

Critical Infrastructure:

2017 Cybersecurity Review and What to Expect in 2018

January 24, 2018

Van Ness Feldman LLP

Van Ness Feldman LLP

INTRODUCTION

In response to increasing concerns about cyber threats, there were several federal policy and legislative developments in 2017 aimed at improving U.S. cyber resiliency and strengthening national security. Many of the developments are focused on protecting the nation's critical infrastructure[1] in recognition of the fact that large-scale cyber-attacks have the potential to cripple an entire nation and worst case scenarios are no longer limited to privacy-related breaches on an individual level. There is growing awareness that, due to advances in technology, cyber-attacks can also jeopardize critical infrastructure operations and could potentially result in broad-scale catastrophic disruption or loss. In the absence of an overarching single piece of legislation or comprehensive approach, these varied federal initiatives have created a more complex patchwork of requirements, guidelines, and best practices regarding proper cyber risk assessment and mitigation. Further complicating the mix, several states are bolstering their own cyber readiness through legislation or other initiatives to provide additional layers of protections for their constituents.[2] Although not yet tested in the courts, these new developments have the potential to re-shape the definitions of due diligence, reasonableness, and the appropriate standards of care necessary to drive down the risk of an attack that could have catastrophic effects.

Van Ness Feldman, LLP (VNF) recognizes that many of our clients, as stewards of critical infrastructure resources, are on the frontline in the fight against this new realm of threats to national security. Given the firm's understanding of clients' business models, VNF is aware that clients are not only concerned about customers' and employees' data privacy and information technology (IT), but are also facing emerging concerns about protecting their operational technology from cyber threats. With that in mind, our goal is to help clients make sense of this complex web of obligations and recommendations by demystifying the policy, regulatory and statutory requirements, advising on best practices, and explaining the associated legal risks to enable clients to make sound business decisions that serve their customers and the public. As new initiatives and developments unfold, VNF is available to advocate for clients' interests, and help shape the next round of policy, regulatory, and legislative changes.

[1] Executive Order No. 13636 defines "critical infrastructure" as "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety or any combination of those matters." 78 Fed. Reg. 11,739 (Feb. 19, 2013) (Improving Critical Infrastructure Cybersecurity). To further clarify, Presidential Policy Directive 21 (PPD-21): *Critical Infrastructure Security and Resilience* has identified sixteen critical infrastructure sectors based on this definition including chemical, dams, energy, water and waste water systems, transportation as well as nuclear reactors, materials and waste sectors. *See* https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.

[2] *See* National Governors Ass'n, States Pledge to Meet the Cyber Threat (July 14, 2017), https://www.nga.org/cms/news/2017/states-pledge-to-meet-the-cyber-threat.

Van Ness Feldman LLP

To aid our clients and friends of the Firm in navigating this constantly evolving area of law and policy, we are pleased to provide a summary of major federal initiatives throughout 2017 and identify common developments and themes that will be helpful as clients plan for the year ahead.

Summary of Key Federal Cybersecurity Initiatives of 2017

Executive Branch

- Executive Order No. 13800, Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure, 82 Fed. Reg. 22,391 (May 16, 2017);

- National Infrastructure Advisory Council (NIAC), Final Report, Securing Cyber Assets: Addressing Urgent Cyber Threats to Critical Infrastructure (Aug. 2017);[3]

- National Institute of Standards and Technology (NIST), Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1 Draft 2 (Rev. Dec. 5, 2017) (Framework v.1.1).[4]

Legislative Branch

- Strengthening Cybersecurity Information Sharing and Coordination in Our Ports Act of 2017, H.R. 3101, 115th Cong.;

- Cybersecurity and Infrastructure Security Agency Act of 2017, H.R. 3359, 115th Cong.;

- NIST Cybersecurity Framework, Assessment and Auditing Act of 2017, H.R. 1224, 115th Cong.;

- Enhancing State Energy Security Planning and Emergency Preparedness Act, H.R. 3050, 115th Cong.;

- Grid Cybersecurity Research and Development Act, H.R. 4120, 115th Cong.;

- Securing Energy Infrastructure Act, S. 79, 115th Cong.;

- Securing the Electric Grid to Protect Military Readiness Act of 2017, S. 1800, 115th Cong.

[3] https://www.dhs.gov/sites/default/files/publications/niac-securing-cyber-assets-final-report-508.pdf.
[4] https://www.nist.gov/sites/default/files/documents/2017/12/05/draft-2_framework-v1-1_without-markup.pdf.

Sector-Specific Developments

- Cyber Security Incident Reporting Reliability Standards, 82 Fed. Reg. 61,499 (Dec. 28, 2017) (Notice of Proposed Rulemaking (NOPR), comments due February 2018);

- Revised Critical Infrastructure Protection Reliability Standard CIP-003-7—Cyber Security—Security Management Controls, 82 Fed. Reg. 49,541 (Oct. 26, 2017) (NOPR, pending before the Federal Energy Regulatory Commission (FERC));

- Pipeline and Liquefied Natural Gas cybersecurity measures;

- Environmental Protection Agency (EPA) Office of Water "Incident Action Checklist—Cybersecurity" (Oct. 2017).[5]

THE EXECUTIVE BRANCH AND CYBERSECURITY

I. Executive Order No. 13800, Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure

On May 11, 2017, President Trump, building upon the work of prior Administrations,[6] issued Executive Order No. 13800 "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure,"[7] which has served as the impetus for many subsequent public and private sector partnerships and initiatives in the cyber realm. The Executive Order was broken down into five sections, three of which are substantive:[8] Section 1 – Cybersecurity of Federal Networks; Section 2 – Cybersecurity of Critical Infrastructure; and Section 3 – Cybersecurity for the Nation. Collectively, the sections established deadlines for approximately fifteen reports to be delivered to the President, some of which have been designated to be classified, in whole or in part. The reports focus on new requirements to bolster cybersecurity within federal agencies, outlining the federal government's role and ability to maximize its support of critical infrastructure entities on the frontline in the fight against cyber-attacks, and addressing how the federal government promotes market transparency of cyber risk management practices of critical infrastructure entities. Some of these reports and supporting documents were delivered and published in 2017 including:

[5] https://www.epa.gov/sites/production/files/2017-11/documents/171013-incidentactionchecklist-cybersecurity_form_508c.pdf.

[6] Exec. Order No. 13636, 78 Fed. Reg. 11,739; Exec. Order No. 13691, 80 Fed. Reg. 9,349 (Feb. 20, 2015) (Promoting Private Sector Cybersecurity Information Sharing); Commission on Enhancing National Cybersecurity, Report on Securing and Growing the Digital Economy (Dec. 1, 2016).

[7] Exec. Order No. 13800, 82 Fed. Reg. 22,391 (May 16, 2017).

[8] Sections 4 and 5 contain definitions and general provisions respectively.

- The National Infrastructure Advisory Committee's NIAC's "*Securing Cyber Assets: Addressing Urgent Cyber Threats to Critical Infrastructure*," August 2017, which will be summarized below.

- A report issued by the Department of Homeland Security (DHS), entitled "Cybersecurity Workforce Development Toolkit: How to Build a Strong Cybersecurity Workforce" updated in November 2017.[9]

- "Report to the President on Federal IT Modernization" by the American Technology Council, December 2017.[10]

- Draft "Report to the President on Enhancing the Resilience of the Internet and Communications Ecosystem Against Botnets[[11]] and other Automated, Distributed Threats" by the Secretaries of the Departments of Commerce and DHS, published January 5, 2018.[12]

Several non-classified reports are still outstanding and in various stages of internal agency review with delivery expected in 2018, including:

- The final report on efforts to improve the resilience of the internet and the communications system by reducing threats perpetrated by botnets and other automated, distributed attacks is anticipated for release on May 11, 2018. The National Telecommunications and Information Administration (NTIA) is seeking public comment on the draft through February 5, 2018.

- A report from the Secretaries of Commerce and DHS on marketplace transparency of cyber risk management practices for critical infrastructure agencies, especially those that are publicly traded.

There is a perception held by some that the federal government typically lags far behind the private sector in modernizing cyber technologies. By adopting these requirements for federal agencies, the

[9] U.S. Dep't of Homeland Security, Cybersecurity Workforce Development Toolkit (Nov. 15, 2017), https://niccs.us-cert.gov/workforce-development/cybersecurity-workforce-development-toolkit.
[10] American Technology Council, Report to the President on Federal IT Modernization (2017), https://itmodernization.cio.gov/assets/report/Report%20to%20the%20President%20on%20IT%20Modernization.pdf.
[11] The term "botnet" is derived from "robot" and "network" to indicate a "network of computers linked together by malware" that is controlled remotely without the knowledge of the users of those computers. https://www.merriam-webster.com/dictionary/botnet. Botnets are an increasing concern in the cyber realm because they are used for a variety of malicious activities, including denial of service and ransomware attacks as well as other nefarious purposes that jeopardize data integrity, operational systems and national security.
[12] https://www.ntia.doc.gov/report/2018/report-president-enhancing-resilience-internet-and-communications-ecosystem-against.

current Administration appears to be trying to move the federal government into a leadership position on the assessment and mitigation of cyber risks. Many of the steps outlined in the various reports may have already been implemented in the private sector; however, it is possible that many of the new federal requirements will encourage lagging companies to reassess their own cyber practices to avoid or manage legal risk.

II. NIAC Report, "Securing Cyber Assets: Addressing Urgent Cyber Threats to Critical Infrastructure," August 2017

As previously noted, Section 2 of Executive Order 13800 calls for the Secretary of DHS, in coordination with other cabinet members, to identify federal authorities and capabilities that could be best used to support the cybersecurity efforts of critical infrastructure entities and then engage such entities to determine how best to maximize those federal resources and identify any obstacles for doing so.[13] While the resulting official report to the President may be classified, all or in part, a draft of a public report on the same topic was released in August 2017 and gives stakeholders a peak behind the curtain to at least understand how organizations outside of the federal government view the divide between the private sector and government in the fight to maintain cybersecurity, as well as the opportunities and obstacles to bridging the gap.

Following the release of the Executive Order in May 2017, the National Security Council tasked NIAC[14] to "assess how existing federal authorities and capabilities could be employed to assist and better support the cybersecurity of critical infrastructure assets that are at greatest risk of a cyber-attack."[15] Three months later, NIAC issued a 45-page document that was written with an urgent tone, stressing that strong leadership was required to meet the risks of a "cyber 9/11"—type event. The paper, which included a review of over 140 federal capabilities and authorities, called for action-oriented leadership to shrink the gaps between partners in the fight against cyber-attacks.[16] NIAC's 11 recommendations can be grouped in four categories: 1) Developing a Comprehensive Governance Strategy; 2) Improving Cyber Readiness; 3) Simplifying Information Sharing; and 4) Bolstering Incident Response. Given that the draft report was advisory in nature, there may be opportunities for critical infrastructure entities or their affiliates to advocate for policies and reforms that benefit the organizations facing cyber risks to critical infrastructure.

[13] Exec. Order No. 13800, 82 Fed. Reg. at 22,393.
[14] NIAC, established by executive order in October 2001, "is composed of senior executives from industry, state and local government who own and operate the critical infrastructure essential to" our democracy and "advise the President on practical strategies for industry and government to reduce complex risks to the designated critical infrastructure sectors." NIAC, Securing Cyber Assets: Addressing Urgent Cyber Threats to Critical Infrastructure at 2.
[15] *Id.* at 5.
[16] *Id.* at 3.

III. NIST, "Framework for Improving Critical Infrastructure Cybersecurity," Version 1.1 Draft 2, (Revised December 5, 2017) (Framework v.1.1)

On December 5, 2017, NIST published long-awaited updates to the "Framework for Improving Critical Infrastructure Cybersecurity," originally authored in February 2014 pursuant to Executive Order No. 13636, "Improving Critical Infrastructure Cybersecurity" issued February 12, 2013, and its companion document "NIST Roadmap for Improving Critical Infrastructure Cybersecurity." Framework v1.1 "refines, clarifies and enhances Version 1.0" and while the document has several notable changes from the original, the authors were deeply committed to making the new version compatible with its predecessor document to create a seamless progression for an organization's continued cyber readiness and resiliency.[17] NIST accepted public comment on the document through January 18, 2018, and expects to release a final version in the next few months.

While Framework v1.1 is touted to apply to all organizations, regardless of size, sector or cyber maturity, for critical infrastructure, it reiterates that "[d]ue to the increasing pressures from external and internal threats, organizations responsible for critical infrastructure need to have a consistent and iterative approach to identifying, assessing and managing cybersecurity risk. This approach is necessary regardless of an organization's size, threat exposure or cybersecurity sophistication."[18] This admonition makes it clear that critical infrastructure entities have significant responsibilities in shoring up their individual and collective cybersecurity and that a failure to do so could create unnecessary legal risk, adversely affect their customers and the company's bottom line, as well as jeopardize our national security.

IV. The National Security Strategy

In addition to Executive Order No. 13800, the White House released its National Security Strategy (NSS)[19] on December 18, 2017, which, in an effort to provide a comprehensive approach to national security, includes several priority action items to strengthen the country's protection against cyber intrusions. These priorities recognize many of the challenges and opportunities outlined in the publicized cybersecurity reports published to date and encapsulate many of the recommendations. The NSS outlines a desire to improve the security and resilience of critical infrastructure in six areas including energy and power, transportation, communication as well as health and safety. Specific examples include improving information sharing, reducing the barriers to the exchange of critical intelligence by addressing time lags and cumbersome classification levels; coordinating the

[17] Framework v1.1 at ii.
[18] *Id.* at 3.
[19] National Security Strategy of the United States (Dec. 2017), https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf.

cybersecurity authorities across the federal family to increase their effectiveness in the fight against cyber intrusions; improving incident response by deterring malicious cyber actors as well as improving attribution and disrupting their attacks; and recruiting, training and retaining a workforce able to meet the ever-evolving challenges.

THE LEGISLATIVE BRANCH AND CYBERSECURITY

On Capitol Hill, policymakers also continued to take steps to address cybersecurity threats to critical energy infrastructure. Much like the Executive Branch, committees in both the House and Senate have held hearings to clarify the role of Congress and federal agencies to identify and act upon cybersecurity threats and vulnerabilities. Congress has passed only one bill on this topic that has become law.

The FY 2018 National Defense Authorization Act, signed into law on December 12, 2017, requires the President to develop a national cybersecurity policy that includes options that "prioritize the defensibility and resiliency against cyber-attacks and malicious cyber activities that are carried out against infrastructure critical to the political integrity, economic security and national security of the United States."[20] It also includes a provision requiring an assessment of the strategic benefits of isolating the national electric grid from military infrastructure "and the use of microgrids" to protect from cyber threats.[21]

Members of Congress have also introduced a number of pending bills that address cybersecurity for critical energy and transportation infrastructure.

- Strengthening Cybersecurity Information Sharing and Coordination in Our Ports Act of 2017, H.R. 3101 and its companion legislation S. 2083, promote increased cybersecurity information sharing among federal agencies, port owners and operators. They require DHS to develop and implement voluntary reporting guidelines for port-specific cybersecurity risks and vulnerabilities. Given that 25 percent of the petroleum used in the United States is imported and is processed through these ports, the petroleum industry would be most directly impacted if these bills were to become law. The bill passed the House by voice vote on October 24, 2017, and awaits Senate action.

- Cybersecurity and Infrastructure Security Agency Act of 2017, H.R. 3359, would rename the National Protection and Programs Directorate (NPPD) to be the Cybersecurity and Infrastructure Agency (CISA) and clarify its mission as a cybersecurity-focused agency. The CISA would operate as a stand-alone operational organization, like the Federal Emergency Management Agency (FEMA) or the Transportation Security Administration (TSA), and the leading civilian

[20] Pub. L. No. 115-91, § 1633(b)(3).
[21] *Id.* § 1643(3). Microgrids are a local energy grid that can operate independently when disconnected from the traditional grid.

cybersecurity agency. The bill was passed by the House by voice vote on December 11, 2017, and awaits Senate action.

- NIST Cybersecurity Framework, Assessment and Auditing Act of 2017, H.R. 1224, would direct federal agencies to implement the NIST Cybersecurity Framework and direct NIST to produce guidelines for agency implementation. It should be noted, that this was already mandated in Executive Order No. 13800. The bill was reported out of the House Science, Space and Technology Committee in March 2017, with an amendment (H. Rept. No. 115-376) and recommended that the bill be passed on October 31, 2017.

- Enhancing State Energy Security Planning and Emergency Preparedness Act, H.R. 3050, requires states to address potential cybersecurity threats and vulnerabilities in their energy security plans. The bill passed the House by voice vote on July 18, 2017, and awaits Senate action.

- Grid Cybersecurity Research and Development Act, H.R. 4120, requires the Department of Energy (DOE) to develop a research and demonstration program to improve energy sector cybersecurity capabilities. The bill was introduced in the House on Oct. 25, 2017, and referred to the Committee on Homeland Security, the Committee on Energy and Commerce and the Committee on Science, Space and Technology.

- Securing Energy Infrastructure Act, S. 79, establishes a two-year DOE pilot program to identify cybersecurity vulnerabilities of energy sector entities. The bill was introduced in the Senate on January 10, 2017, and has been referred to the Senate Energy and Natural Resources Committee, which held a hearing on the bill in March 2017. A companion bill (H.R. 3958) was also introduced in the House on October 4, 2017, and referred to the House Committee on Science, Space and Technology.

- Securing the Electric Grid to Protect Military Readiness Act of 2017, S. 1800, requires the Secretary of Defense to issue a report on significant security risks to the Defense Department's critical electric infrastructure. This report must include an identification of security risks posed by malicious cyber activity. The bill was introduced in the Senate on September 12, 2017, and has been referred to the Senate Committee on Armed Services. A companion bill (H.R. 3855) was introduced in the House and referred to the House Committee on Armed Services.

The discussion on cybersecurity is not solely limited to the electricity sector. Last year, Congress for the first time delved into legislating the development of automated vehicle (AV) technologies through the passage of the SELF DRIVE Act[22] in the House and passing the AV START Act[23] through the Senate Commerce, Science and Transportation Committee. Unmanned technologies like AVs and unmanned aerial systems (UAS) bring about significant cyber and data security challenges, and both bills contain

[22] H.R. 3388, 115th Cong..
[23] S. 1885, 115th Cong..

sections addressing those challenges. Congress will need to act decisively to address these issues as those industries continue their rapid progress towards getting their technologies to the market.

Cybersecurity will continue to be a primary topic of deliberation on Capitol Hill in 2018. Legislators already face a condensed legislative year due to the 2018 mid-term elections and a crowded calendar of "must-pass" bills. Cyber threats to critical infrastructure will necessitate that Congress act quickly on this issue, particularly if there are additional high-profile cyber-attacks on critical infrastructure facilities or significant data breaches against prominent U.S. companies. The Senate will likely act on the Cybersecurity and Infrastructure Security Agency Act in 2018, though changes are expected to be made to the bill. Among the issues that will be closely evaluated by the Senate Homeland Security and Government Affairs Committee are the bill's effect on the private sector as well as how other government agencies will be able to address cybersecurity issues after the establishment of the CISA.

SECTOR-SPECIFIC CYBERSECURITY DEVELOPMENTS

I. Electric Grid

Protecting the electric grid against cyber threats and maintaining its reliability has become increasingly important for the United States given the large-scale cyber-attacks that foreign actors have conducted elsewhere over the past few years. Given that the United States depends on electricity for basic needs such as food, water, shelter, communication, employment, and healthcare, the entire nation could be instantly destabilized without access to reliable electricity service. It should come as no surprise, then, that the power system and its physical components (e.g., generators, substations, and transmission lines) are a central component of critical infrastructure. U.S. standards for electric grid reliability and security are developed by a private non-profit corporation, the North American Electric Reliability Corporation (NERC), and reviewed and approved by the FERC. At the end of 2017, FERC issued two cybersecurity-related proposed rules with the intent of strengthening the Critical Infrastructure Protection (CIP) reliability standards already in place.

A. Proposal on Cyber Security Incident Reporting [24]

FERC issued a NOPR which, if adopted, would instruct NERC to modify its CIP standards to include stricter reporting requirements for cybersecurity incidents. The proposal would expand the types of incidents that must be reported, and would increase the information required in each report. Reports would have to be submitted to the Electricity Information Sharing and Analysis Center (E-ISAC) and DHS Industrial Control Systems Cyber Emergency Response Team (ICS-CERT). The NOPR would

[24] 82 Fed. Reg. 61,499.

also require NERC to file an annual, anonymized report with FERC reporting aggregated information. Comments on this NOPR are due at the end of February 2018.

B. Proposal on Revised CIP Standard on Security Management Controls [25]

On October 19, 2017, FERC proposed new security management controls for grid cyber systems to address the risks posed by malware from transient electronic devices like laptop computers, thumb drives and other devices used at low-impact bulk electric system cyber systems. FERC proposed to approve CIP-003-7 (Cyber Security—Security Management Controls), which is designed to mitigate cybersecurity risks that could affect the reliable operation of the Bulk-Power System. The proposed standard "improves upon the current Commission-approved CIP Reliability Standards by clarifying the obligations pertaining to electronic access control for low-impact [cyber systems]; adopting mandatory security controls for transient electronic devices," such as thumb drives and laptop computers; "and requiring responsible entities to have a policy for declaring and responding to CIP Exceptional Circumstances related to low-impact [cyber systems]."[26] The proposed rule was published in the *Federal Register* on October 26, 2017. The comment period has closed and the proposed rule is before FERC.

It should be noted that on January 18, 2018, FERC issued a NOPR proposing three CIP standards which would modify currently effective CIP standards to reduce cybersecurity risks associated with supply chain management. This NOPR and all recent electric-related cybersecurity developments are covered in our bi-monthly Electric Reliability Updates.

II. Pipeline and LNG

Since there have been no recent cybersecurity developments in the natural gas pipeline sector, the Pipeline Security Guidelines,[27] issued in April 2011 by the Pipeline and Hazardous Materials Safety Administration and the TSA, still serve as the most recent guidance for pipeline operators. While no mandatory cybersecurity rules for gas companies exist, the existing TSA's Pipeline Security Guidelines set forth "baseline cyber security measures" and "enhanced cybersecurity measures" that should be applied to all pipeline control system cyber assets.[28] Given the current Administration's stance on federal regulations,[29] it is unlikely that the current Administration will issue any new cybersecurity

[25] 82 Fed. Reg. 49,541.
[26] *Id.*
[27] Transportation Security Administration, U.S. Dep't of Homeland Security, Pipeline Safety Guidelines (2011), *available at* https://www.tsa.gov/sites/default/files/tsapipelinesecurityguidelines-2011.pdf
[28] *Id.* at 18.
[29] Introduction to the Unified Agenda of Federal Regulatory and Deregulatory Actions-Fall 2017, 83 Fed. Reg. 1664 (Jan. 1, 2018).

regulations for pipelines. However, it has been reported that, in response to concerns raised by lawmakers about TSA's oversight of cybersecurity threats, the TSA has refreshed the Pipeline Security Guidelines.[30] While the document is still under review, it is expected that the updated guidelines will track the step-by-step security framework published by NIST in 2014 and provide an "objective benchmark" of pipelines' cyber readiness.[31] VNF will be tracking this development closely and will be ready to advise clients on its implications when the guidelines are released.

III. Water and Wastewater Utilities

Over the past year, the water sector has made strides to identify the problems and vulnerabilities within water infrastructure. The American Society of Civil Engineers' (ASCE) 2017 Infrastructure Report Card gave the U.S. water infrastructure system a letter "D" grade based on the current conditions, the risks the systems face, and the capacity to respond to these risks.[32] In response to the alarming issues identified in the ASCE report and others like it, the Association of Metropolitan Water Agencies (AMWA) states that "[p]rotecting water utility infrastructure from terrorism and enhancing resilience against disasters are top priorities for AMWA member utilities."[33] The EPA stepped up to aid the industry in this effort. In October 2017, EPA's Office of Water published an "Incident Action Checklist – Cybersecurity" intended to help water and wastewater utilities by identifying actions that utilities can take to prepare for, respond to, and recover from cyber incidents.[34] This checklist references a number of resources, many of which are not specific to the water resource sector. For example, the checklist identifies a repository of advisories issued by the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT).[35] Other resources, such as the Water ISAC "10 Basic Cybersecurity Measures," are directed specifically at the water and wastewater utility sector but contain recommendations that could be implemented in the business or industrial sector.[36]

---

[30] Peter Behr & Blake Sobczak, *TSA to expand gas pipeline cybersecurity oversight*, Energywire (Dec. 22, 2017), https://www.eenews.net/energywire/stories/1060069743/search?keyword=%22TSA+to+expand+gas+pipeline%22

[31] *Id.*

[32] American Society of Civil Engineers, 2017 Infrastructure Report Card, https://www.infrastructurereportcard.org/wp-content/uploads/2017/01/Drinking-Water-Final.pdf.

[33] https://www.amwa.net/water-sector-security-disaster-response (last visited Jan. 24, 2018).

[34] That checklist is available here: https://www.epa.gov/sites/production/files/2017-11/documents/171013-incidentactionchecklist-cybersecurity_form_508c.pdf.

[35] https://ics-cert.us-cert.gov/advisories (last visited Jan. 24, 2018).

[36] Water Information Sharing & Analysis Center, 10 Basic Cybersecurity Measures, Best Practices to Reduce Exploitable Weaknesses and Attacks (June 2015), https://ics-cert.us-cert.gov/sites/default/files/documents/10_Basic_Cybersecurity_Measures-WaterISAC_June2015_S508C.pdf. This guidance was developed in June 2015 by Water Information Sharing and Analysis Center (Water ISAC, a congressionally authorized organization led and managed by stakeholders in the water sector) in partnership with the DHS Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), the Federal Bureau of Investigations, and the IT ISAC.

Van Ness Feldman LLP

CONCLUSION

The vast and varied legislative and policy developments in cybersecurity during 2017 demonstrate that the White House and Congress are committed to building a foundation for additional progress in the fight to protect infrastructure and national security. This momentum will continue in 2018, and the Cybersecurity Team at VNF stands ready to keep its clients informed and at the forefront of these discussions. Please do not hesitate to contact Gwen Keyes Fleming, Mike Farber, or Darsh Singh, if you have any questions or need more information.

T.C. Richmond, Tracy Nagelbush, and Mike Weiner contributed to this report.