A Primer on Cybersecurity Regulations

MEET the THREAT

March 2017

A joint publication of:

NGA NATIONAL GOVERNORS ASSOCIATION

DAY PITNEY LLP

As chair of the National Governors Association, I am excited to announce that I have selected cybersecurity as the focus of my chair's initiative. *Meet the Threat: States Confront the Cyber Challenge* places states at the center of finding solutions to the growing cyber threats facing our country.

A primary goal of the initiative is for states to develop strategies for strengthening cybersecurity practices as they relate to state IT networks, health care, education, safety, energy, transportation, critical infrastructure, economic development and workforce. We will be hosting several regional summits and bringing together policy leaders from every state, as well as private sector experts and federal partners, to highlight innovative practices and identify ways in which state-driven solutions can be replicated nationwide. This website will serve as a library of resources for states. As the year progresses, we will add to the library and encourage state policymakers to use it.

In addition, participating state teams will develop strategies for improving cybersecurity that they will present to their governors for consideration. The initiative will conclude in Virginia with the National Summit on State Cybersecurity, which will bring together representatives from each state, commonwealth and territory to share best practices and lessons learned.

These are ambitious goals. With your engagement, however, I know we can succeed. The initiative has the potential to shape the nation's response to the growing cyber threats we face by underscoring the critical role state leaders play in securing the cyber environment.

- Virginia Governor Terry McAuliffe

A Primer on Cybersecurity Regulations

Cybersecurity risk pervades all sectors of the U.S. economy. For years, the federal government has required private companies in a handful of industries to institute security measures intended to reduce this risk. Until recently, no state had issued similar cybersecurity regulations applicable to private entities. That changed in 2015, when **Rhode Island** enacted a law requiring *any* person or company that manages personal information about a state citizen to implement "a risk-based information security program."[1] Both **Illinois**[2] and **Kansas**[3] followed suit with similar legislation in 2016. Regulators in **New York** have issued more detailed standards for the financial sector.[4]

State officials eyeing cybersecurity regulation should first review the relevant federal framework. Full awareness of national mandates will help to avoid duplicative or conflicting rules at the state and local levels. Federal analogues also provide a useful starting point for engaging private sector partners whose input is critical to fashioning effective incentives for reducing cyber risk. To assist in this effort, this memo summarizes the current landscape of federal cybersecurity regulations covering private industry.[*]

CRITICAL INFRASTRUCTURE

Nuclear Power. The Nuclear Regulatory Commission (NRC) has established extensive cybersecurity controls for civilian nuclear power plants. Licensed operators must "provide high assurance" that "critical digital assets" are protected from cyber attacks.[5] NRC guidance requires a long list of specific measures, including defense-in-depth strategies, vulnerability mitigation plans, personnel training, and the integration of cybersecurity programs with existing physical security protocols.[6]

Bulk Power System. The Federal Energy Regulatory Commission (FERC) oversees the reliable operation of the nation's Bulk Power System (BPS), i.e., the major components of the interstate electrical grid. With permission from FERC, the non-profit North American Electric Reliability Corporation (NERC) develops and enforces mandatory Reliability Standards for approximately 1,400 operators of power plants and long-distance transmission lines.[7] FERC can disapprove of Reliability Standards proposed by NERC, as well as order NERC to create or modify a standard to address a specific matter.[8] Current Reliability Standards include a set of comprehensive cybersecurity controls known as the Critical Infrastructure Protection (CIP) standards,[9] which are regularly updated to account for changing threats.[10] BPS operators who fail to implement CIP cybersecurity measures are subject to fines and restrictions on business activities, functions, and operations.[11] Importantly,

---

NERC cybersecurity rules do not apply to a large portion of electric infrastructure, as the BPS specifically excludes facilities used in the local distribution of electric energy.[12]

Water Utilities. Federal law requires any "community water system" serving more than 3,300 people to assess the risk of intentional service disruptions. The assessment must include a review of operational vulnerabilities arising from "electronic, computer or other automated systems," to be incorporated into an emergency response plan.[13] EPA enforces these obligations through orders, civil penalties, and court injunctions.[14]

Chemical Facilities. In 2007, DHS issued the Chemical Facility Anti-Terrorism Standards (CFATS) to control security at high-risk chemical facilities across the country.[15] Owners and operators of potentially dangerous chemical facilities must "deter cyber sabotage"[16] of critical systems and any connected business networks.[17] Facilities that do not comply with the standards and refuse to follow corrective orders face possible fines or closure.[18]

Special Note: Pipelines. The Transportation Security Administration has primary authority to issue cybersecurity standards for the nation's pipeline infrastructure.[19] The agency has yet to issue regulations in this area.[20]

HEALTH INFORMATION

The U.S. Department of Health and Human Services (HHS) regulates how health providers—including doctors, hospitals, pharmacies, health plans, and health insurers—must protect electronic health records. The HHS standards are embodied in two complementary regulations—the HIPAA Privacy Rule and Security Rule. Under the Security Rule, covered health providers shall: (1) ensure the confidentiality, integrity, and availability of health information that could be used to identify an individual; (2) defend that information against "reasonably anticipated threats" and "impermissible uses or disclosures;" and (3) ensure compliance by employees.[21]

The Security Rule requires physical, administrative, and technical controls. Physical and administrative safeguards are generally mandatory. They include risk assessments, incident response planning, training, system activity reviews, and policies for punishing violators.[22] There are fewer mandatory technical controls. They include user tracking and ensuring emergency access to health records.[23] Providers have flexibility to implement any additional technical solutions, such as encryption and automatic logoff, based on what is "reasonable and appropriate" under the circumstances.[24] In determining whether specific measures are indeed reasonable and appropriate, HHS considers the provider's size, complexity, and technical capabilities, as well as potential risks to the health information at issue.[25] HHS has imposed multi-million dollar fines for violations of the Security Rule.[26]

MEDICAL DEVICES

The Food and Drug Administration (FDA) has not issued cybersecurity-specific regulations. FDA oversight of the sale and maintenance of medical devices and medical software has, however, included cybersecurity requirements. FDA supervision of basic medical equipment, such as thermometers, is not strict.[27] By contrast, more advanced devices (e.g., MRI scanners) must pass an intensive safety review before the FDA will certify them for sale.[28] Among the many safety factors the agency considers is the presence of security controls that align to five core cybersecurity functions identified by the National Institute for Standards and Technology (NIST).[29] FDA's nonbinding recommendations provide incentives for manufacturers to submit documentation demonstrating consideration and adherence to the NIST Framework.[30]

CONSUMER PROTECTION

Congress has authorized the Federal Trade Commission (FTC) to prevent persons and companies from engaging in "unfair or deceptive acts or practices."[31] Since 2005, the FTC has used this general language to fine companies who practice "unreasonably" poor cybersecurity, under the theory that exposing customer data to compromise is either fundamentally unfair or inconsistent with user privacy agreements.[32] Federal courts have validated this position.[33] A company does not need to suffer a security breach to attract FTC scrutiny and subsequent fines. The FTC has recently targeted companies for deficient cybersecurity practices even without evidence of a security incident.[34]

Several FTC guides suggest baseline security practices it believes will assist private business in protecting sensitive data.[35] These include, but are not limited to: disposing of unnecessary data; restricting employee access to sensitive data; limiting administrative privileges; mandating strong passwords and guarding against brute force attacks; testing for known vulnerabilities; using end-to-end encryption; and segmenting networks.

TELECOMMUNICATIONS

The Federal Communications Commission (FCC) oversees how telecommunications carriers "protect the confidentiality of proprietary information" belonging to customers and other companies.[36] The FCC has relied on this language to investigate and enforce data security obligations.[37] The agency has been aggressive in seeking civil fines against telephone companies that suffer data breaches after failing to implement what the FCC deems to be reasonable security precautions.[38]

In November 2016, the FCC adopted formal rules requiring internet service providers (ISPs)—which were previously exempt from FCC regulation in this area—to adopt "reasonable data security."[39] On March 1, 2017, the FCC halted these rules before they could take effect.[40]

FINANCE

Federal regulation of the financial sector is highly complex, involving a variety of federal agencies with overlapping jurisdictions.[41] This section provides only general brief overview of the rules governing cybersecurity for such financial institutions. These rules generally fall into one of four categories.

Safety and Soundness. Several agencies enforce joint standards to ensure the "safety and soundness" of federally insured banks. In accordance with this requirement, banks must, among other things, establish internal controls and information systems for use in managing risk, reporting, safeguarding assets, and monitoring compliance.[42]

Customer Information. A second set of standards deal with the security and proper disposal of customer information via administrative, technical, and physical controls.[43] Four agencies have issued a joint regulation[44] mandating that each financial institution's senior leadership approve and oversee a written security program designed to safeguard customer information. The program must subject security controls to regular testing. Managers must use risk assessment when deciding on technical controls, such as encryption, multi-factor authentication, and intrusion detection systems.[45] Separately, the FTC and Securities Exchange Commission (SEC) enforce their own, generalized standards for protecting customer information. Both require the

institutions under their respective jurisdictions to establish written information security programs "reasonably designed"—considering the size, complexity, and type of institution—to secure customer information.[46]

Identity Theft. Third, most financial institutions must detect, prevent, and mitigate identity theft by instituting a "reasonable" security program to (1) identify patterns indicating identify theft, (2) detect such patterns, (3) respond to identity theft, and (4) evolve their program to adapt to changing threats.[47] The board of directors of each entity must approve of the program, and either the board or senior manager must oversee its implementation.[48]

Securities Markets. The SEC enforces standards intended to ensure the continuous operation of the stock market. The agency mandates that the trading firms, clearinghouses, and data organizations[49] who run securities markets must maintain written policies and procedures "reasonably designed" to maintain critical business operations and promote market stability.[50] These policies and procedures must adhere to industry-standard information technology practices that are widely available in the financial sector and issued by an "authoritative body."[51]

Special Note: Insurance. The regulation of insurance companies, brokers, and agents is generally left to the states, and data security standards in the insurance industry are not necessarily governed by the above rules.

CONCLUSION

Government regulation of cybersecurity is a controversial subject. Some analysts argue it can correct market failures that are responsible for lax security in certain industries. Others point out that regulation is unfit in a rapidly shifting technology environment. The variety of approaches taken by federal agencies demonstrate possible avenues for state lawmakers and regulators. They also provide a baseline for the private sector to work with state officials to avoid a regulatory framework that unduly hampers business growth.

The federal government takes a sector-specific approach to cybersecurity regulations. In the energy sector, where a sophisticated attack could cause serious harm, Congress, the NRC, and the FERC mandate detailed, comprehensive security measures. In other areas, federal agencies favor a "reasonableness" standard, affording flexibility to regulated entities while also creating incentives for those companies to draw on existing industry best practices. The FDA employs its market access control, using cybersecurity standards to vet the safety of advanced medical devices. Consequently, FDA cybersecurity rules burden only those firms that choose to sell in that market. The consumer-based approach used by the FTC charges companies with misleading consumers as to the level of security they can expect, thereby tying security to transparency. In the banking sector, agencies provide wide latitude to financial entities, but ensure accountability by requiring that company leaders remain involved in risk-based planning. There is no one-size-fits-all approach to regulation. Working with the private sector, states should identify regulatory gaps, determine whether those gaps require state action, define what they hope to achieve by filling those gaps, and model any subsequent regulatory action accordingly.

---

[1] Rhode Island requires "any individual . . . association, corporation, or . . . business . . . or other commercial entity" that collects or uses personal information about a Rhode Island resident to "implement and maintain a risk-based information security program which contains reasonable security procedures and practices appropriate to the size and scope of the organization, the nature of the information and the purpose for which the information was collected in order

to protect the personal information from unauthorized access, use, modification, destruction or disclosure and to preserve the CIA of such information." R.I. GEN. LAWS § 11-49.3-2. Violations can earn penalties of up to 100 dollars per record if they are reckless, and up to 200 dollars per record if they are knowing and willful. *Id.*

[2] 815 ILL. COMP. STAT. 530/5.

[3] Kansas requires any individual or entity that, "in the ordinary course of business", collects or uses personal information "of any other person," to "implement and maintain reasonable procedures and practices appropriate to the nature of the information, and exercise reasonable care to protect" it "from unauthorized access, use, modification or disclosure." KAN. STAT. ANN. § 50-6,139b(b)(1).

[4] *See* Romaine C. Marshall & C. Matt Sorensen, *New York's New Cybersecurity Regulation for Financial Institutions Will Have National Reach*, THE NATIONAL LAW REVIEW, March 1, 2017, http://www.natlawreview.com/article/new-york-s-new-cybersecurity-regulation-financial-institutions-will-have-national.

[5] 10 C.F.R. § 73.54(a).

[6] NUCLEAR REGULATORY COMMISSION, REGULATORY GUIDE 1.152: CRITERIA FOR USE OF COMPUTERS IN SAFETY SYSTEMS OF NUCLEAR POWER PLANTS (2010), *available at* http://www.nrc.gov/docs/ML1028/ML102870022.pdf; NUCLEAR REGULATORY COMMISSION, REGULATORY GUIDE 5.71: CYBER SECURITY PROGRAMS FOR NUCLEAR FACILITIES (2010), *available at* http://www.nrc.gov/docs/ML0903/ML090340159.pdf.

[7] North American Electric Reliability Corporation, *Organization Registration*, http://www.nerc.com/pa/comp/Pages/Registration.aspx.

[8] 18 C.F.R. § 39.5(c).

[9] The current CIP Reliability Standards relating to cybersecurity are:

- Security Management Controls (CIP 003)
- Personnel and Training (CIP 004)
- Electronic Security Perimeter (CIP 005)
- Physical Security of Cyber Systems (CIP 006)
- Systems Security Management (CIP 007)
- Incident Reporting and Response Planning (CIP 008)
- Recovery Plans for Cyber Systems (CIP 009)
- Configuration Change Management and Vulnerability Assessments (CIP 010)
- Information Protection (CIP 011)
- Physical Security (CIP 014)

[10] NERC released revised CIP standards on January 19, 2017. North American Electric Reliability Corporation, *Project 2016-03 Cyber Security Supply Chain Risk Management*, http://www.nerc.com/pa/Stand/Pages/Project201603CyberSecuritySupplyChainManagement.aspx

[11] 16 U.S.C. § 824o(e). For example, after the Southwest Blackout in 2011, NERC fined Arizona Public Service Company (APS) over $3 million for failing to follow NERC reliability standards. *See* North American Electric Reliability Corporation, *APS, FERC and NERC Reach Settlement Agreement on September 2011 Southwest Blackout*, July 7, 2014, available at http://www.nerc.com/news/Pages/APS,-FERC-and-NERC-Reach-Settlement-Agreement-on-September-2011-Southwest-Blackout.aspx.

[12] One authoritative study estimates that 80 to 90 percent of the assets that compose the nation's electric generation, transmission, and distribution system are not covered by the NERC CIP framework. Richard J. Campbell, *Cybersecurity Issues for the Bulk Power System*, CONGRESSIONAL RESEARCH SERVICE 13 n.61 (June 10, 2015), *available at* http://www.fas.org/sgp/crs/misc/R43989.pdf.

[13] 42 U.S.C. § 300i-2.

[14] 42 U.S.C. §§ 300(f)(7), 300g-3.

[15] *See* 6 C.F.R. Part 27; Homeland Security Appropriations Act of 2007, Pub. L. 109-295, Section 550

[16] 6 C.F.R. § 27.230(8).

[17] *See generally* U.S. DEP'T OF HOMELAND SECURITY, *RISK-BASED PERFORMANCE STANDARDS GUIDANCE*: CHEMICAL FACILITY ANTI-TERRORISM STANDARDS (2009), https://www.dhs.gov/sites/default/files/publications/CFATS-Risk-Based-Performance-Standards-508.pdf.

[18] *Id.* at 71.

[19] *See, e.g.*, ANNEX TO THE MEMORANDUM OF UNDERSTANDING BETWEEN THE DEPARTMENT OF HOMELAND SECURITY AND THE DEPARTMENT OF TRANSPORTATION CONCERNING TRANSPORTATION SECURITY ADMINISTRATION AND PIPELINE AND HAZARDOUS MATERIALS SAFETY ADMINISTRATION COOPERATION ON PIPELINE AND HAZARDOUS MATERIALS TRANSPORTATION SECURITY (Aug. 9, 2006), http://www.phmsa.dot.gov/staticfiles/PHMSA/DownloadableFiles/Annex%20to%20MOU%20between%20TSA-PHMSA.PDF.

[20] In a 2016 statement to the Senate Committee on Commerce, Science and Transportation, TSA Administrator Peter Neffenger stated that TSA was coordinating a voluntary cyber-assessment program with FERC to conduct cybersecurity assessments of pipeline entities and working with the pipeline industry to identify and reduce cybersecurity vulnerabilities through classified briefings.

[21] 45 C.F.R. § 164 et seq.

[22] *Id.* § 164.308.

[23] *Id.* § 164.312.

[24] *Id.* §§ 164.306(d), 164.312(e)

[25] *Id.* §§ 164.306(b).

[26] HHS has imposed fines totaling millions of dollars against health providers that have experienced data breaches, although in many cases they were the result of misplacing equipment, and not malicious hacking. *See, e.g.*, Erin Dietsche, *Advocate to pay largest HIPAA settlement to date*, BECKER'S HEALTH IT & CIO REVIEW (Aug. 5, 2016). Available at: http://www.beckershospitalreview.com/healthcare-information-technology/advocate-to-pay-largest-hipaa-settlement-to-date.html.

[27] 21 U.S.C. §§ 360(l), 360c(a)(1)(A).

[28] Food & Drug Administration, *Benefit-Risk Factors to Consider When Determining Substantial Equivalence in Premarket Notifications [510(k)] with Different Technological Characteristics: Draft Guidance for Industry and Food and Drug Administration Staff* (July 15, 2014). Available at: http://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm282958.htm.

[29] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, FRAMEWORK FOR IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY (4) (2014) ("The Framework Core consists of five concurrent and continuous Functions—Identify, Protect, Detect, Respond, Recover."), https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf. NIST published a draft revision of its Framework on January 10, 2017. NIST continues to seek public comment on the draft Framework, with an aim to publish a final version of the document in the fall 2017.

[30] FOOD & DRUG ADMINISTRATION, CONTENT OF PREMARKET SUBMISSIONS FOR MANAGEMENT OF CYBERSECURITY IN MEDICAL DEVICES 4-5 (Oct. 2, 2014), *available at* http://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm356190.pdf ("This guidance provides recommendations to consider and information to include in FDA medical device premarket submissions for effective cybersecurity management."). The FDA has also finalized nonbinding recommendations for postmarket cybersecurity management. These recommendations provide that medical device manufacturers and operators are generally not required to notify the FDA about routine cybersecurity updates and patches for medical devices that have been approved and are in use. Manufacturers are, however, required to notify the FDA when action is taken to correct device cybersecurity vulnerabilities that pose a risk to patient health. The FDA's guidance also provides robust recommendations for ongoing cyber risk management for marketed devices by manufacturers. FOOD & DRUG ADMINISTRATION, POSTMARKET MANAGEMENT OF CYBERSECURITY IN MEDICAL DEVICES (Dec. 28, 2016), http://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm482022.pdf.

[31] 15 U.S.C. § 45(a)(1).

[32] *See generally* Bruce Heiman, *The FTC Has Already Set Cybersecurity Standards*, LAW360, Mar. 5, 2015, http://www.law360.com/articles/626447/the-ftc-has-already-set-cybersecurity-standards.

[33] *See, e.g.*, FTC V. WYNDHAM WORLDWIDE CORP., 799 F. 3d 236 (3d Cir. 2015).

[34] For instance, the FTC recently filed a lawsuit against a manufacturer of Internet-connected video cameras, alleging the company failed to plug a well-known security flaw that creates a "significant risk" of harm to consumers. *See* Federal Trade Commission, *FTC Charges D-Link Put Consumers' Privacy at Risk Due to the Inadequate Security of Its Computer Routers and Cameras*, January 5, 2017, https://www.ftc.gov/news-events/press-releases/2017/01/ftc-charges-d-link-put-consumers-privacy-risk-due-inadequate.

[35] Federal Trade Commission, *Data Security*, https://www.ftc.gov/tips-advice/business-center/privacy-and-security/data-security.

[36] 47 U.S.C. § 222(a).

[37] The FCC has relied upon 47 U.S.C. §§ 201(b), 222(a) as the statutory basis for assessing fines.

[38] Federal Communications Commission, *AT&T To Pay $25M To Settle Investigation Into Three Data Breaches* (Apr. 8, 2015), https://www.fcc.gov/document/att-pay-25m-settle-investigation-three-data-breaches-0.

[39] Acknowledging the diversity among ISPs in terms of size and technical capability, the FCC favored a highly flexible standard over specific cybersecurity controls. As in other sectors, the FCC recommends measures that are likely to survive "reasonableness" scrutiny, including: practicing data minimization, i.e., disposing of unnecessary data; implementing industry-standard risk management

tools; developing a written comprehensive data security program (in line with FTC guidance); designating officials to oversee and take responsibility for data security practices; and using modern authentication techniques with traditional user-generated passcodes or security questions. In the Matter of *Protecting the Privacy of Customers of Broadband and Other Telecommunications Services*, Report and Order, FCC 16-148, Oct. 27, 2016, at 6; 96-109, 102-108, 137-140.

[40] *See* In the Matter of *Protecting the Privacy of Customers of Broadband and Other Telecommunications Services*, Order Granting Stay Petition in Part, FCC 17-19, March 1, 2017.

[41] This term "Financial Institution" refers to "national banks, federal savings associations, state savings associations, state member banks, state nonmember banks, and credit unions." FEDERAL FINANCIAL INSTITUTIONS EXAMINATION COUNCIL, FFIEC INFORMATION TECHNOLOGY EXAMINATION HANDBOOK: INFORMATION SECURITY 1 n.2 (2016), http://ithandbook.ffiec.gov/ITBooklets/FFIEC_ITBooklet_InformationSecurity.pdf.

[42] 12 U.S.C. § 1831p-1; 12 C.F.R. § 364.101, appendix A.II.

[43] 15 U.S.C. §§ 6801(b), 6805(b).

[44] The Treasury Department, Federal Reserve, Federal Deposit Insurance Corporation (FDIC), and the National Credit Union Administration (NCUA) have promulgated the *Interagency Guidelines Establishing Information Security Standards*. *See* 12 C.F.R. § 30, appendix B; § 570, appendix B (Treasury); 12 C.F.R. § 208, appendix D-2 and § 225, appendix F (FRB); 12 C.F.R. § 364, appendix B (FDIC); and 12 C.F.R. § 748, appendix A (NCUA).

[45] *See, e.g.*, 12 C.F.R. § 30, appendix B.III.C.1.

[46] 16 C.F.R. §§ 314.3, 314.4; 17 C.F.R. § 248.30.

[47] *See* 15 U.S.C. §§ 1681m(e); 12 C.F.R. §§ 41.90 *et seq.*, 222.90 *et seq*., 334.90 *et seq.*, 571.90 *et seq.*, 717.90 *et seq.*; 16 C.F.R. § 681.1 *et seq.*; 17 C.F.R. § 248.201.

[48] *See, e.g.*, 17 C.F.R. § 248.201(d).

[49] 17 C.F.R. § 240.13n-6

[50] *Id.* § 242.1001

[51] *Id.* § 242.1001(a)(2)-(4).

David Forscey is a Policy Analyst for the Homeland Security & Public Safety Division of the National Governors Association. The NGA Center for Best Practices Homeland Security & Public Safety Division provides information, research, policy analysis, technical assistance and resource development for governors and their staff about emerging policy trends across a range of homeland security and public safety issues.

Steven A. Cash, Counsel at Day Pitney and member of its Cyber Security and Data Protection practice, represents individual and corporate clients in criminal, commercial litigation and national security matters. He has broad experience at the federal and state level in the executive, legislative and judicial branches, including serving as Chief Counsel and Staff Director (Minority) to the U.S. Senate's Judiciary Committee, Subcommittee on Terrorism, Technology, and Homeland Security; Chief Counsel to Senator Dianne Feinstein; Chief of Staff to the Director of Intelligence, Department of Energy; Staff Director to the U.S. House of Representative's Select Committee on Homeland Security; and Professional Staff Member and Counsel to the Senate Select Committee on Intelligence.

Benjamin H. Nissim, an Associate at Day Pitney and member of its Cyber Security and Data Protection practice, represents corporate clients in commercial litigation in state and federal courts and arbitration proceedings. His practice includes representing insurance companies and agents in a wide range of insurance and reinsurance disputes, creditors and trustees in bankruptcy and bankruptcy related proceedings, and advising companies and individuals on cybersecurity and data protection issues.

About National Governors Association

Founded in 1908, the National Governors Association (NGA) is the collective voice of the nation's governors and one of Washington, D.C.'s most respected public policy organizations. Its members are the governors of the 55 states, territories and commonwealths. NGA provides governors and their senior staff members with services that range from representing states on Capitol Hill and before the Administration on key federal issues to developing and implementing innovative solutions to public policy challenges through the NGA Center for Best Practices. NGA also provides management and technical assistance to both new and incumbent governors.

About Day Pitney

Day Pitney LLP is a full-service law firm with close to 300 attorneys in Boston, Connecticut, Florida, New Jersey, New York, and Washington, DC. The firm offers clients strong corporate and litigation practices, with experience on behalf of large national and international corporations as well as emerging and middle-market companies. With one of the largest and most sophisticated individual clients practices in the country, the firm also has extensive experience assisting individuals and their families, fiduciaries and tax-exempt entities plan for the future.

"Cybersecurity is no longer just an issue for Information Technology professionals - it affects everyone. Cybersecurity involves an increasingly complex set of federal and state laws, regulations and policies. *A Primer on Cybersecurity Regulations*, produced as a joint publication by the National Governor's Association and Day Pitney, will be an essential tool for anybody, in or out of government, who needs a quick reference guide to the key federal statutes and regulations."

– Stanley A. Twardy
Managing Partner, Day Pitney LLP