Statement on Cybersecurity

Chairman Jay Clayton

Sept. 20, 2017

Introduction

Data collection, storage, analysis, availability and protection (including security, validation and recovery) have become fundamental to the function and performance of our capital markets, the individuals and entities that participate in those markets, and the U.S. Securities and Exchange Commission ("Commission" or "SEC"). As a result of these and other developments, the scope and severity of risks that cyber threats present have increased dramatically, and constant vigilance is required to protect against intrusions. The Commission is focused on identifying and managing cybersecurity risks and ensuring that market participants – including issuers, intermediaries, investors and government authorities – are actively and effectively engaged in this effort and are appropriately informing investors and other market participants of these risks.

I recognize that even the most diligent cybersecurity efforts will not address all cyber risks that enterprises face. That stark reality makes adequate disclosure no less important. Malicious attacks and intrusion efforts are continuous and evolving, and in certain cases they have been successful at the most robust institutions and at the SEC itself. Cybersecurity efforts must include, in addition to assessment, prevention and mitigation, resilience and recovery.

In today's environment, cyberattacks are perpetrated by identity thieves, unscrupulous contractors and vendors, malicious employees, business competitors, prospective insider traders and market manipulators, so-called "hacktivists," terrorists, state-sponsored actors and others. Cyber intrusions can create significant risks to the operational performance of market participants and of markets as a whole. These risks can take the form of denials of service and the destruction of systems, potentially resulting in impediments to account access and transaction execution, and disruption of other important market system functionalities. The risks associated with cyber intrusions may also include loss or exposure of consumer data, theft or exposure of intellectual property, and investor losses resulting from the theft of funds or market value declines in companies subject to cyberattacks, among others. Market participants also face regulatory, reputational and litigation risks resulting from cyber incidents, as well as the potential of incurring significant remediation costs.

Ultimately, a large portion of the costs incurred in connection with these risks, including the costs of mitigation, are borne by investors, consumers, and other important constituents.

Cybersecurity risks extend beyond data storage and transmission systems. Maintaining reliability of data operations also depends on the continued functioning of other services that themselves face significant cyber risks, including, most notably, critical infrastructure such as electric power and communications grids.

In May 2017, I initiated an assessment of our internal cybersecurity risk profile and our approach to cybersecurity from a regulatory and oversight perspective. Components of this initiative build on prior agency efforts in this area and include establishing a senior-level cybersecurity working group to coordinate information sharing, risk monitoring, and incident response efforts throughout the agency. This Statement is one part of our effort to analyze, improve and communicate our work in this area to market participants and the American public more generally. In more detail below we provide an overview of our approach to cybersecurity as an organization and as a regulatory body, including:

- the types of data we collect, hold and make publicly available;
- how we manage cybersecurity risks and respond to cyber events related to our operations;
- how we incorporate cybersecurity considerations in our risk-based supervision of the entities we regulate;
- how we coordinate with other regulators to identify and mitigate cybersecurity risks; and
- how we use our oversight and enforcement authorities in the cybersecurity context, including to pursue cyber threat actors that seek to harm investors and our markets.

This Statement describes various specific cybersecurity risks that we and our regulated entities face, as well as cybersecurity events that we have experienced. These descriptions provide context, but are not exhaustive.

We also expect to provide a discussion of internal cybersecurity matters each year in our annual Agency Financial Report.

I. Collection and Use of Data by the Commission

In support of its mission, the Commission receives, stores and transmits data falling under three broad categories. These activities are critical to our tri-partite mission of investor protection, the maintenance of fair, orderly and efficient markets, and the facilitation of capital formation.

The first category of data includes public-facing data that is transmitted to and accessed through Commission systems. Since its creation in 1934, a critical part of the SEC's mission has been its oversight of the system of public reporting by issuers and other registrants, and in 1984 the Commission began collecting, and making publicly available, disclosure documents through its EDGAR system. In 2017, on a typical day, investors and other market participants access more than 50 million pages of disclosure documents through the EDGAR system, which receives and processes over 1.7 million electronic filings per year.

The second category of data the Commission receives, stores and transmits includes nonpublic information, including personally identifiable information, generally related to our supervisory and enforcement functions. This data, which relates to the operations of issuers, broker-dealers, investment advisers, investment companies, self-regulatory organizations ("SROs"), alternative trading systems ("ATSs"), clearing agencies, credit rating agencies, municipal advisors and other market participants, may be sensitive to individuals, organizations and our markets generally.

For example, staff in our Division of Trading and Markets often receive nonpublic drafts of proposed rule filings by SROs, and staff in our Division of Investment Management and Division of Corporation Finance often receive drafts of applications for exemptive relief under the federal securities laws. Staff in our Office of Compliance Inspections and Examinations ("OCIE"), among other divisions and offices, receive nonpublic data, including personally identifiable information, in connection with their ongoing oversight and examinations of broker-dealers, investment advisers, and other regulated entities. Staff in our Division of Enforcement receive nonpublic and personally identifiable information in connection with their investigations into potential violations of the federal securities laws.

In addition, at this time it is expected that the Commission will have access to significant, nonpublic, market sensitive data and personally identifiable information in connection with the implementation of the Consolidated Audit Trail ("CAT"). CAT is intended to provide SROs and the Commission access to comprehensive data that will facilitate the efficient tracking of trading activity across U.S. equity and options markets. CAT, which is being developed and operationalized by the SROs, is in the later stages of its multi-year development, and its first stage of operation is scheduled to commence in November 2017. Cybersecurity has been and will remain a key element in the development of CAT systems.

The third category of data includes nonpublic data, including personally identifiable information, related to the Commission's internal operations. This includes, for example, personnel records, records relating to internal investigations, and data relating to our risk management and internal control processes. This category also includes materials that Commission staff generate in connection with their daily roles and responsibilities, including work papers and internal memoranda.

As required by the Privacy Act of 1974 (5 U.S.C. § 552a), the Commission discloses on its website the types of personally identifiable information it receives, whether in connection with its outward-facing or internal operations. The Commission also publishes privacy impact assessments to inform the public about the information it collects and the safeguards that have been put in place to protect it.[1]

II. Management of Internal Cybersecurity Risks

As described above, the Commission receives, stores and transmits substantial amounts of data, including sensitive and nonpublic data. Like many other governmental agencies, financial market participants and other private sector entities, we are the subject of frequent attempts by unauthorized actors to disrupt access to our public-facing systems, access our data, or otherwise cause damage to our technology infrastructure, including through the use of phishing, malware and other attack vectors. For example, with respect to our EDGAR system, we face the risks of cyber threat actors attempting to compromise the credentials of authorized users, gain unauthorized access to filings data, place fraudulent filings on the system, and prevent the public from accessing our system through denial of service attacks. We also face the risks of actors attempting to access nonpublic data relating to our oversight of, or enforcement actions against, market participants, which could then be used to obtain illicit trading profits. Similarly, with respect to CAT, we expect we will face the risk of unauthorized access to the CAT's central repository and other efforts to obtain sensitive CAT data.[2] Through such access, intruders could potentially obtain, expose and profit from the trading activity and personally identifiable information of investors and other market participants.

Notwithstanding our efforts to protect our systems and manage cybersecurity risk, in certain cases cyber threat actors have managed to access or misuse our systems. In August 2017, the Commission learned that an incident previously detected in 2016 may have provided the basis for illicit gain through trading. Specifically, a software vulnerability in the test filing component of our EDGAR system, which was patched promptly after discovery, was exploited and resulted in access to nonpublic information. We believe the intrusion did not result in unauthorized access to personally identifiable information, jeopardize the operations of the Commission, or result in systemic risk. Our investigation of this matter is ongoing, however, and we are coordinating with appropriate authorities. As another example, our Division of Enforcement has investigated and filed cases against individuals who we allege placed fake SEC filings on our EDGAR system in an effort to profit from the resulting market movements.[3]

In addition, like other organizations, we are subject to the risk of unauthorized actions or disclosures by Commission personnel. For example, a 2014 internal review by the SEC's Office of Inspector General ("OIG"), an independent office within the agency, found that certain SEC laptops that may have contained nonpublic information could not be located.[4] The OIG also has found instances in which SEC personnel have transmitted nonpublic information through non-secure personal email accounts.[5] We seek to mitigate this risk by requiring all personnel to complete privacy and security training and we have other relevant risk mitigation controls in place.

Similarly, we are subject to cybersecurity risk in connection with vendors we utilize. For example, a weakness in vendor systems or software products may provide a mechanism for a cyber threat actor to access SEC systems or information through trusted paths. Recent global supply chain security incidents such as compromises of reputable software update services are illustrative of this type of occurrence.

In light of the nature of the data at risk and the cyber-related threats faced by the SEC, the Commission employs an agency-wide cybersecurity detection, protection and prevention program for the protection of agency operations and assets. This program includes cybersecurity protocols and controls, network protections, system monitoring and detection processes, vendor risk management processes, and regular cybersecurity and privacy training for employees. That said, we recognize that cybersecurity is an evolving landscape, and we are constantly learning from our own experiences as well as the experiences of others. To aid in this effort, and notwithstanding limitations on our hiring generally, we expect to hire additional expertise in this area.

Governance

It is our experience, consistent with the President's Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure, that a focus by senior management on cybersecurity is an important contributor to the effective identification and mitigation of cybersecurity risks.[6] To that end, SEC Commissioners and senior management have emphasized cybersecurity awareness and compliance. Senior management across the SEC's offices and divisions are required to coordinate with respect to cybersecurity efforts, including through risk reporting and the development and testing of agency-wide procedures and exercises for responding to both internal and external cyber threats.

Although all SEC personnel are responsible for employing practices that minimize cybersecurity risks, the SEC's Office of Information Technology has overall management responsibility for the agency's information technology program, including cybersecurity. The Chief Information Officer and Chief Information Security Officer lead cybersecurity efforts within the agency, including with respect to maintaining and monitoring adherence to the agency's Information Security Program Plan (described further below).

The SEC periodically assesses the effectiveness of its cybersecurity efforts, including through penetration testing of internal and public-facing systems, ongoing monitoring by the Department of Homeland Security, independent verification and validation, and security assessments conducted by impartial third parties.

Policies and procedures

The SEC maintains a number of internal policies and procedures related to cybersecurity, as set forth in the agency's Information Security Program and Program Plan. These documents, which are developed in accordance with standards set forth by the National Institute of Standards and Technology ("NIST"), delineate the roles and responsibilities of various agency officials, offices, committees and system owners in carrying out the SEC's information security objectives, including our training efforts.

The Commission also is in the process of implementing the NIST Framework for Improving Critical Infrastructure Cybersecurity.[7] Among other things, the NIST Framework is expected to help the agency define and achieve appropriate cybersecurity goals and outcomes, including identifying key assets, protecting against intrusions, detecting incidents, containing impacts and planning for recovery.

Independent audits and reviews

The SEC's cybersecurity program is subject to review from internal and external independent auditors. The SEC's OIG audits the agency's information technology systems, and components of these audits have included cybersecurity controls. The OIG also audits compliance with applicable federal cybersecurity requirements in accordance with the Federal Information Security Modernization Act of 2014 ("FISMA").[8]

In addition, the Government Accountability Office ("GAO"), an external audit agency, performs annual audits of the effectiveness of the Commission's internal control structure and procedures for financial reporting. In connection with these audits, the GAO has examined the effectiveness of information security controls designed to protect the confidentiality, integrity, and availability of key financial systems and information.[9] The Commission takes seriously identified deficiencies, documents the corrective actions it undertakes, and provides documentation to auditors to close out recommendations.

External reporting

The SEC submits reports on its cybersecurity performance to the Office of Management and Budget. The agency also reports privacy and cybersecurity incidents to the Department of Homeland Security's Computer Emergency Readiness Team ("US-CERT") in accordance with established protocols. Further, the SEC has established relationships with the National Cybersecurity and Communications Integration Center ("NCCIC"), the Financial and Banking Information Infrastructure Committee ("FBIIC"), and Financial Services Information Sharing and Analysis Center ("FS-ISAC") to share information regarding cybersecurity threats.

III. Incorporation of Cybersecurity Considerations in the Commission's Disclosure-Based and Supervisory Efforts

Promoting effective cybersecurity practices by market participants is critical to all three elements of the SEC's mission. As described in more detail below, the Commission incorporates cybersecurity considerations in its disclosure and supervisory programs, including in the context of the Commission's review of public company disclosures, its oversight of critical market technology infrastructure, and its oversight of other regulated entities, including broker-dealers, investment advisers and investment companies.

Promoting effective public company disclosures

With respect to U.S. public company issuers, the SEC's primary regulatory role is disclosure based. To that end, the staff of the Division of Corporation Finance has issued disclosure guidance to help public companies consider how issues related to cybersecurity should be disclosed in their public reports.[10]

The staff guidance discusses, among other things, cybersecurity considerations relevant to a company's risk factors, management's discussion and analysis of financial condition and results of operations ("MD&A"), description of business, discussion of legal proceedings, financial statements, and disclosure controls and procedures. The staff guidance is principles based and, while issued in 2011, remains relevant today. Accordingly, issuers should consider whether their publicly filed reports adequately disclose information about their risk management governance and cybersecurity risks, in light of developments in their operations and the nature of current and evolving cyber threats. The Commission also will continue to evaluate this guidance in light of the cybersecurity environment and its impacts on issuers and the capital markets generally.

Oversight of market infrastructure

The Commission's regulatory role with respect to market infrastructure such as exchanges and clearing agencies extends beyond compliance with applicable disclosure requirements and includes ongoing supervision and oversight. In furtherance of its statutory objectives, the Commission adopted Regulation Systems Compliance and Integrity ("Regulation SCI") and Form SCI in November 2014 to strengthen the technology infrastructure of the U.S. securities markets. The regulation applies to "SCI entities," a term which includes SROs (including stock and options exchanges, registered clearing agencies, FINRA and the MSRB), ATSs that exceed specified trading volume thresholds, disseminators of consolidated market data, and certain exempt clearing agencies.[11]

Regulation SCI is designed to reduce the occurrence of systems issues, improve resiliency when systems problems do occur, and enhance the Commission's ability to oversee and enforce rules governing market infrastructure. In addition to requiring SCI entities to maintain policies and procedures reasonably designed to ensure operational resiliency, the regulation requires SCI entities to take corrective action with respect to systems disruptions, compliance issues and intrusions (*e.g.*, cybersecurity breaches). SCI entities are also required to provide notification, including to the Commission, of such events. SCI entities are subject to examinations by OCIE, and OCIE's Technology Controls Program reviews Regulation SCI filings as part of CyberWatch, OCIE's internal program responsible for triaging all system events reported to the SEC under Regulation SCI.

Oversight of broker-dealers, investment advisers and other market participants

The SEC also conducts supervisory oversight of broker-dealers, investment advisers, investment companies, credit rating agencies and other market participants registered with the Commission. Many of these entities act as the primary interface between the securities markets and investors, including Main Street investors. Not only do their systems provide investors access to their securities accounts, but those systems in many cases also hold customers' personally identifiable information.

Certain SEC regulations directly implicate information security practices of regulated entities. For example, Regulation S-P requires registered broker-dealers, investment companies and investment advisers to adopt written policies and procedures governing safeguards for the protection of customer information and records.[12] Similarly, Regulation S-ID requires these firms, to the extent they maintain certain types of covered accounts, to establish programs addressing how to identify, detect and respond to potential identity theft red flags.[13] In addition, SEC staff engage with regulated firms to provide guidance on cybersecurity practices. For example, in April 2015, the SEC's Division of Investment Management issued staff guidance to highlight the importance of cybersecurity and discuss measures for funds and advisers to consider when addressing cybersecurity risks.[14]

The risk-based examinations of registered entities conducted by OCIE staff have included reviews of risk management programs and other operational components in order to evaluate compliance with Regulations S-P and S-ID, as well as with other federal securities laws and regulations. In recent years, OCIE has placed increasing emphasis on cybersecurity practices and has included cybersecurity in its examination priorities.[15] In August 2017, OCIE published a summary of observations from its second major initiative to assess cybersecurity preparedness in the securities industry.[16] The initiative focused its review on the content and implementation of firms' written cybersecurity policies and was part of a series of OCIE publications on cybersecurity.[17] Recognizing that there is no single correct approach to cybersecurity, the publication was not intended to provide a checklist of required practices, but rather to share information about practices the staff identified that may be useful to firms as they engage in cybersecurity planning.

IV. Coordination With Other Governmental Entities

Effective interagency coordination facilitates the identification, mitigation and remediation of broad and potentially systemic cybersecurity risks, and it also can sharpen the focus by regulated entities on risk management efforts. As a general matter, the Commission shares oversight responsibility for large financial institutions with other financial regulators, which in the U.S. include the Board of Governors of the Federal Reserve System, the Commodity Futures Trading Commission, the Office of the Comptroller of the Currency and the Federal Deposit Insurance Corporation, among others. Our oversight may also require coordination with other regulatory agencies. For example, consumer protection matters with respect to SEC registrants are largely overseen by other federal regulators, including the Federal Trade Commission and the Consumer Financial Protection Bureau.

The Commission coordinates on cybersecurity matters with the Department of the Treasury and other federal financial regulatory agencies within the framework of the FBIIC, an interagency working group. The FBIIC was designed to improve coordination and communication among financial regulators, enhance financial sector resiliency and promote private-public partnership. In addition to being a vehicle for federal agencies to communicate timely alerts regarding cyber threats or vulnerabilities in the financial sector, the FBIIC identifies and assesses critical infrastructure assets and holds periodic cyber incident response simulations with the FBIIC members, law enforcement and industry.

The FBIIC also engages with the private sector on regulatory harmonization and critical cybersecurity and other infrastructure issues, primarily through industry groups such as the Financial Services Sector Coordinating Council ("FSSCC").[18] FBIIC and FSSCC members coordinate exercises to identify critical issues that could impact the resiliency of the U.S. financial system and that may need to be addressed by private industry, the public sector, or both.

With respect to cyber-related issues that could pose a systemic risk to our markets or U.S. financial stability, we also coordinate with other financial regulators through the Financial Stability Oversight Council. In addition, we seek to coordinate with non-U.S. regulators both bilaterally and through international organizations such as the International Organization of Securities Commissions.

V. Enforcement of the Federal Securities Laws

Issuers and other market participants must take their periodic and current disclosure obligations regarding cybersecurity risks seriously, and failure to do so may result in an enforcement action.

In addition, the Commission has used its enforcement authority under the federal securities laws to vigorously pursue cyber threat actors who seek to harm investors and our markets. The use of innovative technology and analytical tools, many of which were developed internally, has enabled the Division of Enforcement to increasingly identify suspicious trading activity across multiple issuers, traders and geographic locations.

The Commission recently has brought several cases alleging the hacking and stealing of nonpublic information in connection with illicit trading activity. For example, in December 2016, the Commission charged three traders for allegedly participating in a scheme to hack into two prominent New York-based law firms to steal information pertaining to clients that were considering mergers or acquisitions, which the hackers then used to trade.[19] The Commission also brought charges against two defendants who allegedly hacked into newswire services to obtain non-public information about corporate earnings announcements, as well as dozens of other defendants who allegedly traded on the information.[20]

In another type of case, the Commission brought charges concerning a scheme to gain unauthorized access to online brokerage accounts of U.S. investors and make unauthorized stock trades, thereby driving up share prices and allowing those who allegedly perpetrated the scheme to generate profits in other trading accounts.[21]

In an effort to proactively and efficiently address securities fraud in connection with cyberattacks, the Division of Enforcement has developed substantial expertise in the detection and pursuit of fraudulent conduct across the increasingly technological and data-driven landscape, devotes substantial resources to this effort, and works closely with its law enforcement counterparts.

VI. Looking Forward

The Commission will continue to prioritize its efforts to promote effective cybersecurity practices within the Commission itself and with respect to the markets and market participants it oversees. This requires an ongoing, thoughtful evaluation of the data we obtain. When determining when and how to collect data, we must continue to thoughtfully evaluate our approach in light of the importance to our mission of each type of data we receive, particularly in the case of sensitive data, such as personally identifiable and nonpublic information.

There are certain types of sensitive data that we must obtain from market participants in order to fulfill our mission. When determining when and how to collect data, it is important that we regularly review whether our related data protections are appropriate in light of the sensitivity of the data and the associated risks of unauthorized access. We should also continue to evaluate whether alternatives exist that may allow us to further our mission while reducing the sensitivity of data we collect. For example, one way in which we have reduced the market sensitivity of certain data we collect has been to obtain it on a delayed basis when appropriate.

Cybersecurity is critical to investors, market participants, our markets, and the Commission itself. By promoting effective cybersecurity practices in connection with both the Commission's internal operations and its external regulatory oversight efforts, it is our objective to contribute substantively to a financial market system that recognizes and addresses cybersecurity risks and, in circumstances in which these risks materialize, exhibits strong mitigation and resiliency.

---

[1] These disclosures and assessments can be accessed at https://www.sec.gov/about/privacy/secprivacyoffice.htm.

[2] Although the CAT central repository is hosted and managed by the independent CAT plan processor, not the Commission, the Commission and SROs will have means to access that data.

[3] *See, e.g.*, Press Release 2017-107, *SEC Charges Fake Filer With Manipulating Fitbit Stock* (May 19, 2017), *available at* https://www.sec.gov/news/press-release/2017-107.

[4] SEC Office of Inspector General, Controls Over the SEC's Inventory of Laptop Computers, Rep. No. 524 (Sep. 22, 2014), *available at* https://www.sec.gov/files/524.pdf.

[5] Memorandum from Carl W. Hoecker, Inspector General, The Inspector General's Statement on the SEC's Management and Performance Challenges, October 2016, at 8 (Oct. 7, 2016), *available at* https://www.sec.gov/files/Inspector%20General%27s%20Statement%20on%20the%20SEC%27s%20Management%20and%20Performance%20Challenges.pdf.

[6] Exec. Order No. 13800, 82 Fed. Reg. 22391 (May 11, 2017).

[7] National Institute of Standards and Technology, Framework for Improving Critical Infrastructure Cybersecurity, v. 1.0 (Feb. 12, 2014), *available at* https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf.

[8] *See, e.g.,* SEC Office of the Inspector General, Audit of the SEC's Compliance With the Federal Information Security Modernization Act for Fiscal Year 2016, Rep. No. 539 (Mar. 7, 2017), *available at* https://www.sec.gov/files/Audit-of-the-SECs-Compliance-with-the-Federal-Information-Security-Modernization-Act-for-Fiscal-Year-2016.pdf. FISMA provides a comprehensive framework designed to ensure the effectiveness of security controls over information resources that support federal operations and assets, as well as a mechanism for oversight of federal information security programs. FISMA also requires federal agencies to develop, document and implement an agency-wide information security program to protect the data and information systems that support the operations and assets of the agency.

[9] *See, e.g.,* Government Accountability Office, Information Security: SEC Improved Control of Financial Systems But Needs to Take Additional Actions, Rep. No. GAO-17-469 (July 2017), *available at* https://www.gao.gov/assets/690/686192.pdf.

[10] *See* SEC Division of Corporation Finance, CF Disclosure Guidance: Topic No. 2—Cybersecurity (Oct. 31, 2011), *available at* http://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm. In addition, the SEC staff has regularly reviewed issuer disclosures to assess and comment on the information provided and its consistency with the Division's guidance.

[11] 79 Fed. Reg. 72251 (Dec. 5, 2014). Regulation SCI applies primarily to the systems of SCI entities that directly support any one of six key securities market functions – trading, clearance and settlement, order routing, market data, market regulation, and market surveillance. It is anticipated that the CAT central repository will be covered by the regulation as an SCI system.

[12] 17 C.F.R. part 248, subpart A.

[13] 17 C.F.R. part 248, subpart C.

[14] Cybersecurity Guidance, IM Guidance Update (Apr. 2015), *available at* http://www.sec.gov/investment/im-guidance-2015-02.pdf.

[15] OCIE Examination Priorities for 2017 (Jan. 12, 2017) *available at* https://www.sec.gov/about/offices/ocie/national-examination-program-priorities-2017.pdf; Examination Priorities for 2016 (Jan. 11, 2016) *available at* https://www.sec.gov/about/offices/ocie/national-examination-program-priorities-2016.pdf; Examination Priorities for 2015 (Jan. 13, 2015) *available at* https://www.sec.gov/about/offices/ocie/national-examination-program-priorities-2016.pdf.

[16] OCIE National Exam Program Risk Alert, Observations from Cybersecurity Examinations (Aug. 7, 2017), *available at* https://www.sec.gov/files/observations-from-cybersecurity-examinations.pdf.

[17] *See, e.g.,* OCIE National Exam Program Risk Alert, OCIE Launching Cybersecurity Preparedness Initiative (Apr. 15, 2014) *available at* https://www.sec.gov/ocie/announcement/Cybersecurity-Risk-Alert--Appendix---4.15.14.pdf; National Exam Program Risk Alert, Cybersecurity Examination Sweep Summary (Feb. 3, 2015) *available at* https://www.sec.gov/about/offices/ocie/cybersecurity-examination-sweep-summary.pdf; National Exam Program Risk Alert, OCIE's 2015 Cybersecurity Examination Initiative (Sept. 15, 2015) *available at* https://www.sec.gov/ocie/announcement/ocie-2015-cybersecurity-examination-initiative.pdf; National Exam Program Risk Alert, Cybersecurity: Ransomware Alert (May 17, 2017) *available at* https://www.sec.gov/files/risk-alert-cybersecurity-ransomware-alert.pdf. In particular, the initiative focused on the areas of governance and risk assessment, access rights and controls, data loss prevention, vendor management, training and incident response.

[18] The FSSCC, established in 2002 by financial sector market participants, coordinates critical infrastructure and homeland security activities within the financial services industry. Its 70 members consist of financial trade associations, financial utilities, and financial firms. *See* http://www.fsscc.org .

[19] Press Release 2016-280, *Chinese Traders Charged With Trading on Hacked Nonpublic Information Stolen From Two Law Firms* (Dec. 27, 2016), *available at* https://www.sec.gov/news/pressrelease/2016-280.html.

[20] Press Release 2015-163, *SEC Charges 32 Defendants in Scheme to Trade on Hacked News Releases* (Aug. 11, 2015), *available at* https://www.sec.gov/news/pressrelease/2015-163.html; Litigation Release No. 23471, *SEC Charges Nine Additional Defendants in Hacked News Release Scheme* (Feb. 18, 2016), *available at* https://www.sec.gov/litigation/litreleases/2016/lr23471.htm.

[21] Press Release 2016-127, *SEC Sues UK-Based Trader for Account Intrusion Scheme* (June 22, 2016), *available at* https://www.sec.gov/news/pressrelease/2016-127.html.