cybersecurity-and-the-maryland-electric-grid (1).p
Uploaded by: Katie Fry Hester
Position: FAV

CYBERSECURITY AND THE MARYLAND ELECTRIC GRID

Findings and Recommendations for the Office of the Attorney General and the Maryland Cybersecurity Council

December 2021

Abstract

This report offers findings and cybersecurity policy recommendations for electric distribution systems in Maryland, with an emphasis on the regulated electric distribution systems. Examples of actions taken by other states are also included. The recommendations provided in this paper are tailored to the electricity sector, but may be useful to other sectors of critical infrastructure as well.

Corcoran, Laura
lcorcoran@oag.state.md.us

Contents

Cybersecurity and The Maryland Electric Grid[1]

This paper provides cybersecurity policy recommendations for electric distribution systems in Maryland, with an emphasis on the regulated electric distribution systems. Although there are many forms of critical infrastructure, including financial services, communications, healthcare, and water systems, these all rely on the electric grid for operation. Therefore, damage, disruption, or unauthorized access to the electric grid can disrupt the reliable operation of other critical infrastructure assets. The recommendations provided in this paper are tailored to the electricity sector, but may be useful to other sectors of critical infrastructure as well.

The electric grid is currently undergoing a dramatic transformation which has massive cybersecurity implications. New technology is being connected to the grid, combining legacy systems and smart grid components, but technical standards for interconnection and cybersecurity are still in development. Legislation and regulations are emerging at the state and federal levels to address smart grid development. However, cybersecurity advancements are not often integrated with these efforts.

The policy recommendations made here are based on research and interviews with electric grid cybersecurity stakeholders. Legislative and regulatory actions, academic and technical reports, published standards and best practices, and news media reporting provided a foundation. Interviews were conducted with members of various state agencies, including the Maryland Public Service Commission (MPSC), Maryland Energy Administration (MEA), and Maryland Department of Emergency Management. Public Utility Commissions in other states were also contacted. Subject matter experts from non-government entities such as the Institute of Electrical and Electronics Engineers (IEEE) and Auburn University McCrary Institute provided additional insights.

Some of the recommendations in this paper may be implemented by utilities currently. The cybersecurity posture and practices of utilities are not made public. Detailed information about regulator preparations for cybersecurity reporting also were not accessible. A complete picture of the current state of cybersecurity for the electric grid was not available to the author. The recommendations made are based on best practices and standards, but do not necessarily address an existing shortcoming of current practices.

Climate Change and the Evolving Electric Grid

How problems are perceived combined with power dynamics can be strong indicators of which problems will be addressed.[2] Let's compare climate change to cybersecurity.

[1] This report was authored by Laura Corcoran, an NSA Fellow, who served for twelve months in the Office of the Maryland Attorney General. She completed the report in fulfillment of her Fellowship's scope of work. The report was conducted for both the Office of the Attorney General and the Maryland Cybersecurity Council. The findings and recommendations were briefed to the Council's Subcommittee on Critical Infrastructure and then to the full Council. The Office of the Attorney General is extremely grateful to the NSA for approving Ms. Corcoran's fellowship with its office and for the excellent report that she produced.

[2] "Encouraging Employee Engagement With Cybersecurity: How to Tackle Cyber Fatigue", A. Reeves, P. Delfabbro, D. Calic, SAGE Journals, March 10, 2021. https://doi.org/10.1177/21582440211000049

Climate change is perceived by the majority of Americans as an existential threat.[3] Corporate lobbying efforts are well funded. "With massive economic interests at stake with each regulation aimed at curbing climate change, it comes as no surprise that vast sums are spent to petition government about them. For example, one of the greenest utilities in the nation, Pacific Gas and Electric (PG&E) spent the second highest amount (an estimated $27 million) of all firms lobbying on climate change in 2008 — just behind ExxonMobil, which spent $29 million lobbying and produces an estimated 306 million tons of [greenhouse gas] emissions."[4]

Maryland has several state entities focused on addressing climate change, including the Department of the Environment, Department of Natural Resources, and the Maryland Energy Administration.[5] There are state funds available to encourage climate change programs, such as the Maryland Strategic Energy Investment Fund which received $47 million in the 2020 Maryland Budget.[6,7] Recently $93 million in federal funding was provided by the Federal Emergency Management Agency (FEMA) to strengthen Maryland's ability to prevent and respond to climate change related natural disasters.[8]

On the other hand, cybersecurity is perceived by many as a "technical issue" as opposed to an existential threat. A review of twelve publicly traded security firms showed a combined nationwide total of $3.29 million in lobbying spending in 2019.[9]

Maryland has an Office of Security Management within the Department of Information Technology that oversees security for the executive branch of state government entities only.[10] The Maryland Cybersecurity Investment Fund received $0.9 million in 2020.[11,12]

---

[3] "How Americans see climate change and the environment in 7 charts", Cary Funk, Brian Kennedy, Pew Research Center, April 21, 2020. https://www.pewresearch.org/fact-tank/2020/04/21/how-americans-see-climate-change-and-the-environment-in-7-charts/

[4] "Research: Who's Lobbying Congress on Climate Change", Magali Delmas, Harvard Business Review, October 27, 2016. https://hbr.org/2016/10/research-whos-lobbying-congress-on-climate-change

[5] See e.g. "Climate Change Program", https://mde.maryland.gov/programs/Air/ClimateChange/Pages/index.aspx, "Strategic Energy Investment Fund Powers Valuable State Energy Programs Supporting Clean Energy Advancement and Greenhouse Gas Reduction", February 24, 2021 https://news.maryland.gov/mea/2021/02/24/maryland-energy-administration-data-points/.

[6] MD Code, State Government, § 9-20B-05. Maryland Strategic Energy Investment Fund, Effective: July 1, 2021.

[7] "Maryland Budget Highlights Fiscal Year 2020", Lawrence J. Hogan jr., Governor, Boyd K. Rutherford, LT. Governor, January 18, 2019. https://dbm.maryland.gov/budget/Documents/operbudget/2020/proposed/FY2020-BudgetHighlights-WebFinal.pdf

[8] "MARYLAND DELEGATION ANNOUNCES $93 MILLION TO FIGHT CLIMATE CHANGE AS LANDMARK REPORT WARNS OF DEVASTATING GLOBAL IMPACTS", Office of Chris Van Hollen, August 11, 2021. https://www.vanhollen.senate.gov/news/press-releases/maryland-delegation-announces-93-million-to-fight-climate-change-as-landmark-report-warns-of-devastating-global-impacts

[9] "Cybersecurity Lobbying Spending Mounts as Privacy, Security Laws Take Shape", James Rundle, David Uberti, Wall Street Journal, May 4, 2020. https://www.wsj.com/articles/cybersecurity-lobbying-spending-mounts-as-privacy-security-laws-take-shape-11588619239

[10] COMAR 01.01.2019.07 Maryland Cyber Defense Initiative.

[11] MD Code, Economic Development, § 10-464. Cybersecurity Investment Fund. Effective: October 1, 2020.

[12] "Maryland Budget Highlights Fiscal Year 2020", Lawrence J. Hogan jr., Governor, Boyd K. Rutherford, LT. Governor, January 18, 2019. https://dbm.maryland.gov/budget/Documents/operbudget/2020/proposed/FY2020-BudgetHighlights-WebFinal.pdf

This contrast of perceptions and power dynamic between climate change and cybersecurity is stark. Yet climate change and cybersecurity are intimately connected when it comes to the electric grid. The electric grid is changing from a relatively closed system to a complex, highly interconnected environment.[13] A main driver for this transformation: climate change.[14]

To address climate change, the electric grid is modernizing to allow for two-way communications with distributed energy resources (DER) such as solar farms, battery storage, electric vehicle charging stations, and microgrids, as well as monitoring and control systems. These changes to the grid are undertaken to enable adoption and implementation of climate change mitigation policies.

Who oversees this transformation? As a general rule, the federal government regulates the generation and transmission of electricity, whereas the distribution systems are regulated primarily by states.[15] Electricity distribution systems are "growing more vulnerable, in part because their industrial control systems increasingly allow remote access and connect to business networks. As a result, threat actors can use multiple techniques to access those systems and potentially disrupt operations."[16]

"As the lead federal agency for the energy sector, the Department of Energy (DOE) has developed plans to implement the national cybersecurity strategy for the grid, but these plans do not fully address risks to the grid's distribution systems."[17] DOE plans prioritized addressing risks to the grid's generation and transmission systems.[18] Since states are responsible for cybersecurity of distribution systems, prioritizing federal support to states and industry to improve grid distribution systems' cybersecurity likely will require additional planning by DOE.[19]

There are important aspects of grid security that are not controlled by the federal government, but are left to the states. Each state has a regulatory body that oversees electric distribution operations. In Maryland, the Public Service Commission is the regulatory authority for the utility companies. In 2016 the MPSC opened a docket to address certain issues of electric grid modernization.[20] Technologies to be addressed included advanced metering infrastructure, electric vehicles, distributed energy resources such as solar and wind, and energy storage.

---

[13] Guidelines for Smart Grid Cybersecurity Volume 1 - Smart Grid Cybersecurity Strategy, Architecture, and High-Level Requirements. NISTIR 7628 Revision 1 (2018). http://dx.doi.org/10.6028/NIST.IR.7628r1

[14] There are others as well, including protecting the ecological environment and guaranteeing the energy supply.

[15] "Federal/State Jurisdictional Split: Implications for Emerging Electricity Technologies", Jeffery S. Dennis, Suedeen G. Kelly, Robert R. Nordhaus, and Douglas W. Smith, Energy Analysis and Environmental Impacts Division Lawrence Berkeley National Laboratory, December 2016. https://www.energy.gov/sites/prod/files/2017/01/f34/Federal%20State%20Jurisdictional%20Split--Implications%20for%20Emerging%20Electricity%20Technologies.pdf

[16] "ELECTRICITY GRID CYBERSECURITY DOE Needs to Ensure Its Plans Fully Address Risks to Distribution Systems", Report to Congressional Requesters by the United States Government Accountability Office, March 2021. https://www.gao.gov/assets/gao-21-81.pdf

[17] Ibid.

[18] Ibid.

[19] Ibid.

[20] "IN THE MATTER OF TRANSFORMING MARYLAND'S ELECTRIC DISTRIBUTION SYSTEMS TO ENSURE THAT ELECTRIC SERVICE IS CUSTOMER-CENTERED, AFFORDABLE, RELIABLE AND ENVIRONMENTALLY SUSTAINABLE IN MARYLAND", PC44, filed September 26, 2016.

The MPSC describes Maryland's clean energy goals as ambitious.[21] Maryland has been recognized for its efforts in grid modernization.[22] Maryland state officials have taken a leading role in setting grid modernization policy.[23] Likewise, cybersecurity goals for Maryland's electric grid should be equally ambitious and Maryland should hold a leading role in setting grid cybersecurity policy. This will require policymakers and regulators to embrace the intimate relationship between climate change, grid modernization, and cybersecurity risk management.

Cybersecurity Challenges of Utilities Serving Maryland

The cooperation and coordination challenges involved in minimizing the security risks of the modernized electric grid have many similarities to the governance of climate change. "Both are 'superwicked' problems that are transboundary in nature, occur at multiple levels across sectors, between institutions, and will impact all actors, both public and private, in complex, interconnected, and often highly politicized ways."[24]

A variety of cybersecurity barriers exist with respect to the electric grid.[25] For example, cyber threats are unpredictable and evolve faster than the industry's ability to develop and deploy countermeasures. Security upgrades to legacy systems are constrained by inherent limitations of the equipment and architectures. Performance/acceptance testing of new control and communication solutions is difficult without disrupting operations. Threat, vulnerability, incident, and mitigation information sharing is insufficient among government and industry. Pre-incident, the business case for cybersecurity investment by industry seems weak. Regulatory uncertainty for cybersecurity of emerging technology exists. The adversaries that target the electric grid are advanced persistent threats.[26]

The stakes for protecting the grid are extremely high. According to President Biden, "It's more than likely we're going to end up, if we end up in a war - a real shooting war with a major power - it's going to be as

[21] "Maryland PSC Statement on FERC Ruling on PJM Capacity Resource Market", Maryland Public Service Commission, December 20, 2019. https://www.psc.state.md.us/wp-content/uploads/MD-PSC-statement-on-FERC-MOPR-decision_12202019.pdf

[22] See e.g. "Grid Modernization Index 2018: Key Indicators for a Changing Electric Grid", Gridwise Alliance, December 5, 2018. https://gridwise.org/grid-modernization-index-2018/

[23] For example, MPSC is an active member of the National Association of Regulatory Utility Commissioners (NARUC) and The Hon. Anthony O'Donnell has served as a panelist on Electric Vehicle Charging Infrastructure for the NARUC 2019 Winter Policy Summit. Dr. Mary Beth Tung, the Director of the Maryland Energy Administration is a Board Member for the National Association of State Energy Officials (NASEO). https://www.naseo.org/board (last accessed September 21, 2021). See also "Maryland Announces Plan for Electric Grid of the Future", February 11, 2021 https://news.maryland.gov/mea/2021/02/11/maryland-announces-plan-for-electric-grid-of-the-future/

[24] "Internet of Things, cybersecurity and governing wicked problems: learning from climate change governance", Madeline Carr, Feja Lesniewska, International Relations 2020, Vol. 34(3) 391–412, University College London, 2020. https://journals.sagepub.com/doi/10.1177/0047117820948247

[25] "Roadmap for Photovoltaic Cyber Security", Jay Johnson, SANDIA REPORT SAND2017-13262, Unlimited Release, Printed December 2017. http://sunspec.org/wp-content/uploads/2017/08/RoadmapforPhotovoltaicCyberSecurity-DraftforReview.pdf.

[26] "An adversary that possesses sophisticated levels of expertise and significant resources which allow it to create opportunities to achieve its objectives by using multiple attack vectors, including cyber, physical, and deception." Security and Privacy Controls for Information Systems and Organizations, NIST Special Publication 800-53 Revision 5, September 2020. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf.

a consequence of a cyber breach of great consequence, and [our adversaries' capabilities are] increasing exponentially."[27]

The process of modernizing the grid is ongoing. "The very nature of Grid Modernization dictates that there isn't an end state where we celebrate our final successes and catalog accomplishments for posterity's sake. In reality, we're developing systems that will require input and management for generations to come."[28]

Perhaps the greatest barrier to grid cybersecurity is due to a lack of resources. Cost-effectiveness is a statutory requirement placed on utilities regulated by the Maryland Public Service Commission.[29] However, methods for measuring the effectiveness of cyber security investments are evolving. "Currently, significant uncertainty surrounds cyber security investments."[30] The relationship between investment in countermeasures verses increased costs due to cyber-attacks has not been definitively characterized. "Anecdotal evidence and cybersecurity practitioners point out that an inadequate level of cybersecurity exposes entities to a higher risk of a successful attack and higher costs."[31] Although recent publications addressing theoretical aspects of cybersecurity investment decision-making are available, empirical literature is at an early stage, likely because of data scarcity.[32]

Human resources are also in scarce supply. "In the United States, there are around 879,000 cybersecurity professionals in the workforce and an unfilled need for another 359,000 workers, according to a 2020 survey by (ISC)2, an international nonprofit that offers cybersecurity training and certification programs. The US Bureau of Labor Statistics projects 'information security analyst' will be the 10th fastest growing occupation over the next decade, with an employment growth rate of 31% compared to the 4% average growth rate for all occupations."[33]

All of these challenges increase the complexity of building, maintaining, and regulating the grid. This report will make recommendations for legislators and regulators to address some of these challenges.

---

[27] Quoting President Biden during a half-hour speech while visiting the Office of the Director of National Intelligence (ODNI). "Biden: If U.S. has 'real shooting war' it could be result of cyber attacks". Nandita Bose, July 28, 2021. https://www.reuters.com/world/biden-warns-cyber-attacks-could-lead-a-real-shooting-war-2021-07-27/

[28] Private LTE as Communications for Grid Modernization. Ryan Gerbrandt, May 26, 2021. https://energycentral.com/c/gr/grid-modernization

[29] "It is the goal of the State that each electric company provide its customers with high levels of service quality and reliability in a cost-effective manner, as measured by objective and verifiable standards, and that each electric company be held accountable if it fails to deliver reliable service according to those standards." Md. Code Ann., Pub. Util. § 7-213.

[30] "Risk in Cyber Systems", Marshall Kuypers, Elisabeth Paté-Cornell, Stanford Center for International Security and Cooperation. https://cisac.fsi.stanford.edu/publication/risk-cyber-systems.

[31] "Dangerous games: A literature review on cybersecurity investments", Alessandro Fedele, Cristian Roner, Journal of Economic Surveys. 26 July 2021. https://doi.org/10.1111/joes.12456

[32] Ibid.

[33] "Wanted: Millions of cybersecurity pros. Salary: Whatever you want", Clare Duffy, May 28, 2021. https://www.cnn.com/2021/05/28/tech/cybersecurity-labor-shortage/index.html

Recommendations

The following sections provide recommendations that can be implemented by state officials. Some are legislative actions, others are regulatory recommendations, and a number can be implemented at the agency level.

Regulatory Goals

The entity that regulates electric companies in Maryland is the Public Service Commission.[34] Maryland has set forth a goal in statute "that each electric company provide its customers with high levels of service quality and reliability in a cost-effective manner, as measured by objective and verifiable standards, and that each electric company be held accountable if it fails to deliver reliable service according to those standards."[35] The statute includes six specific topics to be addressed by the standards and allows for "a separate reliability standard for each electric company in order to account for system reliability differentiating factors." There should be a clear mandate for cyber resiliency as a regulatory goal.

RECOMMENDATION 1. Amend Md. Code Ann., Pub. Util. § 7-213(e)(1)(i) "Service quality and reliability standards" to include "cyber resiliency" in the list of topics to be addressed by the standards.

Objective and verifiable standards are the key to measuring reliability.[36] Grid reliability grid is accomplished through resiliency – the ability to withstand certain types of failure and yet remain functional from the customer perspective. In particular, *cyber resiliency* is the ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on cyber resources.[37]

Maryland law has addressed resiliency in the context of climate change. "'Resilience infrastructure' means infrastructure that mitigates the effects of climate change. 'Resilience infrastructure' includes flood barriers, green spaces, building elevation, and stormwater infrastructure."[38] There is one statute within the Maryland Public Utilities Code that mentions "resiliency": the Energy Storage Pilot Program.[39] It requires investor-owned utility companies participating in the pilot program to report on resiliency benefits, but not risks. In fact, "benefit" appears ten times in the statute, "risk" is not mentioned at all.[40]

[34] MD Code, Public Utilities, § 2-101. Public Service Commission. Effective: October 1, 2020; MD Code, Public Utilities, § 2-112. Jurisdiction and powers of Commission. Effective: May 8, 2020.
[35] Md. Code Ann., Pub. Util. § 7-213 Service quality and reliability standards
[36] Ibid.
[37] "Cyber Resiliency Design Principles", Deborah Bodeau, Richard Graubart, MITRE Technical Report, January 2017.
[38] Md. Code Ann., Local Gov't § 22-101 Definitions.
[39] Md. Code Ann., Pub. Util. § 7-216. Energy Storage Pilot Program. Effective: June 1, 2019.
[40] Bulk Energy Storage Systems can pose a significant fire and explosion hazard. See e.g. "The Arizona Battery Explosion Is Changing Conventional Wisdom on Safety", Julian Spector, October 10, 2019. https://www.greentechmedia.com/articles/read/arizona-battery-explosion-conventional-wisdom-safety; "Protecting Battery Energy Storage Systems from Fire and Explosion Hazards", https://www.powermag.com/protecting-battery-energy-storage-systems-from-fire-and-explosion-hazards/.

RECOMMENDATION 2. Climate change is a long-term problem that motivates modernization of the electric grid. Solutions to address climate change must not invite near-term catastrophe. Any changes to the grid made for the sake of resiliency, efficiency, conservation, or climate change concerns must be accompanied by a careful assessment to document security risks prior to grid integration and implement appropriate mitigations during integration. The risk assessments must take into account the scope of specific projects and the project's interfaces with other systems.

The "Resilient Maryland Program" managed by the Maryland Energy Administration (MEA) does not include any cybersecurity requirement for the microgrid grant.[41] The current statutory definition of "resilience infrastructure" focuses on climate change. Increased vulnerability of the electric grid from cyber threats is an effect of climate change. Any programs that involve software or hardware connections to the grid must address cyber resilience.

RECOMMENDATION 3. Define "resilience" to include "the ability to prepare for and adapt to changing conditions and withstand and recover rapidly from deliberate attacks" so that cybersecurity will be an essential factor in determining system resilience.

Other states have defined "resilience" in ways that include grid modernization and cybersecurity issues. For example, Connecticut law includes "deliberate attacks" in their definition:

> "'Resilience' means the ability to prepare for and adapt to changing conditions and withstand and recover rapidly from deliberate attacks, accidents or naturally occurring threats or incidents, including, but not limited to, threats or incidents associated with the impacts of climate change."[42]

Illinois definition of "Resiliency improvement" goes beyond the environmental infrastructure and includes grid modernization components:

> "Resilient improvement" means any fixture, product, system, equipment, device, material, or interacting group thereof intended to increase resilience or improve the durability of infrastructure, including but not limited to, … energy storage, microgrids, and backup power generation."[43]

Taking cybersecurity issues into consideration when adopting statutory definitions will elevate cybersecurity priority. Additional definitions will be recommended in the following sections.

Building Cyber Resiliency

The path to cyber resiliency is paved with cybersecurity best practices and standards compliance. Cyber resiliency design principles should be applied to enhance the security of the grid. Cyber resiliency design

[41] A review of application materials and announcements for the program reveals no information concerning cybersecurity requirements. Interviews with the Maryland Energy Administration confirmed the lack of cybersecurity requirements. See https://energy.maryland.gov/business/pages/ResilientMaryland.aspx.
[42] C.G.S.A. § 16-244aa. Performance-based regulation of electric distribution companies. Effective: October 2, 2020. Also C.G.S.A. § 16-243y. Microgrid and resilience grant and loan pilot program to support distributed energy generation for critical facilities. Effective: October 2, 2020
[43] 50 ILCS 50/5 Definitions. Effective July 29, 2019.

strategies incorporate the assumption that compromised resources exist in the system.[44] The concept of zero-trust architecture has emerged in response to this assumption. "Zero-trust is a cybersecurity paradigm focused on resource protection and the premise that trust is never granted implicitly but must be continually evaluated."[45]

RECOMMENDATION 4. Require utility providers to adopt security best practices such as the NIST Cybersecurity Framework and advance toward zero-trust architecture both with on-premises services *and* cloud services. Report to regulators on steps already completed. Identify the steps that will have the most immediate security impact, and a schedule to implement them.

RECOMMENDATION 5. Require utility providers to incrementally implement zero trust principles, process changes, and technology solutions that protect data assets and business functions by use case.[46] Develop and maintain dynamic risk-based policies for resource access. Authenticate all connections and encrypt data. Design cybersecurity of newly interconnected resources around zero-trust principles.

RECOMMENDATION 6. Consult with grid owners and operators, and state and local government agencies to establish a process to identify, assess, and prioritize risks to the electric grid, considering current and foreseeable future cyber and physical threats, vulnerabilities, and consequences. Apply the process to periodically report to regulators on the risks. Use the report to establish a risk-based grant program focused on systematically increasing the resilience of the electric grid against the prioritized cybersecurity risks where market forces do not provide sufficient private-sector incentives to mitigate the risk without Government investment.

RECOMMENDATION 7. Maryland is a leader in grid modernization efforts in the US. Engage state employees in cybersecurity standards development efforts to share knowledge and insights, and influence future directions.

A list of standards and guidelines for distributed energy resources can be found in Appendix D.

Opportunities to Incorporate Security by Design Principles

The most cost-effective approach to cybersecurity incorporates cybersecurity best practices in the design phase. This is known as "Security by Design." Cybersecurity risks are considered from the beginning of a project and the design incorporates security from the ground up.

"While integrating information technologies is essential to building the smart grid and realizing its benefits, the same networked technologies add complexity and also introduce new interdependencies

[44] "Cyber Resiliency Design Principles", Deborah Bodeau, Richard Graubart, MITRE Technical Report, January 2017.
[45] "Zero-Trust Architecture", NIST Special Publication 800-207, Scott Rose, Oliver Borchert, Stu Mitchell, Sean Connelly, August 2020. https://doi.org/10.6028/NIST.SP.800-207
[46] Zero Trust Architecture, NIST Special Publication 800-207, National Institute of Standards and Technology, August 2020. https://doi.org/10.6028/NIST.SP.800-207.

and vulnerabilities. Approaches to secure these technologies and to protect privacy must be designed and implemented early in the transition to the smart grid."[47]

Maryland is a leader in grid modernization which means Maryland must be a leader in incorporating security by design. There are many opportunities for Maryland to apply Security by Design in the transition to a smart grid by creating a requirement to consider and report on cybersecurity risks and mitigations where changes start, including pilot programs, grant programs, working groups, and with permit applications such as a Certificate of Public Convenience and Necessity for new generating stations.[48]

RECOMMENDATION 8. Include a formal requirement for all state funded grant recipients working on electric grid resilience or modernization to address cybersecurity risk both in the design and reporting phases of their work.

RECOMMENDATION 9. Include a formal requirement for all MPSC working groups developing policy and planning for the grid to address cybersecurity risk in the reporting phase of their work.

RECOMMENDATION 10. Require electric grid resilience or modernization pilot programs to establish formal requirements for a cybersecurity plan. Cybersecurity vulnerabilities arise from weaknesses in: policy and procedure; architecture and design; configuration and maintenance; supply chain; hardware; physical access controls; software development; and communications and networks.[49] An effective cybersecurity plan must address all of these areas.

Utility Cybersecurity Reporting and Transparency

In 2019 the MPSC Cybersecurity Reporting Working Group submitted a final report providing procedural recommendations to the Commission.[50] Based on that report, MPSC issued an order requiring Maryland electric, gas, and water companies with more than 30,000 customers to provide periodic in-person confidential cybersecurity briefings.[51]

The order contains definitions for "Information Technology System", "Operational Technology System", "Smart Grid System", and "Security Breach". It also includes a short list of authorized state representatives who may attend the briefings, ten topic areas to be addressed, and a briefing schedule for years 2019-2024. The original cybersecurity briefing schedule had two electric companies report each year, with each company reporting once every three years (see Table 1 - Original Three-Year Audit

[47] Guidelines for Smart Grid Cybersecurity Volume 1 - Smart Grid Cybersecurity Strategy, Architecture, and High-Level Requirements. NISTIR 7628 Revision 1 (2018). http://dx.doi.org/10.6028/NIST.IR.7628r1

[48] See MD Code, Public Utilities, § 7-207. Certificate of public convenience and necessity required before construction of generation station or qualified generator lead line, effective May 18, 2021.

[49] NIST SP 1800-32B: Securing the Industrial Internet of Things: Cybersecurity for Distributed Energy Resources. Volume B. Preliminary Draft, April 2021.

[50] "Cyber-Security Reporting Work Group ("CSRWG") Final Report", John Borkoski, MPSC Case 9207, ML 219883. April 6, 2018.

[51] MPSC Order No. 89015, February 4, 2019, Case No. 9492. BGE, Potomac Edison, Pepco and Delmarva, Choptank, SMECO, and Washington Gas and Light (WGL) were the electric companies affected by the order.

Cycle for Cybersecurity Briefings).[52] The order also requires security breaches to be reported verbally to the MPSC within one business day of confirmation, with certain exceptions.[53]

In 2019 the two largest companies presented briefings to the Commission as required by the order.[54] In 2020, the two scheduled briefings were deferred due to COVID-19.[55] MPSC planned to reach out to companies to reschedule deferred briefings in late 2021.[56]

	First Maryland Cyber-Security Briefing under New Protocols	Second Cycle Maryland Cyber-Security Briefing under New Protocols
BGE	2019	2022
Choptank	2020	2023
Potomac Edison	2021	2024
Pepco and Delmarva	2020	2023
SMECO	2021	2024
WGL	2019	2022
Columbia Gas	2021	2024

Table 1 - Original Three-Year Audit Cycle for Cybersecurity Briefings

The ten topic areas listed in the order are adopted from the National Association of Regulatory Utility Commissioners (NARUC) Cybersecurity Primer.[57] The time period for reporting was selected because it is in sync with the FERC auditing schedule.[58] All materials are collected by the utility at the end of the briefing and the MPSC does not store any cybersecurity briefing material.[59] The utilities are required to retain the materials for at least five years.[60]

The first two cybersecurity briefings were presented by BGE and Washington Gas and Light. The information provided centered on metrics such as phishing attempts, intrusion attempts, and cybersecurity maturity levels.[61]

[52] Ibid.
[53] Ibid.
[54] "Maryland Public Service Commission 2019 Annual Report", March 25, 2020.
[55] "Maryland Public Service Commission 2020 Annual Report", March 17, 2021.
[56] "Status of Utility Cybersecurity Briefings with the Commission", Email from John Borkoski, Chief Engineer MPSC, June 3, 2021.
[57] "Cybersecurity: A Primer for State Utility Regulators, Version 3." National Association of Regulatory Utility Commissioners, with the US Department of Energy. January 2017. https://pubs.naruc.org/pub/66D17AE4-A46F-B543-58EF-68B04E8B180F.
[58] Interview with John Borkoski, Maryland Public Service Chief Engineer, January 19, 2021.
[59] Email from Ted Davis, PSC Associate General Counsel Maryland Public Service Commission, May 28, 2021.
[60] MPSC Order No. 89015, February 4, 2019, Case No. 9492.
[61] Interview with John Borkoski, Maryland Public Service Chief Engineer, January 19, 2021.

RECOMMENDATION 11. Maturity level of a cybersecurity program should be a factor in establishing an appropriate reporting period for each utility. Each utility should provide sufficient evidence to establish the maturity level of the company's cybersecurity program. The MPSC should then tailor the reporting period accordingly. For utilities that can provide persuasive evidence of a high level of maturity in their cybersecurity program, three years may be an adequate MPSC reporting period. For less mature programs, more frequent reporting to evidence growth in maturity level is recommended. An example of a maturity model available is The Cybersecurity Capability Maturity Model (C2M2) Version 2.0 (V2.0) which was released in July 2021.[62]

RECOMMENDATION 12. Information technology (IT) and operational technology (OT) systems of utilities were likely developed separately and with separate groups of people. However, without strict network segregation, vulnerabilities in IT enable attacks on OT. Regulators must understand the extent to which utility IT and OT security experts work together to protect the grid and make recommendations to enhance communication within utility provider entities.

RECOMMENDATION 13. Utilities should work together and report together on risks and cybersecurity events. Bring GridEx participants together after the exercises are complete to assess and categorize impacts of issues that were identified.[63]

RECOMMENDATION 14. Each confidential cybersecurity brief required should be accompanied by a written report suitable for public release that summarizes the cybersecurity efforts of the company, especially with respect to modernization efforts.

Other states have addressed the issue of cybersecurity reporting to regulators. In Texas, the Public Utility Commission of Texas (PUCT) and the Electric Reliability Council of Texas (ERCOT) "contract with an entity to act as the PUCT's cybersecurity monitor. The cybersecurity monitor manages a cybersecurity outreach program, communicating emerging threats and best business practices, reviewing cybersecurity self-assessments, researching and developing best business practices for cybersecurity, and reporting to the PUCT on cybersecurity preparedness for monitored utilities. In addition to monitored utilities, an electric utility, municipally owned utility, or electric cooperative operating solely outside the ERCOT region (non-ERCOT utility) may elect to participate in the Texas Cybersecurity Monitor Program."[64] Texas has confidential cybersecurity reports filed with ERCOT.[65]

[62] "Cybersecurity Capability Maturity Model (C2M2)", US Department of Energy. https://www.energy.gov/ceser/cybersecurity-capability-maturity-model-c2m2.

[63] GridEx, a distributed play grid exercise that allows participants to engage remotely, simulates a cyber and physical attack on the North American electricity grid and other critical infrastructure. Led by the North American Electric Reliability Corporation (NERC), GridEx gives participants a forum to demonstrate how they would respond to and recover from coordinated cyber and physical security threats and incidents. https://www.nerc.com/pa/CI/ESISAC/Pages/GridEx.aspx

[64] "Texas Cybersecurity Monitor Program", Electric Reliability Council of Texas. http://www.ercot.com/services/programs/tcmp.

[65] See e.g. Docket no. 51878. http://interchange.puc.texas.gov/search/dockets/

Michigan allows electric providers to report "individually or jointly with other electric providers" on their cybersecurity program and related risk planning.[66] It also specifies four types of incidents that must be orally reported "as soon as reasonably practicable and prior to any public notification".[67]

California Public Service Commission does not require cybersecurity reporting by utilities.[68] Instead, they have two fulltime staff members dedicated to providing cybersecurity guidance to utilities. The California Cybersecurity Integration Center (CalCSIC) takes the lead on cybersecurity detection, response, mitigation, and recovery.[69] "The California Cybersecurity Integration Center's primary mission is to reduce the likelihood and severity of cyber incidents that could damage California's economy, its critical infrastructure, or public and private sector computer networks in [California]."[70]

Transparency is another area that should be addressed. The utility companies and the MPSC understand that cybersecurity reporting information is sensitive and confidential so needs to be protected. Utilities are concerned that sensitive security specific information, if publicly released, could allow adversaries to identify, target, and attack potential weaknesses.[71] The MPSC order states that cybersecurity reporting authorized representatives are prohibited from divulging information learned from the briefings.[72] MPSC does not retain written material from briefings, but requires the utilities to store the briefing materials.[73] However, public access to basic cybersecurity information is essential for public awareness and trust.

RECOMMENDATION 15. When smart meters were incorporated into the Maryland power grid, utilities were required to publicize security information about the change. This practice should be continued to include changes created by DER integration.[74]

RECOMMENDATION 16. Although details of security processes and mechanisms should be protected as sensitive information, general information about utility security programs should be publicly available and easily accessible.[75]

By providing general information on cybersecurity planning as the grid modernizes, the public will have a basis for trusting that cyber resiliency of the grid is being maintained. MPSC Commissioners Jason Stanek and Mindy Herman raised a transparency issue related to distributing grid planning. Chairman Stanek acknowledged that up until now, distribution planning was in the private domain of the utilities

[66] Mich. Admin. Code R 460.3205. Security Reporting.
[67] Ibid.
[68] Interview with James Cho and Junaid Rahman, California Public Utilities Commission, June 10, 2021.
[69] West's Ann.Cal.Gov.Code § 8586.5. California Cybersecurity Integration Center; duties; information sharing. Effective January 1, 2020.
[70] Ibid.
[71] "Understanding Cybersecurity Preparedness: Questions for Utilities", Lynn P. Costantini, Matthew Acho, National Association of Regulatory Utility Commissioners (NARUC), June 2019. https://pubs.naruc.org/pub/3BACB84B-AA8A-0191-61FB-E9546E77F220.
[72] MPSC Order No. 89015, February 4, 2019, Case No. 9492.
[73] Ibid.
[74] See e.g. "SMART METERS AND YOUR PRIVACY", BGE informational brochure for customers. Author unknown, undated.
https://www.bge.com/SmartEnergy/SmartMeterSmartGrid/Documents/SmartMeters_HealthPrivacyInfo.pdf
[75] See e.g. PJM (a regional transmission organization that coordinates the movement of wholesale electricity in all or parts of 13 states and the District of Columbia) webpage that talks about cybersecurity practices at a very high level. https://learn.pjm.com/three-priorities/keeping-the-lights-on/safeguarding-the-grid.

with approval from MPSC. He asked if the utility was prepared to make the process more transparent. The Exelon representative said the company is open to a more transparent distribution planning process. Commissioner Herman mentioned the distinction between planning input verses planning specifics and commented, "I hope we don't use confidentiality to keep parties out" of the planning sessions.[76] A similar exchange between Commissioner Tony O'Donnel and the SMECO and Potomac Edison representatives took place. Commissioner O'Donnel referred to the asymmetry of information existing between stakeholders and named it as a crucial piece in planning interconnections.[77] He said the utilities have used a closely held planning process for a very long time but they need to open it up. He said the first step is for utilities to acknowledge that it has to occur. Transparency in general cybersecurity distribution planning will help to bolster public confidence.

Supply Chain[78]

Cybersecurity issues arising from the supply chain have been around for a long time. With regard to software,

> "Supply chain attacks were first demonstrated around four decades ago, when Ken Thompson, one of the creators of the Unix operating system, wanted to see if he could hide a backdoor in Unix's login function. Thompson didn't merely plant a piece of malicious code that granted him the ability to log into any system. He built a compiler—a tool for turning readable source code into a machine-readable, executable program—that secretly placed the backdoor in the function when it was compiled. Then he went a step further and corrupted the compiler that compiled the compiler, so that even the source code of the user's compiler wouldn't have any obvious signs of tampering. "The moral is obvious," Thompson wrote in a lecture explaining his demonstration in 1984. "You can't trust code that you did not totally create yourself. (Especially code from companies that employ people like me.)"[79]

The Federal Acquisition Regulations System recently published a new rule that defines *supply chain risk* as "the risk that any person may sabotage, maliciously introduce unwanted function, extract data, or otherwise subvert the design, integrity, manufacturing, production, distribution, installation, operation, maintenance, disposition, or retirement of covered articles so as to surveil, deny, disrupt, or otherwise manipulate the function, use, or operation of the covered articles or information stored or transmitted by or through covered articles."[80] The new rule also describes supply chain risk information and includes

---

[76] PC44 Electric Distribution System Planning Pre-Working Group Educational Session 1. September 2, 2021. https://www.youtube.com/watch?v=WtvgTYs4IG4

[77] Ibid.

[78] NIST defines supply chain as a "Linked set of resources and processes between and among multiple tiers of organizations, each of which is an acquirer, that begins with the sourcing of products and services and extends through their life cycle." Security and Privacy Controls for Information Systems and Organizations, NIST Special Publication 800-53 Revision 5, September 2020. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf.

[79] "Hacker Lexicon: What Is a Supply Chain Attack? From NotPetya to SolarWinds, it's a problem that's not going away any time soon", Andy Greenberg, May 31, 2021. https://www.wired.com/story/hacker-lexicon-what-is-a-supply-chain-attack/

[80] 41 CFR 201 and 201-1, Federal Acquisition Security Council Rule, Federal Register, August 26, 2021. https://public-inspection.federalregister.gov/2021-17532.pdf. This is a modification of 10 U.S.C.A. § 3252 – Supply Chain Risk. Effective February 15, 2019.

lists of characteristics and relevant factors to consider.[81] These lists could serve as a guide when collecting and assessing information for supply chain risk determination.

Currently, Maryland has regulations that mention "supply chain" with respect to pharmaceuticals, food, offshore wind facilities,[82] and demographic diversity.[83] Drugs are required to have a record of the tracking of a drug or device through the supply chain, with each trading partner authenticating the drug or device upon receipt and transfer. [84] Food safety plans are required to include written preventative controls that address the supply chain. [85] MPSC has established a Supplier Diversity Program to "promote economical delivery of utility services and positively impact the economy of the State." In addition, the Maryland Offshore Wind Business Development Advisory Committee, that advises the Maryland Energy Administration (MEA) on how to best spend funds, is required to have one individual with experience in offshore wind supply chain issues.[86]

Other states have considered supply chain issues with respect to cybersecurity. For example, Texas created the "Cybersecurity Coordination Program for Utilities" to monitor cybersecurity efforts among utilities in the state.[87] The program includes "guidance on best practices for cybersecurity controls for supply chain risk management of cybersecurity systems used by utilities, which may include, as applicable, best practices related to: (A) software integrity and authenticity; (B) vendor risk management and procurement controls, including notification by vendors of incidents related to the vendor's products and services; and (C) vendor remote access."[88]

After the major power outage Texas experienced in early 2021, the Texas state legislature created the "Texas Electricity Supply Chain Security and Mapping Committee".[89] "Electricity supply chain" is defined to include "facilities and methods used for producing, treating, processing, pressurizing, storing, or transporting natural gas for delivery to electric generation facilities; and critical infrastructure necessary to maintain electricity service."[90] The purpose of the committee is to plan and prepare for extreme weather events. It is required to prepare a public report by January 1, 2022, that includes a list of the established best practices and recommended oversight and compliance standards adopted by the commission.[91]

In New York, supply chain was addressed in the context of electronic voting systems devices. "The minimum security standards for such devices shall be commensurate with the level of security risk

[81] Ibid.
[82] COMAR 20.61.06.03 Evaluation criteria.
[83] COMAR 20.08.01.01 Declaration of Public policy.
[84] COMAR 10.13.02.02 Definitions.
[85] COMAR 10.15.09.17 Milk Facility Construction and Plan Submission.
[86] Md. Code Ann., State Gov't § 9-20C-02. Maryland Offshore Wind Business Development Advisory Committee. Efffective June 1, 2017.
[87] V.T.C.A., Utilities Code § 31.052. Cybersecurity Coordination Program for Utilities. Effective September 1, 2019.
[88] Ibid.
[89] V.T.C.A., Utilities Code § 38.201 - Texas Electricity Supply Chain Security and Mapping Committee. Effective June 8, 2021.
[90] Ibid.
[91] V.T.C.A., Utilities Code § 38.204 - Mapping Report. Effective June 8, 2021.

applicable to such devices and shall specifically take into account any security risk associated with voting equipment-related supply chains in addition to any other applicable security risk."[92]

To improve security with respect to the supply chain, uncover blind spots in partnerships and extend the reach of information sharing.

RECOMMENDATION 17. Require all utilities that rely on third party IT or OT providers to include standard contract language with service providers to collect and preserve data for cybersecurity analysis and share such data, or report third party security breaches to the utility or to a government entity such as CISA.

RECOMMENDATION 18. Adopt the NIST definition of "critical software" and require utilities to maintain a list of the categories of software and software products in use or in acquisition that meet the definition. Adopt NIST security guidance for critical software use, applying practices of least privilege, network segmentation, and proper configuration.[93]

RECOMMENDATION 19. Require utilities to establish minimum security standards for IT and OT devices commensurate with the level of security risk applicable to such devices and specifically take into account any security risk associated with supply chains.

Financial and Human Resources

Investing in cybersecurity is investing in the future of the organization.[94] "In today's data-driven, global, mobile, always-connected economy, cybersecurity is an enabling technology that allows you do to business. It is the foundation for everything you do."[95]

Maryland has taken important steps to address the financial and human resource barriers affecting cybersecurity of critical infrastructure within the state. For example, The Joint Committee on Cybersecurity and the Maryland Cybersecurity Council work to evaluate and advance cybersecurity in the state.[96] There are Maryland tax credits for cybersecurity development and services.[97] A cybersecurity investment fund is available to provide funding for emerging cybersecurity technology development.[98] Maryland has a Cybersecurity Public Service Scholarship Program to support students who are pursuing an education in programs that are directly relevant to cybersecurity.[99] Maryland universities have

[92] N.Y. Elec. Law § 1-104 (McKinney) – Definitions. (Election Law). Effective November 12, 2020.
[93] See "Security Measures for "EO-Critical Software" Use Under Executive Order (EO) 14028", National Institute of Standards and Technology, July 9, 2021. https://www.nist.gov/system/files/documents/2021/07/09/Critical%20Software%20Use%20Security%20Measures%20Guidance.pdf.
[94] "Treat Cybersecurity as a Strategic Investment, Not a Sunk Cost", Sean Duca, circa 2018. https://www.securityroundtable.org/its-time-to-treat-cybersecurity-as-a-strategic-investment-not-a-sunk-cost/
[95] Ibid.
[96] MD Code, State Government, § 2-10A-13. Joint Information Technology and Biotechnology Committee. Effective July 1, 2019. MD Code, State Government, § 9-2901. Maryland Cybersecurity Council. Effective July 1, 2021 to September 30, 2021.
[97] MD Code, Tax – General § 10-733.1. Tax credit for the purchase of cybersecurity technology or a cybersecurity service from one or more qualified sellers. Effective June 1, 2018.
[98] MD Code, Economic Development, § 10-464. Cybersecurity Investment Fund. Effective October 1, 2020.
[99] MD Code, Education, § 18-3502. Cybersecurity Public Service Scholarship Program. Effective July 1, 2018.

specialized development programs for cybersecurity.[100] There are also endowments available to further basic and applied research in cybersecurity.[101]

Yet significant barriers still exist.

According to MPSC's Chief Engineer, none of the current MPSC engineering team members have cybersecurity expertise and there is no dedicated cybersecurity staff.[102] Generally, MPSC engineers are hired without experience in the energy sector and without previous cybersecurity experience.[103] This creates a very significant learning curve for new hires, who have an average tenure at MPSC of four years. The Chief Engineer expressed a need for more cybersecurity expertise within MPSC since they are facing a growing slate of cybersecurity issues. He cited salary levels as a potential barrier to hiring cybersecurity expertise.[104]

RECOMMENDATION 20. Allocate funds to provide Maryland Public Service Commission with staff dedicated to regulatory cybersecurity policy, strategy, auditing, and reporting.

RECOMMENDATION 21. Ensure MPSC employees involved in cybersecurity activities attend periodic training to keep skills and knowledge current regarding emerging trends in distributed energy resource cybersecurity issues.

RECOMMENDATION 22. MPSC engineers should take an active role in standards organizations upon which they rely to ensure that cybersecurity concerns are addressed during standards development.[105]

MPSC is funded by the utilities they regulate and MPSC sets the rates that utilities may charge.[106] "The only statutory imperative of Public Service Commission (PSC) in regulating utility rates is to construct and approve just and reasonable rates, which, among other things, fully consider and are consistent with the public good."[107] Rates that the commission sets are "designed to yield to [a public utility] a 'revenue requirement' sufficient to pay its prudent expenses and to allow it the opportunity to earn a fair return on investments."[108] However, measuring a return on cybersecurity investment is complicated.

"If an organization doesn't see cybersecurity as a strategic investment, it won't treat the people responsible for cybersecurity as part of the strategic team. Conversely, if cybersecurity leaders are not

[100] MD Code, Education, § 12-123. Center for Cybersecurity at the University of Maryland Baltimore County. Effective: July 1, 2021; MD Code, Education, § 12-306. University of Maryland Center for Economic and Entrepreneurship Development (UMCEED). Effective: July 1, 2021.
[101] MD Code, Economic Development, § 6-614. Expenditure of endowment proceeds. Effective: March 13, 2021.
[102] Interview with John Borkoski, January 19, 2021. See Appendix C for summary of interview.
[103] Ibid.
[104] Ibid.
[105] For example, the MPSC relies on IEEE standards for interconnection. MPSC engineers should participate in IEEE standards efforts to contribute their knowledge about the Maryland grid and related security needs and concerns.
[106] "The costs and expenses of the Commission and the Office of People's Counsel shall be borne by the public service companies that are subject to the Commission's jurisdiction." Md. Code, Pub. Util. § 2-110 - Public Utility Regulation Fund
[107] Maryland Off. of People's Couns. v. Maryland Pub. Serv. Comm'n, 226 Md. App. 176, 127 A.3d 582 (2015) citing Md.Code, Public Utility Companies, §§ 2–112, 2–113, 4–102. This case has a simplified explanation of how rates are determined.
[108] Ibid. Citing Office of People's Counsel v. Maryland Pub. Serv. Comm'n, 355 Md. 1, 7–8, 733 A.2d 996 (1999).

part of the executive team, the organization won't have the knowledge and commitment to treat cybersecurity as a strategic investment."[109]

"Workforce experts say the main reason many firms don't list their security leaders within their top executives is that these people typically do not report directly to the company's board of directors or CEO. More commonly, the CSO or CISO reports to the CTO, or to the chief information officer."[110] This reporting structure can turn conflicts of interest during product selection or budget decisions into unacceptable cybersecurity risk.[111] This may be the case with investor-owned utilities in Maryland.[112]

RECOMMENDATION 23. Encourage utilities to establish a procedure where cybersecurity leadership of utilities may report directly to the company's Board of Directors or CEO.

The People's Counsel fills an important role in oversite and is included in the short list of representatives who may attend the utility cybersecurity reporting briefs with the MPSC.[113] In order to fulfill their duty to protect the interests of residential and noncommercial users, the Office of People's Counsel should have access to cybersecurity expertise to participate in rate cases and other court appearances.

RECOMMENDATION 24. Expand MD Code, Public Utilities, § 2-203(f) to include cybersecurity expertise in the list the Office of People's Counsel may retain or hire as necessary for a particular matter.

Other states have addressed the resource issues in different ways. For example, Michigan has created a "Cyber Civilian Corp"(CCC), a program under which volunteers may provide services to organizations to respond to cybersecurity incidents.[114] The program is administered by the Michigan department of technology, management, and budget.[115] The CCC is available to assist critical infrastructure organizations in rapid response.[116] A cybersecurity incident is defined to be an event that "actually or imminently jeopardizes the integrity, confidentiality, or availability of computers, information or communications systems or networks, physical or virtual infrastructure controlled by computers or

[109] "Treat Cybersecurity as a Strategic Investment, Not a Sunk Cost", Sean Duca, circa 2018. https://www.securityroundtable.org/its-time-to-treat-cybersecurity-as-a-strategic-investment-not-a-sunk-cost/
[110] "A Chief Security Concern for Executive Teams", Brian Krebs, December 18, 2018. https://krebsonsecurity.com/2018/12/a-chief-security-concern-for-executive-teams/
[111] See e.g. The House Committee report on the Equifax breach which explains that the CSO reported to the chief legal officer due to prior conflicts with CIO. The Chief Legal Officer was referred to as "head of security". https://republicans-oversight.house.gov/wp-content/uploads/2018/12/Equifax-Report.pdf
[112] See e.g. these investor owned utilities: Exelon's "Leadership and Governance Executive Profiles" page which does not list a security officer. https://www.exeloncorp.com/leadership-and-governance/executive-profiles; BGE's "Leadership & Values" page which does not list a security officer. https://www.bge.com/AboutUs/Pages/LeadershipValues.aspx; Pepco's ""Leadership & Values" page which does not list a security officer. https://www.pepco.com/AboutUs/Pages/LeadershipValues.aspx; Delmarva's page which does not list a security officer. https://www.delmarva.com/AboutUs/Pages/LeadershipValues.aspx; Potomac Edison's parent company FirstEnergy's "Leadership Team" page which does not list a security officer. https://www.firstenergycorp.com/about/leadership_team.html
[113] MPSC Order No. 89015, February 4, 2019, Case No. 9492.
[114] Mich. Comp. Laws Ann. § Ch. 18, Refs & Annos (West). Effective January 24, 2018.
[115] Mich. Comp. Laws Ann. § 18.222 – Definitions. Effective March 24, 2021.
[116] Ibid.

information systems, or information resident on any of these."[117] The volunteers must meet qualifying criteria as determined by an advisory board.[118] Volunteers must consent to a criminal background check and sign a contract.[119] Michigan law declares that a CCC volunteer is not an agent of the state and the state is not liable for any damage they cause.[120] In 2020 the CCC had "approximately 50 volunteers hailing from the government, academia, business, financial, and healthcare sectors."[121]

Connecticut has created a Technology Talent Advisory Committee to develop pilot programs to recruit cybersecurity software developers and train state residents in cybersecurity.[122]

Data Privacy

Maryland electricity customer data is protected in that energy usage data and personally identifiable information may not be disclosed without the customer's consent.[123]

Direct Load Control, a component of The EmPOWER Maryland Act demand response programs, allows utilities to remotely control some customers' appliances.[124] "Customers who have chosen to participate in the Direct Load Control programs … have a switch or thermostat installed at their properties to briefly curtail usage of central air conditioning or an electric heat pump in instances of system reliability issues or high electricity prices during critical peak hours."[125]

"While the utility is presumed to have the direct relationship with the consumer, there may be intermediated situations where a third-party energy service provider manages the consumer relationship as a demand-response or other aggregator, or manages Direct Load Control (DLC) on behalf of the consumer. The consumer may not be aware of all the entities involved in their participation in Time of Use (TOU) pricing programs."[126]

[117] Ibid.
[118] Mich. Comp. Laws Ann. § 18.224 - Contract to serve as volunteer or advisor; requirements. Effective March 24, 2021.
[119] Ibid. Mich. Comp. Laws Ann. § 18.225. Criminal history and records checks; conduct; appeal. Effective March 24, 2021.
[120] Mich. Comp. Laws Ann. § 18.226. Authority of volunteers and advisors; personal injury or property damage suffered by volunteer or advisor. Effective March 24, 2021.
[121] "BUILDING A CIVILIAN CYBER CORPS", National Governors Association. https://www.nga.org/wp-content/uploads/2020/05/MiC3-Memo.pdf
[122] C.G.S.A. § 32-7p. Technology Talent Advisory Committee. Membership. Duties. Pilot programs. Report. Effective July 1, 2021.
[123] COMAR 20.62.05.10 - Disclosure of Subscriber Information.
[124] Md. Code Ann., Pub. Util. § 7-211 - Energy efficiency and conservation programs and services. Effective: June 1, 2021. The EmPOWER Maryland Act requires utilities to implement cost-effective demand response programs.
[125] "The EmPOWER Maryland Energy Efficiency Act Report of 2021", Maryland Public Service Commission, https://www.psc.state.md.us/wp-content/uploads/2021-EmPOWER-Maryland-Energy-Efficiency-Act-Standard-Report.pdf
[126] NISTIR 7628 Revision 1 Guidelines for Smart Grid Cybersecurity Volume 2 - Privacy and the Smart Grid. The Smart Grid Interoperability Panel – Smart Grid Cybersecurity Committee. http://dx.doi.org/10.6028/NIST.IR.7628r1

RECOMMENDATION 25. The utility should make available clear, simple identification of all entities or some formal statement of the data management principle to help educate consumers as to the "data chain" that may be in place based on their relationships with utility, utility-authorized third parties, and energy service providers that are not affiliated with a utility.[127]

Load shaping is an alternative to Direct load Control.[128] "Load shaping techniques aim to control customers' total electric consumption and utility's load factor."[129] MPSC has a load shaping pilot program.[130] The project requires a participant to "demonstrate an ability to shape customer load profiles through load shifting, peak shaving, and energy efficiency. Applicants can propose any mechanism for load shaping such as sending appropriate price signals (real time rates), using technology to control usage (controllable thermostats), payment of rebates or behavioral modification treatments. A secondary goal is to test whether load shaping can lower customer bills or reduce the customers' overall effective rate for electricity by avoiding energy usage during high cost periods."[131]

When two-way communications are implemented in load shaping, the communication channel from the consumer "may allow granular monitoring of energy consumption by appliance. Such direct monitoring may provide more accurate load management, but could also pose certain privacy risks."[132]

RECOMMENDATION 26. Incorporate existing privacy standards and frameworks to identify privacy risks, then apply privacy mitigation processes to match proportionate privacy controls for each relevant business activity that creates a risk to privacy.

Privacy issues may also arise from state and utility entities sharing threat information.

RECOMMENDATION 27. Develop guidelines relating to privacy and civil liberties governing the receipt, retention, use, and dissemination of cyber threat indicators by the state, including safeguards such as sanctions for activities by officers, employees, or agents of state or local Government for misuse of information.

Definitions

Establishing a common language improves the chances that expectations are understood and achieved. By defining key terms related to cyber resiliency efforts, a common language will be available to clearly communicate expectations. There are benefits to adopting established definitions, especially those that

[127] Ibid.
[128] "Quantifying the Opportunity Limits of Automatic Residential Electric Load Shaping", Robert Cruickshank, Gregor Henze, Rajagopalan Balaji, Bri-Mathias Hodge, and Anthony Florita, 21 August 2019. https://www.mdpi.com/journal/energies
[129] A. M. Attia, K. H. Youssef and N. H. Abbasy, "A Comparative Analysis and Simulation of Load Shaping Techniques," 2018 IEEE PES/IAS PowerAfrica, 2018, pp. 664-669, doi: 10.1109/PowerAfrica.2018.8521019.
[130] In the Matter of Transforming Maryland's Electric Distribution Systems to Ensure that Electric Service is Customer-Centered, Affordable, Reliable and Environmentally Sustainable in Maryland; PC44 Rate Design Retail Supplier Load Shaping Pilot RFP Statement of Work
[131] In the Matter of Transforming Maryland's Electric Distribution Systems to Ensure that Electric Service is Customer-Centered, Affordable, Reliable and Environmentally Sustainable in Maryland; PC44 Rate Design Retail Supplier Load Shaping Pilot RFP Statement of Work
[132] NISTIR 7628 Revision 1 Guidelines for Smart Grid Cybersecurity Volume 2 - Privacy and the Smart Grid. The Smart Grid Interoperability Panel – Smart Grid Cybersecurity Committee. http://dx.doi.org/10.6028/NIST.IR.7628r1

have stood the test of time in a dynamic field such as cybersecurity. In particular, adopting a definition of cybersecurity and cyber resiliency will be foundational to building resiliency in the cyber domain.

For example, currently Maryland has adopted the following definition for cybersecurity in the Economic Development portion of the Code, in relation to the Cybersecurity Investment Fund:

> "Cybersecurity" means information technology security. "Cybersecurity" includes the protection of networked devices, networks, programs, and data from unintended or unauthorized access, change, or destruction. "Information technology" means all electronic information processing hardware and software, including: (1) maintenance; (2) telecommunications; and (3) associated consulting services. [133]

This definition covers some but not all of the five goals of cybersecurity: availability, integrity, authentication, confidentiality, and nonrepudiation. For example, protection from "destruction" does not cover other ways in which data may become unavailable, such as infrastructure overload. Also, nonrepudiation is not covered.[134] By specifying the five goals of cybersecurity in the definition, important functions will not be excluded.

RECOMMENDATION 28. Modify the current Maryland statutory definition of "cybersecurity" to include the five goals of cybersecurity so that procurement will be guided by specific reference to availability, integrity, authentication, confidentiality, and nonrepudiation.[135]

In addition to defining cybersecurity, other key terms should be considered.

RECOMMENDATION 29. Adopt a statutory definition of "cyber resilience", "critical infrastructure", "supply chain risk", and "critical software".

See Appendix A Recommended Definitions for more information, including sample definitions and explanations for key terms.

Conclusion

Maryland is a leader in grid modernization efforts. Continuous integration of new technologies into the electric grid without a proportional investment and effort in securing those systems leads to unacceptable risk. By requiring Security by Design in these ongoing efforts, systems will be conceived and implemented in a more secure fashion. Adopting Zero-Trust strategies will increase resiliency in the face of advanced persistent threats. Tailoring cybersecurity reporting requirements based on program maturity will improve scarce resource allocation. Assuring state oversight efforts are properly resourced will help ensure a secure future for the Maryland electric grid.

---

[133] MD Code, Economic Development, § 10-463. Definitions. Effective: October 1, 2020.

[134] Nonrepudiation is "Protection against an individual who falsely denies having performed a certain action and provides the capability to determine whether an individual took a certain action, such as creating information, sending a message, approving information, or receiving a message." Security and Privacy Controls for Information Systems and Organizations, NIST Special Publication 800-53 Revision 5, September 2020. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf.

[135] Ibid.

Appendix A. Recommended Definitions

This section provides samples and descriptions of key terms that should be adopted to create a common language for cybersecurity activities. Statutes and regulations using these terms should first introduce the definitions. The context in which the terms are used may influence the definitions chosen for that particular instance. For example, defining "critical infrastructure" in the criminal code would likely require more specificity than in an emergency management statute.

Critical Infrastructure

The following detailed analysis describes how states have defined and used the term "critical infrastructure" in various contexts. The information is up-to-date as of mid-2021.

The Maryland Code does not include a definition of critical infrastructure, but uses the term in a few places, including in MD Code, State Government, § 9-2901 Maryland Cybersecurity Council. The Maryland Code of Regulations (COMAR) also uses the term, but does not define it.

A search of state and federal statutes identifies six broad categories where "critical infrastructure" is defined. See Table 2.

Category	Number of examples found
Criminal	9
Economic/business/taxes	6
Emergency management/public safety	11
Administrative/government procedure	3
Military and defense	4
Transportation	1

Table 2 Statutory Topics Containing Definitions of "Critical Infrastructure"

Of these six categories, the criminal code definitions are distinct in their specificity, likely to satisfy the procedural due process requirements that stem from the Bill of Rights. Among the other five categories, similar structure and wording are found in many of the definitions, but wide variations in scope exist. Several states have adopted the federal definition. Other trends are visible as well.

Criminal Code Definitions

Criminal statutes that lack sufficient definiteness or specificity are commonly held "void for vagueness." Cantwell v. Connecticut, 310 U.S. 296 (1940). To provide specificity, all the definitions found in criminal code include a detailed list of examples of critical infrastructure. Some statutes limit the definition to only those facilities, services, or resources listed, while others are subject to a broader interpretation by "including" examples but not restricting to only those listed. See Table 3.

For example,

> "Critical infrastructure" means critical public or private infrastructure resource systems involved in providing services necessary to ensure or protect the public health, safety and welfare, including, but not limited to, a public water system or a public water source; an emergency, governmental, medical, fire or law enforcement response system; a public utility system; a financial system; an educational system; or a food or clothing distribution system. 17–A M.R.S.A. § 2

The systems and facilities most commonly listed in the criminal code address electric, water, and communications. Texas has two separate definitions for "critical infrastructure facility", one for flying drones in restricted areas and the other for computer crimes.

year	state	citation	topic
2020	Arizona	A.R.S. § 13-2301	Organized crime, fraud, and terrorism
2020	Maine	17–A M.R.S.A. § 2	Maine Criminal Code - General Principles
2020	South Dakota	SDCL § 22-1-2	Crimes
2019	Texas	V.T.C.A., Government Code § 423.0045	Law Enforcement and Public Protection - Use of Unmanned Aircraft
2019	Texas	V.T.C.A., Penal Code § 33.01	Offenses Against Property - Computer Crimes
2018	Iowa	I.C.A. § 716.11	Criminal Acts - criminal damage and trespass to property
2017	Georgia	Ga. Code Ann., § 16-11-220	Crimes and Offenses - Offenses Against Public Order and Safety - Domestic Terrorism
2017	Utah	U.C.A. 1953 § 76-6-702	Criminal Code - offenses against property - computer crimes act
2014	Hawaii	HRS § 708-890	Penal Code - Offenses Against Property Rights - Computer Crime

Table 3 Criminal Code Definitions of Critical Infrastructure

The Federal Definition

"Critical infrastructure" (CI) was first defined in American law in 2001 by the federal government in a Critical Infrastructure Protection statute, 42 U.S.C.A. § 5195c. The same definition was adopted in 2009 for the War and Defense Production General Provisions, by the NIST Committee on National Security Systems in 2015, included in the Homeland Security definitions in 2016, adopted by the Commerce Department in 2018, and most recently adopted in the 2021 Defense Spending Law.

> "Critical infrastructure" means 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. 42 U.S.C.A. § 5195c.

Note that the federal definition does not enumerate any specific types of facilities. Instead, it qualifies "systems and assets" based on the impact that would result from "incapacity or destruction".

Six states and the District of Columbia have adopted the federal definition, modifying it slightly to make it applicable to state government. See Table 4. Michigan is the most recent state to have adopted a definition for CI, and selected the federal definition. All of the definitions adopted in the administrative and government procedure sections of the state codes followed the federal definition, specifically in relation to Freedom of Information. Five of the eleven emergency management/public safety did as well.

year	state	citation	topic
2021	Michigan	M.C.L.A. 18.222	Cyber Civilian Corps Act
2020	D.C.	DC ST § 2-539	Administrative Procedure - Freedom of Information
2020	New York	McKinney's Public Officers Law § 86	Freedom of Information Law
2019	Hawaii	HRS § 127A-2	Public Safety and Internal Security
2018	Oregon	O.R.S. § 276A.500	Public Facilities, Contracting and Insurance - Information Technology - Oregon Geographic Information Council
2013	Arizona	A.R.S. § 41-1801	Public Safety - Critical Infrastructure Information System
2012	Colorado	C.R.S.A. § 24-33.5-1602	Public Safety - Division of Homeland Security and Emergency Management

Table 4 - States that adopted the federal definition

Equipment and Property

Another popular variation, first appearing in the 2015 Texas code, focuses on "equipment and property" used for electric, gas, water, and communications:

> "Critical infrastructure" means property and equipment owned or used by communication networks, electric generation, transmission, and distribution systems, gas distribution systems, water pipelines and related support facilities that service multiple customers and residents including, but not limited to, real and personal property such as buildings, offices, lines, poles, pipes, structures, and equipment. N.J.S.A. 54:50-40

This version is found in the economic/business/taxes and the emergency management/public safety categories of the code. See Table 5. The "but not limited to" phrase was a modification added to the Oregon Emergency Management 2015 language, then adopted by Mississippi in their 2018 Tax Code. The identical wording was adopted in the New Jersey Tax Code the following year.

Other Definitions - Variation of Scope

The most limited definition is the 2015 Vermont definition for Business Rapid Response for Declared State Disasters:

> "Critical infrastructure" means property and equipment owned or used by communications networks and electric generation, transmission, and distribution systems. 11 V.S.A. § 1701.

Whereas the Texas Homeland Security definition has a sweeping scope. It is the only definition that includes "morale" in the qualifiers:

> "Critical infrastructure" includes all public or private assets, systems, and functions vital to the security, governance, public health and safety, economy, or morale of the state or the nation. V.T.C.A., Government Code § 421.001

North Dakota has modified the federal definition, narrowing the scope to adopt a 2017 Military – Disaster or Emergency Remediation Work. The borrowed federal definition phrases are in bold:

> **"Critical infrastructure" means** real and personal natural gas, electrical, and telecommunication transmission property **so vital to the state that the incapacity or destruction** of that natural gas, electrical transmission or distribution system, or telecommunications transmission system **would have a debilitating impact on public health or safety and the economic and physical security of the state or region**. NDCC, 37-17.5-01

year	state	citation	topic
2019	Arkansas	A.C.A. § 12-88-103	Emergency management - Business Rapid Response to State Disasters Facilitation Act
2019	New Jersey	N.J.S.A. 54:50-40	Taxation - State Uniform Procedure Law - Administration
2015	Mississippi	Miss. Code Ann. § 27-113-5	Taxation and Finance - Facilitating Business Rapid Response to State Declared Disasters Act of 2015
2015	Oregon	O.R.S. § 401.685	Emergency Management and Services - Disaster or Emergency Related Work Conducted by Out-of-State Businesses
2015	Texas	V.T.C.A., Bus. & C. § 112.003	Regulation of Businesses and Services - Facilitating Business Rapid Response to State Declared Disasters Act

Table 5 - Equipment and Property Definition of Critical Infrastructure

Critical Infrastructure by other Names

Kentucky uses the term "Key Infrastructure assets" in the penal code and lists eleven specific categories of assets.[136] Louisiana defines "targeted facility" in the criminal code in relation to unlawful use of drones and lists four specific categories of facilities.[137]

Cyber Resilience

The reality of cybersecurity today is that there are a variety of sophisticated adversaries that can make detection of compromised systems difficult. This brings resiliency to the forefront of planning and strategy since adapting to adverse conditions is important in such an environment.

"Cyber Resilience" means "The ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources."[138]

"'Resiliency' means the ability of communities to rebound, positively adapt to, or thrive amidst changing conditions or challenges, including human-caused and natural disasters, and to maintain quality of life, healthy growth, durable systems, economic vitality, and conservation of resources for present and future generations."[139]

Supply Chain Risk

A new rule was recently published by the Federal Acquisition Regulations System that defines supply chain risk. The definition covers an extensive list of actions a person might take in an attempt to manipulate protected items.

> '"Supply Chain Risk" means the risk that an adversary may sabotage, maliciously introduce unwanted function, or otherwise subvert the design, integrity, manufacturing, production, distribution, installation, operation, or maintenance of a covered system or covered item of supply so as to surveil, deny, disrupt, or otherwise degrade the function, use, or operation of the system or item of supply.'[140]

Critical Software

In May 2020, President Biden signed an executive order addressing cybersecurity issues. The order required certain federal government agencies to work together to characterize what software performs functions that are critical to trust, i.e. software used for security functions such as network control, endpoint security, and network protection.[141] The National Institute of Standards and Technology (NIST)

---

[136] KRS § 511.100 Trespass upon key infrastructure assets

[137] LSA-R.S. 14:337 Unlawful use of an unmanned aircraft system

[138] "Developing Cyber Resilient Systems: A Systems Security Engineering Approach", NIST Special Publication 800-160 Volume 2, Ron Ross, Victoria Pillitteri, Richard Graubart, Deborah Bodeau, Rosalie Mcquaid, National Institute of Standards and Technology, November 2019. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160v2.pdf.

[139] Colo. Rev. Stat. Ann. § 24-33.5-703 – Emergency Management – Definitions. Effective August 8, 2018.

[140] Department of Energy Acquisition Regulation number AL-2021-06, September 1, 2021. https://www.energy.gov/sites/default/files/2021-09/AL%202021-06%20Chief%20Information%20Officer%E2%80%99s%20Supply%20Chain%20Risk%20Management%20%28SCRM%29.pdf

[141] "Executive Order on Improving the Nation's Cybersecurity", Executive Order 14028, The White House, May 12, 2021. https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

created a definition for “critical software” to apply in the context of securing the software supply chain.[142] Their method for crafting the definition involved research and collaboration with a variety of stakeholders.[143] The definition will act as a basis for “guidance identifying practices that enhance the security of the software supply chain.”[144]

> “[C]ritical software is defined as any software that has, or has direct software dependencies upon, one or more components with at least one of these attributes:
>
> - is designed to run with elevated privilege or manage privileges;
> - has direct or privileged access to networking or computing resources;
> - is designed to control access to data or operational technology;
> - performs a function critical to trust; or,
> - operates outside of normal trust boundaries with privileged access.”[145]

The designation of software as critical is based on the functions of the software, not its use.[146] Once a definition has been established, utilities can work to identify critical software in use within their organization and follow NIST guidance on use of critical software.[147]

[142] “Definition of Critical Software Under Executive Order (EO) 14028”, June 25, 2021. https://www.nist.gov/system/files/documents/2021/06/25/EO%20Critical%20FINAL_1.pdf
[143] Ibid.
[144] “Executive Order on Improving the Nation's Cybersecurity”, Executive Order 14028, The White House, May 12, 2021. https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/
[145] “Definition of Critical Software Under Executive Order (EO) 14028”, June 25, 2021. https://www.nist.gov/system/files/documents/2021/06/25/EO%20Critical%20FINAL_1.pdf
[146] Ibid.
[147] See ‘Security Measures for “EO-Critical Software” Use Under Executive Order (EO) 14028’, National Institute of Standards and Technology, July 9, 2021. https://www.nist.gov/system/files/documents/2021/07/09/Critical%20Software%20Use%20Security%20Measures%20Guidance.pdf

Appendix B. Addressing Drone Threats to Critical Infrastructure

This section provides recommendations on the use and legislation of unmanned aircraft systems (UAS). UAS are relatively inexpensive, widely available, and their use is rapidly expanding. These systems can be useful tools for utilities and can also pose threats to utilities. Several states have created legislation to address drones in the context of critical infrastructure. There have been documented drone attacks on the electric grid in the US.[148]

Cybersecurity Recommendations Regarding Drone Use

With a complex federal statutory and regulatory environment in place, states must take care to avoid pre-emption conflicts and must be proactive in protecting constitutional rights when crafting cybersecurity rules concerning drones. See Constitutional Issues for more information.

Before entities test, acquire, install, or use drone detection, interception, or mitigation systems, federal and state criminal, surveillance, and communication laws and regulations should be carefully reviewed. Research and implement legally approved counter-UAS technology.[149]

Develop regulations requiring owners/operators of Critical Infrastructure facilities to provide evidence that counter-UAS technology in use complies with federal and state laws. Require owner/operators to update incident response plans to include UAS security and response strategies. Require potential UAS threats reporting in cybersecurity reporting to regulators.

Consult with the FAA regarding proposed restrictions on flight altitude, flight paths, operational bans, or any regulation of the navigable airspace. Know the air domain around the critical infrastructure and identify which government entity has authority to take action to enhance security.[150]

Create a registry of critical infrastructure of both government owned and privately owned facilities for state reference and in preparation for FAA implementation of Public Law 114-190.[151] See "Identifying Critical Infrastructure" section below.

Adopt clear and specific definitions of key terms such as "critical infrastructure" in statutes and regulations. Adopt federal terminology and definitions were possible to avoid the need for translations between state and federal law.

Review state laws regarding digital evidence to ensure that information acquired from drones will be handled appropriately. Ensure that policy and training are in place to protect evidence and respect privacy rights.

---

[148] See e.g. "Likely Drone Attack On U.S. Power Grid Revealed In New Intelligence Report (Updated)", Joseph Trevithick, November 4, 2021. https://www.thedrive.com/the-war-zone/43015/likely-drone-attack-on-u-s-power-grid-revealed-in-new-intelligence-report.

[149] "Advisory on the Application of Federal Laws to the Acquisition and Use of Technology to Detect and Mitigate Unmanned Aircraft Systems", Federal Aviation Administration, Department of Justice, Federal Communications Commission, Department of Homeland Security, August 2020. https://www.cisa.gov/sites/default/files/publications/20_0817_ogc_interagency-legal-advisory-uas-detection-mitigation-technologies_1.pdf

[150] State and Local UAS Regulation of UAS Fact Sheet. FAA Office of the Chief Counsel, December 17, 2015. https://www.faa.gov/uas/resources/policy_library/media/UAS_Fact_Sheet_Final.pdf. See also DHS, "UAS and Critical Infrastructure – Understanding the Risk", Mar 29, 2019. https://www.youtube.com/watch?v=o6x-cj1wXZk

[151] See Public Law 114-190.

Create a state emergency response plan that specifically addresses drone threats and meets federal, state, and local regulatory requirements.

Develop processes to allow UAS operators to communicate more effectively with State and local law enforcement to enable law enforcement to determine if a UAS operation poses a potential security or safety risks associated with UAS operating in close proximity to critical infrastructure.

Overview

Drones present a threat to critical infrastructure. For example, drones can carry lethal payloads that can physically damage equipment. They can be used for surveillance in planning an attack. Drones can be used to steal information from vulnerable computer systems, or simply for disruption or harassment. The Federal government has taken steps to protect federal infrastructure from these threats, and several state governments have created statutes to address the threats posed by drones.

Multiple federal entities have authorities concerning drone use. The Federal Aviation Administration (FAA) under the U.S. Department of Transportation regulates safety in the national airspace. The Cybersecurity and Infrastructure Security Agency (CISA) under the Department of Homeland Security (DHS) has statutory authority to counter credible threats from drones.[152] The U.S. Attorney General is also authorized to take certain counter-drone actions and establish drone policies for federal law enforcement entities. DHS and the U.S. Attorney General coordinate with the U.S. Secretary of Transportation and the FAA before issuing any guidance if it might affect aviation safety, civilian aviation and aerospace operations, aircraft airworthiness, or the use of airspace.

To address the threat drones pose to critical infrastructure, several states have adopted statutes restricting drones from operating near critical infrastructure facilities, prohibiting lethal payloads on drones, and establishing criminal offenses such as trespass by drones. Municipalities have also attempted to restrict drone use through ordinances. In contrast, some states have restricted local governments from enacting restrictions on drone use. A limited number of court decisions are available for guidance.

Countering threats from UAS activity will become increasingly complex and will require the use of emerging and converging technologies in the future, requiring additional resources to maintain adequate security of critical infrastructure.

Highlights of Existing State Laws

Maryland

Currently Maryland has two statutes that address UAS issues explicitly. “Unmanned Aircraft” and Unmanned Aircraft System” are defined.[153] These definitions are circular in that each term relies on the other as a component of the definition.[154] The Maryland definition of UA uses the term “ground control system”, which would arguably exclude a piloted drone from an airborne or open-water control system. The federal definitions for UA and UAS do not have these disadvantages.

---

[152] ¶ 3568o, Sec. 1602. Protection of Certain Facilities and Assets From Unmanned Aircraft., Av. L. Rep. P 3568O t.

[153] MD ECON DEV § 14-301. Laws governing the testing and operation of unmanned aircraft systems. Effective July 1, 2015.

[154] In the Maryland statute MD ECON DEV § 14-301, the term “unmanned aircraft” is defined using the term “unmanned aircraft system”, and vice versa.

"Only the State may enact a law or take any other action to prohibit, restrict, or regulate the testing or operation of unmanned aircraft systems in the State."[155] The Department of Transportation is assigned to monitor the FAA for any proposed regulations or rulemaking, consult with county and local governments regarding such FAA actions, and report to the governor and general assembly.[156]

"Except for federal, State, and local government entities or law enforcement services agencies, an individual may not launch, land, or retrieve an unmanned aircraft system (UAS) on any State real property without prior written approval from the Secretary or the Secretary's designee."[157]

Definitions

Federal statutes and most state laws refer to drones as "unmanned aircraft", and the remote-control system and drone together are called "unmanned aircraft systems" (UAS). However, some states use other terms.[158] Most states with UAS statutes have adopted the federal terms and definitions, some with modification.

> **Unmanned aircraft.** -- The term "unmanned aircraft" means an aircraft that is operated without the possibility of direct human intervention from within or on the aircraft.
>
> **Unmanned aircraft system.** -- The term "unmanned aircraft system" means an unmanned aircraft and associated elements (including communication links and the components that control the unmanned aircraft) that are required for the operator to operate safely and efficiently in the national airspace system.
>
> 49 U.S.C.A. § 44801

Usually, the definition of UAS can be found in either the aviation or criminal section of statutes. The criminal code is often used since trespass using a drone is generally classified as a misdemeanor criminal offense.

In addition to defining UAS, states define other terms such as "operator", "image", and "harassment". Failing to define UAS statute terms with specificity has been an issue in at least one federal district court case.[159] The definition of "critical infrastructure" would be key in having a valid criminal statute forbidding intended harm to critical infrastructure. (See 'Defining "Critical Infrastructure"' for more on this topic.)

Michigan Treats Drones as "Extensions of Self"

Michigan enacted the "Unmanned Aircraft Systems Act" in 2017 and with it created a task force to develop recommended rules governing the use of UAS within the state.[160] The desire of the task force was to foster a regulatory environment that respects state and local authority but also creates an

---

[155] MD ECON DEV § 14-301. Laws governing the testing and operation of unmanned aircraft systems. Effective July 1, 2015.
[156] MD Code, Economic Development, § 14-302. Monitoring of regulation of small commercial unmanned aircraft systems. Effective: July 1, 2019.
[157] Md. Code Regs. 04.05.01.08 – Department of General Services; Buildings and Grounds; Demonstrations and Rallies.
[158] For example, Washington uses "Remote controlled aircraft", Hawaii uses "drone", Nevada and Indiana use "unmanned aerial vehicle". Louisiana calls a UAS an "unmanned *aerial* system", but uses "unmanned aircraft system" UAS to reference the aircraft only.
[159] Nat'l Press Photographers Ass'n v. McCraw, 504 F. Supp. 3d 568 (W.D. Tex. 2020)
[160] Mich. Comp. Laws Ann. § 259.331

innovative environment for UAS testing, development, and deploying the technology.[161] The Task Force generated thirteen recommendations. This included a recommendation to "enact legislation establishing an "extension of self" principle. This means actions which are currently allowed or prohibited by persons would apply to persons using an UAS."[162] The recommendation was implemented in 2019.[163]

Using the "extension of self" approach, a specific definition of "critical infrastructure" is not included in the Michigan penal code. This whole approach may leave a gap in prosecuting trespass based on the current Michigan trespass law. The trespass offense is defined in terms of "land and premises". "Premises" is defined in the penal code in such a way as to reasonably exclude airspace.[164] Since flying a drone 300 feet above a critical infrastructure facility for surveillance is something a person could not do without a drone, arguably the act is not prohibited under current Michigan laws.

Michigan also adopted a statute concerning UAS use by government entities to collect information about a regulated facility.[165] If regulators wish to inspect a facility with a UAS, the facility owner/operator may condition the inspection on the use of the facility's drone, or may refuse the request for using a UAS for inspection. However, the facility owner/operator must provide a written explanation giving the health and safety reasons for the condition or refusal.

In addition, any political subdivision of the state must allow for UAS operation for maintenance performed by a public utility or independent transmission company if that operation "does not result in a knowing and intentional interference with the safe use of a horse in a commercial activity."[166]

The Michigan aeronautics commission is responsible for providing advice to the public about regulations of UAS and restrictions on the use of UAS.[167]

Kentucky Defines a Specific Offense for Trespass on Key Infrastructure Assets

Kentucky defines UAS and "Key infrastructure", which includes "Any critical node of a system used in the production or generation of electrical energy."[168] The misdemeanor offense of Trespass Upon Key Infrastructure Assets" explicitly includes reference to UAS.[169] "A person commits the offense of trespass upon key infrastructure assets if he or she knowingly uses, or retains or authorizes a person to use, an unmanned aircraft system to fly above real property on which key infrastructure assets are located with the intent to cause harm or damage to or conduct surveillance of the key infrastructure asset without

[161] Michigan UAS Task Force Final Report, November 20, 2017. https://www.michigan.gov/documents/aero/UASTF_Final_Report_v2_Full_606520_7.pdf
[162] Ibid.
[163] Mich. Comp. Laws Ann. § 259.320. Offenses committed with aid of unmanned aircraft system
[164] Mich. Comp. Laws Ann. § 750.141a. '"Premises" means a permanent or temporary place of assembly, other than a residence, including, but not limited to, any of the following: (i) A meeting hall, meeting room, or conference room; (ii) A public or private park.'
[165] Mich. Comp. Laws Ann. § 259.307. Use of unmanned aircraft system to surveil, inspect, gather evidence, or collect information; conditions; disclosure of data collected; applicability.
[166] Mich. Comp. Laws Ann. § 259.305. Regulation by political subdivisions; construction with other laws
[167] Mich. Comp. Laws Ann. § 259.330. Duties of commission; support.
[168] Ky. Rev. Stat. Ann. § 511.100 Trespass upon key infrastructure assets
[169] Ibid.

the prior consent of the owner, tenant, or lessee of the real property." [170] In this statute, using the phrase "flying above" without specifying a height limit might create pre-emption issues.

Kentucky penal code also forbids equipping UAS with lethal payload, except for military entities and the Coast Guard.[171]

Pre-emption[172]

A major issue facing state law makers when drafting UAS legislation is pre-emption. The federal government has exclusive sovereignty of airspace of the United States and FAA has regulatory authority over matters pertaining to aviation safety.[173]

Because federal registration is the exclusive means for registering UAS for purposes of operating an aircraft in navigable airspace, no state or local government may impose an additional registration requirement on the operation of UAS in navigable airspace without first obtaining FAA approval.[174] Cities and municipalities are not permitted to have their own rules or regulations governing the operation of aircraft.[175] However, they may generally determine the location of aircraft landing sites through their land use powers.

At least three states have addressed the pre-emption issue in statutes to some degree. Virginia adopted a pre-emption statute restricting "localities" from legislating UAS use other than for take-off and landing.[176] A subsequent official advisory opinion concluded that since the term "locality" means only "a county, city, or town",[177] the Fairfax County Park Authority may adopt rules or regulations concerning the operation of unmanned aircraft systems, commonly known as drones, in its parks.[178] In 2020 the Virginia House introduced a bill that would amend the rule to add "time, place, or manner restrictions regarding the takeoff or landing of unmanned aerial systems on property owned by the political subdivision."[179] The bill was not adopted.

Michigan and Delaware adopted a pre-emption clause that allows only the state government to take action to prohibit or restrict the testing and operation of UAS.[180]

---

[170] Ky. Rev. Stat. Ann. § 511.100 Trespass upon key infrastructure assets

[171] Ky. Rev. Stat. Ann. § 500.130 Operation of unmanned aircraft system; Citizen's Freedom from Unwarranted Surveillance Act

[172] The Supremacy Clause of the United States Constitution provides that federal laws are supreme, U.S. Const. art. VI, cl. 2, thus requiring that federal laws preempt any conflicting state or local regulations, see Maryland v. Louisiana, 451 U.S. 725, 746, 101 S.Ct. 2114, 68 L.Ed.2d 576 (1981) (citing McCulloch v. Maryland, 4 Wheat. 316, 427, 4 L.Ed. 579 (1819)).

[173] 49 U.S.C. § 40103(a)(1)

[174] 14 C.F.R. part 107. See e.g. Singer v. City of Newton, 284 F. Supp. 3d 125 (D. Mass. 2017) – local ordinance's registration requirements for pilotless aircraft were subject to conflict preemption.

[175] "Press Release – FAA Statement–Federal vs. Local Drone Authority", July 20, 2018. https://www.faa.gov/news/press_releases/news_story.cfm?newsId=22938

[176] VA Code Ann. § 15.2-926.3. Local regulation of certain aircraft.

[177] VA Code Ann. § 15.2-102 (2012).

[178] 2018 WL 2215258, at *2 (Va. A.G. Mar. 1, 2018)

[179] 2020 Virginia House Bill No. 311, Virginia 2020 Regular Session.

[180] MCLA 259.303. Definitions; 11 Del. C. § 1334. Unlawful use of an unmanned aircraft system; unclassified misdemeanor; class B misdemeanor; class A misdemeanor.

The City of Newton, MA was sued over portions of a city ordinance relating to ownership registration and operation of pilotless aircraft.[181] The Court found that The City of Newton failed to get FAA approval for the registration requirement. Also, the restrictions on UAS flight did not limit its reach to any altitude so is "ground for preemption … because it certainly reaches into navigable airspace."[182] The Court decided that the effective total ban on UAS flight over any part of the city without prior permission from the land owner thwarts the federal government's objective of integrating drones into the national airspace.

Pre-emption was also an issue addressed in the Texas case.[183] The Court ruled that the Federal Aviation Act (FAA) did not preempt state statutes regulating operation of unmanned aircraft flying over certain structures at under 400 feet, notwithstanding FAA's goal of integrating unmanned aircraft into national airspace system. The Texas regulations were related to state's police powers, federal regulations applied only to unmanned aircraft flying over 400 feet, and state's prohibitions did not cover broad area of state's airspace.

Federal rules require that anyone controlling a AUS keep the aircraft below an altitude of 400 feet above ground level or within a 400-foot radius of a structure.[184] Taking this into account, some states have specified the height of the drone as an element of the criminal statute. Oklahoma, Texas, and Oregon make operating an unmanned aircraft lower than 400 feet *above* critical infrastructure a criminal offense. Tennessee sets the limit to within 250 feet of the *perimeter* of critical infrastructure facility. However, a Kentucky statute only specifies "flies above" which may conflict with federal authority, but limits the restriction to operators "with the intent to cause harm or damage to or conduct surveillance of the key infrastructure asset without the prior consent of the owner, tenant, or lessee of the real property."[185]

Constitutional Issues

Constitutional issues may also be implicated in state UAS statutes. In Texas, a district court case filed by media organizations and reporters against law enforcement officials of the state sufficiently pled that the Texas statute outlining when unmanned aerial vehicles (UAV) could be used to capture images impermissibly imposed speaker-based and content-based restrictions, in violation of First Amendment, by alleging that statute exempted certain speakers from liability, but subjected other speakers such as journalists to civil and criminal liability for same conduct.[186]

The Plaintiffs' also assert that state statutes regulating the use of unmanned aircraft were impermissibly vague under First Amendment Free Speech Clause and Due Process Clause by alleging that statutes did not define "surveillance" that they prohibited,[187] that dictionary definitions of the term were so broad that application of surveillance provisions was unclear, and that the State had made no attempt to

[181] Singer v. City of Newton, 284 F. Supp. 3d 125, 126 (D. Mass. 2017)
[182] Ibid.
[183] Nat'l Press Photographers Ass'n v. McCraw, 504 F. Supp. 3d 568 (W.D. Tex. 2020)
[184] 14 CFR § 107.51(b)
[185] KRS 511.100 Trespass upon key infrastructure assets
[186] Nat'l Press Photographers Ass'n v. McCraw, 504 F. Supp. 3d 568 (W.D. Tex. 2020)
[187] "'It is a basic principle of due process that an enactment is void for vagueness if its prohibitions are not clearly defined." United States v. Kim, 449 F.3d 933, 941 (9th Cir. 2006) (quoting Grayned v. City of Rockford, 408 U.S. 104, 108 (1972))

define the term or point to any authority or evidence that outlined what type of unmanned aircraft use was prohibited under "surveillance".

Plaintiffs' Constitutionally based claims survived a Motion to Dismiss.[188]

Identifying Critical Infrastructure

In 2018, Congress ordered the Secretary of Transportation, within six months, to implement a process where critical infrastructure facilities could be registered.[189] The plan has been implemented for federal facilities, but has not yet been implemented for State or local governments.[190] The FAA states that the decision as to which facilities could be added to the "Security Sensitive Airspace Restriction list" is not within their authority.

In April 2020, the US Attorney General provided instructions to Department of Justice (DOJ) components on the processes and standards for seeking the Department's designation of a DOJ facility or asset for protection, as well as the legal framework for exercising measures to protect those designated facilities and assets.[191] "The request will describe the facility or asset proposed for designation with specificity, including its nature and location; its surroundings, including proximity to air traffic, airports, air traffic control facilities, or other airspace features; whether it is stationary or mobile; and whether a significant portion of the facility or asset belongs to or is operated by any person or entity other than the Department."[192]

In October 2020, a group of commercial drone owner/operators wrote an open letter urging action by the federal government to implement the process for registering critical infrastructure.[193] The letter states, "the tremendous growth of the UAS industry prompted many state and local policymakers to enact legally questionable UAS operating restrictions around many different types of facilities, some of which directly challenge the federal sovereignty of the National Airspace System." It claims that state and local statutes are "impacting the public's right to access navigable airspace and putting operators at risk of local prosecution even when flying in accordance with FAA regulations" and that these laws "create an unworkable patchwork of prohibitions that impacts UAS operators' access to airspace and thus should be addressed expeditiously."

The current situation leaves law enforcement, critical infrastructure facilities, and drone operators in an ambiguous enforcement environment.

---

[188] Nat'l Press Photographers Ass'n v. McCraw, 504 F. Supp. 3d 568 (W.D. Tex. 2020)

[189] Pub. L. 114-190 s. 2209.

[190] FAA response to email inquiry received from uashelp@faa.org on 6/8/21. The response stated, "only Federal properties are eligible to be on the Security Sensitive Airspace Restriction list, although the FAA is working on a mechanism to eventually make this eligibility available to state and local governments. Eligible federal entities must contact Dept of Energy, Dept of Interior, or Dept of Defense, as applicable, to see if those agencies want to include the facility on the list. The decision is not the FAA's."

[191] Guidance Regarding Department Activities to Protect Certain Facilities or Assets from Unmanned Aircraft and Unmanned Aircraft Systems. US Attorney General Barr Memo, April 13, 2020. https://www.justice.gov/archives/ag/page/file/1268401/download

[192] Ibid.

[193] Coalition Letter Urging the FAA to Comply with Section 2209 Requirements, dated Oct 22, 2020. https://americaninnovators.com/research/coalition-letter-urging-the-faa-to-comply-with-section-2209-requirements/

Conclusions

A variety of state laws created to protect critical infrastructure have developed recently. Several states have adopted definitions of “unmanned aircraft systems” and “critical infrastructure”, and created criminal trespass offenses for drones flying over or near critical infrastructure. At least one state has treated drones as an extension of self in terms of prohibited acts. States have addressed the issue of pre-emption relating to both federal and local rules. It would be helpful to all concerned to have clear notice of areas where drones are prohibited and the conditions under which the prohibition applies.

Appendix C. Interview with MPSC Chief Engineer (January 19, 2021)

I had the pleasure of meeting with the Chief Engineer of the Maryland Public Service Commission (MPSC). He worked for 35 years as an engineer at BGE and eventually became Vice President (VP) of Engineering, managing the regulatory relationships for the utility with the MPSC Engineering Division. He worked with MPSC regulators and has known every MPSC Chief Engineer since the late 1980s. He was also the NERC CIP audit executive sponsor for their 2014 audit, leading BGE in the Federal regulatory efforts related to transmission grid cybersecurity. He retired from BGE in 2015, then in 2017 was requested to consider applying for the open MPSC Chief Engineering position. It is clear the Chief Engineer came to MPSC with a deep understanding of the regulatory process as seen from the utility company perspective.

The MPSC Chief Engineer described the MPSC Engineering Division as a group of sixteen engineers, all who have come to MPSC with no experience in the utility industry. Five of these engineers are on the team that gets involved in cybersecurity. The MPSC Engineering Division has three open positions presently. None of the current team members have cybersecurity expertise and there is no dedicated cybersecurity staff. The team is learning about utilities and cybersecurity. Chief Engineer expressed a need for more cybersecurity expertise since they are facing cybersecurity issues more and more. He cited salary levels as a potential barrier to hiring cybersecurity expertise.

One source of support used and appreciated by MPSC Engineers is the National Association of Regulatory Utility Commissioners (NARUC). He said that NARUC had released new products in 2020 to gather and evaluate information from utilities about their cybersecurity risk management and preparedness. These tools haven't yet been integrated into MPSC processes. These products may influence the reporting process currently in use. Members of the MPSC Engineering Team will be attending the NARUC cybersecurity training for three days in February. NARUC was also a helpful resource in understanding the Solarwinds incident and potential impacts.

The Maryland Coordination and Analysis Center (MCAC) was also mentioned as a useful liaison for cybersecurity.

The Chief Engineer mentioned that the NERC GridX exercise brought to light cybersecurity issues but it is difficult to estimate the impact they might have or to develop a standard way to deal with the information gained. He thinks it might be helpful to get the utilities together and come up with different levels of impact and to categorize impacts. For cybersecurity breach incidents, the MPSC encourages utilities to interact with the DHS National Cybersecurity and Communications Integration Center (NCCIC) and MCAC initially. MPSC receives information later. GridX participation also emphasized the interrelationship between physical security and cyber security.

MPSC ordered the creation of a Cybersecurity Reporting Working Group (CSRWG) in 2018. Chief Engineer led that group and authored a report presented to MPSC commissioners with a proposed process for utilities to inform MPSC about their cybersecurity strategies, implementations, and breaches. MPSC adopted the proposals, with modification, and the first cybersecurity reporting took place in 2019. Utilities would report once every three years, a time period in sync with the FERC auditing schedule. MPSC started with the two largest utilities in 2019 and planned for others to report in 2020 and 2021. However, the COVID-19 emergency suspended the reporting process since in-person

meetings were to be avoided for health reasons and providing sensitive information in virtual meetings was not an option the participants found acceptable.

The information that came from the reporting centered on metrics such as phishing attempts, intrusion attempts, and cybersecurity program maturity levels. Both the C2M2 and the NIST Framework are used by utilities in the state. Both of the reporting utilities referenced maturity models. The NARUC list of questions from their Cybersecurity Primer were used a bit, but mostly the Commissioners were heavily engaged with their own questions and also relied on senior advisors for their preparation and back office work.

The MPSC will complete one reporting cycle and then the CSRWG will be reconvened to review lessons learned. To date, only two utilities have reported. Chief Engineer noted that of the two, one utility was more transparent than the other. A discussion was held by Chief Engineer on the need to improve transparency between the regulators and that utility company in future briefings. He noted that no entity wants to look bad in front of a regulator, and so the "Nothing to See Here" approach may be an issue that needs to be addressed. Utilities want to avoid follow-up from regulators. In his experience, information coming from utilities to regulators is tightly controlled, and presentations and statements to be made are reviewed and edited by in-house counsel.

There is no formal mechanism for follow-up after the periodic reporting meeting takes place. Chief Engineer said there are no on-site inspections for cybersecurity. The current process provides for a half day meeting with specified participants from the utility, the MPSC, and the People's Counsel. The CSRWG will further consider the frequency of cybersecurity program reporting after the first cycle of utility reports are completed.

Part of the 2018 CSRWG report included proposed regulatory language. I asked Chief Engineer why that language had not yet been incorporated into COMAR. He said MPSC wanted to gain experience with the reporting before codifying the recommendations. This would allow for modification based on lessons learned during the first reporting cycle. He felt that the regulations recommended were on target so far, but in light of the Solarwinds incident, a broader approach may be needed. There will also need to be consideration given to an assessment phase after the reporting phase is completed. Chief Engineer also said that the gas and water side of the MPSC Engineering Division is currently not involved with cybersecurity, but gas and water utilities are included in the MPSC cybersecurity reporting procedures developed by the CSRWG.

Chief Engineer stated that MD Delegate Neil Parrott had introduced bills in the past related to utility cybersecurity and physical security multiple times, but those bills were not adopted.

We discussed cybersecurity funding by the utilities. Chief Engineer stated that a multi-year rate plan was a "forward-looking" view to spending. This is a new approach to rate recovery. The usual "backward-looking" approach allows utilities to plan their systems and programs with a determination if their expenses were prudently incurred to be made after the expenses have been incurred. Forward-looking rate cases can potentially affect future operations of the utilities if the utility adjusts spending on systems and programs as a result of a disallowance. MPSC Engineering Division Staff has to be careful when recommending disallowing expenses in a forward-looking approach because if a denial of funds for a particular purpose ultimately can be pointed to as a cause of a problem, then the utility may come back and place blame for the problem on the denial of funds. This approach clouds accountability

between the utility company and regulators, which will be required to pass judgment on the utility if something goes wrong. For rate cases, MPSC staff has to take an independent approach that considers both the utility company view and the consumer view when making recommendations to the Commission.

Chief Engineer described the difficulty in addressing cybersecurity funding in a rate case since sensitive information related to spending is difficult to disclose in that forum and associated discovery requests to the utilities are treated confidentially. There is a need for more specific and detailed information about funding needs in the periodic cybersecurity reporting with the MPSC. However, rate cases are filed by utilities as the need arises and not on any predetermined schedule. Cybersecurity reporting is currently on a three year schedule. Therefore, timing the of funding disclosures during periodic cybersecurity reporting doesn't naturally sync with rate case schedules.

Appendix D. Standards and Security Guidelines for Distributed Energy Resources[194]

- IEEE C37.240 2014: IEEE Standard Cybersecurity Requirements for Substation Automation,
- Protection, and Control Systems
- NIST SP 800 82 Revision 2: Guide to Industrial Control Systems (ICS) Security
- NIST Interagency/Internal Report 7628: Guidelines for Smart Grid Cybersecurity
- NIST Cybersecurity Framework
- IEEE 2030.5 2018: SEP2 Smart Energy Profile 2.0
- NERC Reliability Guideline : Cyber Intrusion Guide for System Operators
- IEC 62351 : Information Security for Power System Control Operations
- IEC 62443 : Industrial Automation and Control Systems Security
- DOE/DHS ES C2M2 : Electricity Subsector Cybersecurity Capability Maturity Model (ES C2M2)
- DOE/NIST/NERC RMP : Electricity Subsector Cybersecurity Risk Management Process Guideline
- IEEE 1547.3: Guide for Cybersecurity of DERs Interconnected with Electric Power Systems
- Potential to leverage ISA/IEC 62443 for DER: Cybersecurity Certification Scheme for DER

[194] This list was part of a presentation to the California Public Utility Commission on January 14, 2014 given by UL.

Appendix E. Summary of Recommendations

RECOMMENDATION 1. Amend Md. Code Ann., Pub. Util. § 7-213(e)(1)(i) "Service quality and reliability standards" to include "cyber resiliency" in the list of topics to be addressed by the standards.

RECOMMENDATION 2. Climate change is a long-term problem that motivates modernization of the electric grid. Solutions to address climate change must not invite near-term catastrophe. Any changes to the grid made for the sake of resiliency, efficiency, conservation, or climate change concerns must be accompanied by a careful assessment to document security risks prior to grid integration and implement appropriate mitigations during integration. The risk assessments must take into account the scope of specific projects and the project's interfaces with other systems.

RECOMMENDATION 3. Define "resilience" to include "the ability to prepare for and adapt to changing conditions and withstand and recover rapidly from deliberate attacks" so that cybersecurity will be an essential factor in determining system resilience.

RECOMMENDATION 4. Require utility providers to adopt security best practices such as the NIST Cybersecurity Framework and advance toward zero-trust architecture both with on-premises services *and* cloud services. Report to regulators on steps already completed. Identify the steps that will have the most immediate security impact, and a schedule to implement them.

RECOMMENDATION 5. Require utility providers to incrementally implement zero trust principles, process changes, and technology solutions that protect data assets and business functions by use case.[195] Develop and maintain dynamic risk-based policies for resource access. Authenticate all connections and encrypt data. Design cybersecurity of newly interconnected resources around zero-trust principles.

RECOMMENDATION 6. Consult with grid owners and operators, and state and local government agencies to establish a process to identify, assess, and prioritize risks to the electric grid, considering current and foreseeable future cyber and physical threats, vulnerabilities, and consequences. Apply the process to periodically report to regulators on the risks. Use the report to establish a risk-based grant program focused on systematically increasing the resilience of the electric grid against the prioritized cybersecurity risks where market forces do not provide sufficient private-sector incentives to mitigate the risk without Government investment.

RECOMMENDATION 7. Maryland is a leader in grid modernization efforts in the US. Engage state employees in cybersecurity standards development efforts to share knowledge and insights, and influence future directions.

[195] Zero Trust Architecture, NIST Special Publication 800-207, National Institute of Standards and Technology, August 2020. https://doi.org/10.6028/NIST.SP.800-207.

RECOMMENDATION 8. Include a formal requirement for all state funded grant recipients working on electric grid resilience or modernization to address cybersecurity risk both in the design and reporting phases of their work.

RECOMMENDATION 9. Include a formal requirement for all MPSC working groups developing policy and planning for the grid to address cybersecurity risk in the reporting phase of their work.

RECOMMENDATION 10. Require electric grid resilience or modernization pilot programs to establish formal requirements for a cybersecurity plan. Cybersecurity vulnerabilities arise from weaknesses in: policy and procedure; architecture and design; configuration and maintenance; supply chain; hardware; physical access controls; software development; and communications and networks.[196] An effective cybersecurity plan must address all of these areas.

RECOMMENDATION 11. Maturity level of a cybersecurity program should be a factor in establishing an appropriate reporting period for each utility. Each utility should provide sufficient evidence to establish the maturity level of the company's cybersecurity program. The MPSC should then tailor the reporting period accordingly. For utilities that can provide persuasive evidence of a high level of maturity in their cybersecurity program, three years may be an adequate MPSC reporting period. For less mature programs, more frequent reporting to evidence growth in maturity level is recommended. An example of a maturity model available is The Cybersecurity Capability Maturity Model (C2M2) Version 2.0 (V2.0) which was released in July 2021.[197]

RECOMMENDATION 12. Information technology (IT) and operational technology (OT) systems of utilities were likely developed separately and with separate groups of people. However, without strict network segregation, vulnerabilities in IT enable attacks on OT. Regulators must understand the extent to which utility IT and OT security experts work together to protect the grid and make recommendations to enhance communication within utility provider entities.

RECOMMENDATION 13. Utilities should work together and report together on risks and cybersecurity events. Bring GridEx participants together after the exercises are complete to assess and categorize impacts of issues that were identified.[198]

RECOMMENDATION 14. Each confidential cybersecurity brief required should be accompanied by a written report suitable for public release that summarizes the cybersecurity efforts of the company, especially with respect to modernization efforts.

---

[196] NIST SP 1800-32B: Securing the Industrial Internet of Things: Cybersecurity for Distributed Energy Resources. Volume B. Preliminary Draft, April 2021.

[197] "Cybersecurity Capability Maturity Model (C2M2)", US Department of Energy. https://www.energy.gov/ceser/cybersecurity-capability-maturity-model-c2m2.

[198] GridEx, a distributed play grid exercise that allows participants to engage remotely, simulates a cyber and physical attack on the North American electricity grid and other critical infrastructure. Led by the North American Electric Reliability Corporation (NERC), GridEx gives participants a forum to demonstrate how they would respond to and recover from coordinated cyber and physical security threats and incidents. https://www.nerc.com/pa/CI/ESISAC/Pages/GridEx.aspx

RECOMMENDATION 15. When smart meters were incorporated into the Maryland power grid, utilities were required to publicize security information about the change. This practice should be continued to include changes created by DER integration.[199]

RECOMMENDATION 16. Although details of security processes and mechanisms should be protected as sensitive information, general information about utility security programs should be publicly available and easily accessible.[200]

RECOMMENDATION 17. Require all utilities that rely on third party IT or OT providers to include standard contract language with service providers to collect and preserve data for cybersecurity analysis and share such data, or report third party security breaches to the utility or to a government entity such as CISA.

RECOMMENDATION 18. Adopt the NIST definition of "critical software" and require utilities to maintain a list of the categories of software and software products in use or in acquisition that meet the definition. Adopt NIST security guidance for critical software use, applying practices of least privilege, network segmentation, and proper configuration.[201]

RECOMMENDATION 19. Require utilities to establish minimum security standards for IT and OT devices commensurate with the level of security risk applicable to such devices and specifically take into account any security risk associated with supply chains.

RECOMMENDATION 20. Allocate funds to provide Maryland Public Service Commission with staff dedicated to regulatory cybersecurity policy, strategy, auditing, and reporting.

RECOMMENDATION 21. Ensure MPSC employees involved in cybersecurity activities attend periodic training to keep skills and knowledge current regarding emerging trends in distributed energy resource cybersecurity issues.

RECOMMENDATION 22. MPSC engineers should take an active role in standards organizations upon which they rely to ensure that cybersecurity concerns are addressed during standards development.[202]

RECOMMENDATION 23. Encourage utilities to establish a procedure where cybersecurity leadership of utilities may report directly to the company's Board of Directors or CEO.

---

[199] See e.g. "SMART METERS AND YOUR PRIVACY", BGE informational brochure for customers. Author unknown, undated. https://www.bge.com/SmartEnergy/SmartMeterSmartGrid/Documents/SmartMeters_HealthPrivacyInfo.pdf

[200] See e.g. PJM (a regional transmission organization that coordinates the movement of wholesale electricity in all or parts of 13 states and the District of Columbia) webpage that talks about cybersecurity practices at a very high level. https://learn.pjm.com/three-priorities/keeping-the-lights-on/safeguarding-the-grid.

[201] See "Security Measures for "EO-Critical Software" Use Under Executive Order (EO) 14028", National Institute of Standards and Technology, July 9, 2021. https://www.nist.gov/system/files/documents/2021/07/09/Critical%20Software%20Use%20Security%20Measures%20Guidance.pdf.

[202] For example, the MPSC relies on IEEE standards for interconnection. MPSC engineers should participate in IEEE standards efforts to contribute their knowledge about the Maryland grid and related security needs and concerns.

RECOMMENDATION 24. Expand MD Code, Public Utilities, § 2-203(f) to include cybersecurity expertise in the list the Office of People's Counsel may retain or hire as necessary for a particular matter.

RECOMMENDATION 25. The utility should make available clear, simple identification of all entities or some formal statement of the data management principle to help educate consumers as to the "data chain" that may be in place based on their relationships with utility, utility-authorized third parties, and energy service providers that are not affiliated with a utility.[203]

RECOMMENDATION 26. Incorporate existing privacy standards and frameworks to identify privacy risks, then apply privacy mitigation processes to match proportionate privacy controls for each relevant business activity that creates a risk to privacy.

RECOMMENDATION 27. Develop guidelines relating to privacy and civil liberties governing the receipt, retention, use, and dissemination of cyber threat indicators by the state, including safeguards such as sanctions for activities by officers, employees, or agents of state or local Government for misuse of information.

RECOMMENDATION 28. Modify the current Maryland statutory definition of "cybersecurity" to include the five goals of cybersecurity so that procurement will be guided by specific reference to availability, integrity, authentication, confidentiality, and nonrepudiation.[204]

RECOMMENDATION 29. Adopt a statutory definition of "cyber resilience", "critical infrastructure", "supply chain risk", and "critical software".

[203] NISTIR 7628 Revision 1 Guidelines for Smart Grid Cybersecurity Volume 2 - Privacy and the Smart Grid. The Smart Grid Interoperability Panel – Smart Grid Cybersecurity Committee. http://dx.doi.org/10.6028/NIST.IR.7628r1

[204] Nonrepudiation is "Protection against an individual who falsely denies having performed a certain action and provides the capability to determine whether an individual took a certain action, such as creating information, sending a message, approving information, or receiving a message." Security and Privacy Controls for Information Systems and Organizations, NIST Special Publication 800-53 Revision 5, September 2020. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf.

Bibliography

Acharya, S., Dvorkin, Y., & Karri, R. (2020, February 27). Public Plug-in Electric Vehicles + Grid Data: Is a New Cyberattack Vector Viable? IEEE. Retrieved December 23, 2020, from https://arxiv.org/pdf/1907.08283.pdf

Alliance for Drone Innovation, et al. (2020, October 22). Coalition Letter Urging the FAA to Comply with Section 2209 Requirements. Retrieved June 7, 2021, from https://americaninnovators.com/research/coalition-letter-urging-the-faa-to-comply-with-section-2209-requirements/

Alvarez, P. (2020, June 24). Grid Modernization – A Counter Narrative Policymakers Should Consider. *EnergyCentral.com*. Retrieved January 30, 2021, from https://energycentral.com/c/gr/grid-modernization-%E2%80%93-counter-narrative-policymakers-should-consider

Alvarez, P., & Stephens, D. (2019, January 31). MODERNIZING THE GRID IN THE PUBLIC INTEREST: GETTING A SMARTER GRID AT THE LEAST COST FOR SOUTH CAROLINA CUSTOMERS. Retrieved January 30, 2021, from http://gridlab.org/wp-content/uploads/2019/04/GridLab_SC_GridMod.pdf

American Public Power Association. (2020, July). Grid Security Issue Brief. Retrieved January 14, 2021, from https://www.publicpower.org/system/files/documents/July%202020%20-%20Grid%20Security.pdf

Application of Baltimore Gas and Electric Company for an Electric and Gas Multi-Year Plan, 9645 - ORDER NO. 89678 (Maryland Public Service Commission December 16, 2020). Retrieved May 14, 2021

Bayuk, J. L., Healey, J., Rohmeyer, P., Sachs, M. H., Schmidt, J., & Weiss, J. (2012, April 24). *Cybersecurity Policy Guidebook.* Wiley. Retrieved May 6, 2021

Bing, C. (2021, June 3). Exclusive: U.S. to give ransomware hacks similar priority as terrorism. Retrieved June 4, 2021, from Exclusive: U.S. to give ransomware hacks similar priority as terrorism

Borkoski, J. (2018, April 6). Proposal for Addressing the Cyber-Security Reporting Process for Maryland Utilities: Cyber-Security Reporting Work Group ("CSRWG"). Retrieved December 15, 2020, from https://webapp.psc.state.md.us/newIntranet/maillog/content.cfm?filepath=//Coldfusion/Admin%20Filings/200000-249999/219883\/CSRWG_Report_Final(2).pdf

California Public Utilities Commission. (n.d.). Rule 21 Interconnection. Retrieved from https://www.cpuc.ca.gov/Rule21/

California, S. o. (2021). California Cybersecurity Integration Center. Retrieved June 22, 2021, from https://www.caloes.ca.gov/cal-oes-divisions/law-enforcement/california-cybersecurity-integration-center

Campo-Flores, A. (2021, February 8). Hacker Changed Chemical Level in Florida City's Water System. Wall Street Journal. Retrieved February 16, 2021, from https://www.wsj.com/articles/hacker-changed-chemical-level-in-florida-citys-water-system-11612827672

Canales, K. (2020, December 15). A security expert reportedly warned SolarWinds in 2019 that anyone could access the company's update server with the password 'solarwinds123'. *Business Insider*. Retrieved June 7, 2021, from https://www.businessinsider.com/solarwinds-warned-weak-123-password-could-expose-firm-report-2020-12

Carlton, J., & Blunt, K. (2021, June 18). West Risks Blackouts as Drought Reduces Hydroelectric Power. *wsj.com*. Retrieved June 21, 2021, from https://www.wsj.com/articles/west-risks-blackouts-as-hydroelectric-power-dries-up-11624008601

Carr, M., & Lesneiwska, F. (2020, September 17). Internet of Things, cybersecurity and governing wicked problems: learning from climate change governance. *International Relations, Vol. 34(3)*. doi:https://doi.org/10.1177/0047117820948247

Chen, J. (2021, April 19). Question to Senior Advisor to the Chairman of PSC about Criminal Investigative Authority. (Laura, Interviewer)

Christiansen, M. R., & Macey, J. C. (2021, February 10). Long Live The Federal Power Act's Bright Line. Retrieved May 25, 2021, from https://harvardlawreview.org/2021/02/long-live-the-federal-power-acts-bright-line/

Clements, J. (2019, June 19). Solar Farm Land Requirements: How Much Land Do You Need? Retrieved April 30, 2021, from https://greencoast.org/solar-farm-land-requirements/#:~:text=When%20we%20use%20thin-film%20technology%2C%20a%201MW%20plant,by%20the%20efficiency%20of%20the%20panels%20and%20technology.

Cleveland, M., Andersen, G., & Shea, D. (2019, November). Modernizing the Electric Grid: State Role and Policy Options. Retrieved December 22, 2020, from https://www.ncsl.org/Portals/1/Documents/energy/Modernizing-the-Electri-Grid_112519_34226.pdf

Coats, D. R. (2019, January 29). Worldwide Threat Assessment of the US Intelligence Community: Statement for the Record.

Code of Federal Regulations. (n.d.). Title 42 CFR §411.351 Definitions. Retrieved February 5, 2021, from https://ecfr.federalregister.gov/on/2021-02-05/title-42/chapter-IV/subchapter-B/part-411/subpart-J/section-411.351

Commission, P. S. (2018, August 31). REVIEW OF COMMENTS OF THE ENGINEERING DIVISION OF THE STAFF OF THE PUBLIC SERVICE COMMISSSION.

Council, M. C. (2019, July 1). Maryland Cybersecurity Council's Activity Report 2017-2019. Retrieved December 11, 2020, from https://www.umgc.edu/documents/upload/maryland-cybersecurity-council-activities-report-2017-2019.pdf

Cybersecurity and Infrastructure Security Agency (CISA). (2020, October 24). NSA and CISA Recommend Immediate Actions to Reduce Exposure Across Operational Technologies and Control Systems. *NSA and CISA Recommend Immediate Actions to Reduce Exposure Across Operational*

Technologies and Control Systems. Retrieved December 21, 2020, from https://us-cert.cisa.gov/ncas/alerts/aa20-205a

Cybersecurity Incentives, Docket No. RM21-3-000 (Federal Energy Regulatory Commission February 5, 2021).

daqamseh, s. (2020, May 18). How do Utilities, Nuclear and Gas plants Return of Capital and Return on Investment works? [sic]. energycentral.com. Retrieved February 9, 2021, from https://energycentral.com/c/pip/how-do-utilities-nuclear-and-gas-plants-return-capital-and-return-investment

Datta, A. (2020, September 05). Vulnerabilities of GPS is a big concern: Dana Goward. *Geospatial World*. Retrieved September 9, 2021, from https://www.geospatialworld.net/blogs/vulnerabilities-of-gps-is-a-big-concern-dana-goward/

De Martini, P., Taft, J., Geiger, R., & Wang, L. (2017, June 28). Modern Distribution Grid Volume 3: Decision Guide. Pacific Northwest National Laboratories. Retrieved December 24, 2020, from https://gridarchitecture.pnnl.gov/modern-grid-distribution-project.aspx

De Vynck, G. (2021, July 25). Workers and consumers hurt by ransomware attacks are starting to sue the companies who got hacked - The Washington Post. *WashingtonPost.com*. Retrieved July 25, 2021, from https://www.washingtonpost.com/technology/2021/07/25/ransomware-class-action-lawsuit/

Delmarva Power and Light Company, Potomac Electric Power Company. (2009, June 26). Proposal for Advanced Metering Infrastructure (AMI). Retrieved May 27, 2021, from https://www.psc.state.md.us/search-results/?q=9207&x.x=16&x.y=12&search=all&search=case

Department of Energy. (n.d.). ESF 12 Events - Office of Cybersecurity, Energy Security, and Emergency Response. *energy.gov*. Retrieved March 16, 2021, from https://www.energy.gov/ceser/esf-12-events

DEPARTMENT OF JUSTICE AND FEDERAL TRADE COMMISSION. (2021, February). ANTITRUST POLICY STATEMENT ON SHARING OF CYBERSECURITY INFORMATION. *2 Materials on Antitrust Compl § 22:11*. Westlaw. Retrieved February 9, 2021

DOUGLAS, E. (2021, February 18). Texas was "seconds and minutes" away from catastrophic monthslong blackouts, officials say. *Texas Tribune*. Retrieved February 20, 2021, from https://www.texastribune.org/2021/02/18/texas-power-outages-ercot/

Dudley, R., & Golden, D. (2021, May 24). The Colonial Pipeline Ransomware Hackers Had a Secret Weapon: Self-Promoting Cybersecurity Firms. Retrieved May 25, 2021, from https://www.propublica.org/article/the-colonial-pipeline-ransomware-hackers-had-a-secret-weapon-self-promoting-cybersecurity-firms

Eaton, C. (2021, July 12). Cyberattacks and Ransomware: How Can We Protect Our Energy Infrastructure? *Wall Street Journal*. Retrieved July 12, 2021, from https://www.wsj.com/articles/cyberattacks-ransomware-energy-infrastructure-11626097901

Eaton, C. (2021, July 12). Cyberattacks and Ransomware: How Can We Protect Our Energy Infrastructure? *The Wall Street Journal*. Retrieved July 20, 2021, from https://www.wsj.com/articles/cyberattacks-ransomware-energy-infrastructure-11626097901?mod=hp_jr_pos1

El Hariri, M., Parvania, M., & Saleh, M. (2020). Implementation of IEEE Standard 1547-2018 for DER Communication Interface using Data Distribution Service. Retrieved May 6, 2021

Elkind, J., & Peter, G. (2021, March 17). America's Drinking Water Is Surprisingly Easy to Poison. *propublica.org*. Retrieved March 17, 2021, from https://www.propublica.org/article/hacking-water-systems

Energy Information Administration. (2020, October 15). Maryland State Profile and Energy Estimates. Retrieved March 13, 2021, from https://www.eia.gov/state/?sid=MD

Engelberg, S. (2021, March 25). Why There's So Much Investigative Journalism About Utility Companies. *ProPublica.com*. Retrieved April 2, 2021, from https://www.propublica.org/article/why-theres-so-much-investigative-journalism-about-utility-companies

Environmental Protection Agency. (2019, May 6). Summary of the Energy Independence and Security Act. Retrieved January 7, 2021, from https://www.epa.gov/laws-regulations/summary-energy-independence-and-security-act

ERCOT. (2019). Texas Cybersecurity Monitor Program. Retrieved from http://www.ercot.com/services/programs/tcmp

Federal Aviation Administration. (2015, December 17). State and Local Regulation of Unmanned Aircraft Systems (UAS) Fact Sheet. *faa.gov*. Retrieved from https://www.faa.gov/uas/resources/policy_library/media/UAS_Fact_Sheet_Final.pdf

Federal Aviation Administration. (2017, April 7). FAA Restricts Drone Operations Over Certain Military Bases. *faa.gov*. Retrieved from https://www.faa.gov/news/updates/?newsId=87865

Federal Aviation Administration. (2021, April 21). Press Release – New Drone Rules Take Effect Today. *faa.gov*. Retrieved June 23, 2021, from https://www.faa.gov/news/press_releases/news_story.cfm?newsId=25980

Federal Aviation Administration, Department of Justice, Federal Communications Commission, Department of Homeland Security. (2020, August). Advisory on the Application of Federal Laws to the Acquisition and Use of Technology to Detect and Mitigate Unmanned Aircraft Systems. Retrieved June 29, 2021, from https://www.cisa.gov/sites/default/files/publications/20_0817_ogc_interagency-legal-advisory-uas-detection-mitigation-technologies_1.pdf

Federal Aviation Authority. (2018, July 20). Press Release – FAA Statement–Federal vs. Local Drone Authority. Retrieved from https://www.faa.gov/news/press_releases/news_story.cfm?newsId=22938

Federal Energy Regulatory Commission. (2020, September 11). FERC Order No. 2222: Fact Sheet. *ferc.gov*. Retrieved June 1, 2021, from https://www.ferc.gov/media/ferc-order-no-2222-fact-sheet

Federal Energy Regulatory Commission. (n.d.). FERC Order No. 2222.

Ferguson, S. (2021, August 12). Cyberspace Solarium Commission Offers Progress Assessment. *govinfosecurity.com*. Retrieved from https://www.govinfosecurity.com/cyberspace-solarium-commission-offers-progress-assessment-a-17277

Ferguson, S. (2021, August 12). Cyberspace Solarium Commission Offers Progress Assessment. *govinfosecurity.com*. Retrieved from https://www.govinfosecurity.com/cyberspace-solarium-commission-offers-progress-assessment-a-17277

Frazier, A., Siracuse, M., & Krogulecki, D. (2017, November 22). UNMANNED AIRCRAFT REGULATIONS - Analysis as Enacted. Retrieved June 7, 2021, from https://www.legislature.mi.gov/documents/2017-2018/billanalysis/Senate/htm/2017-SFA-0917-N.htm

Freed, B. (2019, September 30). Maryland CISO John Evans leaves state government. Retrieved January 10, 2021, from https://statescoop.com/maryland-ciso-john-evans-no-longer-with-state-government/

Gonzalez, O. (2021, February). Texas power outages: Why blackouts hit as temperatures fell. Retrieved February 20, 2021, from https://www.cnet.com/news/texas-power-outages-why-blackouts-hit-as-temperatures-fell/

Gridwise Alliance. (2018). Grid Modernization Index: Key Indicators for a Changing Electric Grid. Retrieved January 7, 2021, from https://gridwise.org/wp-content/uploads/2018/12/GWA_18_GMI-2018_FinalReport_12_17_18.pdf

House, A. A. (2019, October 10). Cover Letter to the Connecticut Critical Infrastructure 2019 Report. Retrieved January 9, 2021, from https://portal.ct.gov/-/media/Office-of-the-Governor/News/20191010-Connecticut-Critical-Infrastructure-2019-Annual-Report.pdf?la=en&hash=6217417B9C8F1440138BC876FD3842C5

Hussain, S., Meraj, M., Abughalwa, M., & Shikfa, A. (2018). Smart Grid Cybersecurity: Standards and Technical Countermeasures. *2018 International Conference on Computer and Applications (ICCA)*. Retrieved May 7, 2021

IEEE Standards Coordinating Committee 21. (2018, February 15). IEEE 1547 Standard for Interconnection and Interoperability of Distributed Energy Resources with Associated Electric Power Systems Interfaces.

In the Matter of Alternative Rate Plans or Methodologies to Establish New Base Rates for an Electric Company or Gas Company, 9618 (Public Service Commission of Maryland September 29, 2020). Retrieved April 20, 2021, from https://webapp.psc.state.md.us/newIntranet/Casenum/NewIndex3_VOpenFile.cfm?FilePath=//Coldfusion/Casenum/9600-9699/9618/42.pdf

IN THE MATTER OF THE APPLICATION OF POTOMAC ELECTRIC POWER COMPANY FOR ADJUSTMENTS TO ITS RETAIL RATES FOR THE DISTRIBUTION OF ELECTRIC ENERGY, 9602 (Maryland Public Service Commission August 12, 2019). Retrieved April 27, 2021, from https://www.psc.state.md.us/wp-content/uploads/Order-No.-89227-Case-No.-9602-Pepco-Rate-Case-Order-Denying-Appeal.pdf

In the matter of the application of WASHINGTON GAS LIGHT COMPANY for authority to increase existing rates and charges and to revise its terms and conditions for gas), 9651 - Surrebuttal Testimony And Exhibits of Sebastian Coppola On behalf of The Maryland Office of People's Counsel (Maryland Public Service Commission December 21, 2020). Retrieved May 14, 2021

IN THE MATTER OF THE REVIEW OF ANNUAL PERFORMANCE REPORTS ON ELECTRIC SERVICE RELIABILITY FILED PURSUANT TO COMAR 20.50.12.11, 9353 (Maryland Public Service Commission March 6, 2019).

IN THE MATTER OF TRANSFORMING MARYLAND'S ELECTRIC DISTRIBUTION SYSTEMS TO ENSURE THAT ELECTRIC SERVICE IS CUSTOMER-CENTERED, AFFORDABLE, RELIABLE AND ENVIRONMENTALLY SUSTAINABLE IN MARYLAND, PC44 (Maryland Public Service Commission January 31, 2017). Retrieved December 31, 2020, from https://www.psc.state.md.us/wp-content/uploads/PC44-Notice.pdf

James, M., McGovern, A., Somelofske, J., Valentine-Fossum, C., & Zweifel, K. (2019, aPRIL). Improving Cybersecurity of the Electric Distribution Grid: Phase One Report. Retrieved December 11, 2020, from https://www.vermontlaw.edu/sites/default/files/2019-04/VLS_IEE_Electricity_Distribution_Grid_Cybersecurity_Phase_1%20Report%5B1%5D.pdf

James, M., Valentine-Fossum, C., McGovern, A., Scarborough, A., Somelofske, J., & Zweifel, K. (2019, November). IMPROVING THE CYBERSECURITY OF THE ELECTRIC DISTRIBUTION GRID: Phase 2 Report. Retrieved March 28, 2021, from https://protectourpower.org/resources/vls-iee-pop-phase-2.pdf

John Borkoski, PSC Chief Engineer. (2021, May 14). PC44 Interconnection Workgroup Phase III Final Report.

Johnson, J., Hoaglund, J. R., Trevizan, R. D., & Nguyen, T. A. (2020). PHYSICAL SECURITY AND CYBERSECURITY OF ENERGY STORAGE SYSTEMS. *2020 U.S. DOE Energy Storage Handbook*. (S. N. Labs, Ed.) Retrieved May 4, 2021, from https://www.sandia.gov/ess-ssl/wp-content/uploads/2021/01/ESHB_Ch18_Physical-Security_Johnson.pdf

Justia US Law. (2021, May 28). Union of Concerned Scientists v. United States Department of Energy, No. 20-1247 (D.C. Cir. 2021). *justia.com*. Retrieved June 1, 2021, from https://law.justia.com/cases/federal/appellate-courts/cadc/20-1247/20-1247-2021-05-28.html

Keogh, M., & Thomas, S. (2017, January). Cybersecurity: A Primer forState Utility Regulators Version 3.0.

Kim, T., Ochoa, J., Faika, T., Mantooth, A., Di, J., & Li, Q. (n.d.). An Overview of Cyber-Physical Security of Battery Management Systems and Adoption of Blockchain Technology. doi:10.1109/JESTPE.2020.2968490

King, A., & Gallagher, T. (2020, March). Cyberspace Solarium Commission Final Report. Retrieved January 4, 2021, from https://www.solarium.gov/report

Kroposki, B., Bernstein, A., King, J., & Ding, F. (2020, November 23). Tomorrow's Power Grid Will Be Autonomous. *IEEE Spectrum*. Retrieved December 29, 2020, from https://spectrum.ieee.org/energy/the-smarter-grid/tomorrows-power-grid-will-be-autonomous

Lee, P. T. (2020, June 23). The Software-Defined Power Grid Is Here. IEEE Spectrum. Retrieved December 29, 2020, from https://spectrum.ieee.org/energy/the-smarter-grid/the-softwaredefined-power-grid-is-here

Lund, P., & Kalavantis, G. (2021, February 4). What Is NERC CIP: The Ultimate Guide. *industrialdefender.com*. Retrieved May 20, 2021, from https://www.industrialdefender.com/what-is-nerc-cip/

Maryland Coordination and Analysis Center. (2017, February 18). Our Mission. Retrieved January 6, 2021, from http://www.mcac.maryland.gov/about_mcac/our_mission/

Maryland Department of Information Technology. (2019, June 18). Governor Hogan Signs Executive Order to Strengthen Cybersecurity in Maryland. Retrieved January 9, 2021, from https://doit.maryland.gov/Pages/press-release06182019.aspx

Maryland Department of Natural Resources. (2020, May 20). Notes from meeting of MET Easement and Stewardship Committee . Retrieved April 28, 2021, from https://dnr.maryland.gov/met/Documents/E-S-Comm-Mtg-Notes-OPEN-SESSION.5.20.2020-and-ClosingStatement.pdf

Maryland Department of Natural Resources. (n.d.). Maryland Power Plant Research Program. Retrieved March 28, 2021, from https://dnr.maryland.gov/pprp/Pages/default.aspx

Maryland Office of People's Counsel. (2016, January). Office of People's Counsel Guide to Understanding Smart Meters and Understanding Fees in Maryland. Retrieved January 15, 2021, from http://opc.maryland.gov/Portals/0/Publications/Consumer%20Publications/Information%20Sheets/OPC%20Guide%20to%20Smart%20Meters%20and%20Fee%20Options..pdf?ver=2020-05-04-152705-933

Maryland Public Service Commission. (2016). *2015 ANNUAL REPORT.* Retrieved April 27, 2021, from http://www.psc.state.md.us/wp-content/uploads/2015-MD-PSC-Annual-Report-1.pdf

Maryland Public Service Commission. (2019, December 31). 2019 Annual Report Pursuant to § 2-122 of the Public Utilities Article Code of Maryland. Retrieved January 11, 2021, from https://www.psc.state.md.us/wp-content/uploads/2019-MD-PSC-Annual-Report.pdf

Maryland Public Service Commission. (2019, December). TEN-YEAR PLAN (2019 - 2028) OF ELECTRIC COMPANIES IN MARYLAND. Retrieved December 23, 2020, from https://www.psc.state.md.us/wp-content/uploads/2019-2028-Ten-Year-Plan-FINAL.pdf

Maryland Public Service Commission. (2019, July). The EmPOWER Maryland Energy Efficiency Act Report of 2019. Retrieved January 6, 2021, from https://www.psc.state.md.us/wp-content/uploads/2019-EmPOWER-Maryland-Energy-Efficiency-Act-Standard-Report.pdf

Maryland Public Service Commission. (2020, February 4). Maryland PSC Establishes Framework for Multi-Year Utility Rate Plans. Retrieved April 9, 2021, from https://www.psc.state.md.us/wp-content/uploads/MD-PSC-Establishes-Framework-for-Multi-Year-Rate-Plans_02042020.pdf

Maryland Public Service Commission. (2021). *2020 Annual Report.* Retrieved April 27, 2021, from https://www.psc.state.md.us/wp-content/uploads/2020-MD-PSC-Annual-Report.pdf

Maryland Public Service Commission. (2021). Energy Efficiency and EmPOWER Maryland. Retrieved March 3, 2021, from https://www.psc.state.md.us/electricity/empower-maryland/

Maryland Resiliency through Microgrids Task Force. (2014, June 23). Maryland Resiliency through Microgrids Task Force Report. Retrieved from https://energy.maryland.gov/Documents/MarylandResiliencyThroughMicrogridsTaskForceReport_000.pdf

Maryland State Profile and Energy Estimates. (2020, October 15). Retrieved December 24, 2020, from https://www.eia.gov/state/analysis.php?sid=MD

MEA, PSC, MEMA. (2012). 2012 Maryland Energy Assurance Plan. Retrieved March 12, 2021, from https://energy.maryland.gov/Documents/MarylandEnergyAssurancePlan.pdf

Mishra, S. (2021, February 19). Huge fire breaks out in Texas apartment building as fighters unable to get water from frozen hydrants. *Independent*. Retrieved February 20, 2021, from https://news.yahoo.com/huge-fire-breaks-texas-apartment-101543291.html

Morehouse, C. (2019, August 22). Controversial Duke multiyear rate plan upended in North Carolina House. *utilitydive.com*. Retrieved April 22, 2021, from https://www.utilitydive.com/news/controversial-duke-multiyear-rate-plan-stalls-in-north-carolina-house/561464/

Mulcahy, S., Agnew, D., & Pollock, C. (2021, February). "What happened is completely unacceptable": Gov. Greg Abbott calls for winterization of Texas energy system. *The Texas Tribune*. Retrieved March 3, 2021, from https://www.texastribune.org/2021/02/18/greg-abbott-winter-storm/

National Association of Regulatory Utility Commissioners - National Association of State Energy Officials. (2021, February). Blueprint for State Action. Retrieved August 3, 2021, from https://pubs.naruc.org/pub/14F19AC8-155D-0A36-311F-4002BC140969

National Association of Regulatory Utility Commissioners. (2020). *THE UTILITY REGULATOR'S ROLE IN PROMOTING CYBERSECURITY: Resilience, Risk Assessment, and Standards.* United States Agency For International Development (USAID). Retrieved May 10, 2021, from https://pubs.naruc.org/pub.cfm?id=C3597EE6-155D-0A36-31AC-3F82F33A665B

National Association of State Energy Officials. (2020, June 5). Enhancing Energy Sector Cybersecurity: Pathways for State and Territory Energy Offices. Retrieved March 12, 2021, from https://www.naseo.org/data/sites/1/documents/publications/Final%20NASEO_Cybersecurity%20Report%20(062020).pdf

National Conference of State Legislatures. (n.d.). Securing the Nation's Energy Future: 2019-2020 State Legislative Action. Retrieved December 21, 2020, from

https://www.ncsl.org/research/energy/securing-the-nation-s-energy-future-2019-2020-state-legislative-action-637304128.aspx

National Institute of Standards and Technology. (2015). Glossary. Retrieved February 5, 2021, from https://csrc.nist.gov/glossary/term/cybersecurity

National Institute of Standards and Technology. (2018, May 7). Smart Grid Communications. Retrieved January 14, 2021, from https://www.nist.gov/programs-projects/smart-grid-communications-0

National Institute of Standards and Technology. (2021, March 11). NIST RMF Quick Start Guide Assess Step FAQs. Retrieved June 14, 2021, from https://csrc.nist.gov/CSRC/media/Projects/risk-management/documents/05-Assess%20Step/NIST%20RMF%20Assess%20Step-FAQs.pdf

National Intelligence Council. (2021, March). Global Trends 2040. *dni.gov*. Retrieved April 15, 2021, from https://www.dni.gov/files/ODNI/documents/assessments/GlobalTrends_2040.pdf

Nat'l Press Photographers Ass'n v. McCraw, 504 F. Supp. 3d 568 (W.D. Tex. 2020) (United States District Court, W.D. Texas, Austin Division November 30, 2020).

NC Clean Energy Technology Center. (2020, October 28). The 50 States of Grid Modernization: Q3 2020 Executive Summary. Retrieved January 29, 2021, from https://nccleantech.ncsu.edu/wp-content/uploads/2020/10/Q32020_gridmod_exec_final.pdf

Neema, H., Volgyesi, P., Koutsoukos, X., Roth, T., & Nguyen, C. (2020, July 7). Online Testbed for Evaluating Vulnerability of Deep Learning Based Power Grid Load Forecasters. (Modeling and Simulation of Cyber-Physical Energy Systems). National Institute of Standards and Technology. doi:https://doi.org/10.1109/MSCPES49613.2020.9133701

North American Electric Reliability Corporation. (n.d.). GridEx V Grid Security Exercise Lessons Learned Report March 2020. Retrieved Dec 22, 2020, from https://www.nerc.com/pa/CI/ESISAC/GridEx/GridEx%20V%20Public%20Report.pdf

NORTH AMERICAN ENERGY STANDARDS BOARD. (2020, June 25). NAESB REACHES SIGNIFICANT MILESTONE IN EFFORT TO SUPPORT THE IMPLEMENTATION OF DISTRIBUTED LEDGER TECHNOLOGIES FOR THE WHOLESALE NATURAL GAS MARKET. Retrieved June 25, 2021, from https://www.naesb.org//pdf4/062520press_release.pdf

Office of the Director of National Intelligence. (2021, April 9). Annual Threat Assessment of the US Intelligence Community. Retrieved April 15, 2021, from https://www.dni.gov/files/ODNI/documents/assessments/ATA-2021-Unclassified-Report.pdf

Ohio Public Utilities Commission. (2018, August 29). PowerForward: A Roadmap to Ohio's Electricity Future. Retrieved December 31, 2020, from https://puco.ohio.gov/wps/wcm/connect/gov/38550a6d-78f5-4a9d-96e4-d2693f0920de/PUCO+Roadmap.pdf?MOD=AJPERES&CONVERT_TO=url&CACHEID=ROOTWORKSPACE.Z18_M1HGGIK0N0JO00QO9DDDDM3000-38550a6d-78f5-4a9d-96e4-d2693f0920de-nawqRqj

Order 89015 - ML 223860, 9492 (Maryland Public Service Commission February 4, 2019). Retrieved December 23, 2020

ORDER NO. 89678 - ORDER ON PILOT APPLICATION FOR A MULTI-YEAR RATE PLAN, 9645 (Maryland Public Service Commission December 16, 2020). Retrieved May 14, 2021

Orlinsky, E., Hickey, K., & Shaf, D. (2014, December). Cybersecurity: A Legal Perspective. 32, 36.

Osborn, C. (2021, May 11). Colonial Pipeline attack: Everything you need to know. *zdnet.com*. Retrieved May 11, 2021, from https://www.zdnet.com/article/colonial-pipeline-ransomware-attack-everything-you-need-to-know/

Owen, K. (2021, February 11). Maryland Announces Plan for Electric Grid of the Future. Retrieved April 27, 2021, from https://news.maryland.gov/mea/2021/02/11/maryland-announces-plan-for-electric-grid-of-the-future/

Oxner, R. (2021, February 19). Texans now face a water crisis after enduring days without power. *Texas Tribune*. Retrieved February 20, 2021, from https://www.texastribune.org/2021/02/19/texas-water-power-outages/

Pavlus, J. (2021, July 14). The Computer Scientist Training AI to Think With Analogiee. *Quanta Magazine*. Retrieved July 20, 2021, from https://www.quantamagazine.org/melanie-mitchell-trains-ai-to-think-with-analogies-20210714/

Perlroth, N., & Benner, K. (2021, June 7). U.S. Seizes Share of Ransom From Hackers in Colonial Pipeline Attack. *New York Times*. Retrieved June 7, 2021, from https://www.nytimes.com/2021/06/07/us/politics/pipeline-attack.html

PJM. (n.d.). Synchrophasors. *PJM Learning Center*. Retrieved September 09, 2021, from https://learn.pjm.com/energy-innovations/synchrophasors

Potential Enhancements to the Critical Infrastructure Protection Reliability Standards, RM20-12-000 (June 18, 2020). Retrieved January 14, 2021, from https://www.nerc.com/FilingsOrders/us/FERCOrdersRules/Order_Version5_CIP_RM13-5_20131122.pdf

PUBLIC SERVICE COMMISSION OF MARYLAND. (2020, December). TEN-YEAR PLAN (2020 – 2029) OF ELECTRIC COMPANIES IN MARYLAND. Retrieved March 3, 2021, from https://www.psc.state.md.us/wp-content/uploads/2020-2029-Ten-Year-Plan-Final-1.pdf

Schwartz, J., Collier, K., & Davila, V. (2021, February 22). “Power Companies Get Exactly What They Want”: How Texas Repeatedly Failed to Protect Its Power Grid Against Extreme Weather. Retrieved March 3, 2021, from https://www.propublica.org/article/power-companies-get-exactly-what-they-want-how-texas-repeatedly-failed-to-protect-its-power-grid-against-extreme-weather

Senator Lee. (2021, January 13). 2021 MD SENATE BILL 49. Retrieved February 5, 2021, from http://mgaleg.maryland.gov/2021RS/bills/sb/sb0049F.pdf

Shea, D. (2020, January 24). Cybersecurity and the Electric Grid. National Conference of State Legislatures. Retrieved December 21, 2020, from https://www.ncsl.org/research/energy/cybersecurity-and-the-electric-grid-the-state-role-in-protecting-critical-infrastructure.aspx

Shea, D., & Bell, K. (2019, August 20). Smart Meter Opt-Out Policies. Retrieved December 30, 2020, from https://www.ncsl.org/research/energy/smart-meter-opt-out-policies.aspx

Soyoye, O., & Stefferud, K. (2019). Cybersecurity Risk Assessment for California's Smart Inverter Functions. *2019 IEEE CyberPELS*. Knoxville, TN: IEEE. doi:10.1109/CyberPELS.2019.8925257

Standards for Business Practices and Communication Protocols for Public Utilities, Docket Nos. RM05-5-029 and RM05-5-030; Order No. 676-J (Federal Energy Regulatory Commission June 2, 2021). Retrieved June 4, 2021, from https://public-inspection.federalregister.gov/2021-11352.pdf

State of Connecticut. (2019, October 10). Connecticut Critical Infrastructure 2019 Annual Report. Retrieved January 9, 2021, from https://portal.ct.gov/-/media/Office-of-the-Governor/News/20191010-Connecticut-Critical-Infrastructure-2019-Annual-Report.pdf?la=en

State of Maryland. (2015, September 29). MARYLAND COMMISSION ON CYBERSECURITY INNOVATION AND EXCELLENCE. Retrieved January 10, 2021, from https://msa.maryland.gov/msa/mdmanual/26excom/defunct/html/10cyber.html

State of Maryland. (2019, June 18). COMAR 01.01.2019.07 Maryland Cyber Defense Initiative. Retrieved December 22, 2020, from http://mdrules.elaws.us/comar/01.01.2019.07

State Of Maryland. (n.d.). Maryland Manual Online. Retrieved December 21, 2020, from https://msa.maryland.gov/msa/mdmanual/19dit/html/dit.html#security

State of Maryland. (n.d.). MD Code, Economic Development, § 10-463 Definitions.

Swinton, S. (2019, July 25). Cybersecurity Governance, Part 1: 5 Fundamental Challenges. Retrieved December 21, 2020, from https://insights.sei.cmu.edu/insider-threat/2019/07/cybersecurity-governance-part-1-5-fundamental-challenges.html

Texas Public Utility Commission. (2017, January 18). RFP to develop a comprehensive cybersecurity and physical security outreach program for texas electric utilities et al. Retrieved from http://interchange.puc.texas.gov/search/filings/?UtilityType=A&ControlNumber=46773&ItemMatch=Equal&DocumentType=ALL&SortOrder=Ascending

The Brattle Group. (2020, September 17). Study by Brattle Economists Evaluates Time-of-Use (TOU) Pilots for Maryland Utilities. *PRNewsWire*. Retrieved January 3, 2021, from https://www.prnewswire.com/news-releases/study-by-brattle-economists-evaluates-time-of-use-tou-pilots-for-maryland-utilities-301133346.html

The National Counterintelligence and Security Center. (2021, March). Insider Threat Mitigation for U.S. Critical Infrastructure Entities: Guidelines from an Intelligence Perspective. Retrieved March 29, 2021, from https://www.dni.gov/files/NCSC/documents/news/20210319-Insider-Threat-Mitigation-for-US-Critical-Infrastru-March-2021.pdf

The White House. (2021, May 12). Executive Order on Improving the Nation's Cybersecurity. Retrieved May 13, 2021, from https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

The White House. (2021, May 12). FACT SHEET: President Signs Executive Order Charting New Course to Improve the Nation's Cybersecurity and Protect Federal Government Networks. Retrieved May 13, 2021, from https://www.whitehouse.gov/briefing-room/statements-releases/2021/05/12/fact-sheet-president-signs-executive-order-charting-new-course-to-improve-the-nations-cybersecurity-and-protect-federal-government-networks/

THOMPSON, T. (2021, May 15). National Cyber Defense Is a "Wicked" Problem: Why the Colonial Pipeline Ransomware Attack and the SolarWinds Hack Were All but Inevitable. *scitechdaily.com*. Retrieved June 8, 2021, from https://scitechdaily.com/national-cyber-defense-is-a-wicked-problem-why-the-colonial-pipeline-ransomware-attack-and-the-solarwinds-hack-were-all-but-inevitable/

THOMPSON, T. (2021, May 15). National Cyber Defense Is a "Wicked" Problem: Why the Colonial Pipeline Ransomware Attack and the SolarWinds Hack Were All but Inevitable. *scitechdaily.com*. Retrieved May 17, 2021, from https://scitechdaily.com/national-cyber-defense-is-a-wicked-problem-why-the-colonial-pipeline-ransomware-attack-and-the-solarwinds-hack-were-all-but-inevitable/

Tobin, C., Scott, J., Nolan, D., & Shenkman, D. (2019). WILL FEDERAL PREEMPTION PUSH DRONE JOURNALISM TO NEW HEIGHTS? STATE, MUNICIPAL REGULATIONS SUSPECT FOLLOWING SINGER v. CITY OF NEWTON. *Communications Lawyer, 34-SPG Comm. Law. 10*. American Bar Association. Retrieved June 28, 2021

Trabish, H. K. (2020, November 25). From Maryland to California and beyond, rate design innovations are boosting the energy transition. Retrieved January 3, 2021, from https://www.utilitydive.com/news/from-maryland-to-california-and-beyond-rate-design-innovations-are-boosti/588595/

TSA orders pipeline companies to disclose breaches after Colonial hack. (2021, May 27). Retrieved May 28, 2021, from https://www.politico.com/news/2021/05/27/tsa-pipeline-breach-regulation-colonial-491123

U.S. Government. (2008). EISA Title XIII Sections 1301-1309 SMART GRID. Retrieved May 13, 2021, from https://www.energy.gov/sites/prod/files/oeprod/DocumentsandMedia/EISA_Title_XIII_Smart_Grid.pdf

United States Environmnetal Protection Agency. (2016, August). What Climate Change Means for Maryland. Retrieved June 22, 2021, from https://19january2017snapshot.epa.gov/sites/production/files/2016-09/documents/climate-change-md.pdf

United States Government Accountability Office. (2021, May). CYBER INSURANCE Insurers and Policyholders Face Challenges in an Evolving Market. Retrieved June 2, 2021, from https://www.gao.gov/assets/gao-21-477.pdf

United States of America. (2020, December 4). Internet of Things Cybersecurity Improvement Act (Public Law 116-207 2020). Retrieved January 31, 2021, from https://www.congress.gov/bill/116th-congress/house-bill/1668/text

US Department of Energy. (2020, May). Securing the United StatesBulk Power System From Adversarial Threat. Retrieved February 5, 2021, from https://www.energy.gov/sites/prod/files/2020/05/f74/DOE%20BPS%20EO%20One%20Pager.pdf

US Department of Energy. (2021, March 18). DOE Announces Cybersecurity Programs for Enhancing Safety and Resilience of U.S. Energy Sector. *energy.gov*. Retrieved March 29, 2021, from https://www.energy.gov/articles/doe-announces-cybersecurity-programs-enhancing-safety-and-resilience-us-energy-sector

US Department of Energy Office of the Chief Information Officer. (n.d.). Integrated Joint Cybersecurity Coordination Center. *energy.gov*. Retrieved April 15, 2021, from https://www.energy.gov/cio/about-our-services/integrated-joint-cybersecurity-coordination-center

US Department of Energy Solar Energy Technologies Office (SETO). (n.d.). Perovskite Solar Cells. *energy.gov*. Retrieved April 15, 2021, from https://www.energy.gov/eere/solar/perovskite-solar-cells

US Department of Energy, Cybersecurity Energy Security and Emergency Response. (2021, January). CESER Blueprint. *energy.gov*. Retrieved March 13, 2021, from https://www.energy.gov/sites/prod/files/2021/01/f82/CESER%20Blueprint%202021.pdf

US Government Accountability Office. (2021, March 18). Electricity Grid Cybersecurity: DOE Needs to Ensure Its Plans Fully Address Risks to Distribution Systems. *GAO-21-81*. Retrieved from https://www.gao.gov/products/gao-21-81

Va. Uranium, Inc. v. Warren, 848 F.3d 590, 605 (4th Cir. 2017) (citing Oneok, 135 S. Ct. at 1595). (4th Circuit 2017).

Vann, A. (2020, January 22). The Legal Framework of the Federal Power Act. United States Congress. Retrieved February 8, 2021, from https://crsreports.congress.gov/product/pdf/IF/IF11411

Velazco, C., & Lerman, R. (2021, July 8). 'Shut down everything': Global ransomware attack takes a small Maryland town offline. *Washington Post*. Retrieved July 26, 2021, from https://www.washingtonpost.com/technology/2021/07/08/kaseya-ransomware-attack-leonardtown-maryland/

Vynck, G. D. (2021, July 25). First came the ransomware attacks, now come the lawsuits. *Washington Post*. Retrieved July 25, 2021, from https://www.washingtonpost.com/technology/2021/07/25/ransomware-class-action-lawsuit/

Wagman, D. C. (2020, August 10). Dispute Erupts Over What Sparked an Explosive Li-ion Energy Storage Accident. *IEEE Spectrum*. Retrieved December 29, 2020, from https://spectrum.ieee.org/energywise/energy/batteries-storage/dispute-erupts-over-what-sparked-an-explosive-liion-energy-storage-accident

Walton, R. (2015, August 5). How Maryland regulators redefined energy efficiency – in 33 pages. *utilitydive.com*. Retrieved April 22, 2021, from https://www.utilitydive.com/news/how-maryland-regulators-redefined-energy-efficiency-in-33-pages/403450/

Walton, R. (2020, February 14). Utilities say they are prepared to meet cyber threats. Are they? utilitydive.com. Retrieved March 21, 2021, from https://www.utilitydive.com/news/utilities-say-they-are-prepared-to-meet-cyber-threats-are-they/572080/

Washington Gas Light Company's Application for Authority to Increase Its Rates and Charges, 9651 - ORDER NO. 89799 (Maryland Public Service Commission April 9, 2021). Retrieved May 14, 2021

SB800 Hester Testimony.docx.pdf
Uploaded by: Katie Fry Hester
Position: FAV

KATIE FRY HESTER
Legislative District 9
Howard and Montgomery Counties

Education, Energy, and
Environment Committee

Chair, Joint Committee on
Cybersecurity, Information Technology
and Biotechnology

THE SENATE OF MARYLAND
ANNAPOLIS, MARYLAND 21401

Annapolis Office
James Senate Office Building
11 Bladen Street, Room 304
Annapolis, Maryland 21401
410-841-3671 · 301-858-3671
800-492-7122 *Ext.* 3671
KatieFry.Hester@senate.state.md.us

Testimony in Support of SB800 - The Critical Infrastructure Cybersecurity Act of 2023

March 7th, 2023

Chair Feldman, Vice Chair Kagan, and members of the Education, Energy, and Environment Committee, thank you for your consideration of SB800, the Critical Infrastructure Cybersecurity Act of 2023.

Last year, the General Assembly took a major step towards improving our state's cybersecurity posture by modernizing systems, extending state resources to units of local government, and by establishing minimum security standards and protocols for our state agencies. However, cybersecurity risk affects every single public and private sector enterprise. As the Colonial Pipeline and Oldsmar, Fl, events have shown us, our critical infrastructure - especially our water, gas, and electrical utilities - are major targets for malicious actors.

In fact, the Cybersecurity and Infrastructure Security Agency under the Department of Homeland Security has warned states that these evolving, persistent threats pose "severe physical and economic harm." I have uploaded a 2-pager as part of my testimony that sketches out these threats which include, but are not limited to, cybersecurity risk, supply chain risk, and physical risk.

Broadly, this bill seeks to mitigate cybersecurity risk by drawing upon years of research by the Maryland Cybersecurity Council and its Critical Infrastructure Subcommittee. Specifically, in 2021, the Council commissioned a Fellow from the National Security Administration, Laura Corcoran, who is here today as part of my panel, to study the gaps in our regulation of utilities' cybersecurity standards. While drafting this report, she consulted the Public Service Commission, other state agencies, the best practices of other states, and other research. Then, when the PSC issued new cybersecurity regulations in 2022, I worked with the PSC and the Council's Critical Infrastructure Subcommittee to compare those regulations with the Fellow's recommendations.

This process took several months, and we ultimately identified the highest priority recommendations that were missing from PSC regulation into the bill you see before you today. During these conversations, we uncovered some worrying gaps in PSC's regulatory authority and staff capacity. First and foremost, the Commission does not receive the documentation necessary to have an informed conversation with utilities about their cybersecurity posture. Right now, the Commission receives cybersecurity briefings by utilities infrequently – once every three years. These briefings are closed

and oral only; the Commission keeps no written reports or minutes to examine, and there are no follow-up visits or audits to address how security challenges are being addressed. This process is out of step with other agencies' record-keeping, compliance, or transparency practices.

So what does SB800 do to address these gaps? The bill's provisions fall into three main buckets:

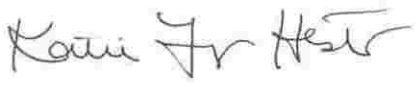
1.) **Requirements on the PSC**. This bill adds "cybersecurity" as one of the seven factors that the Commission must consider when exercising its regulatory power, and requires the Commission to collaborate with the Office of Security Management to establish minimum cybersecurity standards for utilities based on the particular needs of the sector, as well as the size of individual companies. It also requires the PSC to hire at least one subject matter expert in the cyber field to assist in drafting cyber regulations, monitor compliance with minimum standards, and to prepare reports for the Commission's review. This individual would also support utilities in their efforts to improve the maturity of their cybersecurity enterprise.

2.) **Requirements on utility providers.** In addition to requirements on the PSC, this bill would require utility companies to establish minimum security standards for each peripheral device on their networks, commensurate with their risk. These standards would include moving toward a zero trust architecture, and must be used to manage supply chain risk. Many of our larger utilities are already doing this work, but in cybersecurity, you really are limited by your weakest link.

3.) **Reporting requirements.** Finally, this bill would establish two reporting requirements - one for utility companies, and one for the PSC. Specifically, this bill would require each utility company in the state of Maryland to conduct an independent, third-party assessment of their cybersecurity practices at least every other year against the NIST Cybersecurity Framework. The results of these assessments would then be sent to the PSC and the Office of Security Management for their review and remediation through the PSC's workgroup process.

I want to thank the Maryland Cybersecurity Council and its Critical Infrastructure Subcommittee for their partnership in developing this bill. As threats to our systems continue to grow, so too must our capacity to prevent and mitigate them. **For these reasons, I respectfully request a favorable report on SB800.**

Sincerely,



Senator Katie Fry Hester
Howard & Montgomery Counties

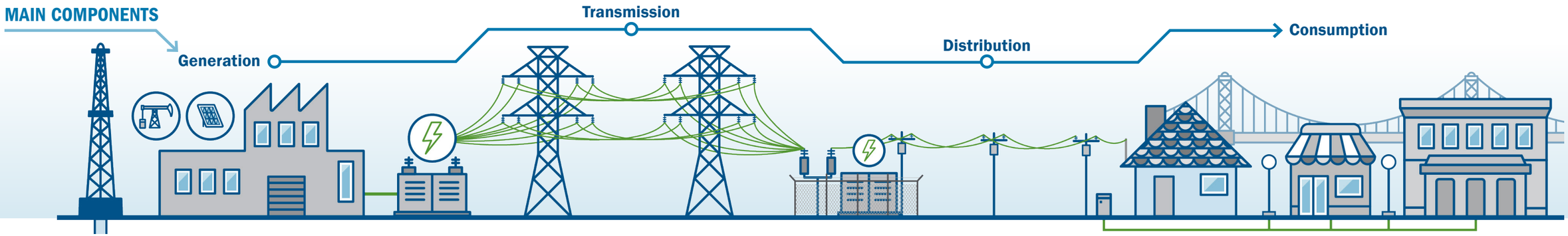
Sector Spotlight Cyber-Physical Security Considera

Uploaded by: Katie Fry Hester

Position: FAV

SECTOR SPOTLIGHT: **Cyber-Physical Security Considerations for the Electricity Sub-Sector**

The Nation's electricity grid could be vulnerable to increasing cyber threats that have physical consequences. New vectors for a disruptive attack on the Nation's grid and operations are emerging as monitoring and control technologies and connected devices become further integrated at the industrial and consumer levels.



AREAS OF RISK

CYBER:
Cybersecurity is an evolving security challenge for the electricity sub-sector. Cyberattacks pose a persistent threat to the electricity sub-sector and can cause severe physical and economic harm. Hackers can disrupt operations through ransomware attacks or by exploiting virtual private networks and gaining access to control systems responsible for critical operational components, such as tap changers on transformers. Malicious actors may continue to use cyber activity to bypass physical security measures.

PHYSICAL:
Physical security requirements for the electricity sub-sector are a complex challenge. For example, the diverse and disparate network of outdoor sub-stations are vulnerable to a number of physical attacks. Trespassers can damage transformers and compromise on-site control systems using firearms, explosives, and motor vehicles. Unauthorized persons are also increasingly using small Unmanned Aircraft Systems to bypass traditional security measures to conduct surveillance, damage transmission lines, and execute other nefarious actions.

SUPPLY CHAIN:
Managing the security and quality control of component acquisition is vital for the electricity sub-sector. A single compromised manufacturer or poorly secured component for Industrial Control Systems (ICS), Supervisory Control and Data Acquisition (SCADA), or software management systems, when broadly distributed across the electricity sub-sector, could compromise utility systems. Additionally, attacks on the sub-sector's supply chain for critical component manufacturers could delay the acquisition of key operational components.

PERIPHERAL DEVICES:
Electricity sub-sector operators are increasingly integrating Industrial Internet of Things (IIoT) devices with ICS to help monitor, regulate, and manage operating environments. These connected devices pose many of the same risks to enterprise security as traditional ICS. Inherent risks of IIoT devices include vulnerabilities in design, manufacturing, implementation, configuration, and disposal. For example, an IIoT device using outdated or unpatched software or firmware could be at greater risk of compromise and used to infiltrate enterprise networks, systems, and data stored in the cloud.

BEST PRACTICES FOR SECURING THE ELECTRICITY SUB-SECTOR

Protect Networks:
- Identify, minimize, and secure all network connections to ICS assets.
- Secure ICS and supporting systems by disabling unnecessary services, ports, and protocols. Enable security features and implement robust configuration management practices.
- Continuously monitor facility networks, applications, and other ICS and SCADA software systems.
- Develop facility-wide cybersecurity standards and implement cybersecurity best practices such as multi-factor authentication for system access. Regularly check, test, and implement ICS security patches.

Secure Vulnerable Infrastructure:
Develop a risk management framework to better understand how to secure vulnerable infrastructure. This framework can identify, analyze, and communicate risk. It can further instruct users on accepting, avoiding, transferring, or controlling risk to an acceptable level at an acceptable cost. The framework should do the following:[1]

- Assess the threats that are most likely to cause significant damage to components and operations.
- Prioritize vulnerability reduction efforts.
- Address physical features or operational attributes that make infrastructure elements open to exploitation.
- Mitigate the potential consequences of incidents proactively or prepare to mitigate them effectively if they do occur.

Formalize Collaboration across Organizational Security Functions:
Implement an integrated approach to security that aligns cybersecurity and physical security teams with grid operators. Cross train security personnel to enable a holistic understanding of cyber-physical threats and their impacts to grid operations and consider implementing an Insider Threat Mitigation Program. This collaboration can ensure personnel have the knowledge and tools to rapidly identify and respond to an incident with cross-sector impacts. See CISA's Cybersecurity and Physical Security Convergence Guide, which provides a framework for establishing formal collaboration between cybersecurity and physical security teams.

Update Outdated Infrastructure and Technology:
Invest in improvements to infrastructure and operational technology (OT) that are critical to daily operations. When installing new OT systems that are connected to information technology (IT) networks, ensure both systems can be readily secured and updated. Understand how OT is interacting with and connected to enterprise networks. Identify, logically isolate, and consider how obsolete or orphaned equipment is utilized in your environment and ensure risk management principles are applied.

Assess the Supply Chain:
Coordinate with individuals within the organization who engage in supply acquisition and management of security and compliance to ensure effective supply chain management practices. Establish protocols to assess already procured hardware and software components to understand which are used for critical functions and what systems have remote access capabilities to these systems. Consider how information and communications technology Supply Chain Risk Management (SCRM) and SCRM essentials integrate into each component to identify risks and vulnerabilities associated with the availability, integrity, and confidentiality of your ICS.

Secure Connected Devices:
Conduct an inventory of IIoT devices, understand how they communicate and link to the network, and disable any unnecessary internet connections, ports, and devices. Ensure connected devices connect only to intended systems. Separate the network supporting IIoT devices from the main IT and OT networks. Consider whether the IIoT device for acquisition supports software updates or security patches. Educate system administrators on the importance of cybersecurity and integrator/vendor collaboration in a connected IIoT environment.

1. CISA, A Guide to Critical Infrastructure Security and Resilience (November 2019), https://www.cisa.gov/publication/guide-critical-infrastructure-security-and-resilience.

SECTOR SPOTLIGHT: **Cyber-Physical Security Considerations for the Electricity Sub-Sector**

MAINTAINING RESILIENCY

REPORT:

Adhere to industry reporting requirements and establish internal processes for voluntary reporting of incidents and intrusions to the proper authorities. Leverage available tools, such as CISA's cyber incident reporting mechanism. Timely reporting enables rapid dissemination of actionable intelligence to sector partners and stakeholders, resulting in greater visibility of industry-wide threats. It creates a common operating picture among industry security stakeholders to facilitate the deployment of detective and preventative technologies that minimize the impacts of identified threats. Incident reporting also informs the process for developing threat-based products and initiatives and supports information sharing efforts that connect public and private sector partners with each other and with resources to help identify, prevent, mitigate, and recover from cyber incidents.

ASSESS:

Conduct periodic, detailed assessments of cyber and physical components to identify dependencies and interdependencies. Understand current threats and known exploited vulnerabilities. Finally, determine potential impacts of a successful cyber or physical attack. These assessments help stakeholders inform risk management plans to analyze threats to, vulnerabilities of, and consequences to critical infrastructure.

COLLABORATE:

Connect with law enforcement and federal, state, local, tribal, and territorial partners to stay informed of the current threat landscape. Collaborate with these partners to understand the layers of defense that should be adopted, develop security plans, and understand the latest tactics, techniques, and procedures used by adversaries. Additionally, communicate with operators of independent critical functions and resources to understand the cascading impacts of a cyber or physical attack.

PLAN FOR CONTINGENCIES:

Develop primary, alternate, contingency, and emergency plans to mitigate the most severe effects of prolonged grid disruptions, including the ability to operate power systems manually without the aid of control systems in the event of a compromise. Ensure redundancies of critical components and data systems to prevent single points of failure that could produce catastrophic results. Conduct exercises to provide personnel with effective and practical mechanisms to identify best practices, lessons learned, and areas for improvement in plans and procedures.

TOOLS

CISA Regional Advisors:

CISA collaborates with sector partners and stakeholders through a robust network of subject matter experts including Protective Security Advisors, Cybersecurity Advisors, and Interagency Security Committee Regional Advisors. These on-the-ground resources connect with organizations nationwide to provide comprehensive security expertise, guidance, and support, including risk assessments, security planning, training, and exercises.

Cybersecurity Capability Maturity Model (C2M2):

The C2M2 helps organizations accurately gauge investment and improvements to their cybersecurity programs and strengthen their operational resilience. The C2M2 tool focuses on implementation and management of cybersecurity practices associated with IT and OT assets and the environments in which they operate.

Incident Reporting:

CISA provides a secure, web-enabled mechanism that facilitates reporting of pertinent information such as date, time, organization, and incident description when a ransomware or other cyber incident occurs. This enables rapid response capabilities as a security incident unfolds and real-time security analysis to understand potential cascading impacts across multiple critical infrastructure sectors. Examples of incidents to report to the proper authorities include phishing emails, unauthorized access attempts to systems, malware, and unauthorized changes to systems, firmware, or software characteristics.

Cybersecurity Operational Technology Environment (CyOTE™):

CyOTE is a DOE Office of Cybersecurity, Energy Security, and Emergency Response (CESER) investment to enhance the electricity sector's threat detection of anomalous behavior that may indicate malicious cyber activity in OT networks. The initiative aims to develop tools and capabilities that can provide electricity asset owners and operators with timely alerts and actionable information.

Cybersecurity Risk Information Sharing Program (CRISP):

CRISP is a public-private partnership between DOE and the Electricity Information Sharing and Analysis Center. CRISP collaborates with energy sector partners to facilitate the timely bidirectional sharing of cyber information, enhancing the sector's ability to protect critical electric infrastructure.

Cyber Testing for Resilient Industrial Control Systems (CyTRICS):

CyTRICS partners across stakeholders to identify high priority OT components, perform expert cyber testing, share test results, and inform on improvements in design of components. CyTRICS leverages best-in-class testing capabilities at four DOE National Laboratories and strategic partnerships with key stakeholders including technology developers, manufacturers, asset owners and operators, and interagency partners.

RESOURCES

Critical Infrastructure Vulnerability Assessments: cisa.gov/critical-infrastructure-vulnerability-assessments

Cybersecurity Advisors: cisa.gov/stakeholder-risk-assessment-and-mitigation

Cybersecurity and Physical Security Convergence Guide: cisa.gov/publication/cybersecurity-and-physical-security-convergence

Cybersecurity Best Practices for Industrial Control Systems: cisa.gov/publication/cybersecurity-best-practices-for-industrial-control-systems

Cyber Hygiene Services: cisa.gov/cyber-hygiene-services

Incident Reporting System: cisa.gov/forms-report

Insider Threat Mitigation: cisa.gov/insider-threat-mitigation

National Cyber Awareness System: cisa.gov/uscert/ncas

Protective Security Advisors: cisa.gov/protective-security-advisors

Ransomware Guide: cisa.gov/stopransomware/ransomware-guide

SCRM Essentials: cisa.gov/sites-supply-chain

Shields UP: cisa.gov/shields-up

Training & Exercises: cisa.gov/cybersecurity-training-exercises

Using and Sharing Protected Critical Infrastructure Information: cisa.gov/using-and-sharing-pcii

For more information or to seek additional help contact us at **Central@cisa.gov**.

C2M2: energy.gov/ceser/cybersecurity-capability-maturity-model-c2m2

CESER: energy.gov/ceser/articles/ceser-releases-supply-chain-assessment-digital-components

CyOTE: energy.gov/ceser/cybersecurity-operational-technology-environment-cyote

CRISP: energy.gov/sites/prod/CRISP

CyTRICS: inl.gov/cytrics

Draffin Testimony SB800 -2023Mar7 final.pdf
Uploaded by: Cyril Draffin
Position: FWA

Cyril W. Draffin, Jr.
Energy Initiative Project Advisor, Massachusetts Institute of Technology

Testimony in Support of

SB800, "Public Service Commission – Cybersecurity Staffing and Assessments (Critical Infrastructure Cybersecurity Act of 2023)**"**
Sponsor: Senator Katie Fry Hester

Senate Education, Energy, and Environment Committee
1 p.m. March 7, 2023

Thank you for the opportunity to provide testimony in support of Senate Bill 800 pertaining to cybersecurity and the Maryland Public Service Commission (cross-filed with HB069).

My name is Cyril Draffin. I am a Project Advisor on cybersecurity, and serve as a member of the Maryland Cybersecurity Council.

The state needs its utilities to be reliable and protected against cybersecurity threats and attacks. We do not want future successful cyber-attacks on our infrastructure by foreign or domestic entities because the Public Service Commission ("PSC") had not been attentive enough to the cybersecurity programs of the electric, gas, water, and other utilities they oversee.

SUPPORT

Senate Bill 800 has several positive provisions, and requires only modest cost and employee resources.

The bill has provision for assuring one or more of the PSC's employees are experts in cybersecurity to advise the Commissioners, consult with the Maryland Office of Security Management, study cybersecurity best practices, assist in drafting cybersecurity regulation, and assist the PSC in monitoring public service company's security standards. This expertise, missing from current Commission staffing, is needed to provide adequate understanding of the challenges and appropriate actions to defend Maryland utilities from cyber-attack or inadequate cyber planning.

The bill has provision to establish and share cybersecurity standards and best practices, and prepare an evaluation of utilities cybersecurity policies, procedures, and expertise. To date no formal or written cybersecurity report about utilities is prepared and made available to key Maryland departments (even on a confidential basis). Only a quick verbal presentation is made to Commissioners with no written documentation provided for further review.

The bill has a provision for zero trust and assessment based on NIST (National Institute of Standards and Technology) framework for cybersecurity protection. This recognizes that ongoing trust in a system should not be assumed, and system must be regularly evaluated because malicious actors (e.g., employees with malicious intent, external people and organizations, foreign governments) can penetrate perimeter firewalls and reach the insides of information technology or operational technology systems. Maryland utilities need to keep up with evolving cybersecurity and physical security threats.

SUPPORT WITH SUGGESTED AMENDMENTS

The bill has a provision that every two years a third-party with cybersecurity expertise should assess the operational technology and information technology of utilities serving Maryland customers, and that it should be shared with the Maryland Department of Information Technology and the Maryland Department of Emergency Preparedness. This assures an independent evaluation is conducted, and Maryland does not only rely on the good intentions and verbal statements of their utilities.

However, we do not want Critical Energy Infrastructure Information (CEII) from cybersecurity assessments to be made public.

A suggested amendment is for SB 800 to have language restricting release of CEII as part of Freedom of Information Act (FOIA) and other public disclosure requests.

This CEII protection has already been adopted in other states for many years. For instance in 2019 the National Governors Association report (their most recent CEII report) "State Protection of Critical Energy Infrastructure Information (CEII)" (https://www.nga.org/publications/state-protection-of-critical-energy-infrastructure-information-ceii/) indicated that 31 states had "open government law" exemptions that protect CEII. Maryland does provide that protection.

Additional details:

- From National Governors Association report: "Twenty-eight states have adopted statutory exemptions from open government laws for critical infrastructure information (CII, defined as systems and assets, whether physical or virtual, so vital that their incapacity or destruction would debilitate social or economic security; CEII is a subset of CII). Three other states, Hawaii, Minnesota, and Washington, do not explicitly exempt CEII, but language from court cases, opinion letters or general statutory language is interpreted to contain this exemption. Only a few states list a specific state

agency and/or authority that is exempted from open disclosure requirements (e.g., Iowa)."

- Federal Energy Regulatory Commission's policy regarding Critical Energy/Electric Infrastructure Information (CEII) is available on their web site: (https://www.ferc.gov/ceii).
- U.S. Cybersecurity & Infrastructure Agency (CISA) and other Federal organizations release advisories, and patches that the PSC may then forward to utility service providers; and PSC needs to know how these interventions are working to enhance cybersecurity. Sharing assessment information on utilities operating in Maryland with the PSC results in a more informed PSC.
- The Federal Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA) requires covered entities to report cyber incidents to the Federal government.
- The PSC assessments provided to the State should include anonymous information when it reports on its evaluations.
- Limitations needed to avoid publicly disclosing cyber infrastructure information under the Maryland Public Information Act.

If language protecting CEII information is not added in Maryland, then written reports on cybersecurity of utilities should be marked "Confidential" and not be shared with other Maryland departments or the public.

A second amendment is to delay "Beginning on or before October 1, 2023, and every 2 years thereafter, evaluate the assessments…" (SB800, page 5, line 7) by six months until April 1, 2024 because bill will not become effective until October 1, 2023 (page 8, line 10).

SUMMARY

SB 800 is a straightforward way to address and improve the cybersecurity readiness of public utilities operating in Maryland.

Because of the need for improved cybersecurity reviews by the Maryland Public Service Commission, I encourage a favorable report on Senate Bill 800-- with the two amendments including adding a provision for Maryland to protect CEII information. I support the committee's continued attention to cybersecurity and physical security of utility operations in Maryland.

(Varonis Systems) SB800 Letter (SUPPORT) Session
Uploaded by: Jason Bonasera
Position: FWA

Senate Bill 800
Public Service Commission - Cybersecurity Staffing and Assessments
(Critical Infrastructure Cybersecurity Act of 2023)
Position:
FAVORABLE with AMENDMENTS

March 7, 2023

Dear Chairman Feldman & the Members of the Senate Education, Energy, & the Environment Committee:

On behalf of Varonis Systems, I would like to take this opportunity to thank you for the opportunity to submit this letter of support with amendments to Senate Bill 800, entitled: *Public Service Commission - Cybersecurity Staffing and Assessments (Critical Infrastructure Cybersecurity Act of 2023).*

If passed, Senate Bill 800, would require the Public Service Commission (PSC) to hire staff in cybersecurity to advise the commission on measures to improve oversight of cybersecurity practices of public services companies. The bill also requires the commission to collaborate with the Office of Security Management to establish cybersecurity standards and best practices for regulated entities. SB 800 would also require public service companies to adopt and implement cybersecurity standards equivalent to or exceeding those held by the commission.

The Public Service Commission regulates natural gas and electric utilities; third-party energy suppliers; and water, sewage disposal, and passenger transportation companies doing business in the state of Maryland. The PSC is also responsible for setting utility rates, enforcing rules and regulations, and a variety of other duties directly involving public service companies. Given PSC's expansive oversight and authority over these companies, it is understandable that they would be involved in the establishment of cybersecurity standards and data privacy threat best practices for these regulated entities.

While we agree with the overall purpose and legislative intent of the bill, we would recommend that the commission procure a vendor, instead of hiring new staff, to be responsible for the tasks mandated under the new provisions, contained in § 2–108 of the Public Utilities Article. The PSC is primarily funded through special funds obtained through assessments of public service companies.

According to the DLS budget analysis, the PSC's FY24 allowance indicates that 79% will support personnel expenses for the agency's 143 regular positions and 12 contractual full-time equivalents (FTE). The current language of the bill authorizes the PSC to hire "*one or more employees that are experts in cybersecurity*". The responsibilities expressed in the bill would ultimately require several key staff with multiple levels of skills and expertise in cybersecurity, risk assessment, cloud security, data protection, and identify access management.

The number of staff needed to conduct this work will require more staff position and the level of expertise and skills needed for this role are highly specialized and competitive. The PSC is an independent agency that is primarily funded through assessments of public service companies. Hiring new staff within the PSC will increase the demands to supplement its annual operating budget to cover these new costs. By contrast, procuring a vendor to perform these specific duties could reduce the costs of creating and hiring new personnel, thereby allowing current personnel to carry out other necessary tasks at the PSC.

Finally, the bill would also require SB 800 would also require public service companies to:

- Adopt and implement cybersecurity standards equivalent to or exceeding those held by the commission;

- A zero-trust cybersecurity approach for on-premises services and cloud-based services;

- Establish minimum security standards for each operational technology and information technology devise based on the level of security risks associated with supply chains.

Companies would be required to contract with a third-party to conduct an assessment base on the National Institute of Standards and Technology (NIST) and submit those results to the PSC.

The level of IT security safeguards that a public service company must assess before reporting back to the PSC should be evaluated by a vendor who specializes in cybersecurity and "zero trust" protections, and should therefore be reflected in the bill. This will ensure that companies are in compliance with the expressed provisions under § 5-306 of this legislation.

For these reasons, we strongly encourage this committee to provide a **FAVORABLE** report with amendments for Senate Bill 800.

Thank you for your consideration.

Sincerely,

Jason Bonasera
Varonis Systems, Inc.

John_Abeles_SB800_FAVORABLE_W_AMENDMENTS.pdf
Uploaded by: John Abeles
Position: FWA

SUPPORT WITH AMENDMENTS

John M. Abeles
President and CEO of System 1, Inc.
a Cybersecurity and Critical Infrastructure Consultancy

Testimony in Support of

SB 800, **"**Public Service Commission – Cybersecurity Staffing and Assessments (Critical Infrastructure Cybersecurity Act of 2023)**"**
Sponsor: Senator Katie Fry Hester

Senate Education, Energy, and Environment Committee,
1 p.m. March 7, 2023

Honorable Chair and members of the committee, thank you for the opportunity to provide testimony in support of Senate Bill 800 pertaining to cybersecurity and the Maryland Public Service Commission ("PSC").

My name is John M. Abeles. I have over 30 years supporting the Energy Sector and serve as a member of the Maryland Cybersecurity Council. I have supported and led efforts in critical infrastructure protection, risk management, and cybersecurity for the White House; Departments of Energy, Commerce, Interior, and Treasury; some private sector utilities; and states.

Context – Maryland needs to build a resilient approach to cybersecurity and needs to foster an agile culture to counter the evolving threat and vulnerability landscape. Under Senate Bill 800, the PSC is the organization responsible for establishing the aiming points and for monitoring how utilities are meeting these requirements.

A GAO report[1] for Congress in August 2019, on "Critical Infrastructure Protection on Actions Needed to Address Significant Cybersecurity Risks Facing the Electric Grid," highlighted that the threat environment has increased from hostile nations, criminal groups, terrorists; and others are increasingly capable of attacking the grid. The cyber systems in Maryland have vulnerabilities, including those that involve industrial control systems that support grid operations. While large scale impacts on the grid have not yet been realized, the report indicates that federal assessments indicate that cyberattacks could cause widespread power outages in the United States.

In addition, industry and the Government have noted the importance of improving their cybersecurity posture. A Price Waterhouse Cooper (PWC) document[2] from the 2023 Global Digital Trust Insights shows that senior executives worry that their enterprise isn't fully prepared to address heightened threats. Topping the 2023 list of rising organizational threats are cybercriminal activity (65%); mobile devices (41%), emails (40%), cloud-based breaches (38%); and business email compromise/account takeovers (33%) and ransomware (32%). Forty-two

[1] https://www.gao.gov/products/gao-19-332

[2] A C-suite united on cyber-ready futures: PwC

percent of senior executives say cyber breaches of their systems have increased since 2020. These apply to a broad range of industries including energy generation and distribution.

Support for the Bill -- Senate Bill 800 has a number of essential provisions that requires only minimal cost and employee resources, and can be scaled based the size and complexity of the utility. The bill needs to counter the expanding threat and evolving vulnerability landscape.

The bill has a provision for assuring one or more of the PSC's employees are experts in cybersecurity to advise the Commissioners, ensure that there is sufficient funding, consult with the Maryland Office of Security Management, study cybersecurity best practices, assist in drafting cybersecurity regulation, provide oversight of public service practices, and assist the PSC in monitoring public service company's security standards. Agility is required as many of the nation-wide cybersecurity regulations and guidance are currently being enhanced. The National Cybersecurity Strategy[3] was issued by the White House on March 2, 2023. The strategy seeks to build and enhance collaboration around five pillars, the first of which is to defend critical infrastructure. This will include the expansion of minimum cybersecurity requirements, harmonize regulations to reduce the burden of compliance, and enable public-private partnerships. Three recent examples of cybersecurity regulations and guidance that are enhanced include:

- Nuclear Regulatory Commission Regulatory Guide 5.71, revision 1, Cybersecurity Program for Nuclear Power Reactor, issued February 2023[4]
- Department of Energy, Cybersecurity Capability Maturity Model, Version 2.1, issued in June 2022[5]
- National Institute of Standards and Technology (NIST) Cybersecurity Framework 2.0, Is in the process of development and public comments. Last meeting February 2023[6]

During the Winter Meeting of the National Association of Regulatory Utility Commissioners (NARUC) in Washington, DC, in February 2023, CISA reminded the audience that minimizing physical and cybersecurity is a priority for state regulators and utilities and that information sharing was key to developing a proactive security posture, improve on developing and mitigating security challenges both for utilities and regulators, and improving response and recovery efforts to security events through effective private and public relationships.

As an amendment to SB 800, at least one of the experts should be required to have (or obtain) a Top Secret or Q clearance, so that that sensitive information and responses can be shared with state personnel. The added expertise, missing from current Commission staffing, is needed to provide adequate understanding of the challenges and appropriate actions necessary to defend Maryland utilities from cyber-attack or inadequate cyber planning.

---

[3] https://www.whitehouse.gov/briefing-room/statements-releases/2023/03/02/fact-sheet-biden-harris-administration-announces-national-cybersecurity-strategy/

[4] https://www.govinfo.gov/content/pkg/FR-2023-02-13/pdf/2023-02941.pdf

[5] https://www.energy.gov/sites/default/files/2022-06/C2M2%20Version%202.1%20June%202022.pdf

[6] https://www.nist.gov/cyberframework/updating-nist-cybersecurity-framework-journey-csf-20

In addition, the bill parallels many of the Federal and industry requirements and guidance but will focus on those items at the state level.

Specific issues -- The bill has provisions to establish and share cybersecurity standards and best practices, and prepare an evaluation of utilities cybersecurity policies, procedures, and expertise. It also requires the development of formal reports on cybersecurity threats and sources and the efficacy of protective cybersecurity practices. To date no formal or written report has been prepared or made available to key Maryland departments (even on a confidential basis). Only a quick verbal presentation is made to Commissioners with no written documentation provided for further review. Currently there is no assurance that weaknesses identified during the briefings are documented or later mitigated. Having documentation would provide a basis to judge the ongoing adequacy of a utility's cybersecurity program. Understanding the sensitivity of vulnerability and weakness information of specific corporate entities might hinder the open reporting of information to the PSC. To counter this issue, as a second amendment, the information could be identified as Critical Energy Infrastructure Information[7] (CEII). This is a class of information that is sensitive and is exempt from disclosure through the Freedom of Information Act (FOIA) and other public disclosure requests. I support amending the bill to include the use of CEII.

The bill is predicated on a zero-trust approach. That requires all users, whether in or outside the organization's network, to be authenticated, authorized, and continuously validated for security configuration and posture before being granted or keeping access to applications and data. Zero Trust is a framework for securing infrastructure and data for today's modern digital transformation. It uniquely addresses the modern challenges of today's business, including securing remote workers, hybrid cloud environments, and ransomware threats.

The bill also requires the identification of security risks associated with supply chains and a bi-annual third-party review in concert with NIST's security frameworks that will be submitted to the PSC.

Path Forward -- Senate Bill 800 with suggested amendments provides a path forward to protect Maryland's critical energy infrastructure. Further enabling the PSC's function by adding expertise and formality to their processes will advance a culture of continuous improvement. The added funding and resources will allow agility to progressively update and keep pace with the evolving challenges that Maryland utilities will encounter.

[7] https://www.ecfr.gov/current/title-18/chapter-I/subchapter-X/part-388/section-388.113

THayes Testimony_Submitted on 3-6-23.pdf
Uploaded by: Terri Hayes
Position: FWA

Terri Jo Hayes
Executive Consultant, Cybersecurity Strategy and Policy, Mfusion, Inc.

Testimony in Support of

SB800, "Public Service Commission – Cybersecurity Staffing and Assessments (Critical Infrastructure Cybersecurity Act of 2023)"
Sponsor: Senator Katie Fry Hester

Senate Energy, Education, and Environment Committee, 1 p.m. March 7, 2023

EXECUTIVE SUMMARY

Honorable Chair and members of the committee, thank you for the opportunity to provide testimony in support of Senate Bill 800 pertaining to cybersecurity and the Maryland Public Service Commission (PSC).

My name is Terri Jo Hayes. I have over 30 years of combined engineering and management, technology, and cybersecurity consulting experience, with over 15 years focused on critical infrastructure protection and cybersecurity operations and policy; and I serve as a member of the Maryland Cybersecurity Council.

Maryland is referred to as the Cyber Capital of America, the Hub of Cybersecurity Innovation. In 2019, the U.S. News and World reported[1] that there are more trained cyberengineers in Maryland than in the rest of the U.S. combined. While these are admirable characteristics for our State, these will just be statistics unless we can put the State's robust cybersecurity knowhow into action towards helping our increasingly vulnerable critical infrastructure become more cyber secure. I support the "Public Service Commission – Cybersecurity Staffing and Assessments (Critical Infrastructure Cybersecurity Act of 2023)," SB800, because it places action behind our State as the Cyber Capital of America. It will establish an improved infrastructure that includes resources, technologies, and processes to help us become more intentional and proactive in protecting our most critical assets and provide a formal mechanism for reporting sector-wide cybersecurity posture to State Officials.

The Challenge

The aging U.S. electric grid is increasingly vulnerable as utility companies pursue efficiencies and cost savings through integration, modernization, and

[1] Janke, "Why Maryland is Home to Cyber Innovation," page 1.

digitization. While these modifications enhance the functionality and efficiency of the grid, they also increase their digital footprint for nefarious cyber actors to access and exploit. The Government Accountability Office (GAO) has been studying this environment and providing recommendations to address the increasing vulnerabilities and growing threat. GAO studies in 2019[2], 2021[3] and 2023[4] all state that the nation's grid is becoming more vulnerable to cyberattacks—particularly those involving industrial control systems (ICS) that support grid operations. In the recently published 2023 study, GAO reports that the U.S. grid's distribution systems remain increasingly at risk and need to be urgently addressed.

Some industry experts claim that the U.S. energy grid is completely interconnected, and our major worry is always the cascading failure scenario that would take down the entire grid. In addition, a majority of critical infrastructure, including financial services, communications, healthcare, and water systems rely on the electric grid for operation. Today, our infrastructures are integrated, connected, and dependent such that severe damage to the electric grid can cascade to other critical infrastructures. This integration was done out of efficiency and in some cases necessity. However, the integration comes with risks that have only grown as our systems expand and technology improves.

We have partners in this fight. The White House released the President's National Cybersecurity Strategy in March 2023, highlighting the importance of cybersecurity to the operation of our critical infrastructure. Furthermore, it encourages states that have authorities that can be used to set cybersecurity requirements to use them to enhance protection of our critical infrastructure.

Why I Support SB800

I support the passing of SB800 because it will help Maryland improve the cybersecurity of its increasingly vulnerable critical infrastructure. SB800 helps to proactively raise the bar of cybersecurity defenses by improving processes and structures at the PSC and utility companies, so that State Officials can have better awareness of the current cybersecurity posture of the electric, gas, and water utilities in Maryland. PSC understands the importance of critical infrastructure cybersecurity and has taken steps to bring a focus to addressing cybersecurity for its utilities. However, more rigor and

[2] U.S. Government Accountability Office, "Actions Needed to Address Significant Cybersecurity Risks Facing the Electric Grid", Aug 2019

[3] U.S. Government Accountability Office," Electricity Grid Cybersecurity – DOE Needs to Ensure Its Plans Fully Address Risks to Distribution Systems, March 2021

[4] U.S. Government Accounting Office, "Cybersecurity High-Risk Series: Challenges in Protecting Cyber Critical Infrastructure, February 2023

comprehensive practices are needed. For utilities, this Bill provides baseline protection of the infrastructure within a more formalized program, building upon the processes that are currently in place at the PSC. It provides a consistent framework that all utilities adhere to, not just those that have 30,000 or more customers. The framework may be resized for smaller utilities, who also need to implement robust cybersecurity practices. Information sharing may be challenging initially because of the culture and traditional barriers to sharing; but when implemented, it will help us better understand and address threats, and potentially avoid cyber attacks.

This Bill calls for establishing minimum security standards for each operational technology (OT) and information technology (IT) device, which requires utilities to inventory and baseline their systems, to understand the interconnections between IT and OT and the vulnerabilities that result. This process allows utilities to establish well-informed risk management plans and addresses CISA's best practices of identifying, minimizing, and securing all network connections to ICS assets.

The Zero Trust provisions is another feature of SB800 I fully support. The core principle behind Zero Trust is 'never trust, always verify'. Incorporating Zero Trust will significantly support a stronger defense, protecting IT/OT systems and stakeholder privacy information, and make it more challenging for an attacker to gain system access. It will help to establish the resiliency needed in our critical systems across the grid. This component of the Bill aligns with the Federal Government's Executive Order on Improving the Nation's Cybersecurity, which calls for agency heads to develop plans to implement a Zero Trust Architecture.

SB800 helps bring state legislation in better alignment with Federal priorities.

Amendments That Would Strengthen SB800

Two suggested amendments deal with information sharing and handling since such duties are key elements to most cybersecurity programs. The first amendment would recommend that certain classes of information and data shared by utilities under SB800 be given the protections provided by the Critical Energy Infrastructure Information (CEII) classification label and handled accordingly. CEII includes information about the production, transmission, or distribution of energy. In addition, any information that could be useful in planning an attack on critical infrastructure is considered CEII. According to the National Governor's Association, 28 states have adopted statutory exemptions from open government laws for critical infrastructure information (CII, defined as systems and assets, whether physical or virtual,

so vital that their incapacity or destruction would debilitate social or economic security; CEII is a subset of CII).[5]

The second amendment would recommend that the Commission staff responsible for handling utility cybersecurity assessment information hold a Top Secret clearance. Granting clearances to the appropriate members and staff enables better information sharing within the state government and amongst similarly cleared personnel throughout the federal government.

The final amendment is regarding timelines for public service company implementation activities. Providing timeline guidance in SB800 for public service company implementation may help clarify when such activities should begin or occur.

Cyber threats and vulnerabilities are growing in number and sophistication and will continue to be a threat to the electric grid and every other portion of our critical infrastructure. Though it will take time to reduce the risk, it is now clear to most that action must be taken at all levels of government and society to keep our country and State safe from the effects of cyber attacks on our critical infrastructure. I believe SB800 is a step in the right direction.

[5] National Governor's Association (NGA), "State Protection of Critical Energy Infrastructure Information (CEII)", https://www.nga.org/wp-content/uploads/2019/05/CEII-Paper-June-2019-Revised.pdf

FINAL - Opposition Letter SB 0800.pdf
Uploaded by: Kim Mayhew
Position: UNF

PotomacEdison
A FirstEnergy Company

Timothy R. Troxell, CEcD
Advisor, Government Affairs
301-830-0121
ttroxell@firstenergycorp.com

10802 Bower Avenue
Williamsport, MD 21795

Oppose – Senate Bill 0800
SB0800 – Public Service Commission - Cybersecurity Staffing and Assessments (Critical Infrastructure Cybersecurity Act of 2023)
Education, Energy, and the Environment Committee
Tuesday, March 7, 2023

Potomac Edison, a subsidiary of FirstEnergy Corp., serves approximately 280,000 customers in all or parts of seven Maryland counties (Allegany, Carroll, Frederick, Garrett, Howard, Montgomery, and Washington Counties). FirstEnergy is dedicated to safety, reliability, and operational excellence. Its ten electric distribution companies form one of the nation's largest investor-owned electric systems, serving customers in Ohio, Pennsylvania, New Jersey, New York, West Virginia, and Maryland.

Potomac Edison / FirstEnergy requests an <u>Unfavorable</u> report on SB 0800 for the following reasons.

Potomac Edison / FirstEnergy recognizes the importance of implementing effective cybersecurity controls consistent with established and evolving security standards to protect critical infrastructure and maintain safe, reliable, and affordable energy delivery for our customers. From a practical security perspective, we do not believe that Senate Bill 0800 would materially improve upon what Maryland's investor-owned utilities are already doing in the cybersecurity arena under the supervision of the Public Service Commission.

From the "providing compliance" perspective of SB-800, however, we do have some concerns. Most cyber issues are normally worked out through the rulemaking process with the Public Service Commission, but the bill's inclusion of a third-party assessor give us pause. Potomac Edison / FirstEnergy is constantly improving our cybersecurity programs to stay ahead of threats pursuant to federal cybersecurity requirements and advances in industry approved frameworks. Inserting a third-party expert certification approach may introduce unintended risks to the consistent and successful compliance programs we and the other Maryland utilities currently maintain in close coordination with the Commission.

We also have noted areas where the legislation is likely to become overly burdensome and expensive to implement without creating any benefit to customers. For example, if section 5-306(C)(2) were applied to our field systems and not just our corporate business systems, this could be nearly impossible to accomplish. "Zero trust architectures" within substation environments must be researched to make certain they are even viable. Inherent in existing systems' design is a level of trust. We have a lot of substations on our system, and it would become very costly even to just try to determine what new equipment or processes would need to be implemented or installed in order to comply, if it is even possible. In addition, sections 5-306(C)(3) & 5-306(C)(4) could require costly documentation and retention of compliance evidence for assets within just our Potomac Edison Maryland footprint, since this is not required anywhere else in our 5-state corporate footprint. Potomac Edison / FirstEnergy manages cyber-security costs, and performance is enhanced, by managing the corporation's entire multi-utility system on a central and uniform basis. Developing custom approaches just for Maryland will impose substantial costs on the Maryland systems and would have to be paid for by the Maryland ratepayers. For example, requirements in this bill would likely require significant additions of new staff at both the corporate level and the Potomac Edison Operating Company level.

The rapidly evolving nature of cybersecurity threats pose unique challenges for utilities, and warrants careful consideration, but we respectfully request that utilities be allowed to continue to align our programs with federal industry standards that incorporate strong cybersecurity controls and best practices. Moreover, allowing this process to continue to be overseen by the Public Service Commission without the use of a third-party assessor is preferred.

For the above reasons, Potomac Edison / FirstEnergy respectfully request an **Unfavorable** report on Senate Bill 0800.

SB800 - Public Service Commission -Cybersecurity S
Uploaded by: Natalie Cotton
Position: UNF

Southern Maryland Electric Cooperative
1-888-440-3311
P.O. Box 1937, Hughesville, MD 20637
www.smeco.coop

People. Power. Progress.

March 6, 2023

SB 800: Public Service Commission – Cybersecurity Staffing and Assessments (Critical Infrastructure Cybersecurity Act of 2023)

Committee: Senate Education, Energy and the Environment

Position: OPPOSED

Southern Maryland Electric Cooperative (SMECO), a member-owned electric cooperative based in Hughesville that provides electricity to more than 170,000 member accounts in Charles, St. Mary's, Calvert and southern Prince George's County, opposes Senate Bill 800. This bill requires the Public Service Commission (PSC) to include one or more employees that are experts in cybersecurity on its staff for specified purposes. In supervising and regulating public service companies, PSC must also consider the protection of a public service company's infrastructure against cyberattack threats. Each public service company, except common carriers and telephone companies, must take specified actions related to cybersecurity, including contracting with a third party every two years beginning in 2024 for an assessment of operational technology and information technology (IT) devices based on specified security frameworks and submitting related information to PSC. PSC is required to conduct related evaluations of the assessments for three consecutive years starting with October 1, 2023, and then every two years thereafter.

SMECO opposes SB 800 because the bill is redundant of current federal cybersecurity requirements. The bill would require significant additions of new staff, documentation, configuration changes and management of distribution level assets at a cost to the Cooperative's ratepayers. The bill also requires that utilities adopt a zero-trust cybersecurity approach for on-premises services, which is duplicative of our current practice as SMECO currently adopts the principle of least privilege and zero-trust approach through our environment, specifically in the SCADA environment through CIP.

For more information, contact: Natalie Cotton, SMECO
Government Affairs & Community Relations Director
240-393-3919 • Natalie.cotton@smeco.coop

Southern Maryland Electric Cooperative
1-888-440-3311
P.O. Box 1937, Hughesville, MD 20637
www.smeco.coop
People. Power. Progress.

SMECO recognizes the importance of implementing effective cybersecurity controls consistent with established and evolving security standards to protect critical infrastructure and maintain safe, reliable, and affordable energy delivery. The rapidly evolving nature of cybersecurity threats poses unique challenges for the critical infrastructure community, including utilities, and warrants careful consideration.

While we appreciate the need to ensure that cybersecurity tools and approaches keep pace with new cyber threats, the General Assembly should also keep in mind that the utility industry has not been idle. SMECO is constantly improving their cybersecurity programs to stay ahead of threats pursuant to federal cybersecurity requirements and advances in the industry.

The bill would also require that at least once every other year that utilities contract with a third party to conduct an assessment of operational technology and information technology devices based on National Institute of Standards and Technology (NIST) frameworks. The PSC currently requires utilities to present their cybersecurity posture to them every three years. We respectfully ask that utilities be allowed to continue to align our programs with federal industry standards and requirements that incorporate strong cybersecurity controls and best practices which will be overseen by the PSC without the use of a third-party assessor. A third-party expert certification approach will introduce additional costs and may result in unintended risks such as inconsistencies with third-party evaluators. A key factor in successful compliance programs is consistency—relying solely on third parties to perform compliance verifications may result in divergent compliance monitoring approaches and interpretations.

SMECO believes that the current federal regulations via FERC, NERC and Reliability First, which deals with Critical Infrastructure Protection (CIP) adequately addresses the bill's requirements. For that and the reasons explained above, SMECO urges the committee to give an unfavorable report to SB 800.

For more information, contact: Natalie Cotton, SMECO
Government Affairs & Community Relations Director
240-393-3919 • Natalie.cotton@smeco.coop

SB0800_Information_Stanek.pdf
Uploaded by: Jason Stanek
Position: INFO

STATE OF MARYLAND

OFFICE OF THE CHAIRMAN

JASON M. STANEK

PUBLIC SERVICE COMMISSION

March 7, 2023

Chair Brian Feldman
Education, Energy and Environment Committee
2 West, Miller Senate Office Building
Annapolis, Maryland 21401

RE: SB 800 – INFORMATION – Public Service Commission – Cybersecurity Staffing and Assessments (Critical Infrastructure Cybersecurity Act of 2023)

Dear Chair Feldman and Committee Members:

SB 800 requires the Maryland Public Service Commission to include one or more cybersecurity experts on its Staff to advise the Commission and perform certain duties, collaborate with the Office of Security Management ("OSM") to establish cybersecurity standards and best practices for regulated entities, share cybersecurity-related information and best practices with municipal electric utilities, require certain public service companies to adopt and implement cybersecurity standards and conduct assessments, and require the Commission to conduct and submit an evaluation of the public service companies' assessments to OSM and the Maryland Department of Emergency Management ("MDEM").

In 2019, the Commission established a three-year audit cycle framework for periodic cybersecurity reporting based recommendations from a two-year stakeholder process. All applicable Maryland utilities have completed their first cycle of briefings.[1] On July 25, 2022, the Commission adopted cybersecurity regulations that incorporate critical lessons learned from the cybersecurity reports. Maryland thus became only the third state in the nation to promulgate cybersecurity regulations for its public service companies, consistent with President Biden's request to State Governors on March 18, 2022, to promulgate standards to secure critical infrastructure, among other things.

The Commission will need to hire three cybersecurity experts to perform the mandates of SB 800. The specific duties and responsibilities of these experts listed in Section 2-108(d)(3)— include, among other things, advising the Chairman and the Commissioners on cybersecurity, studying and monitoring cybersecurity best practices, and assisting in drafting cybersecurity-

[1] Commission issued Order No. 89015 on February 4, 2019, establishing various cybersecurity definitions and establishing a three-year audit cycle framework for periodic cybersecurity reporting to the Commission by Maryland electric, gas, or water companies that have 30,000 or more customers in Maryland. In addition, the Commission established a cybersecurity breach reporting protocol for all Maryland electric, gas, and water companies under their jurisdiction.

related regulations—and are inherent to the unique technical and advisory role of Commission Staff. These functions are best integrated in the Commission's hiring documents, pursuant to State personnel procedures, rather than in statute. **The Commission therefore recommends simplifying the language under subsection (d)(3), by striking (I)-(VII), to be consistent with comparable subsections (d)(5) and (d)(6) of Section 2-108. Finally, the Commission would also require an appropriation for the PINS and appropriate salaries** (or condition the hiring of the personnel on the availability of these resources).

Specifically, where SB 800 calls for the technical cybersecurity expert to convene workshops with public service companies that fail to meet the minimum cybersecurity standards in (d)(3)(VI), this requirement is unnecessary. The Commission is authorized under the *Public Utilities Article* to impose an appropriate civil penalty for a violation of law, Commission order, or regulation, as well as require a public service company to file a corrective action plan as opposed to conducting a workshop.[2]

Some of the information sharing requirements in SB 800 raise confidentiality concerns. Under the *PUA*, the Commission has broad oversight authority over public service companies.[3] Cybersecurity matters are extremely confidential, including how breaches are reported, and the Commission has emphasized the proper safeguarding of this information. SB 800 requires the Commission to evaluate the utilities' security assessments of its own operational and informational technologies and submit this evaluation to the OSM and MDEM. Notwithstanding the scope of authority given to DoIT and MDEM, expanding the number of agency representatives with knowledge of a utility's cybersecurity and data privacy threat protections weakens its ability to safeguard this critical information. **Therefore, the Commission recommends striking 2-108(d)(8)(IV).**

SB 800 requires public service companies to adopt NIST security frameworks, which may be unreasonable and burdensome for some utilities, especially smaller ones. While the NIST framework is appropriate for larger utilities, alternative frameworks have been developed for smaller utilities.[4] The COMAR regulations provide utilities the ability to utilize the cybersecurity framework applicable to its situation as opposed to prescribing a "one size fits all" approach.[5] Where Maryland's larger investor-owned utilities manage cybersecurity at the enterprise level across multiple affiliate companies operating in several states, prescriptive and narrowly focused requirements at the state level may be incompatible with broader corporate cybersecurity policy, strategy, and operational requirements for multi-state public utilities. This may require significant utility resources solely for compliance with the Critical Infrastructure Security Act of 2023, without producing any net cybersecurity improvements. **The Commission recommends replacing "based on the National Institute of Standards and Technology Security Frameworks" in (C)(4)(I) with "based on industry-accepted cybersecurity frameworks."**

[2] Public Utilities Article (PUA) Sect. 13-201(b)(1).
[3] PUA Sect. 2-113.
[4] American Water Works Association's ("AWWA") Cybersecurity Guidance and Assessment Tool for small water utilities or the National Rural Electric Cooperative Association ("NRECA") Essence Cybersecurity Tool for smaller electrical cooperative utilities.
[5] COMAR 20.06.01.01.

Additionally, the third-party utility audits required in (C)(4) would involve substantial costs that will be passed on to ratepayers. Finally, notwithstanding the previous concerns, the Commission notes that *annual* cybersecurity assessments of public service companies are an expensive undertaking. **A cybersecurity assessment every three years is more appropriate and aligns with the North American Electric Reliability Council ("NERC") Critical Infrastructure Protection ("CIP") audit frequency for electric transmission.**

I appreciate the opportunity to provide information on SB 800. Please contact Lisa Smith, Director of Legislative Affairs, at (410) 336-6288 if you have any questions.

Sincerely,

Jason M. Stanek
Chairman

BGE - SB 800 - LOI - PSC - Cybersecurity Staffing

Uploaded by: John Quinn

Position: INFO

bge
AN EXELON COMPANY

Position Statement

Information
Education, Energy and Environment
3/7/2023

Senate Bill 800 - PSC - Cybersecurity Staffing & Assessments (Critical Infrastructure Cyber - Security Act of 2023)

Baltimore Gas and Electric Company (BGE) offers this letter of information on *Senate Bill 800 - PSC - Cybersecurity Staffing & Assessments (Critical Infrastructure Cyber - Security Act of 2023).* The bill requires that the Public Service Commission (Commission) maintain expertise, establish cyber security standards, conduct periodic assessments, and require certain companies to implement certain cybersecurity standards.

The utility industry has been comprehensively addressing cyber- and physical-security threats and BGE and other Exelon companies are viewed as leaders in this space. We urge the General Assembly to continue to allow utilities to align our programs with federal industry standards and requirements that incorporate strong cybersecurity controls and best practices which will be overseen by the Commission without the use of a third-party assessor. A third-party expert certification approach may introduce unintended risks such as inconsistencies among these third-party evaluators. A key factor in successful compliance programs is consistency—relying solely on third parties to perform compliance verifications may result in divergent compliance monitoring approaches and interpretations.

BGE is well-positioned on cyber security and has concerns with the additional elements Senate Bill 800 would place on us. We look forward to working with the sponsor on amendments to align efforts to ensure a comprehensive and protective cybersecurity program is in place at public service companies.

Charles Washington | John Quinn 410.269.5281

2023-SB 800 INF PHI-FINAL.pdf
Uploaded by: Katie Lanzarotto
Position: INFO

March 7, 2023

112 West Street
Annapolis, MD 21401

Letter of Information – Senate Bill 800- Public Service Commission - Cybersecurity Staffing and Assessments (Critical Infrastructure Cybersecurity Act of 2023)

Potomac Electric Power Company (Pepco) and Delmarva Power & Light Company (Delmarva Power) respectfully submit this letter of information on *Senate Bill 800- Public Service Commission - Cybersecurity Staffing and Assessments (Critical Infrastructure Cybersecurity Act of 2023)*. Senate Bill 800 would require a public service company to adopt and implement cybersecurity standards that are equal to or exceed standards adopted by the Public Service Commission (PSC). These standards would include adopting a zero-trust cybersecurity approach for on-premises services and cloud-based services, establishing minimum security standards for each operational technology and information technology device based on the level of security risk and any security risks associated with supply chain issues. The bill would also require, beginning in 2024, that public service companies contract with a third party to conduct an assessment of operational technology and information technology devices based on the National Institute of Standards and Technology Security Frameworks ("NIST Standards") and report those assessments to the PSC.

Pepco and Delmarva Power recognize the importance of having and continuing to implement effective cybersecurity controls consistent with established and evolving security standards to protect critical infrastructure and maintain safe, reliable, and affordable energy delivery. The rapidly evolving nature of cybersecurity threats poses unique challenges for the critical infrastructure community, including utilities, and warrants careful consideration. While we appreciate the need to ensure that cybersecurity tools and approaches keep pace with new cyber threats, the General Assembly should also keep in mind that the utility industry has been aggressively and holistically addressing cyber- and physical-security threats in order to stay ahead of bad actors. Utilities across the nation, including Pepco and Delmarva Power are constantly improving their cybersecurity programs to stay ahead of threats pursuant to federal cybersecurity requirements and advances in industry approved frameworks. We respectfully ask that the utilities be allowed to continue to align our programs with federal industry standards and requirements that incorporate strong cybersecurity controls and best practices which will be overseen by the PSC without the use of a third-party assessor. A third-party expert certification approach may introduce unintended risks such as inconsistencies among these third-party evaluators. A key factor in successful compliance programs is consistency—relying solely on third parties to perform compliance verifications may result in divergent compliance monitoring approaches and interpretations.

Pepco and Delmarva Power understand that Senate Bill 800 is well intentioned and if the Committee is inclined to pursue this legislation, we respectfully ask to continue conversations with the bill sponsors as to how we can address our concerns.

Contact:
Anne Klase
Senior Manager, State Affairs
240-472-6641
Anne.klase@exeloncorp.com

Katie Lanzarotto
Manager, State Affairs
202-428-1309
Kathryn.lanzarotto@exeloncorp.com