Morgan Lewis

white paper

SEC Adopts Regulation SCI

December 2014

On November 19, 2014, the U.S. Securities and Exchange Commission (SEC) unanimously adopted Regulation Systems Compliance and Integrity (Regulation SCI) under the Securities Exchange Act of 1934 (Exchange Act).[1] Regulation SCI applies to an "SCI entity," which includes certain self-regulatory organizations (SROs) (including registered clearing agencies), certain alternative trading systems (ATSs), plan processors, and exempt clearing agencies subject to the SEC's Automation Review Policy statements (ARP). SCI entities are the market participants that the SEC considers the most essential to the U.S. securities markets' efficient functioning. The SEC is addressing five key aspects of "SCI systems"[2] through Regulation SCI: capacity, integrity, resiliency, availability, and security.

An SCI entity must do the following:

- Develop policies and procedures reasonably designed to ensure that its SCI systems have levels of capacity, integrity, resiliency, availability, and security adequate to maintain the SCI entity's operational capability and promote the maintenance of fair and orderly markets.
- Develop policies and procedures reasonably designed to ensure that its SCI systems operate in a manner that complies with the Exchange Act, the rules and regulations thereunder, and the SCI entity's rules and governing documents.
- Take corrective action and notify the SEC and affected members or participants when an "SCI event" has occurred (i.e., a systems disruption, compliance issue, or intrusion).
- Submit a quarterly report to the SEC describing completed, ongoing, and planned material systems changes.
- Conduct an annual review of its compliance with Regulation SCI, submit a report of the review to senior management within 30 days after its completion, and submit the report, as well as any response by senior management, to the SEC and the SCI entity's board of directors (or its equivalent) within 60 days of submission to the entity's senior management.

Regulation SCI consolidates and supersedes ARP, Rule 301(b)(6) of Regulation ATS, and prior SEC staff guidance for SCI entities.

Regulation SCI takes effect on February 3, 2015. The compliance date for Regulation SCI is November 3, 2015.[3]

Background

For more than two decades, the SEC has overseen the U.S. securities markets' technology primarily through a voluntary set of principles articulated in the SEC's ARP statements, which are applied through the SEC's ARP inspection program.[4] In light of the evolution and greater complexity and sophistication of the securities markets, several recent systems malfunctions and outages at exchanges, security information processors (SIPs), and other trading venues, and in light of concerns over "single points of failure" in the securities markets, the SEC proposed Regulation SCI in March 2013 to update, formalize, and expand on the ARP inspection program.

1. Regulation Systems Compliance and Integrity, Exchange Act Release No. 73639 (Nov. 19, 2014), 79 Fed. Reg. 72252 (Dec. 5, 2014) (to be codified at 17 C.F.R. pts. 240, 242, and 249) (Adopting Release). The Adopting Release is available at http://www.gpo.gov/fdsys/pkg/FR-2014-12-05/pdf/2014-27767.pdf#page=2. The SEC also made conforming amendments to Regulation ATS (17 C.F.R. § 232.301). Regulation SCI is numbered Rules 1000 through 1007 under the Exchange Act.

2. Regulation SCI defines "SCI systems" to mean "all computer, network, electronic, technical, automated, or similar systems of, or operated by or on behalf of, an SCI entity that, with respect to securities, directly support trading, clearance and settlement, order routing, market data, market regulation, or market surveillance."

3. An ATS that newly meets the thresholds in the definition of "SCI ATS" will have six months from the time it first meets the applicable thresholds to comply with the requirements of Regulation SCI. The compliance date for an SCI entity to coordinate testing of its business continuity and disaster recovery plans on an industry- or sector-wide basis will be November 3, 2016.

4. Adopting Release, 79 Fed. Reg. at 72253.

SEC Chair Mary Jo White emphasized the importance of Regulation SCI to the SEC's ongoing efforts to "strengthen the technology infrastructure of the U.S. securities markets, improve its resilience, and to enhance the SEC's ability to oversee it."[5]

In proposing and adopting Regulation SCI, the SEC cited numerous events of the type that Regulation SCI is designed to address. These include the following:

- The May 2010 "Flash Crash"
- The February 2011 announcement by the NASDAQ Stock Market ("NASDAQ") that hackers penetrated certain of its computer networks that were not related to trading
- The March 2012 announcement by BATS that a "software bug" forced it to shut down its own IPO
- The May 2012 issues with NASDAQ's trading systems that delayed trading in Facebook, Inc.'s IPO
- The August 2012 technology issue at Knight Capital Group, Inc. related to its installation of trading software
- Hurricane Sandy in October 2012 and its impact on the markets
- The August 2013 NASDAQ trading halt of all NASDAQ-listed securities for more than three hours after the NASDAQ UTP SIP was unable to process quotes from exchanges for dissemination to the public[6]

SCI Entities

Regulation SCI applies to an "SCI entity," which includes national securities exchanges,[7] certain larger-volume ATSs, registered clearing agencies, exempt clearing agencies subject to ARP,[8] the Financial Industry Regulatory Authority (FINRA), the Municipal Securities Rulemaking Board (MSRB), and plan processors.[9] ATSs subject to Regulation SCI include those that had, during at least four of the preceding six calendar months, one of the following:

- 5% or more in any single national market security (NMS) stock[10] and 0.25% or more in all NMS stocks of the average daily volume reported by applicable transaction reporting plans
- 1% or more in all NMS stocks of the average daily volume reported by applicable transaction reporting plans
- 5% or more in all non-NMS stocks for which transactions are reported to an SRO of the average daily dollar volume as calculated by the SRO to which the transactions are reported

5. Chair Mary Jo White, Statement at Open Meeting on Regulation SCI (Nov. 19, 2014).

6. Adopting Release, 79 Fed. Reg. at 72255 n.32.

7. Regulation SCI would not apply to an exchange that is notice registered with the SEC pursuant to Section 6 of the Exchange Act (15 U.S.C. § 78f(g)) or a limited purpose national securities association registered with the SEC pursuant to Section 15A of the Exchange Act (15 U.S.C. § 78o-3(k)).

8. Currently, this would cover only Omgeo Matching Services – US, LLC.

9. The term "plan processor" is defined in reference to Rule 600(b)(55) of Regulation NMS to mean "any self-regulatory organization or securities information processor acting as an exclusive processor in connection with the development, implementation and/or operation of any facility contemplated by an effective national market system plan." This includes entities that process and disseminate quotation and transaction data for the Consolidated Tape Association System; Consolidated Quotation System; Joint Self-Regulatory Organization Plan Governing the Collection, Consolidation, and Dissemination of Quotation and Transaction Information for Nasdaq-Listed Securities Traded on Exchanges on an Unlisted Trading Privileges Basis; and Options Price Reporting Authority.

10. An NMS stock is "any NMS security other than an option." 17 C.F.R. § 242.600(b)(47). An NMS security is "any security or class of securities for which transaction reports are collected, processed, and made available pursuant to an effective transaction reporting plan, or an effective national market system plan for reporting transactions in listed options." 17 C.F.R. § 242.600(b)(46).

Required Policies and Procedures

An SCI entity will need to establish policies and procedures related to its SCI systems' operational capability and systems compliance.

Capacity, Integrity, Resiliency, Availability, and Security

Any SCI entity must establish, maintain, and enforce written policies and procedures reasonably designed to ensure that its SCI systems and, for purposes of security standards, its indirect SCI systems, have levels of capacity, integrity, resiliency, availability, and security adequate to maintain the SCI entity's operational capability and promote the maintenance of fair and orderly markets. An "indirect SCI system" includes those systems of an SCI entity, or that are operated by or on its behalf, that would reasonably be likely to pose a security threat to an SCI system if breached. The policies and procedures must include, at a minimum, the following:

- Reasonable current and future technological infrastructure capacity-planning estimates
- Periodic stress tests of the systems to determine their ability to process transactions in an accurate, timely, and efficient manner
- A program to review and keep current systems development and testing methodology
- Regular reviews and testing of the systems to identify vulnerabilities pertaining to internal and external threats, physical hazards, and natural or manmade disasters
- Business continuity and disaster recovery plans that include maintaining backup and recovery capabilities that are sufficiently resilient and geographically diverse and that are reasonably designed to achieve resumption of trading on the next business day and resumption of critical SCI systems[11] within two hours following a wide-scale disruption[12]
- Standards that result in the systems being designed, developed, tested, maintained, operated, and surveilled in a manner that facilitates the successful collection, processing, and dissemination of market data
- Ongoing monitoring to identify potential disruptions, compliance issues, or intrusions

An SCI entity must periodically review its policies and procedures and take prompt action to remedy any deficiencies. The required policies and procedures will be deemed to be reasonably designed if they are consistent with current "SCI industry standards."[13] The SEC staff issued accompanying guidance (SCI Staff Guidance) that identifies examples of publications that an SCI entity can look to in developing reasonable policies and procedures.[14] Chair White indicated that the SEC's goal is to eventually set uniformly high technical

11. "Critical SCI systems" are SCI systems that support functionality relating to (1) clearance and settlement systems of clearing agencies; (2) opening, reopening, and closing on the primary listing market; (3) trading halts; (4) initial public offerings; (5) the provision of consolidated market data; or (6) exclusively listed securities. The definition also includes systems that "[p]rovide functionality to the securities markets for which the availability of alternatives is significantly limited or nonexistent and without which there would be a material impact on fair and orderly markets," a category the SEC says currently is not applicable to existing SCI systems, but is available to capture future technological advances.

12. An SCI entity must establish standards to designate members or participants that the entity reasonably determines are, taken as a whole, the minimum necessary for the maintenance of fair and orderly markets in the event the plans are activated; designate and require those members or participants to participate in scheduled functional and performance testing of the operation of the plans no less than once every 12 months; and coordinate the testing on an industry- or sectorwide basis with other SCI entities.

13. SCI industry standards are those information technology practices that are widely available to information technology professionals in the financial sector and issued by an authoritative body that is a U.S. governmental entity or agency, association of U.S. governmental entities or agencies, or widely recognized organization.

14. Staff Guidance on Current SCI Industry Standards (Nov. 19, 2014), *available at* http://www.sec.gov/rules/final/2014/staff-guidance-current-sci-industry-standards.pdf.

standards. However, without a single set of existing, widely used industry or government standards, the SEC has issued the SCI Staff Guidance that "could potentially lay the foundation for the development of a uniform set of SCI standards."[15]

Systems Compliance

An SCI entity must also establish, maintain, and enforce written policies and procedures reasonably designed to ensure that its SCI systems operate in a manner that complies with the Exchange Act, the rules and regulations thereunder, and the SCI entity's rules and governing documents, as applicable. An SCI entity is required to periodically review its policies and procedures and take prompt action to remedy any deficiencies. Those policies and procedures must include, at a minimum, the following:

- Testing of all SCI systems and any changes to SCI systems prior to implementation
- A system of internal controls over changes to SCI systems
- A plan for assessments of the functionality of SCI systems designed to detect systems compliance issues
- A plan of coordination and communication between regulatory and other personnel of the SCI entity

Obligations Related to SCI Events

An SCI entity, upon any responsible SCI personnel[16] having a reasonable basis to conclude that an SCI event has occurred, must begin to take appropriate corrective action, including, at a minimum, mitigating potential harm to investors or market integrity and devoting adequate resources to remedy the systems disruption, compliance issue, or intrusion as soon as reasonably practicable. In addition, except for SCI events that have no or a de minimis impact on the SCI entity's operations or on market participants,[17] the SCI entity must do the following:

- Immediately notify the SEC of the SCI event
- Submit a written notification to the SEC within 24 hours that describes the SCI event and provides a current assessment of the types and number of market participants potentially affected; the potential impact on the market; the steps the SCI entity is taking; the time the event was, or the timeframe in which the event will be resolved; and any other pertinent information
- Until the SCI event is resolved, provide regular updates to the SEC to correct any materially incorrect information previously provided or when new information is discovered
- Submit a final written notification to the SEC about the SCI event that includes a description of the SCI event, as discussed above; a copy of any information disseminated to members or participants that any responsible SCI personnel has reasonably estimated may have been affected by the SCI event; and an analysis of parties that may have experienced a monetary or other loss because of the SCI event, the number of parties, and an estimate of the aggregate amount of the loss[18]

15. Chair Mary Jo White, Statement at Open Meeting on Regulation SCI (Nov. 19, 2014).

16. Regulation SCI defines "responsible SCI personnel" to include senior manager(s) of the SCI entity having responsibility for a particular SCI system or indirect SCI system, and their designee(s). An SCI entity is required to establish, maintain, and enforce reasonably designed written policies and procedures that include (1) the criteria for identifying responsible SCI personnel; (2) the designation and documentation of responsible SCI personnel; and (3) escalation procedures to quickly inform responsible SCI personnel of potential SCI events.

17. For SCI events that have no or a de minimis impact on the SCI entity's operations or on market participants, the SCI entity must keep records of the events and, within 30 calendar days after the end of each calendar quarter, submit a report to the SEC describing the systems disruptions and intrusions, including the SCI systems and, for intrusions, the indirect SCI systems, affected.

18. If an SCI entity resolves and closes an investigation of an SCI event within 30 days of the occurrence of the SCI event, the final written notification must be submitted within five business days of resolving and closing the investigation. For SCI events and investigations lasting more than 30 calendar days, an SCI entity must submit an interim written notification within 30 calendar days of the occurrence of the SCI event and a final written notification within five business days of resolving the SCI event and closing the entity's investigation of the event.

- Disseminate information regarding the SCI event to affected members or participants, except that information regarding major SCI events must be disseminated to all members or participants

The notification, review, description, analysis, or report that an SCI entity is required to submit to the SEC generally must be filed electronically on the new Form SCI.

Systems Changes and SCI Review

An SCI entity must submit to the SEC, within 30 calendar days after the end of each calendar quarter, a report describing any completed, ongoing, and planned material changes to its SCI systems and the security of indirect SCI systems during the prior, current, and subsequent calendar quarters, including the dates or expected dates of commencement or completion, and must also promptly submit a supplemental report notifying the SEC of any material errors in or omissions from a previously submitted report.

In addition, an SCI entity is required to conduct the following:

- Annual reviews of its compliance with Regulation SCI
- Penetration test reviews of the network, firewalls, and production systems no less than once every three years
- Assessments of SCI systems directly supporting market regulation or market surveillance at a frequency based on the risk assessment conducted as part of the SCI review, but no less than once every three years

An SCI entity must submit a report of the review to senior management no more than 30 calendar days after the completion of an SCI review. Within 60 calendar days after submitting the report to senior management, the SCI entity must submit the report, as well as any response by senior management, to the SEC and to the SCI entity's board of directors (or its equivalent).

Business Continuity and Disaster Recovery

Each SCI entity must incorporate into its business continuity and disaster recovery plans functional and performance testing that includes the participation of a minimum number of its members or participants that the SCI entity has determined are "necessary for the maintenance of fair and orderly markets in the event of the activation of such plans." The SEC acknowledged in the Adopting Release that SCI entities may need to adopt new rules or amend existing participation or member agreements to compel participation by these members or participants in this testing.

Observations/Implications

Potential Liability of SCI Entities

Regulation SCI can create liability for an SCI entity that does not establish, maintain, and enforce required written policies and procedures. Regulation SCI does not contain a safe harbor from liability for an SCI entity, as was

originally proposed.[19] In adopting Regulation SCI, the SEC instead provided a non-exhaustive list of minimum elements that an SCI entity must include in its systems compliance policies and procedures. As stated in the Adopting Release, the minimum elements are intended to accommodate the differences in the nature, size, technology, business model, and other aspects of each SCI entity's business, and "each SCI entity will need to exercise judgment in developing and maintaining specific policies and procedures that are reasonably designed to achieve systems compliance."[20]

An SCI entity should take care to establish, maintain, and enforce policies and procedures reasonably designed to ensure systems compliance, including compliance with the SCI entity's own rules and governing documents. Even absent a technology error or problem, the SEC may allege that an SCI entity violated Regulation SCI based on deficient policies and procedures or related processes or controls. An SCI entity should strive to ensure that its legal, business, technology, compliance, and other relevant departments are communicating with one another and are involved in systems developments and changes before implementation. In addition, an SCI entity should clearly identify the information concerning systems issues that should be disclosed and escalated to senior management. Furthermore, an SCI entity should periodically review its policies and procedures and take prompt action to remedy any deficiencies once they are discovered.

In adopting Regulation SCI, the SEC noted that potential liability under Regulation SCI is separate and distinct from any liability that may arise from an underlying SCI event under other laws and rules. The SEC noted in the Adopting Release that SROs are not immune from SEC sanctions and that the SEC is authorized to impose sanctions on an SRO that fails to comply with the Exchange Act, the rules and regulations thereunder, or its own rules.[21] The SEC will now have additional authority under Regulation SCI to impose sanctions on an exchange that has deficient policies and procedures, beyond the existing authority provided in Section 19(g)(1) of the Exchange Act.[22]

In addition, an SCI entity should be aware that Regulation SCI applies not only to the SCI entity's own systems, but also to systems operated on behalf of the SCI entity. In adopting Regulation SCI, the SEC noted that an SCI entity that outsources the operation of systems to third parties should be responsible for managing its relationships with those third parties, including through due diligence, contract terms, performance monitoring, or other methods, and that an SCI entity should reevaluate its relationship with a third-party vendor that is unwilling to provide information that the SCI entity needs to fulfill its obligations under Regulation SCI.[23]

Potential Liability of Responsible SCI Personnel

Regulation SCI includes a safe harbor from liability for personnel of an SCI entity for violations of the systems compliance policies and procedures requirement if the person (1) has reasonably discharged the duties and obligations incumbent upon the person by the SCI entity's policies and procedures and (2) did not have reasonable cause to believe that the policies and procedures relating to an SCI system for which the person was responsible or had supervisory responsibility were not established, maintained, or enforced as required in any material respect.[24] The SEC stated its belief that, in the context of the safe harbor, personnel with responsibility for an SCI system should, upon becoming aware of potential material non-compliance of the policies and procedures pertaining to that SCI system, review and address, or direct other personnel to review and address, the potential material non-compliance.[25] In addition, the SEC stated that in order to reasonably discharge their

19. Regulation Systems Compliance and Integrity, Securities Exchange Act Release No. 69077 (Mar. 8, 2013), 78 Fed. Reg. 18084 (Mar. 25, 2013) (proposing Regulation SCI).

20. Adopting Release, 79 Fed. Reg. at 72306.

21. *Id.* at 72308.

22. Section 19(g)(1) of the Exchange Act provides, in part, that every SRO must comply with the provisions of the Exchange Act, the rules and regulations thereunder, and the SRO's own rules.

23. Adopting Release, 79 Fed. Reg. at 72276.

24. Rule 1001(b)(4), 17 C.F.R. § 242.1001(b)(4).

25. Adopting Release, 79 Fed. Reg. at 72313.

duties and obligations, personnel must be able to understand their duties and obligations, which could be accomplished through training provided by the SCI entity.[26]

An SCI entity and its senior management may also face liability in connection with reports of SCI systems changes and reviews, and any responses by senior management, that are required to be filed using new Form SCI. Section 32(a) of the Exchange Act makes it unlawful for any person to willfully or knowingly make, or cause to be made, any false or misleading statement with respect to any material fact in any application, report, or document required to be filed with the SEC. For purposes of Regulation SCI, senior management includes an SCI entity's chief executive office, chief technology officer, chief information officer, general counsel, and chief compliance officer, or the equivalent of such employees or officers. An SCI entity and its senior management should consider all material information when completing Form SCI and not make any false or misleading statements about the systems changes and reviews or management responses.

Future Changes in Scope of SCI Entities

The SEC emphasized that Regulation SCI is an improvement on the structure that has existed in the past, but also took a view toward areas for future enhancement. The SEC indicated that it may consider extending the types of requirements in Regulation SCI to additional market participants in the future, such as non-ATS broker-dealers, transfer agents, investment advisers, investment companies, security-based swap dealers, and other key market participants. In this regard, Chair White indicated that she has "directed the staff to prepare recommendations for the SEC's consideration as to whether an SCI-like framework should be developed for other key market participants, such as broker-dealers and transfer agents."[27]

The SEC does not, however, seem inclined to extend Regulation SCI to fixed-income ATSs at this time. In adopting Regulation SCI, the SEC determined not to apply the requirements to fixed-income ATSs; instead, those entities will continue to be subject to the existing requirements of Rule 301(b)(6) of Regulation ATS if they meet the 20% threshold for corporate debt or municipal securities provided by that rule. The SEC took the view that subjecting fixed-income ATSs to the requirements of Regulation SCI "could have the unintended effect of discouraging automation in these markets and discouraging the entry of new fixed-income ATSs into the market, which could impede the evolving transparency and efficiency of these markets and negatively impact liquidity in these markets."[28]

Focus on Cybersecurity

The SEC's focus on the importance of cybersecurity to the U.S. securities markets has increased in recent months. In March 2014, the SEC conducted a cybersecurity roundtable that addressed the cybersecurity landscape and issues for which market participants must account.[29] The SEC's Office of Compliance Inspections and Examinations (OCIE) subsequently issued an April 2015 Risk Alert on cybersecurity and also provided a sample list of requests for information that OCIE may use in conducting examinations of registered entities regarding cybersecurity matters.[30] Many of the questions track information outlined in the National Institute of Standards and Technology's (NIST's) *Framework for Improving Critical Infrastructure Cybersecurity*.[31]

The Adopting Release noted that, "[a]lthough the views of [roundtable] panelists varied, many emphasized the

26. *Id.*

27. Chair Mary Jo White, Statement at Open Meeting on Regulation SCI (Nov. 19, 2014).

28. Adopting Release, 79 Fed. Reg. at 72270.

29. *See* Securities Exchange Act Release No. 71742 (Mar. 19, 2014), 79 FR 16071 (Mar. 24, 2014) (File No. 4-673). A webcast of the Cybersecurity Roundtable is available at http://www.sec.gov/news/otherwebcasts/2014/cybersecurity-roundtable-032614.shtml.

30. Office of Compliance Inspections and Examinations, Risk Alert: OCIE Cybersecurity Initiative (Apr. 15, 2014), *available at* http://www.sec.gov/ocie/announcement/Cybersecurity+Risk+Alert++%2526+Appendix+-+4.15.14.pdf.

31. National Institute of Standards and Technology, "Framework for Improving Critical Infrastructure Cybersecurity" (Feb. 12, 2014), *available at* http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf; *see also* Gregory T. Parks, Ezra D. Church, "New Cybersecurity Framework Revealed," Morgan Lewis LawFlash (Apr. 18, 2014), *available at* http://www.morganlewis.com/pubs/ACPP_LF_NewCybersecurityFrameworkRevealed_18april14.pdf.

significant risk that cybersecurity attacks pose to the financial markets and market infrastructure today and the need to effectively manage that risk through measures such as testing, risk assessments, adoption of consistent best practices and standards, and information sharing."[32] In adopting Regulation SCI, the SEC encouraged SCI entities to cooperate with one another by sharing information.[33] SEC Commissioner Michael Piwowar emphasized the importance for vigilance on the part of market participants in identifying and protecting against cybersecurity threats, while also noting the high risk of complacency in this area.[34] Likewise, SEC Commissioner Luis Aguilar highlighted his concern about cybercriminals who have targeted the U.S. capital markets.[35] The SCI Staff Guidance that accompanies Regulation SCI also referenced the NIST *Framework for Improving Critical Infrastructure Cybersecurity* release in February.

The Adopting Release, together with commentary from the SEC commissioners, highlights the SEC's focus on cybersecurity within the U.S. financial markets and the increasing emphasis that market participants must place on resources in this area. For example, the SEC encourages information sharing among market participants in the cybersecurity context. However, this activity could implicate several other considerations surrounding sensitive information, including with respect to the confidentiality of the shared information (both in terms of the participant's own information as well as the privacy of information of the SCI entity's members or participants) as well as related to attorney-client privilege and protection under the Freedom of Information Act.[36] As standards and protocol are discussed and developed, U.S. securities markets participants, including SCI entities, would be wise to familiarize themselves with the related limitations and risks and participate in these ongoing discussions.[37]

Contacts

If you have any questions or would like more information on the issues discussed in this Memorandum, please contact any of the following Morgan Lewis lawyers:

Investment Management

Washington, D.C.

John V. Ayanian	+1.202.739.5946	jayanian@morganlewis.com
Brian J. Baltz	+1.202.739.5665	bbaltz@morganlewis.com
Margaret R. Blake	+1.202.373.6296	margaret.blake@morganlewis.com
Mary M. Dunbar	+1.202.739.5358	mdunbar@morganlewis.com
Mark D. Fitterman	+1.202.739.5019	mfitterman@morganlewis.com
Amy Natterson Kroll	+1.202.373.6118	amy.kroll@morganlewis.com
Nicholas J. Losurdo	+1.202.739.5023	nlosurdo@morganlewis.com
Ignacio A. Sandoval	+1.202.739.5201	isandoval@morganlewis.com
Steven W. Stone	+1.202.739.5453	sstone@morganlewis.com

Boston

David C. Boch	+1.617.951.8485	david.boch@morganlewis.com
Michael R. Weissmann	+1.617.951.8705	michael.weissmann@morganlewis.com

32. Adopting Release, 79 Fed. Reg. at 72256.

33. Regarding information sharing, NIST recently published a related "Guide to Cyber Threat Information Sharing," which advises organizations on enhancing their information-sharing practices. *See* National Institute of Standards and Technology, "Guide to Cyber Threat Information Sharing (Special Publication 800-150)" (October 2014), *available at* http://csrc.nist.gov/publications/drafts/800-150/sp800_150_draft.pdf; *see also* Mark L. Krotoski, Brock D. Dahl, "NIST Draft Guide Advances the Debate on Cybersecurity Issues," Morgan Lewis LawFlash (Nov. 19, 2014), *available at* http://www.morganlewis.com/pubs/Privacy_LF_NISTDraftAdvancesDebateonCybersecurityIssues_19nov14.pdf.

34. Commissioner Michael S. Piwowar, Statement at Open Meeting on Regulation SCI (Nov. 19, 2014).

35. Commissioner Luis A. Aguilar, Statement at Open Meeting on Regulation SCI (Nov. 19, 2014).

36. 5 U.S.C. § 552.

37. For example, the NIST "Guide to Cyber Threat Information Sharing" discusses several categories of restrictions on use of shared information, including establishing non-disclosure agreements or memoranda of understanding among the parties or utilization of a marking convention like the US-CERT Traffic Light Protocol (TLP) (https://www.us-cert.gov/tlp). *See* NIST *Guide to Cyber Threat Information Sharing*, *supra* note 33, at 40-41.

Morgan Lewis

Privacy & Cybersecurity

Chicago		
Merri Jo Gillette	+1.312.324.1134	mgillette@morganlewis.com
Washington, D.C.		
Brock D. Dahl	+1.202.739.5029	bdahl@morganlewis.com
Mark L. Krotoski	+1.202.739.5024 +1.650.843.7212	mkrotoski@morganlewis.com
Philadelphia		
Gregory T. Parks	+1.215.963.5170	gparks@morganlewis.com
San Francisco		
Susan D. Resley	+1.415.442.1351	sresley@morganlewis.com

About Morgan, Lewis & Bockius LLP

Founded in 1873, Morgan Lewis offers 725 partners and nearly 2,000 lawyers—as well as scores of patent agents, benefits advisers, regulatory scientists, and other specialists—in 28 offices across North America, Europe, Asia, and the Middle East. The firm provides comprehensive litigation, corporate, transactional, regulatory, intellectual property, and labor and employment legal services to clients of all sizes—from globally established industry leaders to just-conceived start-ups. For more information about Morgan Lewis or its practices, please visit us online at www.morganlewis.com.