Cybersecurity: 2015's top legal developments and what they mean for key sectors

Cybersecurity Law Alert

11 FEB 2016

By: Sydney M. White | Jim Halpert

At the US federal level, 2015 ushered in significant new laws, regulations, and guidance on cybersecurity as lawmakers, regulators, and businesses continued their efforts to combat cybercrime − one of the most significant drains on the US economy and a source of potentially grave threats from nation states.

This alert provides a synopsis of these important developments.

CYBERSECURITY INFORMATION SHARING LEGISLATION

On December 18, President Barack Obama signed into law the omnibus appropriations and tax bill that included the Cybersecurity Act of 2015, the informally conferenced version of the cybersecurity information sharing bills passed by both the House and Senate earlier this year.[1] The Cybersecurity Act provides a paradigm for the sharing of information on cybersecurity threats and defensive measures among private sector entities and between the private sector and the government. It also provides liability protection to private sector entities for sharing cybersecurity threat information and defensive measures with the government and other private sector entities. Finally, it provides antitrust protection when information is shared only between private entities.

The Cybersecurity Act is largely based on the Senate Intelligence Committee bill, S. 754 (CISA), provisions from H.R. 1560 (the combined House Intelligence Committee and House Homeland Security Committee bills), as well as some newly negotiated language. It provides that the Department of Homeland Security (DHS) will act as the central hub for information sharing. However, in a new twist, the bill provides that if the DHS portal fails to be fully operational and secure, the President may designate a new civilian information-sharing hub. By keeping the hub within a civilian agency, this change softened the language for privacy proponents who objected to sharing information directly with intelligence and law enforcement agencies.

Under the Cybersecurity Act, Congressional oversight committees have ample opportunities to review implementation of information sharing process, and House Homeland Security Committee Chairman Michael McCaul (R-TX) has already announced plans to hold regular oversight hearings in order to insure there is effective implementation of the information-sharing provisions that also protects privacy and civil liberties, another key

component of the Act.

The liability protections included in the Cybersecurity Act largely mirror the language in both CISA and the House Intelligence Committee bill, with some slight variations. Private sector entities are required to remove personal information unrelated to a cybersecurity threat prior to sharing it through the DHS portal. DHS is also required to do a second scrub to remove personal information. The key is that the Act requires the sharing of information in real time vs. other language discussed during Congressional deliberations that might slow the sharing process down and allow the intruder to disappear before countermeasures can be implemented.

The section added to CISA that would create new DHS authority to regulate the cybersecurity practices of covered critical infrastructure and their cyber supply chains and impose what amounts to a cybersecurity breach reporting requirement was removed from the final bill during conference. However, new language was negotiated during the conference that requires DHS to report to Congress on the feasibility of producing a risk informed plan to address multiple simultaneous attacks on critical infrastructure that could have an impact on other critical infrastructure. This language is intended to address critical infrastructure sectors that are interdependent, such as energy, telecom, and IT.

IMPLEMENTING THE INFORMATION SHARING EXECUTIVE ORDER

We last reported on the President's Executive Order on Information Sharing in an alert published in February 2015. The President's Executive Order required DHS to take steps to expand information sharing and analysis organizations (ISAOs) to allow formation of ISAOs by non-critical infrastructure entities, despite the critical infrastructure limitation in the Homeland Security Act of 2002.

Although Congress did not broaden the definition of ISAOs to include non-critical infrastructure under the Homeland Security Act when it passed the Cybersecurity Act, it did provide some additional flexibility for non-critical infrastructure entities by allowing for greater use of voluntary information sharing agreements with DHS. One of the goals of the Executive Order was to encourage creation of ISAOs for purposes other than the protection of critical infrastructure, including both small businesses and larger entities, as well as non-sectoral organized entities, and also allowing for organization around particular threats.

In accordance with the Executive Order, DHS has selected the team tasked with developing guidance and standards for ISAOs: a group composed of the University of Texas at San Antonio's Center for Infrastructure Assurance and Security, the Logistics Management Institute, and the newly formed Retail Cyber Intelligence Sharing Center. The team is called the ISAO Standards Organization. Once the standards-setting group issues guidance for new ISAOs, we expect to see a proliferation of new ISAOs organized around innovative parameters.

Streamlined regulations: not here yet

Streamlining regulation was identified as a priority in the Cybersecurity Executive Order issued in 2012, but many critical infrastructure sectors continue to struggle with what they consider to be overly prescriptive cyber-regulation or the prospect of new cyber-regulation. This month, Executive Branch agencies with regulatory authority over critical infrastructure sectors are required, under the Cybersecurity Executive Order, to report to the Office of Management and Budget (OMB) on any "ineffective, conflicting, or excessively burdensome cybersecurity requirements." Although the Cybersecurity Executive Order required the Secretaries of DHS, Treasury, and Commerce to recommend incentives for companies to adopt the Cybersecurity Framework consistent with the Executive Order's focus on voluntary measures, and these proposed incentives eventually included streamlining regulation, we have seen little indication that federal agencies will voluntarily reduce regulations that they oversee in such a high-profile area as cybersecurity.

INDUSTRY SECTOR-SPECIFIC DEVELOPMENTS

A. Communications sector

The Federal Communications Commission Communications Security, Reliability and Interoperability Council VI (CSRIC) Working Group 4, composed of representatives from communications businesses (telecommunications wireline and wireless, cable, broadcast, and satellite), trade groups, and federal and state government agencies, worked to tailor the 2014 National Institute of Standards & Technology (NIST) Cybersecurity Framework to the communications sector in order to 1) facilitate the voluntary use of the Framework by communications providers and 2) to provide voluntary mechanisms by which communications providers can give public assurance that they are taking adequate steps to protect cybersecurity. The resulting report, "Cybersecurity Risk Management and Best

Practices," (the CSRIC Report) was released in March 2015. The report has been widely heralded as providing a new means for companies of all sizes within the communications sector to improve cybersecurity and is also serving as a paradigm for other critical infrastructure sectors.

The CSRIC Report adheres to the voluntary approach of the Framework. In lieu of new FCC cybersecurity regulations, the Report recommends that companies participate in voluntary and confidential "assurance meetings" between the FCC and individual companies in order to discuss the company's cybersecurity programs including for risk management. The Report emphasized that the FCC would have to conduct the meetings under the DHS Protected Critical Infrastructure Information (PCII) Program or a legally equivalent paradigm that enables the FCC to provide adequate confidentiality protections (including from FOIA), liability protections, and the assurance that the information discussed during meetings would not be used for regulatory or enforcement purposes.

As of this writing, DHS and the FCC are still sorting through the process for the FCC to conduct the meetings under the PCII or a legally equivalent paradigm. Although their decision is not final, we anticipate that there may be some shortcomings in protections against liability in private litigation and the use of information for FCC enforcement and regulatory purposes. This may create a disincentive for companies that, in order to further their cybersecurity, would otherwise be willing to work with the FCC. Despite these potential shortcomings in confidentiality protections, once the FCC's policy statement is finalized, we anticipate that other federal sector-specific agencies will use the statement as a roadmap to establish procedures for similar assurance meetings with other industry sectors.

In a similar vein, the telecommunications sector has been confronted with a proposed Connecticut Public Utilities Regulatory Authority (PURA) Cybersecurity Oversight Program that would establish mandatory reporting and require utilities to participate in mandatory annual assurance meetings between each utility, PURA officials, and other representatives of state emergency management and homeland security agencies. Under the proposed program, the assurance meetings will cover topics such as the status of the utility's cybersecurity, third-party audits, and management's commitment to cybersecurity. The electricity, gas, and water sectors have agreed to participate in the meetings. The telecommunications sector, however, continues to have concerns with sharing this information in conjunction with the assurance meetings without more formalized protections against disclosure, given the sensitivity of the information; the sector has requested that PURPA obtain certification under the DHS PCII Program, which it has not done to date.

The telecommunications sector has also objected to the mandatory nature of the PURPA program, which would conflict with voluntary federal cybersecurity efforts, including under the NIST Cybersecurity Framework.

B. Government contractors

Cybersecurity reporting requirements for government contractors changed significantly in 2015. The major developments are summarized below.

Interim rules on network penetration reporting and contracting for cloud services

In late August 2015, the Department of Defense issued an interim rule, Network Penetration Reporting and Contracting for Cloud Services. The rule – which took effect immediately – made a number of changes to the existing cybersecurity and reporting regime applicable to all DoD contractors that possess unclassified information. This rule was then modified just four months later, on December 30, 2015, through the issuance of another interim rule.

The August rule expanded the class of information subject to the rule's requirements from "unclassified controlled technical information" (UCTI) to "covered defense information" (CDI). The rule defines CDI to include UCTI as well as other broad categories of information including "critical information" and "export controlled information." There is also a catch-all category of "any other information" specifically identified by the government that requires safeguarding consistent with government-wide law or policies. Under the rule, contractors must report any cyber incident that affects or has a "potential adverse effect" on a covered contractor information system or the CDI on that system within 72 hours of discovery. The rule does not expressly state what must be included in the report, but directs contractors to the Defense Industrial Base (DIB) reporting portal, which includes a checklist. These reporting requirements also extend to subcontractors who must report incidents to both the prime contractor and the government.

The August rule also changed the applicable NIST Special Publication (SP) security requirements to require compliance with NIST SP 800-171 instead of the previous NIST SP 800-53. Notably, while the rule contemplates a

procedure under which contractors can seek government approval of an equally secure system that does not satisfy the SP 800-171 requirements, the waiver procedure is not a model of clarity. It does not state what factors the government will consider in evaluating requests or whether a contractor will be able to apply government approval across its portfolio of contracts. Moreover, the modification of the rule issued on December 30 (discussed further below), deleted the requirement that waiver requests be decided "prior to contract award"; therefore, there is no deadline by which the government must decide a waiver request.

The August rule also added specific requirements related to use of cloud computing services. It prescribes policies and procedures that DoD officials must use when procuring cloud computing services. It also places requirements on contractors that provide cloud computing services to the government (known as cloud service providers or CSPs), including a requirement that CSPs maintain safeguards commensurate with previously issued DoD guidance and maintain all government data within the United States or outlying areas. CSPs are also required to report cyber incidents in a manner consistent with the other portions of the rule. Additionally, the rule requires all prospective offerors on contracts covered by the rule, not just CSPs, to represent whether they anticipate using cloud computing services in the performance of the contract.

The August rule took immediate effect without an opportunity for industry comment. In large part due to feedback from industry, DoD issued a modification of the rule on December 30, 2015 via a second interim rule. The most noteworthy change is that the rule extended the deadline for compliance with NIST SP 800-171 security requirements to "as soon as practical, but not later than December 31, 2017." Contractors must still comply with the 72-hour reporting requirement. In addition, contractors must now notify DoD within 30 days of contract award of any NIST SP 800-171 security requirements that could not be implemented at the time of contract award. According to the rule, this reporting will enable DoD to monitor progress across industry and identify common implementation issues. Industry recognizes that it will likely also provide DoD a starting place for evaluating non-compliance beginning in January 2018. Other changes made by the December rule include clarifying flow down requirements and deleting the deadline for acceptance of alternative security measures (discussed above).

The comment period for the first interim rule is closed. The **deadline for comments** on the December interim rule is **February 29, 2016**. We will continue to monitor developments with respect to these rules.

Defense Industrial Base Cybersecurity and Information Assurance Program

In October 2015, following issuance of the August rule on Network Penetration Reporting and Contracting for Cloud Services, DoD issued an interim rule that amended the regulations implementing the DoD Defense Industrial Base Defense Industrial Base Cybersecurity and Information Assurance Program (DIB program). The rule took effect immediately. The DIB program is a voluntary public-private cybersecurity reporting and information sharing regime for certain cleared defense contractors. Notably, while the reporting requirements in the DIB rule are essentially the same as those in the August interim rule, the coverage of this rule is more expansive and includes "all applicable agreements" in which DIB companies participate. While the rule does not define the term "all applicable agreements" or contain a contract clause for inclusion in these agreements, it appears to extend to all types of agreements including contracts, grants, cooperative agreements, etc. In addition, although the DIB is a voluntary program, the rule's reporting requirements extend to subcontractors who are not DIB program participants.

The comment period for this rule closed on December 1. As of this writing, DoD's Semiannual Regulatory Agenda anticipates the issuance of a final rule in August 2016.

Contractor liability protection under 2016 National Defense Authorization Act

Embedded in the 2016 National Defense Authorization Act[2] is an important provision for government contractors. Section 1641 provides liability protection to "cleared defense contractors" and "operationally critical contractors." Under this section, no cause of action may be maintained against these contractors in connection with the reporting of network penetrations unless the contractor engaged in willful misconduct in complying with the requirements.

Rulemaking by other federal agencies

As detailed above, DoD has taken the lead with respect to establishing cybersecurity requirements for government contractors. However, other agencies are currently following agency-specific procedures, and there is little or no uniformity among the agencies. For example, in March 2015, the Department of Homeland Security (DHS) issued a class deviation setting forth DHS-specific cybersecurity requirements.

Nonetheless, we expect that some uniform policy for executive agencies will emerge in 2016, as the Office of

Management and Budget is working toward a cybersecurity rule that applies across all government agencies. On August 11, 2015, OMB issued draft guidance entitled "Improving Cybersecurity Protections in Federal Acquisitions." The guidance is intended to increase cybersecurity controls in federal acquisitions and mitigate the risk of potential incidents in the future. While the guidance does not bind contractors, it directs agencies to promulgate rules consistent with the guidance that contractors will be required to follow. The guidance also contemplates an amendment to the Federal Acquisition Regulation (FAR) that will address (i) security controls, (ii) cyber-incident reporting, (iii) information system security assessments, and (iv) information security continuous monitoring. The guidance, in draft form, is rather high-level. The comment period closed on September 10, 2015. OMB anticipated issuing the final guidance in Fall 2015; however, as of this writing, OMB has yet to do so. OMB also issued other direction to agencies during 2015 such as the October 30, 2015 Cybersecurity Strategy and Implementation Plan and OMB Memorandum M-16-03, "FY 2015-2015 Guidance on Federal Information Security and Privacy Management Requirements." Both address actions that agencies must take to identify and report incidents.

Similarly, in June 2015, the National Archives and Records Administration (NARA) issued a proposed rule seeking to standardize the designation and safeguarding of controlled unclassified information. Comments were due by July 7, 2015; however, a final rule has not yet been issued.

Furthermore, on August 12, 2015, the General Services Administration (GSA) sought feedback on its Cybersecurity/Information Assurance (CyberIA) Project, which proposes to create a special item number (SIN) for cybersecurity services and products under GSA's IT Schedule 70. The SIN may encompass services relating to NIST's risk management framework, cloud security, training, governance and policy. At an industry meeting in October 2015, GSA indicated that final action on this item was not expected for at least six months to a year.

C. Healthcare sector

The sole industry sector explicitly addressed in the Cybersecurity Act of 2015 was healthcare. The Cybersecurity Act requires Department of Health and Human Services (HHS) to establish a taskforce by the end of February 2016 to include healthcare industry stakeholders and other cyber experts, which will submit a report to Congress by December 2016 on the preparedness of HHS and the healthcare industry to respond to cybersecurity threats as well as industry-specific cybersecurity challenges. The task force will also develop voluntary guidelines and best practices on cybersecurity for the sector.

D. Financial services sector

FFIEC cybersecurity guidance

The Federal Financial Institution Examination Council (FFIEC) is a formal interagency body empowered to prescribe uniform principles, standards and report forms for examinations of financial institutions by the Federal Reserve Board, the Federal Deposit Insurance Corporation, National Credit Union Administration, Office of the Comptroller of the Currency, and the Consumer Financial Protection Bureau. During 2015, the FFIEC announced several updates to its guidance on cybersecurity for financial institutions.

In February 2015, the FFIEC updated its IT Examination Handbook by releasing a revised Business Continuity Planning booklet. The update made certain additions to the examination procedures described in Appendix A of the booklet and added a new Appendix J, "Strengthening the Resilience of Outsourced Technology Services." The new appendix provides guidance on identifying third-party relationships that involve critical technology services and ensuring outsourced technology service providers have sufficient recovery capabilities.

The FFIEC released two statements in March 2015 about ways that financial institutions can identify and mitigate cyber-attacks that compromise user credentials or that use destructive software, known as malware. The FFIEC expects its member financial institutions to enhance their security programs to ensure they are able to identify and respond to these types of attacks. The user credentials statement is available here and the malware statement is available here.

On June 30, 2015, the FFIEC released a Cybersecurity Assessment Tool to assist financial institutions by providing a repeatable and measurable process to inform management of the institution's cybersecurity risk and level of preparedness. The Assessment consists of two parts: inherent risk profile and cybersecurity maturity. Inherent risk profile identifies the institution's inherent cybersecurity risk prior to implementing controls. Cybersecurity maturity measures the maturity level of controls in each of five areas, or domains, including cyber risk management and

oversight, threat intelligence and collaboration, cybersecurity controls, external dependency management, and cyber-incident management and resilience. In addition, the Cybersecurity Assessment Tool includes two appendices explaining how the security measures and objectives outlined in the Tool correspond to and incorporate other cybersecurity guidance.

Appendix A maps the Cybersecurity Assessment Tool's baseline measures to the FFIEC's existing risk management and control expectations, as outlined in the FFIEC IT Examination Handbook. Appendix B maps the Tool to the NIST Cybersecurity Framework.

The Assessment Tool is currently undergoing review by FFIEC that will produce a 2.0 version. Industry comments submitted in this review reflect concerns that the Tool abandoned the voluntary approach of the NIST Cybersecurity Framework for a mandatory and overly prescriptive approach. Comments also focused on the lack of industry participation in development of the Assessment Tool as well as concerns that a financial institution could be forced to submit its self-assessment for examination or regulatory purposes.

Most recently, in November, the FFIEC issued a statement alerting financial institutions to the increasing use of cyberattacks involving extortion. Cyber-criminals have increasingly used a variety of tactics, such as "ransomware," denial of service attacks, and theft of sensitive business and customer information to extort payment or other concessions. In some cases, attacks have caused significant impacts on businesses' access to data and ability to provide services. Some businesses have incurred serious damage through the release of sensitive information. The FFIEC encouraged financial institutions to address this threat through ongoing cybersecurity risk assessments and monitoring, as well as the development of effective business continuity plans to respond to this type of cyber-attack.

D. Insurance sector

Cybersecurity has become not only an increasingly important line of business but also an emerging threat to insurance companies as cyberthreats have become increasingly sophisticated. Insurance companies have been responding by strengthening or offering new cyber-risk products to help companies manage this growing area of risk. Insurance companies have also been high-profile victims, most notably Anthem Inc., the second-largest health insurer in the US. Anthem announced that on January 27, 2015, it had discovered that hackers had breached its databases containing personal information for about 80 million customers and employees.

New York Department of Financial Services

New York was the first state to individually respond to the Anthem breach, when its Department of Financial Services (DFS), following its 2014 report on cybersecurity threats in the insurance industry, issued the *Report on Cyber Security in the Insurance Sector* in February 2015, surveying the cybersecurity practices of 43 insurors, including health, property and casualty, and life insurance providers, with collective assets just over $3 trillion. The insurers shared their cybersecurity programs and, where applicable, their enterprise risk management reports, which are required as of 2014 for some insurers under New York State insurance regulations. The Report contained several positive findings.

According to the Report, over 80 percent of insurers surveyed reported that they have cyber-security breach notification plans; participate in information-sharing organizations; use industry standard security technologies; have increased their information security budgets over the past three years; have corporate governance procedures that include well-rounded participants from all important parts of an organization (e.g., IT, compliance officers, general counsel, CEOs); and have a designated information security executive.

On the other hand, while the department found that over half the insurers reported having experienced no cybersecurity breaches in the three years preceding the survey, the department still found room for improvement. Respondents that had experienced breaches reported causes that ranged from malware, hacking, and email ("phishing") scams to gaining control of network computers (e.g., botnets). Forty percent of respondents reported that they believe they should modify existing cybersecurity strategies to address new and emerging risks. The department concluded that insurers continue to be challenged by the sophistication of cybersecurity threats and the speed at which technology is changing (a common theme in many sectors). Two additional interesting findings: the largest insurers did not necessarily have the most robust and sophisticated cyber-defenses, and only 14 percent of respondents' CEOs receive monthly briefings on information security.

Consequently, the DFS urged insurers to implement the following measures:

- report information security issues on a monthly basis to senior management
- report information security issues to boards of directors and CEOs at least quarterly ***plus*** report to them on an ad hoc basis
- avoid relying primarily on penetration testing to determine whether vulnerabilities exist. According to the department, "Ongoing vulnerability scanning is as − if not more − important than penetration testing to identify known weaknesses and potential exposures."

On November 9, 2015, DFS announced it was continuing to consider adopting new regulations to develop a comprehensive cybersecurity framework for banks and insurance companies. According to DFS, the planned regulations would create specific requirements for cybersecurity policies and procedures, third-party vendor management, multi-factor authentication, chief information security officers, application security, cybersecurity personnel and intelligence, audits, and notice of cybersecurity incidents. The announcement was addressed to several different regulatory agencies and advisory groups, including the National Association of Insurance Commissioners (NAIC), and invites analysis and discussion on developing consistent regulations.

In December 2014, the New York Department of Financial Services announced that it would be expanding its IT examination procedures for banks and other financial institutions subject to DFS supervision to focus more attention on cybersecurity. At the time, observers noted that many of the examination requirements imposed by DFS would be tougher and more precise than those imposed by the federal banking regulators. These heightened requirements include providing information on the qualifications, job description, and reporting lines for each bank's chief information security officer, how each bank uses multi-factor authentication, and how it tests new software before putting it into use.

NAIC

At the national level, the NAIC formed the Cybersecurity (EX) Task Force for purposes of monitoring emerging cyber-risks, their impact on the industry and whether regulatory action will be required. In April, the NAIC released the Principles for Effective Cybersecurity: Insurance Regulatory Guidance intended to provide uniform guidance to state insurance regulators. Among the 12 principles is a recommendation to provide guidance that is "flexible, scalable, practical and consistent with nationally recognized efforts such as those embodied in the National Institute of Standards and Technology (NIST) framework issued in 2014.

Further, on December 17, 2015, the Task Force released the NAIC Roadmap for Cybersecurity Consumer Protections, which will function as a consumer bill of rights and will be incorporated in the planned NAIC cybersecurity model act/regulation. The Roadmap lays out the protections that consumers should receive from insurance companies, agents, and other businesses when they collect, maintain, and use consumers' personal information, but acknowledges that not all of the protections exist under current state law.

The Roadmap provides that a consumer has the right to:

- know what kinds of personal information are collected and stored by the insurance company, agent, or any business it contracts with
- expect the insurance company to have a privacy policy that explains its data practices, including how consumers' personal information is protected and what choices they have about the data
- expect the insurance company to take reasonable steps to prevent unauthorized access to consumers' personal information
- receive a notice from the insurance company, agent, or business it contracts with if the consumer's personal information is breached, no later than 60 days after a breach is discovered
- receive at least one year of identity theft protection paid for by the insurer or agent if the consumer's personal information is breached, and
- receive credit report fraud alerts, place a credit freeze on his/her credit report, and get information resulting from the data breach removed from his/her credit report.

E. Securities regulation

SEC

The Securities and Exchange Commission increased its focus on cybersecurity issues in 2015. In February, the SEC released publications addressing cybersecurity at brokerage and advisory firms, providing suggestions to investors on ways to protect their online accounts. These publications included a Risk Alert from the Office of Compliance

Inspections and Examinations (OCIE) setting out a number of observations based on OCIE examinations of broker-dealers and investment advisers.[3] The examinations focused on identifying cybersecurity risks; establishing cybersecurity policies, procedures, and oversight processes; protecting networks and information; and related matters. The SEC also issued an Office of Investor Education and Advocacy investor bulletin to help investors protect their online brokerage accounts from fraud. The bulletin suggested a number of precautions that investors should take to help ensure that their accounts remain secure.

In April, the SEC Division of Investment Management issued a guidance update[4] in which it highlighted the need for registered investment companies and registered investment advisers to protect confidential and sensitive information related to their activities, including information concerning fund investors and advisory clients. The guidance update discussed a number of measures that investment companies and advisers may wish to consider when addressing cybersecurity risks.

In September 2015, OCIE issued another Risk Alert[5] to provide additional information on the areas of focus for its next round of cybersecurity examinations. According to the Risk Alert, these examinations will involve more testing to assess implementation of firm procedures and controls, with areas of focus to include governance and risk assessment, access rights and controls, data loss prevention, vendor management, training and incident response. OCIE noted that examiners might also select additional areas based on risks identified during the course of the examinations. Also in September, the Office of Investor Education and Advocacy issued an Investor Alert to suggest important steps that investors should take immediately regarding their investment accounts if they become victims of identity theft or a data breach.[6]

In December, Commissioner Luis Aguilar issued a public statement discussing the Commission's own responsibilities for ensuring that it has effective cybersecurity protocols for the data that it gathers. Commissioner Aguilar noted the large amounts of data that each of the Commission's divisions and offices collect from various market participants and emphasized the need for the Commission to remain focused on cybersecurity issues in order to meet its obligations to those market participants and the public interest. Earlier in the year, Commissioner Aguilar issued public statements on the importance of focusing on cybersecurity challenges facing small and midsize businesses and those facing small and emerging companies.

FINRA

In February, the Financial Industry Regulatory Authority (FINRA) issued a report detailing practices that broker-dealers can incorporate into their procedures to strengthen their cybersecurity efforts.[7] The report grew out of a targeted examination sweep of a cross-section of FINRA-member firms in 2014, which focused on the types of threats faced by broker-dealers, the areas of vulnerability, and approaches to managing this risk. At the same time, FINRA issued an investor alert that encouraged investors to learn about their brokerage firms' cybersecurity policies and to take personal precautions to safeguard their accounts and personal financial information. The alert included advice on how investors can get to know a broker's cybersecurity practices and confirm that identity authorization methods are sufficient, as well as ways in which investors themselves can enhance the security of their information. FINRA also announced a cybersecurity conference in New York on February 11, 2016.

Commodity Futures Trading Commission

On the futures and derivatives side, in December, the US Commodity Futures Trading Commission voted unanimously to approve two proposals for amending current regulations addressing cybersecurity testing and safeguards for derivatives clearing organizations, trading platforms, and swap data repositories. The proposals, which are open for public comment during a 60-day comment period that ends on February 22, 2016, identify the types of cybersecurity testing that are essential to a sound safeguards program, including vulnerability testing, penetration testing, controls testing, security incident response plan testing, and enterprise technology risk assessments. The proposals require all derivatives clearing organizations, designated contract markets, swap execution facilities, and swap data repositories to conduct each type of testing as frequently as indicated by appropriate risk analysis; specify minimum testing frequency requirements for all derivatives clearing organizations and swap data repositories, and for specified designated contract markets; and require certain tests to performed by independent contractors.[8]

F. Energy sector

DoE Energy Electricity and ONG Subsectors Cybersecurity Framework Implementation Guidance

The Department of Energy worked with the Electricity Subsector and Oil & Natural Gas Subsector to develop this

guidance, released in January 2015, for energy sector owners and operators, which maps the NIST Cybersecurity Framework to the Cybersecurity Capability Maturity Model (C2M2).[9]

The Framework Implementation Guidance is designed to assist energy sector organizations to:

- Characterize their current and target cybersecurity posture
- Identify gaps in their existing cybersecurity risk management programs, using the Framework as a guide, and identify areas where current practices may exceed the Framework
- Recognize that existing sector tools, standards, and guidelines may support Framework implementation
- Effectively demonstrate and communicate their risk management approach and use of the Framework to both internal and external stakeholders.

North American Electric Reliability Corporation Critical Infrastructure Protection – FERC rulemaking on reliability standards for electricity transmission

The North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) establishes baseline reliability standards for the bulk electric system and provides implementation guidance for North America and in the US is subject to the oversight of the Federal Energy Regulatory Commission (FERC). Standards cover sabotage reporting, identification and documentation of critical cyber-assets and perimeters, training and management controls, process and methodology development, incident reporting, and recovery plans.

In July 2015, FERC issued a Notice of Proposed Rulemaking (RM 15-14-000) to revise critical infrastructure protection (CIP) Reliability Standards in order to address risks to communication networks and related bulk electric system assets and the development of standards for supply chain management security controls to protect the bulk electric system from security vulnerabilities and malware threats. The rulemaking will update seven CIP Reliability Standards proposed by NERC. The proposal would modify the scope and applicability of certain CIP standards to protect communication links and sensitive data among bulk electric system control centers, and seeks comments on controls for transient electronic devices used on the bulk electric system. FERC held a technical conference on January 28, 2016, to facilitate a structured dialog on supply chain risk management issues identified in the proposed rulemaking. Any changes to the CIP Reliability Standards are expected to become effective in 2016.

Nuclear subsector

The Nuclear Regulatory Commission (NRC) has continued developing the already comprehensive cybersecurity requirements applicable to the nuclear power industry, which is already the most highly regulated industry sector in the US from a cybersecurity perspective. In September 2015, the NRC expanded the previously voluntary cybersecurity event notification requirements for nuclear power reactor facilities with new mandates covering computer and communications systems and networks not only upon discovery of a cyberattack but also if activities indicate "intelligence gathering or pre-operational planning related to a cyberattack."[10] Generally, reporting requirements for most industry sectors are limited to reporting on actual attacks on critical infrastructure or breaches of customer personal information, depending on the sector; but requiring reporting on information regarding detected pre-operational planning of a cyberattack goes farther for the nuclear subsector.

The NRC is currently considering a petition filed by the Nuclear Energy Institute in 2014 to revise the "Milestone 8" cybersecurity rules established in 2009 that impose overly broad requirements on nuclear power plants for equipment that is not used to protect the health and safety of the public, the key goal of NRC regulations. Industry concerns with the scope of these NRC cybersecurity regulations are being echoed in other sectors with mandatory requirements that are also duplicative, overly burdensome, or otherwise unresponsive to industry concerns.

Learn more about the areas covered in this alert by contacting any of the contributors:

Sydney M. White

Jim Halpert

Senator Saxby Chambliss

Michael Hornstein

Edward J. Johnsen

Evan R. Minsberg

Dawn Stern

---

1 https://www.congress.gov/bill/114th-congress/house-bill/2029/text?q=%7B%22search%22%3A%5B%22%5C%22hr2029%5C%22%22%5D%7D&resultIndex=1.

2 Public Law No: 114-92; https://www.congress.gov/bill/114th-congress/senate-bill/1356/text?q=%7B%22search%22%3A%5B%222016+National+Defense+Authorization+Act%22%5D%7D&resultIndex=1.

3 https://www.sec.gov/about/offices/ocie/cybersecurity-examination-sweep-summary.pdf

4 https://www.sec.gov/investment/im-guidance-2015-02.pdf

5 https://www.sec.gov/ocie/announcement/ocie-2015-cybersecurity-examination-initiative.pdf

6 https://www.sec.gov/oiea/investor-alerts-bulletins/ia_databreaches.html

7 http://www.finra.org/newsroom/2015/finra-issues-report-cybersecurity-practices-cybersecurity-investor-alert

8 http://www.cftc.gov/PressRoom/PressReleases/pr7293-15;

9 http://energy.gov/sites/prod/files/2015/01/f19/Energy%20Sector%20Cybersecurity%20Framework%20Implementation%20Guidance_FINAL_01-05-15.pdf.

10 https://www.federalregister.gov/articles/2015/11/02/2015-27855/cyber-security-event-notifications.

AUTHORS

Sydney M. White
Of Counsel
Washington, DC | T: +1 202 799 4000

Jim Halpert
Partner
Washington, DC | T: +1 202 799 4000
