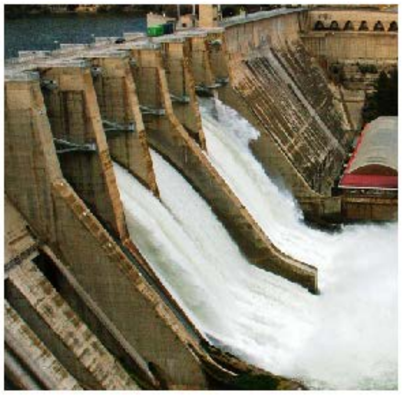


Critical Infrastructure:

3rd Annual Cybersecurity Year in Review/Look Ahead Analysis

January 30, 2020

Van Ness
Feldman LLP

A MESSAGE FROM OUR TEAM LEADERS

As co-chairs of Van Ness Feldman's Cybersecurity and Emerging Technologies team, we are pleased to provide our 3rd Annual Year in Review/Look Ahead Analysis to clients and friends of the firm. Cybersecurity remains of paramount concern to numerous industries. The day-to-day existence of consumers who rely upon utilities to light and control the climate of their homes and businesses, supply water, power their cars and subway systems and other necessities of modern life are at risk as more devices become connected to the grid. Additionally, identities, privacy, and electronic data, as well as health-care institutions and patients who require medical attention and devices to live, are susceptible to theft and exploitation at the hands of cybercriminals. The focus on cybersecurity is heightened not only because of our increased reliance on technology nationally, but also because those connections are directly affected by geopolitical events and threats of aggression from our adversaries.

In keeping with our historic services, the firm continues to monitor and advocate for both legal and policy protections in response to evolving cybersecurity threats and advances in emerging technologies that affect critical infrastructure entities. This year we expanded our team and the services we offer to better serve the diverse interests and needs of our clients. In recognition of the fact that, as noted above, companies in the energy, water, natural resources, and transportation sectors are incorporating emerging technologies into their business activities we have created a new focus in our Cybersecurity Practice to help clients navigate the unique challenges of emerging technologies. These technologies—ranging from machine learning algorithms to connected devices (e.g., sensors) to automated systems—have the potential to provide users with valuable insights and efficiencies that one could only have dreamed of just a half-decade ago. While the potential benefits of these emerging technologies are huge, companies should also be aware that the incorporation of these technologies comes with risks—most notably cyber risk. Accordingly, companies must undertake a fulsome review of the potential vulnerabilities arising from their use of emerging technologies to ensure that potential legal liability arising from cyberattacks and data breaches do not ultimately outweigh the potential benefits. We expect to preview more of the policy developments affecting this area in the months to come.

For clients in Van Ness Feldman's more traditional practice areas who remain concerned about cybersecurity, we also now have team members focused on each of the topics listed in the report below. The team provided essential updates on the activities of federal agencies and industry groups, including new regulatory initiatives and key legislative developments impacting cybersecurity. We invite you to click on the links of interest and reach out to a member of our team listed below if you have questions or want more information.

This document has been prepared by Van Ness Feldman for informational purposes only and is not a legal opinion, does not provide legal advice for any purpose, and neither creates nor constitutes evidence of an attorney-client relationship.

- Legislative Branch: *Lilly Scott, Michael Weiner, and Tracy Tolk*
- Energy (Electric and Oil & Gas Subsectors): *Darsh Singh and Ani Esenyan*
- Water: *Jordan Smith and T.C. Richmond*
- Chemical Facilities: *Gwen Keyes Fleming*
- Transportation (Autonomous Vehicles): *Tracy Tolk, Michael Weiner, and Scott Nuzum*
- Health: *James Bayot*
- Privacy and Data Security: *Scott Nuzum*

The vast and varied legislative and policy developments in cybersecurity during 2019 demonstrate that the White House and Congress are committed to building a foundation for continuing progress to protect infrastructure and national security. Even with the diversity of action by government entities, some common needs and themes have emerged as foundational elements in securing our nation from cyber-attacks. As noted in a December 2019 report from the President's National Infrastructure Advisory Council ("NIAC"), bolstering information sharing, improving response capabilities, and ensuring that legal authorities keep pace with the innovations and evolving threats should be top priorities and will require bold action to be successful.

No matter what new developments, legislation, regulation, funding opportunities or other initiatives emerge in 2020 to help critical infrastructure mitigate and address the latest cyber threats, the Cyber/EmTech team at Van Ness Feldman will continue to keep firm clients informed and at the forefront of these discussions. We are also available to consult on organizational preparedness and, should the unthinkable happen despite proactive measures, assist with incident response and enforcement actions. Please do not hesitate to contact Gwen Keyes Fleming, T.C. Richmond, or Scott Nuzum, if you have any questions or need more information regarding any of the topics discussed in this report or other cyber-related concerns. Have a safe and prosperous 2020.

Respectfully,

Gwen Keyes Fleming & T.C. Richmond

The Legislative Branch

Contributors: Lilly Scott, Michael Weiner, and Tracy Tolk

2019 Developments

Congress took major steps to advance cybersecurity legislation in 2019. Just before adjourning for the year, Congress passed and the President signed into law the fiscal year ("FY") 2020 National Defense Authorization Act ("NDAA"), which included several substantial cybersecurity provisions:

- Energy Sector Cybersecurity: Text of S. 174 / H.R. 680, the "Securing Infrastructure Act," legislation introduced by Senator Angus King (I-ME) and Congressman Dutch Ruppersberger (D-MD), establishes a pilot program within the Department of Energy's ("DOE") national laboratories that will identify security vulnerabilities in the energy sector and evaluate the feasibility of technology that may be utilized to isolate the country's most critical systems to protect them from cyberattacks.

- Department of Defense ("DOD") Supply Chain Concerns: The bill stipulates that the DOD must consider cybersecurity risks in making purchasing decisions, and can no longer solely rely on cost, schedule and performance as criteria. It also requires the agency to report to Congress on its acquisition decision making process as well as any changes to that process.

- Extension of Cyberspace Solarium Commission Recommendation Deadline: The bill extends the deadline for recommendations from the Cyberspace Solarium Commission, which was initially authorized in the FY 2019 NDAA. Additional information on the Commission is included below.

- Huawei Restrictions: The bill includes a provision to prevent the removal of Huawei, a Chinese telecommunications company, from a Commerce Department list that restricts the sale of U.S.-made components to the company.

Election cybersecurity was also a major area of focus over the past year. Stringent security measures were included in House Democrats' first major legislative initiative, H.R. 1, the "For the People Act". Those provisions were also passed independently as a part of H.R. 4617, the "Stopping Harmful Interference in Elections for a Lasting Democracy (SHIELD) Act". While these measures were not taken up by the Senate in 2019, Congress appropriated $425 million in election security funding for states in omnibus spending legislation enacted at the end of the year.

2020 Look Ahead

Cybersecurity remains a top priority for Congress, particularly given concerns surrounding foreign interference in the upcoming Presidential election and heightened tensions with Iran that are refocusing the spotlight on potential cybersecurity vulnerabilities across critical infrastructure. A brief overview of potential cybersecurity measures that could be considered by Congress in 2020 are as follows:

Energy. The Senate Energy and Natural Resources Committee, led by Chairman Lisa Murkowski (R-AK), is set to consider a broad legislative package in the first half of 2020 focused on providing federal research and development support to various energy technologies. Chairman Murkowski is beginning her last year as the Chair of the Energy and Natural Resources Committee and has expressed a strong desire to pass comprehensive energy legislation before she relinquishes her gavel at the end of 2020. The Committee has already reported the following cybersecurity legislation that may be included in the package:

- S. 2556, the Protecting Resources on the Electric grid with Cybersecurity Technology (PROTECT) Act. This bill would direct the Federal Energy Regulatory Commission ("FERC") to issue a rulemaking on rate incentives for advanced cybersecurity technologies and establish a DOE grant program to assist public utilities with deployment of advanced cybersecurity technologies.

- S. 2094, the Enhancing State Energy Security Planning and Emergency Preparedness Act of 2019. This bill would authorize the DOE to provide financial assistance to states for the development, implementation, review, and revision of state energy security plans.

- S. 2095, the Enhancing Grid Security through Public-Private Partnerships Act, which would create a program within DOE to consult with states, industry, and other stakeholders to promote physical and cybersecurity of electric utilities.

- S. 2333, the Energy Cybersecurity Act of 2019. This bill would direct the DOE to develop advanced cybersecurity applications and technologies for the energy sector.

Privacy. Partially driven by the enactment of California's Consumer Privacy Act ("CCPA"), Senate Commerce, Science, and Transportation Committee Chairman Roger Wicker (R-MS) and Ranking Member Maria Cantwell (D-WA) introduced separate legislation in 2019 to drive federal policy on data privacy. Both proposals would preempt at least some state laws on data privacy and security, but the proposals diverge on other key issues. State legislation like the CCPA has instilled a sense of urgency within both parties and both houses of Congress to enact legislation at the federal level, and the Commerce Committee is likely to seek a compromise bill in 2020. The House is also responding to this perceived urgency for federal action and, with 34 co-sponsors, is considering H.R. 2013 entitled "Information Transparency & Personal Data Control Act."

DHS Subpoena Power. The Senate Homeland Security and Governmental Affairs Committee will consider legislation introduced by Chairman Ron Johnson (R-WI) and Senator Maggie Hassan (D-NH) that would grant the Cybersecurity and Infrastructure Security Agency ("CISA") subpoena power to obtain internet service provider ("ISP") information related to critical infrastructure threats, a major legislative priority for CISA. This is largely in response to ongoing disagreements between the federal government and technology companies about how to handle encrypted information when conducting investigations into cyber-related activity.

Cyberspace Solarium Commission Recommendations. As noted above, the FY 2019 NDAA authorized the creation of the Cyberspace Solarium Commission and tasked it with developing a comprehensive national strategy for cybersecurity. The Commission is co-chaired by Senator Angus King (I-ME) and Congressman Mike Gallagher (R-WI) and includes additional Members of Congress along with current and former national security officials. The FY 2020 NDAA extended the deadline for the Commission's recommendations to April 30, and those recommendations are expected to be included in the FY 2021 NDAA. Senator King and Congressman Gallagher have welcomed public input to inform the group's recommendations, which are expected to affect a wide range of critical infrastructure areas and determine the role of both the public and private sectors in defending critical and information infrastructure.

This document has been prepared by Van Ness Feldman for informational purposes only and is not a legal opinion, does not provide legal advice for any purpose, and neither creates nor constitutes evidence of an attorney-client relationship.

Energy Sector

Contributors: Darsh Singh and Ani Esenyan

Electric Subsector

2019 Developments

As cyber threat vectors and bad actors continue to evolve and become increasingly sophisticated, the risk to the electric grid continues to be a threat to the country's national security. In March 2019 there was, what experts are calling, an "unprecedented" attack on the U.S. electric grid when grid operators in the western region of the United States experienced a "denial-of-service" cyber-attack. During this attack, hackers used firewall vulnerabilities to cause periodic "blind spots" for grid operators for a period of ten hours. While the flow of electricity was not ultimately impacted, this event led to broader concerns over the security of the U.S. electric grid. Multiple federal agencies have taken steps to bolster cybersecurity in the electric sector—this section summarizes some of those agency actions.

In August 2019, FERC Staff teamed up with North American Electric Reliability Corporation ("NERC") Staff to issue a joint whitepaper ("Whitepaper") proposing added transparency to NERC's Notice of Penalty ("NOP") process, particularly with respect to violations relating to Critical Infrastructure Protection ("CIP") reliability standards. This effort was triggered by the influx in Freedom of Information Act ("FOIA") requests for non-public information contained in NOP CIP violations from parties seeking additional information about the nature of cybersecurity violation(s). The Whitepaper proposed that NERC would submit a public cover letter with each NOP that discloses the name of the violator, the standards violated, and the amount of the penalty. Further, NOPs would also have non-public attachments that would detail the nature of the violation, mitigation activity, and potential vulnerabilities to cyber systems. FERC and NERC assert that the added transparency would provide the public with helpful information that will ultimately better protect the electric grid. By the end of October, multiple parties had submitted comments on the Whitepaper. As of the date of this publication, FERC has not yet taken action.

In June 2019 DOE published Version 2.0 of its Cybersecurity Capability Maturity Model ("C2M2"), which had not been updated since the issuance of Version 1.0 in 2014. C2M2 Version 2.0 adjusts for new technologies, practices, and environmental factors and better aligns model domains and functional questions with internationally recognized cyber standards and best practices, including the National Institute of Standards and Technology ("NIST") Cybersecurity Framework Version 1.1 released in April 2018. The C2M2 is a tool that organizations can use to evaluate their cybersecurity capabilities, enable organizations to prioritize actions and investments to improve cybersecurity and provide a benchmark of self-evaluation. While the updated C2M2 boasts intended use by "any organization, regardless of ownership, structure, size or industry," the C2M2 was initially developed for the electricity sector and still appears to have an electric sector bias.

The U.S. Government Accountability Office ("GAO") expressed its concerns over the need to address cybersecurity risks facing the electric grid in a report in August 2019. In its report, the GAO assessed the extent to which the DOE has defined a strategy for addressing grid cybersecurity risks and analyzed the extent to which standards approved by FERC address grid cybersecurity risks. Ultimately, the GAO made one recommendation for DOE and two for FERC. The GAO advised DOE to develop a plan aimed at implementing the federal cybersecurity strategy for the grid and ensure that the plan addresses the key characteristics of a national strategy, including a full assessment of cybersecurity risks to the grid. The GAO advised FERC to consider adopting changes to its approved cybersecurity standards to more fully address the NIST Cybersecurity Framework and to evaluate the potential risk of a coordinated cyberattack on geographically distributed targets. Based on the results of that evaluation, GAO requested that FERC determine if changes are needed in the threshold for mandatory compliance with requirements in the full set of cybersecurity standards.

2020 Look Ahead

With multiple CIP standards coming into effect this year, NERC regulated utilities will be focusing significant resources on compliance in 2020 and beyond. The first compliance deadline occurs on April 1, 2020 with the implementation of CIP-003-8 (Security Management Controls), the purpose of which is to establish responsibility and accountability to protect bulk electric system ("BES") cyber systems against attack. Several other CIP Standards are effective July 1, 2020 including:

- CIP-005-6 (Electronic Security Perimeters). This CIP expands on requirements relating to the management of electronic access to BES cyber systems by specifying a controlled perimeter to protect BES cyber systems against attack. The incident reporting and response planning standard.

- CIP-010-3 (Configuration Change Management and Vulnerability Assessments). This CIP's primary purpose is to prevent and detect unauthorized changes to the BES cyber systems through the use of comprehensive assessments.

- CIP-013-1 (Supply Chain Risk Management). While all of the new CIP standards impose obligations on regulated entities, CIP-013-1 has some companies in the electric industry working overtime to meet the July 1st compliance deadline. The supply chain risk management standards are meant to mitigate cybersecurity risks to the BES cyber systems by heightening standards at each step of the supply chain. First, this standard requires responsible entities to develop one or more supply chain security risk management plans for high and medium impact BES cyber systems, and the standard outlines the requirements for these plans. Second, each responsible entity must implement the plan it creates. Third, each responsible entity must review and obtain a CIP Senior Manager's or delegate's approval of its supply chain cybersecurity risk management plans at least once every 15 calendar months. This standard has proven to be a "big push" for utilities with thousands of vendors as it requires utilities to coordinate with each of their vendors to comply with CIP-013-1's requirements and to assess the potential risks posed by each third-party vendor to the BES. As the deadline approaches, CIP-013-1's impact on utilities and their procurement strategies will continue to evolve throughout 2020 and in the years to come as NERC begins active enforcement of this standard.

Lastly, CIP-008-6 (Incident Reporting and Response Planning) becomes effective January 1, 2021. This CIP mitigates the risk to the reliable operation of the BES as a result of cyber incidents by specifying incident response requirements.

Natural Gas Subsector

2019 Developments

While there continues to be no mandatory regulatory regime to oversee pipeline cybersecurity, this lack of regulation was hotly contested in 2019 with pressure to create mandatory regulations coming from multiple directions. The Transportation Security Administration ("TSA") remains the primary federal entity responsible for pipeline cybersecurity, but the adequacy of the agency's Pipeline Security Guidelines has been questioned by legislators and other stakeholders. While the Pipeline Security Guidelines were updated in March 2018 to incorporate the critical infrastructure practices issued by NIST, several policymakers are questioning whether more needs to be done to strengthen this critical component of the energy sector.

According to the 2019 GAO report, the TSA's 2010 Pipeline Security and Incident Recovery Protocol Plan is outdated and therefore does not address changes in pipeline security threats and federal law and policy related to cybersecurity. Per the GAO, TSA's coordination of security-related efforts with agencies such as the Pipeline and Hazardous Materials Safety Administration ("PHMSA") and CISA is similarly outdated. While the Department of Homeland Security and PHMSA entered into a memorandum of understanding ("MOU") in 2006 which delineates each agency's roles and responsibilities in the area of pipeline security (including but not limited to cybersecurity), the GAO points out that the MOU has yet to be reevaluated by the agencies and fails to recognize the establishment and role of CISA. To add to the confusion, PHMSA's role in pipeline cybersecurity remains unclear. PHMSA is responsible for regulating the safety of hazardous materials transportation and the safety of pipeline systems, some aspects of which may relate to pipeline security and perhaps even cybersecurity. In March 2019 the Department of Transportation's ("DOT") Office of Inspector General announced an audit to assess PHMSA's "efforts to foster a positive safety culture." Whether the "positive safety culture" includes cybersecurity remains to be seen; the results from the audit have not yet been released. Regulators and lawmakers are concerned that these disjointed federal efforts related to natural gas pipeline security could mean that the cybersecurity of pipelines falls between the cracks.

In addition, over the past year, FERC Commissioners were very vocal about their pipeline cybersecurity concerns. In February 2019, FERC Chairman Neil Chatterjee testified before the Senate Committee on Energy and Natural Resources that more work is needed to improve the TSA's oversight of pipeline cybersecurity. During a June 2019 oversight hearing, Congress questioned whether the gas pipeline sector, like the power sector, should face mandatory federal cybersecurity regulations. Commissioner LaFleur and Commissioner Glick are on record encouraging the possibility, suggesting that "a structure with some teeth" would be helpful.

2020 Look Ahead

Although the pressure to establish pipeline cybersecurity regulations continues to mount, there has been no indication that a mandatory regulatory regime will be promulgated in the near future. With that said, a cyber-attack on the nation's pipeline infrastructure remains a significant threat to our country's national security and, as the interdependency between the electric sector and the natural gas sector continues to grow, so does the potential for a disruptive energy emergency. For now, the onus to maintain a robust cybersecurity program and effective self-assessments lies with the natural gas pipeline companies. The frameworks, guidance, and regulations relied upon by other industrial sectors are available tools to help govern decision making and resource allocation. NIST's Cybersecurity Framework remains the widely-acceptable baseline for building a cybersecurity program. In addition, the TSA and CISA's Pipeline Cybersecurity Initiative, established in 2018, remains a helpful resource to pipeline companies wishing to assess their cybersecurity vulnerability and risk. As pipeline operators modernize their systems and new technologies become increasingly integrated with industrial control systems, the need to partake in voluntary assessments of threats will continue to grow.

Water Sector

Contributors: T.C. Richmond and Jordan Smith

2019 Year in Review

Last year continued to be a year of risk recognition for the Water Sector. The American Water Works Association's ("AWWA") Cybersecurity Risk and Responsibility in the Water Sector Report details the issues facing business and critical infrastructure:

> *"A survey of more than 20,000 utility employees revealed that cyber threats are what they fear could have the biggest impact on operations, with a lack of resources and conflicting priorities as the greatest challenges. Water and Wastewater Sector entities have suffered a range of attacks, including from ransomware attacks, tampering with Industrial Control Systems, manipulating valve and flow operations and chemical treatment formulations, and other efforts to disrupt and potentially destroy operations."*

Attacks by ransomware, a type of malware that encrypts victims' computer files and demands online payment to unlock them, was apparent among water utilities. For example, Fort Collins-Loveland Water District was hit by ransomware in 2019, prompting the water district to switch out its information technology service provider and call in the FBI. The National Water Resources Association reported in August 2019 that 20 communities in Texas were struck in a coordinated ransomware attack prompting the distribution of recommendations for protections specific to the threat of ransomware by DHS Dams Sector Coordinating Council and the CISA.

The Water Information Sharing and Analysis Center (WaterISAC), the designated information sharing and operations arm of the federally managed Water Sector Coordinating Council and a consulting company reported in 2019 that state-linked adversaries probably considered the water supply sector to be a vulnerable social and economic pain point and that U.S. water utilities should expect reconnaissance activity by nation-states attempting to access and gain insights about them, adding that disruptive attacks by these entities are unlikely. This vulnerability prompted collaborations among water utilities that were otherwise unlikely to collaborate on basic operating functions. In 2019, at the urging of those peer groups, as well as the Environmental Protection Agency ("EPA"), water utilities began vigorous vulnerability self-assessments.

This document has been prepared by Van Ness Feldman for informational purposes only and is not a legal opinion, does not provide legal advice for any purpose, and neither creates nor constitutes evidence of an attorney-client relationship.

In June 2019, WaterISAC published *15 Steps to Keep Foes from Hacking and Hurting Our Water Infrastructure*. Those steps include:

- Perform Asset Inventories.
- Assess Risks.
- Minimize Control System Exposure.
- Enforce User Access Controls.
- Safeguard from Unauthorized Physical Access.
- Install Independent Cyber-Physical Safety Systems.
- Embrace Vulnerability Management.
- Create a Cybersecurity Culture.
- Develop and Enforce Cybersecurity Policies and Procedures (Governance).
- Implement Threat Detection and Monitoring.
- Plan for Incidents, Emergencies and Disasters.
- Tackle Insider Threats.
- Secure the Supply Chain.
- Address All Smart Devices (IoT, IIoT, Mobile, etc.).
- Participate in Information Sharing and Collaboration Communities.

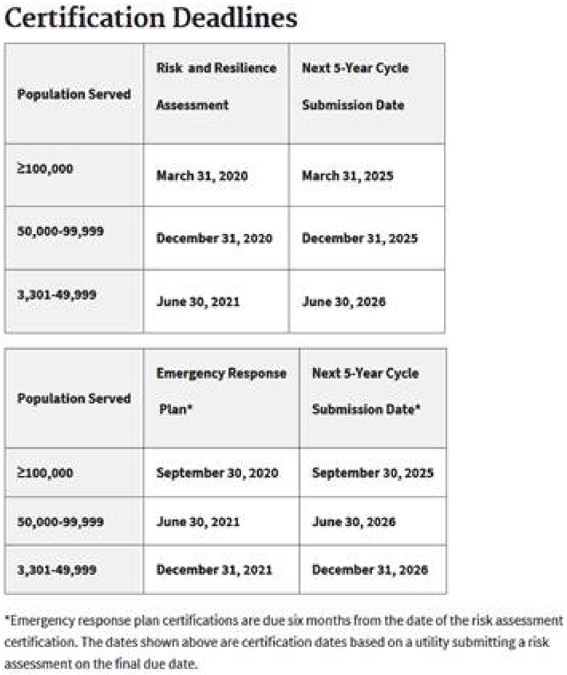
At the prompting of EPA, most drinking water utilities took the first step on self-risk assessment. Under America's Water Infrastructure Act ("AWIA") community water systems serving more than 3,300 people are required to develop or update risk and resilience assessments ("RRAs") and emergency response plans ("ERPs"). In 2019, EPA consulted with federal, state and local agencies and then provided baseline information on malevolent acts of relevance to utilities. Utilities then began assessments in order to be able to meet the EPA certification deadlines to conduct an RRA between March 31, 2020 and June 30, 2021 (based on size).

In 2019, EPA also initiated a cybersecurity steering committee of water industry experts to develop the capability to evaluate and test cybersecurity equipment for the protection of water system infrastructure. Experts from federal agencies and private companies representing water system operators, hydrant manufacturers, intrusion detection and water quality sensor manufacturers, and data management service providers began research to improve the cybersecurity of water utilities that will be carried out at the EPA Water Security Test Bed located at the Department of Energy Idaho National Laboratory.

2020 Look Ahead

As we look to this year, utilities must complete their RRAs under AWIA that are due between March 31, 2020 and June 30, 2021. Within 6 months after completion of their respective RRAs, each provider must prepare to revise its ERP to include:

- strategies and resources to improve the resilience of the system
- plans and procedures that can be implemented, and identification of equipment that can be utilized, in the event of a malevolent act or natural hazard
- actions, procedures, and equipment which can obviate or significantly lessen the impact of a malevolent act
- strategies that can be used to aid in the detection of malevolent acts or natural hazards that threaten the security or resilience of the system.



Certification Deadlines

Population Served	Risk and Resilience Assessment	Next 5-Year Cycle Submission Date
≥100,000	March 31, 2020	March 31, 2025
50,000-99,999	December 31, 2020	December 31, 2025
3,301-49,999	June 30, 2021	June 30, 2026

Population Served	Emergency Response Plan*	Next 5-Year Cycle Submission Date*
≥100,000	September 30, 2020	September 30, 2025
50,000-99,999	June 30, 2021	June 30, 2026
3,301-49,999	December 31, 2021	December 31, 2026

*Emergency response plan certifications are due six months from the date of the risk assessment certification. The dates shown above are certification dates based on a utility submitting a risk assessment on the final due date.

Lawmakers are currently developing the 2020 Water Resources Development Act ("WRDA"), biennial legislation authorizing Corps of Engineers' work on locks and dams, dredging and other water resources projects critical to the nation. The legislation, which is likely to be unveiled in the coming months and considered by Congress throughout the summer and fall, could offer opportunities to include provisions calling for studies or more comprehensive directives in response to potential or actual on cyber threats to the nation's water infrastructure.

Transportation - Autonomous Vehicles

Contributors: Tracy Tolk, Michael Weiner, and Scott Nuzum

2019 Developments

While previous expectations for imminent, widespread deployment of automated vehicles ("AVs") were recalibrated in 2019, Congress reopened opportunities for domestic deployment through the pursuit of legislation that would standardize the federal regulatory environment for AV design and testing. In the second half of 2019, the House Energy and Commerce Committee and the Senate Commerce, Science, and Transportation Committee launched a collaborative effort to solicit stakeholder input to inform such a bill, an effort that will extend into 2020 with the likely introduction of legislation.

The Department of Transportation ("DOT") did not issue new guidance on AV development in 2019, as expected (DOT's newest guidance was issued in January 2020 and is detailed below). However, there was federal agency action that may impact the development of new AV technologies. On December

12, the Federal Communications Commission ("FCC") voted in favor of a proposal that would promote Cellular Vehicle to Everything ("C-V2X") services, which allows vehicles to communicate with other vehicles, infrastructure, and pedestrians. C-V2X is thought to figure into how AVs of the future will communicate with their surroundings. The DOT, however, continues to oppose the FCC proposal because it directs some "spectrum" capability away from transportation safety services towards other uses like Wi-Fi. DOT claims this may interfere with existing transportation safety uses.

2020 Look Ahead

2020 provides an important opportunity for Congress and federal agencies to capitalize on several years of industry momentum and investment in AV technology development. Early signs indicate that these actors will move to ensure U.S. technology leadership on AVs, and there has already been one significant development for AVs in 2020.

On January 8, the DOT rolled out the fourth iteration of its voluntary guidance on AVs, entitled "Ensuring American Leadership in Automated Vehicle Technologies." The guidance attempts to promote a "one federal government" approach to AV regulation and continues giving technology developers and original equipment manufacturers a flexible system aimed to promote innovation. The guidance does not include any regulatory requirements and continues DOT's preference for voluntary safety self-assessments. With regard to cybersecurity, the guidance attempts to clarify the cybersecurity roles and responsibilities of each federal agency with respect to AV development, though it also makes clear that "emphasis for addressing cybersecurity ultimately must be with the industry."

Moreover, Congress will continue to work on its vision for AV regulation, which differs from the Administration's hands-off approach. The joint House and Senate Committee effort noted above will include mandatory safety requirements that are absent from DOT's voluntary guidance. Draft portions of the legislation, which have been shared with industry stakeholders, indicate that the legislation would allow for stricter government regulation of vehicle design, increase testing on public roads, preempt state laws on AV testing and deployment, and require protection in additional areas including data privacy and cybersecurity. There will be additional opportunities for interested stakeholders to provide input on the legislation before it is finalized, particularly as House and Senate Committee leadership seeks to identify opportunities to include a bill in legislative packages that may move in 2020.

Privacy & Data Security

Contributor: Scott Nuzum

2019 Developments

Many of the major privacy law stories to dominate 2018 remained important in 2019. The European Union General Data Protection Regulation ("GDPR") marked its first full year in effect with a string of enforcement actions levied by member states. In July 2019, the U.K. Information Commissioner's Office ("ICO") announced that it had levied a proposed $230 million fine on British Airways stemming from an incident that occurred between June and September 2018 which compromised the data of 500,000 customers. Also in July, the ICO announced that it had assessed Marriott a $123 million proposed penalty following a November 2018-reported incident that resulted in the loss of 339 million guest records. Both companies were provided with the opportunity to respond to the fines before the ICO issues a final decision, and both companies have agreed to an extension of the regulatory process until March 31, 2020.

In the United States, the CCPA dominated the privacy landscape. While many companies spent the past year preparing for the law (which went into effect on January 1, 2020), many companies also lobbied to amend the law, including the section 1798.140 definition of "personal information," which critics argued was overbroad, and section 1798.105, private right of action, which companies worried could lead to an endless cycle of lawsuits. Despite a flurry of activity in Sacramento, attempts to amend the CCPA ultimately fell short.

Many observers were surprised to see the California Attorney General issue proposed CCPA implementation regulations that established new requirements rather than simply clarifying vague provisions. Among other things, the proposed CCPA regulations—which were published on October 10, 2019–would establish additional requirements for the four types of consumer notices outlined in the law—the point of collection notice, the full privacy policy, the notice of right to opt-out of sale ("DNS Notice"), and the financial incentives notice. In addition, the draft CCPA regulations would expand upon the requirements for businesses handling consumer requests for access to their information, including procedures for verifying the requestor's identity. Further, the draft regulations would mandate both that businesses act on "Do Not Sell" requests within 15 days of receipt and inform and instruct all parties sold an individual's data in the prior 90 days to refrain from further sale of the data. The draft regulations also would prescribe that businesses provide two or more methods to submit access and deletion requests. While the regulations would permit businesses to choose a method for receiving deletion requests, one of the methods would need to reflect how the business primarily interacts with the consumer. Finally, the draft regulations would further require businesses to accept requests anywhere they receive them, either by processing the request as if it had been submitted appropriately or directing the user to the business' designated method for receiving requests. The CCPA draft regulations were open for public comment until December 6, 2019.

While there was widespread disappointment over Congress's lack of effort to enact a federal privacy law, the issue nevertheless remained important to many members. Members of Congress introduced no fewer than nine privacy-related bills, while relevant committees of jurisdiction held a number of high-profile hearings on the topic. As was the case last year, members are consumed with a range of other contentious subjects and may be in a position of only acting if state and international privacy frameworks prove to be excessively disruptive to U.S. constituents and interests.

Congress was not the only branch of government to consider privacy issues in 2019. Both the executive and judicial branches confronted the issue of privacy as well. The Trump administration went on the record in 2019 urging Congress to pass a comprehensive privacy law, with Federal Trade Commission chairperson Joseph Simons making the plea to Congress. Likewise, the judicial branch confronted significant privacy issues. Notably, in *Patel v. Facebook,* the U.S. Court of Appeals for the Ninth Circuit confronted issues arising out of the Illinois Biometric Privacy Act ("BIPA"), which requires users to provide informed opt-in consent prior to allowing a service to gather biometric information. BIPA also requires a company to destroy a person's biometric information once the purpose for data collection is satisfied, or within three years of the company's last contact with the person, whichever is sooner. BIPA includes a "private right of action," which enables individuals to file suit against companies that violate the statute. In *Patel*, users in Illinois challenged Facebook's "Tag Suggestions" feature, which utilizes facial recognition to suggest a tag for friends who appear in photos uploaded by users. In August, the Ninth Circuit ruled in favor of the *Patel* plaintiffs, finding that they had constitutional standing to sue Facebook for violating their statutory privacy rights under BIPA. Further, the Ninth Circuit articulated the significant privacy threats posed by Facebook's surveillance measures.

The Federal Trade Commission also had a busy 2019. In July, the Commission and Facebook reached a $5 billion settlement stemming from violations of a 2012 settlement order related to the company's deceptive statements about user privacy through its role in the Cambridge Analytica scandal, which violated the privacy rights of millions of Facebook users.

2020 Look Ahead

In 2020, we again expect the CCPA to dominate the headlines. While the law went into effect on January 1, 2020, companies are still awaiting promulgation of final regulations from the California Attorney General. The regulations—which are expected this spring—should provide companies with additional detail about how to provide notice to covered individuals, how to verify the identity of requesters, and how to respond to requests. While 2020 will also likely see companies continue to implement compliance procedures, we cannot rule out the state engaging in enforcement actions.

In addition CCPA compliance and enforcement, we expect other states to follow California's lead and enact privacy laws of their own. New York, Texas, Massachusetts, and New Jersey have all contemplated CCPA-like laws.

The privacy landscape will also grow more complicated internationally, in addition to GDPR compliance and enforcement, companies will also need to think about complying with the Brazilian General Data Protection Law, which goes into effect in February 2020. In addition to Brazil's privacy law, we also expect other countries to follow the European Union's example and enact their own privacy regimes.

Health Sector
Contributor: James Bayot

2019 Year in Review

In 2019, the Administration led much of the activity on healthcare-related cybersecurity issues, and the Food and Drug Administration ("FDA") began the year with a two-day workshop on medical device cybersecurity and the increasing use of wireless, Internet- and network-connected devices, and the frequent electronic exchange of medical device-related health information.

FDA followed up on its workshop with new guidance that clarifies which products are regulated as medical devices and are subject to the agency's regulations and oversight, including cybersecurity requirements.

In March, the Office of the National Coordinator for Health Information Technology ("ONC") issued a significant proposed rule for the healthcare sector titled "21st Century Cures Act: Interoperability, Information Blocking, and the ONC Health IT Certification Program," which includes requirements on sharing cybersecurity threats and incidents with government agencies.

Over the years, both Congress and the Administration have considered changes to the Stark Law and Anti-Kickback Statute, which prohibits specific physician self-referrals and financial arrangements so as to prevent fraud and abuse in Medicare and Medicaid. This past October, the Department of Health and Human Services ("HHS") issued proposed rules to modernize and clarify the regulations to provide greater certainty for healthcare providers participating in value-based arrangements and providing coordinated care for patients. Most importantly, among the many proposed changes, the rules would allow health providers and hospitals to receive cybersecurity assistance and free software to bolster security.

In the Legislative Branch, Senator Mark Warner (D-VA), the co-chair of the Senate Cybersecurity Caucus, sent two letters to healthcare stakeholders and the federal agencies to seek input on ways to best improve cybersecurity in the healthcare industry. In the letters, Senator Warner pointed to apparent gaps in oversight, expressed concern about the impact of cyber-attacks on the healthcare sector, and conveyed his desire to work with stakeholders to develop strategies that strengthen information security.

2020 Look Ahead

The Administration is in the process of reviewing the comments to the proposed rules discussed above on the Stark Law, Anti-Kickback Statute, and the 21st Century Cures Act. The agencies are expected to finalize the rules this year which could mean new obligations and funding opportunities for entities within the healthcare sector.

The healthcare sector continues to wait for HHS to release a proposed rule to update the Health Insurance Portability and Accountability Act (HIPAA), which specifies protections for healthcare information.

With the upcoming Presidential and Congressional elections in November, the window for legislative action will be severely shortened, and the two main committees with jurisdiction over cybersecurity issues – the House Energy & Commerce Committee and the Senate Commerce, Science, and Transportation Committee – will continue to consider various proposals to address cyber threats.

Chemical Facilities

Contributors: Gwen Keyes Fleming

2019 Year in Review

Facilities that possess large quantities of chemicals that can be exploited or commandeered by terrorists, either through physical or cyberattacks on industrial control systems monitoring and governing the levels of chemicals of interest, continue to be a top concern for the Department of Homeland Security and the Cybersecurity Infrastructure Security Agency ("CISA"). Although not exclusively related to cybersecurity, in July CISA published a Federal Register Notice to fully implement

This document has been prepared by Van Ness Feldman for informational purposes only and is not a legal opinion, does not provide legal advice for any purpose, and neither creates nor constitutes evidence of an attorney-client relationship.

the Chemical Facilities Anti-Terrorism Standard Act ("CFATS") Personnel Surety Program ("PSP") requiring all covered facilities to perform background checks on facility personnel and unescorted visitors to identify terrorist ties. Companies have four options for compliance with this regulation including verifying an individual's Transportation Worker Identification Credentials ("TWIC") or submitting identifying information directly to CISA for the agency to compare the information to terrorist watch lists and databases.

On the legislative front, the House reported H.R. 3256 out of the Homeland Security Committee in December 2019 which included additional training for CISA cyber investigators who assess compliance Risk-Based Performance Standards ("RBPS") 8 – Cybersecurity among its many provisions.

2020 Look Ahead

Recent geopolitical tensions with Iran and the potential for retaliatory aggression against the U.S. prompted the agency to issue a pair of National Terrorism Advisory System ("NTAS") Bulletins in the first weeks of 2020 advising chemical companies that, while the heightened security measures outlined in RBPS 13 and 14 were not required, companies should maintain a heightened level of awareness. CISA also recommended several other initiatives to bolster cybersecurity including backing up systems, reviewing site security plans, and reporting any cyber incidents to the agency.

The chemical industry may also experience a bit of *déjà vu* in the first quarter of 2020 as the federal government considers the reauthorization of CFATS which is set to expire in April 2020. The President signed a 15 month extension hours before CFATS was due to expire in January 2019 and given that there is no Senate companion to H.R. 3256 at the time of this publication, chances are Congress, the Administration and stakeholders will once again scramble to try to avoid a lapse in authorization.