AMERICAN INSURANCE ASSOCIATION

555 12th Street NW
Suite 550
Washington, DC 20004
202-828-7100
Fax 202-293-1219
www.aiadc.org

February 17, 2017

BY ELECTRONIC MAIL

Board of Governors of the
Federal Reserve System
20th Street and Constitution Avenue, NW
Washington, DC 20551
regs.comments@federalreserve.gov

Office of the Comptroller of the Currency
400 7th Street SW, Suite 3E-218
Mail Stop 9W-11
Washington, DC 20219
regs.comments@occ.treas.gov

Federal Deposit Insurance Corporation
550 17th Street NW
Washington, DC 20429
comments@fdic.gov

Re: Enhanced Cyber Risk Management Standards
Docket No. R-1550; FRB RIN 7100-AE-61; FDIC RIN 3064-AE45; OCC Docket ID OCC-2016-0016

Ladies and Gentlemen:

The American Insurance Association ("AIA") appreciates the opportunity to provide comments on the Advanced Notice of Proposed Rulemaking (ANPR) regarding "Enhanced Cyber Risk Management Standards" ("Enhanced Standards"), as announced jointly by the Office of the Comptroller of the Currency ("OCC"), the Board of Governors of the Federal Reserve System ("Federal Reserve"), and the Federal Deposit Insurance Corporation ("FDIC") (collectively, the "Agencies"). Celebrating its 150th year in 2016, AIA is the leading U.S. property-casualty insurance trade organization, representing approximately 320 insurers that write more than $125 billion in premiums each year. AIA member companies offer all types of property -

casualty insurance, including personal and commercial auto insurance, commercial property and liability coverage, specialty, workers' compensation, homeowners' insurance, medical malpractice coverage, and product liability insurance. Our members are keenly interested in the ANPR because cybersecurity is one of our top priorities and, more significantly, the proposal is considering application to nonbank financial companies supervised by the Federal Reserve. Therefore, pursuant to the Dodd-Frank Act, the Enhanced Standards may apply directly to some insurance institutions. Below we have identified some principal observations for your review as you consider translating the ANPR into a more detailed proposal.

Necessity

Respectfully, we question whether the Enhanced Standards are necessary at this point. For instance, the ANPR identifies examples of existing guidance and supervisory tools for financial institutions. However, this list of examples is not exhaustive; we have identified additional, insurance-specific supervision tools.

- For example, at least 34 states and the District of Columbia have adopted regulations implementing Title V, Subtitle A of the Gramm-Leach-Bliley Act (GLBA).[1] These regulations would be equivalent to the "Interagency Guidelines Establishing Information Security Standards" identified in Section II (a) of the ANPR.
- Insurers are also subject to IT examinations by state insurance departments. In 2016, state regulators reviewed existing examination guidance for consistency with the Cybersecurity Framework and also the FFIEC Cybersecurity Assessment Tool. Regulators made changes to the examination guidance to reflect various elements of the Cybersecurity Framework and concluded that, while the assessment tool is not necessarily applicable to insurers, "everything this assessment tool provides is already implemented in the NAIC's current guidance."[2]
- Further, cyber risk assessments are embedded in the overall risk management function. Consequently, the Risk Management and Own Risk and Solvency Assessments (ORSA) required for insurers in most states are another opportunity for cyber risk oversight.

---

[1] Ala. Admin. Code r. 482-1-126.01 et seq.; Alaska Admin. Code tit. 3, §§26.705, 26.715 and 26.749; Ariz. Admin. Code R20-6-2101 et seq.; Ark. Insurance Rules and Regulations 77; Cal. Code Regs. tit. 10, §2689.12 et seq.; 3 Colo. Code Regs. § 6-4-2; Conn. Agencies Regs. §38a-8-124 et seq.; Del. Code Regs. 18-900-905 (alt. cite: 18 Del. Admin. Code §905-1.0 et seq.); D.C. Mun. Regs. Tit. 26, §§3613 to §3620 and 3699 ; Fla. Admin. Code Ann. r. 69J-128.030 et seq. and r. 69O-128.030 et seq. ; Ill. Admin. Code tit. 50, §4003.10 et seq.; Iowa Code §191-90.37(505) et seq.; 806 Ky. Admin. Regs. 3:320; 02-031-980 Me. Code r. §1 et seq. ; 201 Mass. Code Regs. 17.01 et seq. ; Mich. Admin. Code r. 500.551 et seq.; Mich. Bulletin 2010-21-INS (12/29/10); Minn. Stat. §60A.98 et seq.; Mo. Code Regs. Ann. tit. 20, §100-6.110; Mont. Admin. R. 6.6.7001 et seq.; 210 Neb. Admin. Code §77-001 et seq.; N.H. Code Admin R. Ins. 3701.01 et seq.; N.J. Admin. Code §11:1-44.1 et seq.; N.Y. Comp. Codes R. & Regs. tit. 11, §421.0 through 421.10 (Reg. 173); N.C. Gen. Stat. §58-39-130 et seq.; N.D. Admin. Code 45-14-02-01 et seq.; Okla. Admin. Code §365:35-3-1 et seq. ; Or. Admin. R. 836-081-0101 et seq.; 31 Pa. Code §146c.1 et seq. ; R.I. Admin. Code §11-5-107 :1 et seq. (Rule 107); S.D. Admin. R. §20:06:45:03 and 20:06:45:20 through 20:06:45:26; Utah Admin. Code r. 590-216 ; Vt. Code R. 21-020-055 (IH-2002-03) (alt. cite : Vt. Admin. Code §4-3-46 :1 et seq.) ; Va. Code Ann. §38.2-613.2 ; Va. Admin. Letter Nos 2003-4 (05/18/03) & 9-1-2009 (09/01/09) ; W. Va. Code R. §114-62-1 et seq. ; Wy. Rules and Regulations INS GEN. ch. 55, §1 et seq

[2] National Association of Insurance Commissioners. (2015 August 16). National Summer Meeting Minutes, Cybersecurity Task Force. San Diego.

We urge the Agencies to consider whether new federal regulations in this area are necessary, given the existing guidance and supervisory tools mentioned in the ANPR; the existing ability of the agencies to review covered entities' cyber risk programs as part of ongoing oversight; and existing oversight of cyber risk and data security by state insurance regulators, as highlighted above. Since authority already exists to consider the individual risk profiles of firms under the Federal Reserve supervision, it is unnecessary to promulgate a new regulation for all covered entities. Accounting for unique risk profiles is also a concept consistent with the Federal Reserve's approach to capital requirements, which recognizes differences between banking and insurance. The Federal Reserve is taking into consideration the different characteristics and risks of its supervised entities as it fashions a capital assessment regulatory regime.[3]

Scope/Sector-Critical

The tone of the ANPR suggests that the Agencies are trying to address the interconnectedness of the U.S. financial system and the potential systemic impact technology failures and cyber-attacks may have on the safety and soundness of the U.S. financial system. Additionally, section IV identifies a tiered approach with a higher set of expectations for "Sector-Critical Systems." Insurers should not be considered "Sector-Critical" in the context of this ANPR given that they have no connectivity to payment, settlement and clearing systems like banks. In addition, unlike customer deposits held by banks, payment of claims under an insurance policy depends on the occurrence of a covered event. Therefore, as a practical matter, insurance consumers do not have "on demand" access to insurance assets as they do with other financial institutions. Further, insurers are extensively regulated under U.S. state law and are closely supervised by state insurance authorities. As a result, insurers present very low risk to the financial system. Accordingly, insurers engaged in regulated insurance activities do not present significant risk to financial stability either within the U.S. or globally.[4]

To the extent the Agencies consider moving forward with the Enhanced Standards, we would respectfully urge you to specifically consider exempting insurers from the scope of the regulation. At the very least, the Agencies should specifically define "sector-critical" in a way that excludes the business of insurance from the defined term.

---

[3] Tarullo, Governor Daniel K. "Insurance Companies and the Role of the Federal Reserve." National Association of Insurance Commissioner's International Insurance Forum, 20 May 2016, Washington, D.C. https://www.federalreserve.gov/newsevents/speech/tarullo20160520a.htm

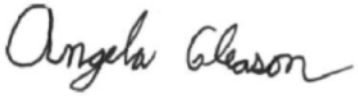
[4] Comments of the American Insurance Association in Response to Advance Notice of Proposed Rulemaking Regarding Authority to Require Supervision and Regulation of Certain Nonbank Financial Companies Pursuant to Section 113 of the Dodd-Frank Wall Street Reform and Consumer Protection Act (Docket No. FSOC– 2010-0001) (Comments filed Nov. 5, 2010) (available at www.regulations.gov, Doc. ID FSOC-2010-001-0029 through FSOC - 2010-0001-0029.3).

Effective Cybersecurity Programs Must be Risk-Based and Flexible

Cybersecurity is an important issue and insurers take guidance, whether binding or not, into serious consideration. However, critical for any information security program is a risk-based approach that is flexible, scalable and adaptable to unique risk profiles. Overall, the Agencies should shy away from being overly prescriptive in their rulemaking. Rather, we strongly recommend that the Agencies collaborate on an ongoing basis with the industry to ensure a strong, non-prescriptive, risk-based framework is promulgated. As noted above, not all financial services companies are the same, especially institutions under the Agencies' jurisdiction (i.e. stark differences between banks and insurers). Therefore, promulgating rules that are not risk-based or more tailored to a framework would impose unduly onerous requirements on insurers.

AIA appreciate the consideration of our comments and are happy to answer any questions you may have.

Respectfully submitted,



Angela Gleason
Senior Counsel
American Insurance Association
555 12th Street, N.W.
Suite 550
Washington, DC 20037
202-828-7181