory authority, Bundesanstalt fur Finanzdienstleistungsaufsicht (BaFin), published a circular outlining information technology (IT) requirements – including information security technical and organizational resources – for the insurance sector,[7] including for the outsourcing of IT services to third parties. The principle of proportionality played a significant role in the circular's design. The circular was based on IT requirements for financial institutions more generally, providing the benefits of a similar and comparable framework for supervisors and the industry in both the insurance sector and the financial sector more broadly.

The requirements for notification by insurers of cyber incidents are subject to provisions in the national laws of EU member states. Some laws may be specific to insurers, while others apply to a variety of businesses (including insurers). For example, in France, all insurers recognized (on a confidential list) as a "Finance Operator of vital importance" must report cyber incidents to the ANSSI (National Cybersecurity Agency of France). Similarly, in Germany, insurers which provide critical services (as defined by the Act on the Federal Office of Information Security, or BSIG) are subject to legal requirements for reporting cyber incidents.

The EU's General Data Protection Regulation (GDPR) requires all companies (not just insurers) to employ appropriate technical and organizational measures to ensure secure processing of personal data.[8] The

[6] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July, 2016 concerning measures for a high common level of security of network and information systems across the Union. https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive

[7] BaFin Circular 10/2018 (July 2018), "Versicherungsaufsichtliche Anforderungen an die IT (VAIT)," https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Rundschreiben/2018/rs_18_10_vait_va.html.

[8] REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation): https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:02016R0679-20160504&from=EN.

GDPR also establishes notification requirements for personal data breaches, including breaches caused by cyber incidents. Failure to fulfil the GDPR's requirements will result in enforcement measures. The European Commission has further strengthened data protection rules by enhancing consistent enforcement across the EU.[9] A European Data Protection Board will be empowered to adopt binding decisions if several EU countries are concerned by the same case. National data protection authorities will be able to impose fines up to EUR 20 million or 4% of a company's worldwide turnover.[10]

B. U.S. Frameworks

In 2017 the National Association of Insurance Commissioners (NAIC) adopted the *Insurance Data Security Model Law* (#668), creating model requirements for insurers, agents, and other licensed entities covering data security, investigation, and notification of breaches.[11] The model law addresses, among other things: maintaining an information security program based on ongoing risk assessment; overseeing third party service providers; investigating data breaches, and notifying regulators of a cybersecurity event.[12] Under the U.S. state-based regulatory system, each state must adopt the model law (or variation on the law) in order for any provisions to take effect in that state. In 2018, South Carolina was the first state to pass legislation adopting the model law, which will go into effect on January 1, 2019.[13]

In 2017, the New York Department of Financial Services (NYDFS) promulgated a regulation establishing cybersecurity requirements for financial services companies (including insurers) that are subject to NYFS jurisdiction, which helped inform the development of the NAIC's Model Law. The New York regulation includes requirements for reporting, audits, consumer privacy, and security measures such as encryption and access controls.[14]

Further, the NAIC's *Financial Condition Examiners Handbook* (*Examiners Handbook*) provides guidance that state regulators use as part of the financial examination process, and includes a review of whether and how the insurer being examined is addressing its cyber risk. The *Examiners Handbook* was recently updated to incorporate the National Institute of Standards and Technology (NIST) Cybersecurity Framework and its five functions: Identify, Protect, Detect, Respond, and Recover.[15] As part of the scoping process, examiners obtain documentation – which typically includes the insurer's cybersecurity

---

[9] European Commission, *2018 Reform of EU Data Protection* Rules, https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en.

[10] *See* EU-US Insurance Project, *Big Data Issues Paper* (2018), for more discussion of the GDPR.

[11] The model law is available at https://www.naic.org/store/free/MDL-668.pdf.

[12] *See, e.g.*, Insurance Data Security Model Law Section 4A (Implementation of an Information Security Program), Section 4D (Risk Management, including potential security measures), Section 4E (Oversight by Board of Directors), Section 4C (Risk Assessment), Section 4F (Oversight of Third-Party Service Provider Arrangements), Section 4G (Program Adjustments), Section 5 (Investigation of a Cybersecurity Event), Section 6 (Notification of a Cybersecurity Event).

[13] S.C. Code Ann. §§ 38-99-10 to 38-99-100 (2018).

[14] New York State Department of Financial Services, Cybersecurity Requirements for Financial Services Companies, 23 NYCRR 500, https://www.dfs.ny.gov/legal/regulations/adoptions/dfsrf500txt.pdf.

[15] *NIST Cybersecurity Framework (CSF) Reference Tool*, https://www.nist.gov/cyberframework/csf-reference-tool.

strategy and framework– in order for the regulators to identify strategy and framework gaps or other issues at the beginning of the examination. The *Examiners Handbook* emphasizes the importance of reviewing an insurer's internal (i.e., Board and senior management) oversight of its cybersecurity program and contains specific procedures for considering how the insurer integrates cybersecurity-related risks into its overall enterprise risk management (ERM) program in addition to specific testing procedures for review and assessment of the adequacy of the IT governance model. The *Examiners Handbook* also includes specific procedures to evaluate network monitoring and reviewing third-party audits. Finally, the *Examiners Handbook* highlights the importance of insurers' continually updating their cybersecurity programs. Unsuccessful cybersecurity incidents (e.g., failed attempts by unauthorized users to access an insurer's network) may not have significant regulatory implications (such as fines, reporting requirements, etc.), but they represent an opportunity for insurers to review and enhance their cybersecurity programs.

In the U.S., insurers are subject to the consumer data privacy and protection requirements of the federal Gramm-Leach-Bliley Act (GLBA), which establishes multiple privacy provisions for data held by financial institutions.[16] Pursuant to the GLBA, the NAIC has developed model regulations to help protect customer information held by insurers. The NAIC's *Privacy of Consumer Financial and Health Information Model Regulation* (#672, adopted in 2000) is designed to protect the privacy of insurance consumers' personal information.[17] The NAIC's *Standards for Safeguarding Customer Information Model Regulation* (#673, adopted in 2002) establishes standards for developing and implementing administrative, technical and physical safeguards to protect security, confidentiality and integrity of customer information.[18]

In an effort to implement additional consumer data protections, the *Insurance Data Security Model Law* (referenced above) establishes standards not only for data security but also for investigation and notification to the insurance commissioner of a "cybersecurity event" such as a data breach. The model law also directs insurers to comply with the relevant state data breach notification law and provide the insurance commissioner with copies of any notice sent to consumers pursuant to such applicable laws. Some individual states also have adopted general consumer data privacy and protection laws.[19]

III. Other Initiatives

Regulators in both the EU and U.S. have engaged in various initiatives – such as cybersecurity exercises and multi-jurisdictional coordination – to gather information and otherwise evaluate and promote insurance industry cybersecurity. A selection of these initiatives is detailed below.

---

[16] Pub. L. No. 106-102, 113 Stat. 1338 (1999).

[17] The model regulation is available at https://www.naic.org/store/free/MDL-672.pdf. All states adopted the model regulation and are in the process of adopting recent 2017 revisions to the regulation.

[18] The model regulation is available at https://www.naic.org/store/free/MDL-673.pdf. The model regulation includes an annex tallying model adoption.

[19] *See, e.g.*, Calif. Civil Code § 1798.100 et seq. ., http://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?lawCode=CIV&division=3.&title=1.81.5.&part=4.&chapter=&article; Colorado House Bill 18-1128, signed by Governor May 29, 2018, https://leg.colorado.gov/sites/default/files/documents/2018A/bills/2018a_1128_signed.pdf.

A. Evaluating Insurer Cyber Incidents and Insurance Industry Cybersecurity

EIOPA included in its 2018 Insurance Stress Test exercise a cyber questionnaire, collecting information from 42 participating European insurance groups related to cyber-risk as an element of their own risk profile.[20] The questionnaire sought information regarding the impact of recent cyber incidents, both in terms of frequency and economic losses.[21] EIOPA is currently analyzing the questionnaire responses and plans to publish the results in its 2018 stress test report, scheduled for release in January 2019.

In France, the Autorité de Contrôle Prudentiel et Résolution (ACPR) released a discussion paper on IT risks for banks and insurers, with the objective of creating a common IT risk management standard across the banking and insurance sectors. The discussion paper emphasized that IT risk management is no longer a topic specific to an IT team or department, but one that should be part of an organization's overall risk management approach and be coordinated by the risk management function.[22] The discussion paper defined and classified categories of IT risks and described risk factors within each category. The discussion paper then highlighted best practices and outlined expectations for risk mitigation and control.

In Germany, BaFin conducted a survey between August and November 2017 to learn more about how German insurers and pension funds handle their cyber risks.[23] BaFin's objective was to spot companies' typical strengths and weaknesses in order to identify appropriate areas for supervision. The survey revealed considerable room for improvement within the industry with respect to cybersecurity. BaFin intends to factor the survey's findings into its selection of audit candidates and define audit focal points. This survey also signaled BaFin's intent to closely monitor companies' IT operations, including third-party service providers, going forward.

In the Netherlands, the Dutch supervisory authority, DeNederlandscheBank (DNB), regularly examines and benchmarks a portion of insurers using the DNB Assessment Framework for Information Security. DNB regularly reports the conclusions of these assessments and benchmark to the insurance industry.[24]

In the UK, the Financial Conduct Authority (FCA) completed a cyber resilience questionnaire in 2017 for both life and non-life insurers and provided feedback to insurers based on the results. The Prudential Regulation Authority (PRA) and FCA also recently published a discussion paper on financial sector

---

[20] *See* EIOPA-ST18_Template, https://eiopa.europa.eu/Publications/Surveys/EIOPA-BOS-18-191_Templates_v20180622.xlsx (worksheet CRQ, part 2).

[21] EIOPA, *Insurance Stress Test 2018 Technical Specifications* (May 14, 2018), https://eiopa.europa.eu/Publications/Surveys/EIOPA-BOS-18-189_Technical%20Specifications_v20180622.pdf.

[22] ACPR, *IT Risk: Discussion Paper* (March 2018), https://acpr.banque-france.fr/sites/default/files/medias/documents/it_risk.pdf; https://acpr.banque-france.fr/en/it-risk.

[23] BaFin, *Cyber security: BaFin Survey of German Insurance Undertakings* (Sept. 24, 2018), https://www.bafin.de/SharedDocs/Veroeffentlichungen/EN/Fachartikel/2018/fa_bj_1808_Cybersicherheit_en.html.

[24] DNB, *Sector terugkoppeling resultaten Informatiebeveiliging / Cyber onderzoek 2017 bij verzekeraars en pensioenfondsen* (Feb. 23, 2018), https://www.dnb.nl/binaries/1%20Sector%20terugkoppeling%20resultaten%20Informatiebeveiliging%20%20-%20Cyber%20onderzoek%202017%20bij%20verzekeraars%20en%20pensioenfondsen_tcm46-373187.pdf?2018101510.

operational resilience and are currently assessing the respondents' feedback.[25] Furthermore, the PRA and FCA have started to develop an operational resilience framework to assist in their assessment of operational resilience as a whole.

On the federal level, the U.S. Department of Treasury's Federal Insurance Office (FIO) monitors cybersecurity in the insurance industry and provides annual updates in its *Annual Report on the Insurance Industry*.[26] FIO is also currently in the process of establishing an interagency working group on insurance industry cybersecurity.[27]

As part of the NAIC's strategic plan, state insurance regulators are studying whether to develop a Cybersecurity Insurance Institute (Institute).[28] The Institute would concentrate on perpetrators of fraud by identity theft, ransomware and other electronic means. The Institute's functions might include: collecting and cataloging data on cyber breaches; studying cybersecurity breach events and continuously tracking cybersecurity risks; providing information on cyber risk mitigation; developing educational materials on cybersecurity matters; creating certifications for successful completion of cybersecurity coursework; creating a federated digital identity to replace personally identifiable information used for identity verification; and other cybersecurity-related activities. The idea for the Institute was explored in joint cybersecurity forums held by the NAIC and Stanford University in October 2017 and October 2018.[29] The next step in this process will be to develop a proposal for a possible framework for the Institute.

B. Cybersecurity Exercises and Other Programs

Cybersecurity tabletop exercises and other programs are useful means for regulators to help the insurance industry and its regulators test their ability to respond effectively to cyber incidents.

The European Commission's FinTech Action Plan includes cybersecurity.[30] The Commission is currently exploring and assessing the barriers that limit market participants from sharing information on cyber threats and may pursue additional actions supporting cybersecurity. Within the context of the FinTech

---

[25] Bank of England and Financial Conduct Authority, *Building the UK financial sector's operational resilience* (July 2018), https://www.bankofengland.co.uk/-/media/boe/files/prudential-regulation/discussion-paper/2018/dp118.pdf.

[26] *See, e.g.*, FIO, *Annual Report on the Insurance Industry* (2018), at 30-32, https://www.treasury.gov/initiatives/fio/reports-and-notices/Documents/2018_FIO_Annual_Report.pdf.

[27] U.S. Department of Treasury, *A Financial System That Creates Economic Opportunities: Asset Management and Insurance* (2017), at 118, *https://www.treasury.gov/press-center/press-releases/Documents/A-Financial-System-That-Creates-Economic-Opportunities-Asset_Management-Insurance.pdf*.

[28] *See* NAIC, *State Ahead: Strategic Plan 2018 2019 2020* (2018), at 22, https://www.naic.org/documents/state_ahead_strategic_plan.pdf?63.

[29] *See, e.g.*, "NAIC, Stanford Host Joint Cybersecurity Forum," press release (Oct. 11, 2017), https://www.naic.org/Releases/2017_docs/naic_stanford_cybersecurity_forum.htm; *2018 NAIC & Stanford Joint Cybersecurity Forum Agenda*, https://www.naic.org/documents/cipr_events_2018_naic_stanford_cybersecurity_form.pdf?55.

[30] European Commission, *Fintech Action plan: For a more competitive and innovative European financial sector* (March 2018), https://ec.europa.eu/transparency/regdoc/rep/1/2018/EN/COM-2018-109-F1-EN-MAIN-PART-1.PDF.

Action Plan, EIOPA has launched a project on data and IT security and governance which includes cyber risks and cyber-incident tests. The project's main objectives are to: (1) analyze the applicability of the Information and Communication Technology (ICT) security and governance requirements to the insurance industry; (2) assess if and how ICT requirements could be implemented in the industry; (3) enhance supervisory convergence with respect to ICT security and governance requirements across sectors; and (4) if needed, provide recommendations on ICT security and governance and a cost benefit analysis on a possible EU-wide, cross-sector cyber-resilience framework for significant market participants.[31]

EIOPA has started the preparation for a walkthrough exercise as part of its strategic objective to enhance crisis preparedness and cooperation between EIOPA and national insurance supervisory authorities. This scenario-based crisis exercise will gather participants who will walk through the crisis response processes of a specific institution over an extended time period (e.g., 1 to 3 months). The exercise's main objective is to assess the information sharing and decision-making procedures in place at the national supervisory authorities and at EIOPA. The exercise will include the following steps: select participants; design the scenario; rehearse and refine the exercise; run the exercise; and gather feedback from the exercise.

In the U.S., through the Financial and Banking Information Infrastructure Committee (FBIIC), the U.S. Department of Treasury, state insurance regulators, and the NAIC have collaborated to facilitate tabletop exercises with insurers to explore cybersecurity incident response and recovery across the insurance industry.[32] Currently under consideration are regional exercises to further engage with small and medium-sized insurers. In addition, the U.S. Department of Treasury has worked with private sector and government partners to develop a Financial Sector Exercise Template that smaller companies can use to carry out internal cybersecurity exercises.[33] NIST also has developed a guide for testing IT plans, which includes material for creating and preparing for tabletop exercises.[34]

C. Multi-Jurisdictional Coordination and Information Sharing

Coordination among regulators is helpful in assisting insurers with responding to and recovering from cyber incidents. Information sharing among regulators and insurance industry participants also is a useful way to identify best practices, share threat intelligence, and improve baseline protections for the industry as a whole.

---

[31] In the EU several cyber resilience testing frameworks have been implemented, such as CBEST in the UK (https://www.bankofengland.co.uk/financial-stability/financial-sector-continuity) and TIBER-EU by ECB (https://www.ecb.europa.eu/press/pr/date/2018/html/ecb.pr180502.en.html). These frameworks are taken into account in the work of the project group.

[32] These insurance industry exercises are part of the "Hamilton Series" of cybersecurity exercises for the financial sector co-sponsored by the U.S. Department of the Treasury and the Financial Services Sector Coordination Council (FSSCC), a private sector body that works with the U.S. Treasury toward the shared goal of maintaining a robust and resilient financial services sector.

[33] *See* FBIIC, *Financial Sector Cyber Exercise Template*, https://www.fbiic.gov/financial-sector-cyber-exercise.html.

[34] *See* NIST, *Guide to the Test, Training, and Exercise Programs for IT Plans and Capabilities*, https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-84.pdf. *See also* DHS, *Homeland Security Exercise and Evaluation Program* (April 2013), https://www.fema.gov/media-library-data/20130726-1914-25045-8890/hseep_apr13_.pdf.

Within the EU, the Solvency II regulatory framework includes requirements for close cooperation in the colleges of supervisors for cross-border operating groups. The College Coordination Arrangements include, as an annex, an emergency plan to support the group supervisor and the college of supervisors in managing emerging crises, including severe cyber incidents. The emergency plan includes instructions for: facilitating the exchange of confidential information within the college on short notice; creating transparency with regard to the group structure; issuing an early crisis alert to maximize time for coordination and cooperation; and ensuring effective and efficient information sharing within the college and to the public as needed. The group supervisor also maintains and regularly updates a register documenting the contact details of all supervisors involved in the supervision of the undertakings belonging to a specific group.[35]

In the U.S., state insurance regulators coordinate regularly with federal and state financial regulators to facilitate communication and consider ways to effectively coordinate regulatory approaches to managing and evaluating cybersecurity risk. As part of these collaborative efforts, state insurance regulators and the NAIC engage with financial regulators through the FBIIC, chaired by the U.S. Secretary of the Treasury. The FBIIC regularly collaborates with the FSSCC. State insurance regulators also participate in the Cybersecurity Forum for Independent and Executive Branch Regulators to discuss best practices and common regulatory approaches to cybersecurity challenges across different sectors of the U.S. economy.

The NAIC's *Principles for Effective Cybersecurity: Insurance Regulatory Guidance* encourage insurers to utilize information sharing and analysis through participation in organizations such as the Financial Services Information Sharing and Analysis Center (FS-ISAC), which aims to help financial services organizations identify, assess, and monitor emerging cyber threats.[36] The *Examiners Handbook* also includes procedures for evaluating how an insurer integrates insights learned from other parties to strengthen their control response.[37]

The NAIC also is developing processes to enhance interstate cooperation when a cyber incident affects multiple states. These processes would supplement existing processes of more general application for responding to major market conduct crises, which could include a crisis caused by a significant cyber incident. The NAIC's Market Action Working Group (MAWG) identifies companies with market conduct issues with potential multi-state or national impact. State insurance regulators then assess the need for a collaborative response and, if a collaborative response is needed, they will identify a small group of Lead States, including a Managing Lead State. The Managing Lead State bears the overall responsibility to facilitate communication, coordinate activities in an efficient manner, and serves as the primary contact with the regulated entity under review. The Managing Lead State will convene the Lead States for initial strategy planning to determine the appropriate course of action and scope of issues to be addressed. Additional jurisdictions may participate in the collaborative action by executing a

[35] As part of the EIOPA 2011 Action Plan for colleges of supervisors, EIOPA conducted a college emergency infrastructure test exercises. The crisis simulation was performed on the basis of the emergency plan with the aim to test if all members of the College can be reached in a reasonable timeframe.

[36] NAIC, *Principles for Effective Cybersecurity: Insurance Regulatory Guidance* (2015), https://hyperlink.services.treasury.gov/agency.do?origin=http://naic.org/documents/committees_ex_cybersecurity_tf_final_principles_for_cybersecurity_guidance.pdf.

[37] For more on examinations, see Section II.B, above.

participation agreement. The Managing Lead State, in coordination with the Lead States, is responsible for negotiations of any settlement, however each Participating State must proactively agree and sign any final Regulatory Settlement Agreement with the entity under review.

Communication and coordination between state insurance regulators has always been a key aspect of U.S. solvency regulation; information sharing for troubled companies is a component of the NAIC Financial Regulation Standards and Accreditation Program.[38] Further, when the crisis involves an insurance group that writes significant amounts of insurance in other jurisdictions, its supervisory college may come into play. The NAIC Financial Analysis Handbook includes standards for supervisory colleges, including the establishment of a crisis management plan for communication, responsibilities and coordinating regulatory actions. Whenever a potential emergency situation is identified by a member of the supervisory college, the regulator should inform the group lead regulator as soon as possible. Based on the information received from the participating regulators, the group lead will assess the nature of the emergency situation and its implications for the group in conjunction with the college members. The supervisory college ultimately may decide to: monitor the situation or specific factors, contact other regulators who may have involvement, and/or intervene.[39]

IV. Conclusions and Next Steps

The EU-U.S. Insurance Project will focus its future efforts on further examining these and other examples and approaches to insurer cybersecurity and post-incident coordination. Project members also are contemplating the development of an exercise template or process that could be used to test inter-jurisdictional responses to a multi-national cybersecurity incident. Initial discussions already have highlighted the need for continued dialogue in order to achieve the goal of improved cross-border coordination.

[38] *See, e.g.*, NAIC, *Accreditation* (website last updated July 18, 2018), https://www.naic.org/cipr_topics/topic_accreditation.htm.

[39] See NAIC, *Financial Analysis Handbook* (2017), at 2-219, https://www.naic.org/prod_serv/FAH-ZU-16-02.pdf.

Appendix

For more information on insurance industry and/or financial sector cybersecurity, the following is a non-exhaustive list of resources:

- Bank of England, *Financial Sector Continuity (including CBEST)* https://www.bankofengland.co.uk/financial-stability/financial-sector-continuity
- FIO, *Annual Report on the Insurance Industry* (2017), https://www.treasury.gov/initiatives/fio/reports-and-notices/Documents/2017_FIO_Annual_Report.pdf
- FIO, *Annual Report on the Insurance Industry* (2018), https://www.treasury.gov/initiatives/fio/reports-and-notices/Documents/2018_FIO_Annual_Report.pdf
- FSB, *Cyber Lexicon – Consultative Document* (2018), http://www.fsb.org/wp-content/uploads/P020718.pdf
- FSB, *Summary Report on Financial Sector Cybersecurity Regulations, Guidance, and Supervisory Practices* (October 2017), http://www.fsb.org/2017/10/summary-report-on-financial-sector-cybersecurity-regulations-guidance-and-supervisory-practices/
- *G-7 Fundamental Elements for Effective Assessment of Cybersecurity in the Financial Sector*, http://www.g7italy.it/sites/default/files/documents/G7%20Fundamental%20Elements%20for%20Effective%20Assessment%20of%20cybersecurity%20in%20the%20financial%20sector.pdf
- IAIS, *Draft Application Paper on Supervision of Insurer Cybersecurity* (2018), https://www.iaisweb.org/page/consultations/current-consultations/application-paper-on-cyber-security
- NAIC Cybersecurity Working Group, *Principles for Effective Cybersecurity: Insurance Regulatory Guidance* (2015), http://www.naic.org/documents/committees_ex_cybersecurity_tf_final_principles_for_cybersecurity_guidance.pdf
- NAIC Cybersecurity Working Group, *Roadmap for Cybersecurity Consumer Protections* (2015), http://www.naic.org/documents/committees_ex_cybersecurity_tf_related_roadmap_cybersecurity_consumer_protections.pdf
- NIST, *Cybersecurity Framework*, https://www.nist.gov/cyberframework
- NCSC, *Networks and Information Systems (NIS) Directive*, https://www.ncsc.gov.uk/guidance/introduction-nis-directive
- PRA, *Survey of Insurers on Cyber Resilience* (2015) https://www.bankofengland.co.uk/-/media/boe/files/prudential-regulation/letter/2015/cyber-resilience-questionnaire-for-insurers.pdf