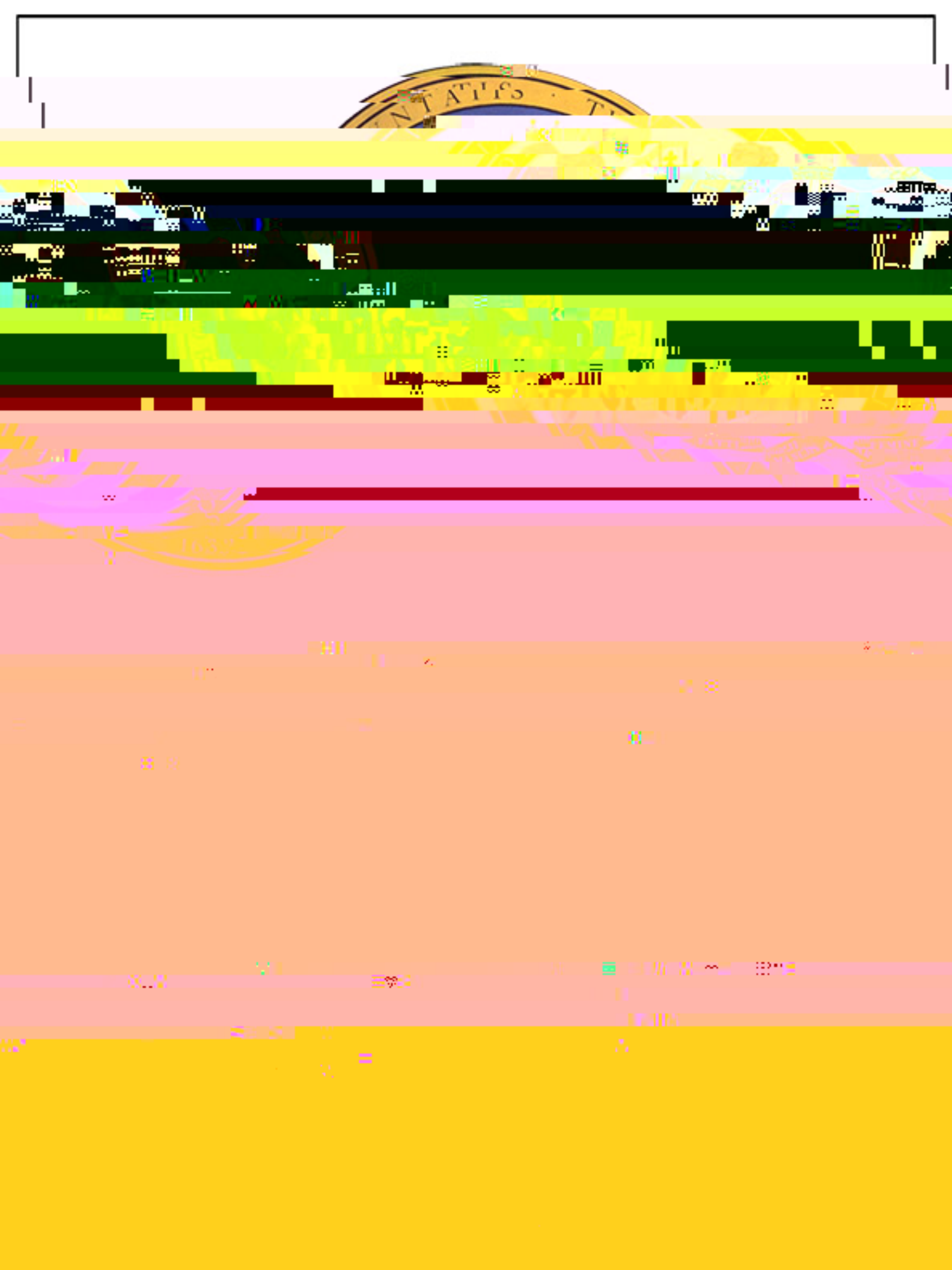

Abstract

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.

Contents

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 š Z Œ] • v [š • š v š v Á Z Œ Á o Œ š } µ Œ ( ] v o • µ • • • v š o } P } u ‰ } • š Œ] š Ç [• • l X / v Œ o] š Ç U Á [Œ quire À input] v] v P • Œ š U • š Z š Á] o o Œ 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 analysts" will be almost 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 C32c1rrifaass(g P (ri b)3 (o hin)6 (lfin).7.5 (4.7.5h)3 (oo)3 (rit12 (s)11 (o)3 (iri9 (n)3 (n)3 (nch)32rrifaw

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. Maryland has set forth a goal in statute

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 idecurity TT3 17 TD [(i/Cr21-3 E6n)3 (s and)eyva95 (n

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 audit 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] ^ D Œ Ç o v W µ o] ^ Œ À] } u u] • •] } v î ì í õ v v µ o Z ‰ } Œ š _ U D Œ Z î ñ U î ì î ì X
[55] ^ D Œ Ç o v W µ o] ^ Œ À] } u u] • •] } v î ì î ì v v µ o Z ‰ } Œ š _ U D Œ Z í ó U î ì î í X
[56] ^ Status of Utility Cybersecurity Briefings with the Commission u] o (Œ } u : } Z v } Œ l } • MPSC, Z] (v P] v June 3, 2021.
[57] ^ Ç Œ • µ Œ] š Ç W W Œ] u Œ (} Œ ^ š š h š] o] š Ç Z P µ Z o P š µ Œ • š U Œ š Ç Œ • }] v] š X Ç _ E š Commissioners, with the US Department of Energy. January 2017. https://pubs.naruc.org/pub/66D17AEA-A46F-B54358EF-68B04E8B01F.
[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 •µ(( ]] vš À] v š} •š o]•Z šZ u šµŒ]šÇ o À o }(šZ }u‰ v
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) with v vš]šÇ š} š •šZ Wh d[• ÇZ Œ ç µŒ•]šµÇ Eu]šv] šÇ}v]vš Œ}v]vP
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)." h ^ ‰ Œšu vš }(v Œ P Ç X 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

applicable to such devices and shall specifically take into account any security risk associated with voting equipment-Œ o š • µ Z ‰] ‰ • o] Ç v] š v] Ç š v Z š } Œ ‰ ‰ o] o [92] • µ Œ] š Ç Œ] • l X _

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] ^ / v š } Ç [-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 ^ ^ µ Œ] š Ç D • µ - Œ Œ •] š ( ] } Œ o ^ ^ } K (š Á Œ _ h • h v Œ Æ µ š] À K Œ Œ ~ K • í ð ì î ô _ U E š] } v o / v • š] š µ š } (^ š v Œ • v d Z v } o } P Ç U : µ o Ç õ U î ì î í X 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 ^ v µ U] Œ î ì í ô X https://www.securityroundtable.org/its-time-to-treat-cybersecurity-as-a-strategic-investment-not-a-sunk-cost/

[95] Ibid.

[96]

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 [• 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

‰ Œ š }(š Z Æ µ š] À š ÁÙvšsZ Z }ÆE Pšz[ ] l š } Ávo P v }u u] š u v š š } š C
cybersecurity as a strategic investment.[109]

^ t } Œ l (} Œ •ÆÇ‰Z Œuš•] v Œ •} v u v Ç ( ] Œ u • } v [š o] • š š Z] Œ • µ Œ] š Ç o
Æ µ š] À •] • š Z š š Z • ‰ } ‰ o š Ç ‰] o o Ç } v } š Œ ‰ } Œ š] Œ š o Ç š
CEO. More commonly, the CSO or CISO reports to the CTO, or to the chief information ot (t)-3ef o ìïîÍ

] v (} Œ u • š [} v š u • U } Œ] v (} Œ u š] v (Œ š Z •] • [117] T h e v o l u n t e e r s must meet qualifying criteria as determined by an advisory board.[118] Volunteers must consent to a criminal background check and sign a contract.[119]

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 } v • µ u Œ • • š } š Z ^ š Z] v _ š Z š u Ç] v ‰ o • } v š Z] 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] d Z ‰ Œ } i š Œ ‹ µ] Œ • ^ u ‰ } v Œ š š Œ] š ‰ w š š] o] š Ç

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:

> ^ Ç Œ • µ Œ] š Ç] v (} Œ u š] } v š Z v } o P Ç _ u v • o o o š Œ } v]] v (} Œ
> of networked devices, networks, programs, and data from unintended or unauthorized access, change, or destruction.^ / v (} Œ u š] } v š Z v } o } P Ç _ u v • o o o š Œ } v]] v (} Œ
> 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 • š š µ š } Œ Ç } (( ] v] š] Œ • µ Œ] š Ç _
> 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. } ‰ š • š š µ š } Œ Ç ( ] v] š] } v } (^ Ç Œ Œ •] o] v
>] v (Œ • š Œ µ š µ Œ _ U ^ • µ ‰ ‰ Œ Ç š] Z o] v • } Œ š] Á l _ Œ U _ X

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] E } v Œ ‰ µ] P r o j e c t i o n 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. µ Œ] š Ç v } v š Œ] À • (Ç Œ / v (} Œ u š] } v
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.

The systems and facilities most commonly listed in the criminal code address electric, water, and }uuµv] š]}v•X d Æ • Z • šÁ} • ‰ Œ š ()v]š]}v• (}Œ ^ Œ]š] o]v(Œ 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 tA 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

^ Œ]š] o]v(Œ •šŒµ šµŒ _ ~ /• Á • (ì]ìŒí•šÇ š{Zv ( ]vŒuoŒP]}ÀvŒovÁ]vš]v Critical Infrastructure Protection statute, 42 U.S.C§. 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]v(Œ •šŒµ šµŒ _ u v• •Ç•š u• v }Œ• À}]ŒšÁµZ oš‰Z •Œ À‰šZ Ç•š} (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§. 5195c.

Note that the federal definition does not enumerate any specific types of facilities. Instead, it qualifies ^•Ç•š u• v ••š•_ • }všZ]u‰ š^šZ š‰Á}}ŒšÇ •Œš Œ µoš]}(vŒ_}Xu

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

Œ š (]v]š]}v (}Œ ^ Œ]š] o • }(šÁ Œ 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:
>
> {]• •]Pv š} Œµv Á]šZ o À š ‰Œ]À]o P }Œ u v P ‰Œ]À
>
> { Z •]Œ š }Œ ‰Œ]À]o P •• š} v šÁ}Œl]vP }Œ }u‰µš]v
>
> {]• •]Pv š} }všŒ}o •• š} š }Œ }‰ Œ š]}v o š Zv}o}
>
> { ‰ Œ(}Œu• critical (µv š]}v trust; or,
>
> { }‰ Œ š • }µš•] }(v}Œu o šŒµ•š }µv [145] Œ] • Á]šZ ‰Œ]À]o

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 restte0sestte0s and restte0s tctr mo

^ K v o Ç š Z ^ šv š š u Ç Á } Œ } š Zl Œ v Ç š] } v š } ‰ Œ } Z]] š U Œ • š ŒŒ š U } Œ Œ
operation of unmanned air Œ (š • Ç • š 019A> UA011]CXR U5ð Àï‰&3E@ Á3]u]CXR U5ð À à

innovative environment for UAS testing, development, and deploying the technology.[101] The Task Force generated thirteen recommendations. This included a recommendation to v š o P] • o š] } v • š o] • Z] v P v ^ Æ š v •] } v } (• o (_ ‰ Œ] v] ‰ o X d Z] • u v • š] } v • Á Z] ‰ Œ } Z]] š Ç ‰ Œ • } v • Á } µ o ‰ ‰ o Ç š } ‰ Œ • } v • µ •] v P v h ^ X _

the prior consent of the owner, tenant, or lessee.[170] The statute is silent as to using the ‰ Z Œ • ^ (o Ç] v] P Z } µ À • ‰] (Ç] v P Z] P Z š -]]] š] P Z š Œ š ‰ Œ

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 registerin<d3MCID 9 >>B8UCID 6Mext ent oent avng(v) 1 (tn(t)-]TJ T*t (v)-ers)-rmTJ T*i (u)3 regitiovajm (si)12 (v)- isi2 (o)3 (lat)1w oltit (aj)11(o)-7(a)12 (s re)-2 (g)4 v ooippinIn t(ac)11 (e)-ers e (tn(t)-- (y)-3)12 (the)]TJ 0 -1. (fTJ Tcren (ty)-4 (.)]TJ EMC /Reference13<</MCID

define the term or point to any authority or evidence that outlined what type of unmanned aircraft use

W o] v š] ((• [} v • š] • š µ š] o } v] u o • o • Œ µ Œ À] À to Dismiss.[188]] } v

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 within their authority.

In April 2020, the US Attorney General provided instructions to Department of Justice (DOJ) components 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 ‰ Œ š u[192] v š X _

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 enact legally questionable UAS operating restrictions around many different types of facilities, some of

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 ‰ Œ ‰ Œ v š • Xo d ZZ • À v [š Ç š ted 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 large7 thgtt(g)4 -e (o)5Be tenersrtin. icyb3 (ta)6 oel9posed

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 tools 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 ae3erse85e ye1.04/tT scre ule. C10 (eT9 (h)3 (e ref)-7 (n)12 (e 11. 571.1/A71.1/A71.1/A71.1/A71.1/A71.1

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 to require service quality and reliability standards

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 8 (p)39fk.(ress)se

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 utiliti • u Ç Œ ‰ } Œ š] Œ š o Ç š } } š Z] Œ } u ‰ } Œ v Ç] • Œ } Œ X

[199] ^ X PART 1 METERS AND YOUR PRIVACY' rmation) nal 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) .024 1MC /Span <<and the ti

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 Policy(s:)-3 (/)shk0 Tdi9spih0s3 (in)5 er Ndii

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

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

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

o l] v U WXšU Œ U ' X ~ î ïñí•UX DuŒŒZ [• Œ] v l] v P tlyšEasy to Pronounce ‰ Œ] •] v P propublica.org. Retrieved March 17, 2021, from https://www.propublica.org/article/hacking-water-systems

IN THE MATTER OF THE APPLICATION OF POTOMAC ELECTRIC POWER COMPANY FOR ADJUSTMENT
ITS RETAIL RATES FOR THE DISTRIBUTION OF ELECTRIC ENERGY, 9602 (Maryland Public Servic
Commission August 12, 2019). Retrieved April 27, 2021, 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.eMC /P <</MCID 3 >>BDC -30.722 -2 g

I4 tdATTER OF THE APPL

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 2dmo0k6y1l-ary2 (2)7 (1)r. arylanmnde13Link <</MCID 16 >>

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

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

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

^}Ç}Ç U KXU ~ ^š ((Œµ U <X ~îìíõ•X Ç Œ• µŒ]šÇ Z]•l •• ••u vš (} Functions2019 IEEE CyberPELSKnoxville, 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, fromhttps://public-inspection.federalregister.gov/2021-11352.pdf

State of Connecticut. (2019, October 10). Connecticut Critical Infrastructure 2019 Annual Report. Retrieved January 9, 2021, fromhttps://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, fromhttp://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 Developm§ent10-463 Definitions.

Swinton, S. (2019, July 25). Cybersecurity Governance, Part 1: 5 Fundamental Challenges. Retrieved December 21, 2020, fromhttps://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, fromhttps://www.dni.gov/files/NCSC/documents/news/20210319-Insider-Threat-Mitigation-for-US-Critical-Infrastru-March-2021.pdf

The t Z]š ,}µ• X ~îìîíU D Ç íî•X /Eu %µŒ}À]vKPŒšZŒE}vš]}v[• Ç Œ• µŒ]šÇ May 13, 2021, fromhttps://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

US Department of Energy. (2020, May). Securing the United States Bulk 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). Z µ š } Á v À Œ Ç š Z] v P [W ' o } o Œ v • } u Á Œ š 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