STATE OF CONNECTICUT
PUBLIC UTILITIES REGULATORY AUTHORITY

April 5, 2021

2020 Connecticut Public Utility Annual Cybersecurity Report

I. Executive Summary

Cybersecurity threats facing Connecticut's public utilities continue to increase in number and grow in sophistication. The 2016 Connecticut Public Utilities Action Plan identified the need for the state to take action to ensure that public utilities are able to meet the evolving cybersecurity landscape. The Public Utilities Regulatory Authority (PURA or Authority) established a collaborative process with Connecticut's electric, natural gas and water public service companies to meet individually with each company to discuss the cybersecurity threats faced and to review in detail the cybersecurity program.

This is the fourth consecutive annual report. Our review team took advantage of interagency relationships and included utility, cybersecurity, and emergency response subject matter experts.

The past year saw the onset of the COVID-19 pandemic, which resulted in the near-instant transition to full remote work status for employees, among other changes. Notably, a cybersecurity-focused statewide exercise set to occur in May was postponed due to the pandemic. Nevertheless, the implementation and improvement of cybersecurity programs continued.

The past year also saw an undeniable increase in activity from state sponsored actors. The speed and sophistication with which these actors could identify and take advantage of vulnerabilities increased notably. That said, the category of attacks did not change much, and phishing attempts remain the most prominent source of cyber-attacks. Cyber vulnerabilities in supply chain and third-party vendors remain a persistent threat.

The State of Connecticut officials and the Connecticut public utilities participating in the 2020 public utility cybersecurity review concur in this report. It is a consensus document. All information included in this report intentionally avoids associating specific facts or situations to a particular company.

II. Meeting Framework

The Authority and its state agency partners and utility companies followed the framework that was established by the Cybersecurity Action Plan in 2017. The framework calls for separate annual meetings with the following utility companies: Eversource Energy, Avangrid, Connecticut Water Company and Aquarion Water Company. The meetings took place largely in July and August, with one being rescheduled for October due to the need to prepare for and respond to Tropical Storm Isaias.

A number of Connecticut officials participated in each of the reviews, including:

- Marissa Gillett; Chairman, PURA;
- Jack Betkoski; Vice Chairman, PURA;
- Jeff Brown; Chief Information Security Officer, State of Connecticut;
- Brenda Bergeron; Principal Attorney, Division of Emergency Management and Homeland Security in the Department of Emergency Services and Public Protection;
- Stephen Capozzi; Supervisor of Technical Analysis, PURA; and
- David Palmbach; Intelligence Analyst, Connecticut Intelligence Center (CTIC).

The meetings followed the structure and process set up in PURA's Cybersecurity Action Plan dated April 6, 2016. A major change this year was that the meetings were held on a virtual meeting platform of each utility company's choosing.

The meetings remained structured around an agenda drafted by PURA, which focused on three main topics:

1. Corporate Culture;
2. Threats; and
3. Cybersecurity Capability Maturity Model (C2M2);

The emphasis on corporate culture is included first to ensure that each company's management has a serious commitment to cybersecurity policy and practices. Next, specific threats faced by the companies during 2020 were discussed. Finally, each meeting incorporated a C2M2 review, which includes a technical review of specific company security controls. The C2M2 is a self-assessment tool, whereby each company reviews the risks and objectives of its cybersecurity program across various technical and managerial domains. A company is able to use this tool to prioritize objectives based on the cyber risk profile of the company. The C2M2 details a list of practices that would need to be employed to meet the objectives for each technical domain. The more practices that are implemented by the company, the more mature the company's cybersecurity program is with respect to that domain. It is important to keep in mind that not all domains or objectives require significant action; all action is based on the specific cybersecurity risks as evaluated by the company.

With regard to running the meetings, prior practice gave much latitude to the utilities to develop their presentations within the established agenda. This year, PURA and its state agency partners further focused the agenda by sending a set of targeted questions to the utilities that addressed both action items from prior meetings and identified specific current matters that should be addressed.

Chief Executive Officers or senior managers led the company review session teams. The professional positions represented included cybersecurity leadership, physical and cyber risk management, operations, finance, human resources, network management and infrastructure services, customer service, threat and incident response management, and law, government relations and regulatory affairs management.

III. Threat landscape

a. COVID-19

It is impossible to discuss 2020 and not begin by discussing the emergence of COVID-19 and its effect on public utility companies and their underlying operations. This, of course, was particularly notable with respect to company cybersecurity programs, where companies had to quickly establish or scale up pandemic health and safety protocols, including the near universal transition of personnel to remote work or work-from-home status. This required massive focus by the companies to facilitate work from home, by enabling company network connectivity from personal devices and environments using virtual private networks (VPNs) through public channels, adapting incident command structures to a pandemic environment, and designating health and safety protocols for essential employees that must perform out in the field.

In general, this massive societal shift to remote work prompted malicious actors as a whole to change priorities. For example, the frequency of ransomware attacks generally declined since schools, businesses, and social organizations stopped or scaled-back operations. Phishing attempts remained the most prevalent form of attack with an increase of attacks now made against personal accounts/systems and virtual meeting platforms. There was a large increase in phishing and other malware threats during the initial months of COVID-19. Often these attempts targeted the desire of individuals and organizations to obtain COVID-19 related information. Due to the prevalence of this information online, this became an obvious focus for cyber criminals. Also, there was a large increase in the targeting of VPNs and online meeting platforms due to the huge increase in their use.

In a way, the new distributed workforce changed the vulnerability of cybersecurity protection systems and protocols. Company networks are now less vulnerable, since there was less centralized activity on those networks. However, this now heavily distributed workforce added new vectors for attack, most notably on individual accounts and systems. Brute force attacks remain a very prevalent means to steal personal log-in credentials and access the now distributed workforce. The reviewers found that all

companies performed admirably to manage the new COVID-19 work environment, enable remote work and adapt their cybersecurity programs.

b. General Threats

Regarding the general types of threats faced by utility companies in 2020, they typically fell under the same categories of vulnerabilities: phishing, ransomware, supply chain dependency risk, business email compromise through third-party vendors, etc. Most notable about this year, excepting COVID, was that threat actors used new technologies to more quickly identify and exploit new vulnerabilities. This indicates increasing activity by sophisticated cyber actors. This position was generally held by the companies. The most prolific state sponsors of these groups remain Russia, China, and Iran.

The Companies did report an increase in activity from less sophisticated actors too. These actors most commonly target employees with brute force or generic phishing attempts to steal credentials or introduce malware. These attempts are most often used for illicit financial gain.

More often than in years past, C-suite level executives were the target of sophisticated phishing attempts, highlighting the need to prioritize training for company executives.

c. Third Party Vendors

Third-party vendors providing external services to the utilities have remained a significant area of vulnerability. This has been emphasized in past reports and remains a challenge to this day. Doing business with external vendors makes the utilities depend to an extent on the security of the vendors themselves. This security dependency requires that the utilities invest significant resources to ensure the vendors have adequate security programs to protect the company.

By way of example, in 2020 there was at least one incident where a utility company vendor was hit with ransomware risking company information. Though in this case the company information was not compromised, this incident reveals the potential risk faced by the companies via third party vendors. Companies have seen malicious emails from compromised accounts of C-suite level executives from vendors, usually attempting some form of business email compromise (BEC). So-called squatting attacks are relatively common, with actors registering similar domain names to the utility company and targeting the companies' vendors.

To address this risk companies have increased the level of security reviews for the vendors, and developed vendor scorecards to assist in this valuation process going forward. This process is information intensive; thus, increasing the automation of the evaluation process helps to manage the level of information that must be retained and updated over time. Another solution has been to hire third-party security experts to perform investigations into security practices of vendors.

d. Phishing

Email phishing attempts continue to be the most common source of all cyber-attacks by far. Attempts frequently target internal corporate finance departments. Phishing attempts target third-party vendors as well, with an eye to pivot attacks towards the utility companies. Therefore, without a major emphasis on mitigating the threat that phishing attacks pose, a cybersecurity program is severely deficient. It is utterly crucial therefore that a company's cybersecurity program include a robust training program for its internal employees. One company starts all company meetings with a safety and cybersecurity tip, most often addressing phishing vulnerabilities. This is a very admirable practice and greatly enhances employee awareness of phishing attempts.

Further, some companies who have performed frequent training see low "click rates" among employees. Click rates do vary quite a bit across companies and not all training programs are effective. In years past, utilities have had to experiment with the best means to reduce employee click rate.[1]

Therefore, in order to measure effectiveness of phishing training, it is equally important that companies perform frequent (as often as monthly) phishing testing of employees. Frequent testing will help measure the effectiveness of a company's phishing mitigation plan. Testing also provides real world examples to employees to keep them vigilant and primed to properly identify phishing attempts. If a company does not currently have a regular testing program in place, then its phishing program is seriously deficient. Email phishing is the most common attack vector and must be addressed with urgency.

IV. Notable Activities/Actions

a. Penetration Tests

Consistent with past years, the companies retained outside firms to perform cybersecurity program audits and penetration tests. Cyber penetration tests are simulations of real world attacks on a company's systems to test their ability to detect and respond to cyber-attacks. Testers frequently employ social engineering methods to gain system information to allow access. Vulnerabilities can often be found in unpatched systems, and so unpatched systems are sought out to test a company's patch management program. Most notable this year was the investment by certain companies in prominent penetration testing companies. Companies like this can launch very sophisticated simulated attacks on a system to exploit unknown vulnerabilities. This type of test truly exercises a company's ability to identify and respond to breaches. This is important since nation-state cyber actors will be able to exploit even minute vulnerabilities. Thus, exercising and testing a company's ability to detect and respond to sophisticated intrusions is crucial.

[1] See page 9 of the 2019 report, which described ways to improve with reward systems, penalties, or just improved identification of potential phishing attempts.

b. Personnel

A cybersecurity industry best practice is to prioritize the hiring and retention of cybersecurity personnel. This has been a major area of focus in past reports and remains one here. All companies have focused on hiring appropriate security personnel.

Of particular emphasis this year has been the targeting of security experts in operational technology (OT) to support control systems. Since the pool of qualified OT security workers is limited, the companies are looking for other ways to manage. Some have provided more tailored training opportunities in the field of OT for existing security personnel.

Further, affiliate companies under a larger service company are making great strides in sharing resources and expertise. For example, one company's security team hosts monthly calls with affiliate companies' security teams to share insights and lessons-learned. This type of resource sharing can be a great benefit when responding to large cyber incidents.

There has also been a fast growing cyber mutual assistance program in North America. This program currently has more than 170 members from the energy and utility sector. The program is designed to facilitate sharing of expertise and resources among members during cyber emergencies. These types of programs are becoming a best practice in the cyber industry and participation in them puts member utilities at the forefront of good cyber practices.

Even with the above effort to expand and improve internal cyber expertise, it is very often beneficial to supplement staff with outside firms to help perform various cybersecurity-specific tasks such as incident response and cyber forensics. The ability to call upon additional resources, during both blue sky days and black sky events, fortifies a company's cybersecurity preparedness and response posture.

c. Exercises

Prior reports identified the need for cybersecurity-related exercises to consider more severe and widespread cyber disruptions. Following the issuance of last year's report, GridEx V was held. GridEx is a national grid exercise that simulates certain cyber and physical attacks on the North American electricity grid and other critical infrastructure. The exercise is held every two years and is led by the North American Electric Reliability Corporation (NERC). GridEx V was held by NERC on November 13-14, 2019.

The Connecticut Division of Emergency Management and Homeland Security (DEMHS) planned its annual 2019 Governor's Emergency Planning and Preparedness Initiative Exercise (EPPI) to coincide with GridEx V. Notably, Eversource assisted the DEMHS and its partners in adapting and expanding the exercise for the state EPPI. Connecticut

had several exercise days planned for both November and December of 2019 with state, local, federal and nongovernmental entities.

The theme of the EPPI was to exercise statewide response and recovery to a largescale and coordinated cyber and physical attack. This was the first statewide exercise focusing primarily on a cybersecurity attack on critical infrastructure. The Emergency Support Function 12 – Energy and Utilities Annex (ESF-12) to the State Response Framework was activated for this exercise and included federal partners such as FEMA and DOE, state agencies, state-regulated public utilities included in this review and other entities, such as transmission gas pipeline companies, power generating plants, and other energy and telecommunications companies.

This exercise proved very fruitful for participants as it involved a major utility disruption affecting a diverse set of public and private entities. There was robust turnout for this exercise.

One of the main findings from the exercise was the importance of communications during a massive cybersecurity event like the one exercised. First, the general reliance of public utility critical infrastructure on communications is immense. That these key dependencies are susceptible to coordinated cyber-attack necessitate new ways of thinking about response and restoration priorities. Second, it was identified that there was a need to develop a communications disruption plan for communicating within a company to its internal employees. Third, since the cyber disruption plans are generally new and are not exercised in response to real world incidents as storm response plans are, employees are not as familiar with the plans and their roles and responsibilities within the plan. Therefore it is crucial to exercise regularly with internal employees cyber-related incident response plans, disaster recovery plans, and business continuity plans.

Finally, there was a planned opportunity to further exercise long-term recovery plans for coordinated and largescale cyber-attacks on critical infrastructure and Lifelines through the FEMA Region 1 National Level Exercise. The exercise was planned to take place in May, 2020. Planning for this exercise by FEMA began in the spring and summer of 2019. Planning by DEMHS began in January, 2020 to incorporate this exercise into its 2020 EPPI. ESF-12 was called by DEMHS to support the development of this exercise. A number of initial planning sessions occurred, such as developing Connecticut-specific scenarios. Ultimately, however, with the full-time activation of the state Emergency Operations Center (EOC) due to the COVID-19 pandemic, this exercise and the planning process were postponed.

d. Participation in Connecticut Cybersecurity Committee

The Connecticut Cybersecurity Committee is run by the state and consists of state agencies, local governments, federal partners, and private companies. The committee meets monthly and includes a briefing on current threats and cyber trends, information

about training and exercise activities, and sharing of information and lessons-learned among members.

In 2020, the committee shared information about: (1) vulnerabilities being exploited by state actors, including supply chain equipment vulnerabilities; (2) the increasing trend in attacks on online meeting platforms; (3) a best-practices guide for preventing and responding to ransomware attacks; (4) guidance to help detect network compromise for employees working from home; (5) systems with vulnerabilities that require patching; and (6) real-time updates on the SolarWinds hack.[2] The list above is just a small sample of the wealth of information available through participation in the committee.

This year saw almost full participation by the utility companies, who acknowledged benefiting greatly from this group. The companies reported that the committee was particularly useful for: (1) identifying timely threat information presented at the meetings and through the CTIC pass-throughs; (2) providing situational awareness around COVID-19; and (3) assisting in reporting of incidents via CTIC's Cyber Incident Reporting Guide.

V. Conclusion

The array and sophistication of cybersecurity threats facing Connecticut's public utilities seems to grow every year. This was made ever more challenging by the onset of the COVID-19 pandemic. In the face of these challenges, the utilities are well aware of the increasing cyber threats and demonstrate that they take such threats seriously. This level of commitment is evidenced across all levels of decision makers.

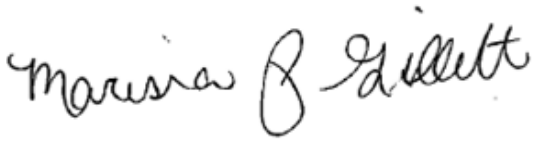
Utilities are constantly looking to strengthen their in-house expertise and supplement it with external partners. All companies are now taking advantage of the Connecticut Cybersecurity committee, both through the monthly meetings and via CTIC pass-throughs.

Many utilities also demonstrated the seriousness with which they approach the consequences of a breach. All utilities should consider testing not just their prevention systems, but their detection and response as well.

[2] The SolarWinds hack was first made public by Fireye in early December, 2020. The hack was an exploit by nation state actors of certain versions of the SolarWinds Orion product. That product is used widely by numerous public and private entities to monitor network traffic. The exploit potentially affected many federal agencies and private companies. CISA, in its December 13, 2020 directive to federal agencies, described the chance of compromise as very high and if system is compromised a grave threat. This hack was particularly notable for utility companies as the product could be used to monitor operational systems network traffic and could therefore affect both IT and OT environment. Much guidance has been provided by CISA and other experts on how to respond to the exploit. This exploit was identified after all annual review meetings had been held I 2020. Nevertheless, PURA has received updates from the utility companies regarding the exploit and their subsequent actions. It is premature at this time discuss each companies response actions in detail.

This past year saw all regulated electric, gas and water public service companies participate more fully in cyber-related exercises. The companies should continue to exercise their cyber incident response plans and participate in national, regional and statewide cyber exercises moving forward.

Sincerely,



Marissa P. Gillett
Chairman