Steven J. Foley
Vice President & CISO
Corporate & Information Security Services
Steven.Foley@Exeloncorp.com

November 14, 2022

Via Regulations.gov

Mr. Todd Klessman
Cybersecurity Incident Reporting for Critical Infrastructure Act of 2022 ("CIRCIA") Rulemaking Team
Cybersecurity and Infrastructure Security Agency ("CISA")
circia@cisa.dhs.gov

Re: Request for Information on the Cyber Incident Reporting for Critical Infrastructure Act of 2022
Agency/Docket Number: CISA-2022-0010; Document Number: 2022-19551
September 12, 2022

Dear Mr. Klessman:

Exelon appreciates the opportunity to provide comments on the Request for Information ("RFI") for the Cyber Incident Reporting for Critical Infrastructure Act[1] ("CIRCIA") rulemaking. As part of the U.S. energy sector, one of the 16 critical infrastructure sectors defined by Presidential Policy Directive-21[2] ("PPD-21") and which is therein identified as "uniquely critical due to the enabling functions [it] provide[s] across all critical infrastructure sectors,"[3] Exelon is well-positioned to provide feedback on this Request for Information, particularly as it relates to shaping essential definitions and the scope of reporting requirements for an effective reporting regime that is well-harmonized with other federal reporting requirements.

About Exelon

Since Exelon was formed as a combined generation and distribution utility company in 2000, we have been committed to generating and delivering energy safely, reliably, affordably and in a manner that meets the environmental and societal goals of the communities we serve. We recognize the critical role energy plays in both the national economy and the daily lives of our customers. As a result, over the decades we have consistently aimed to maintain the security of our systems while maximizing the generation and delivery of zero-carbon energy through investments in nuclear upgrades and renewables,

[1] PL 117-103 (Mar. 15, 2022).
[2] *See* Presidential Policy Directive – Critical Infrastructure Security and Resilience (Feb. 12, 2013) https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.
[3] *Ibid.*

driving best-in-class operations, optimizing our transmission and electric and gas delivery systems and facilitating electrification to support a clean energy transition. Today, as a stand-alone utility business and the premier energy delivery company, Exelon will lead the industry to a cleaner, more adaptable, but also more secure and resilient grid while protecting consumer choice and energy affordability. Exelon's "Path to Clean" commitment builds on our historic efforts to address climate change by aligning carbon reduction efforts throughout our utility operations to the national goal and net-zero emissions targets that support a 1.5 degrees Celsius future. The jurisdictions Exelon has the privilege to serve are among the most progressive in driving renewable energy development and electrification. But it must be recognized that as generation becomes more complex and more and more of our activities are electrified, grid security becomes both more important and more difficult. This heightened security burden will only increase as our nation's aspirations approach net-zero carbon emissions. The cybersecurity tools and approaches we apply must keep pace with energy innovations, electrification, shifting consumer demands and new threats to our grid infrastructure.

Exelon is a member of the Edison Electric Institute ("EEI") and the American Gas Association ("AGA") and supports the general comments made by each, but because of the ever-evolving cyber threats, it is critical for Exelon to respond to the request for comments regarding reporting requirements for cyber incidents. Below, we have offered some insights that we hope CISA will consider as it restructures the CIRCIA and considers approaches to managing cybersecurity incidents.

General Comments

Exelon recognizes the importance of adopting effective cybersecurity incident reporting requirements that align and balance the protection of interests between the federal government and critical infrastructure owners/operators, while incentivizing sound, safe, and responsible security practices. We strongly encourage CISA to avoid creating a compliance program, but rather institute a collective defense capability – which would benefit all, provided that the reporting and non-attributable information is released quickly to the Information Sharing & Analysis Centers ("ISACs") and relevant stakeholders. Given the rapidly evolving threat landscape, it is more important than ever for policymakers to work with critical infrastructure representatives to identify key principles that guide a practical, reliable, flexible, and sustainable cybersecurity incident reporting regime.

There is a distinction between information sharing outside of the regulatory regime and incident reporting as driven by mandates. There is also a shared responsibility on the part of the government to process what is reported, analyze, and then share lessons learned with covered entities in a proactive manner to help them protect their systems in the future. The Department of Homeland Security ("DHS") is compelled to share timely, actionable information based on the reporting in a manner that implores on CISA to be a producer and not just a consumer of the reports received.

Exelon is committed to collaboratively partnering with key stakeholders in defining key terms, identifying appropriate information and timing requirements, and establishing reciprocal responsibilities. A framework that promotes constructive cybersecurity incident reporting is important to all critical infrastructure stakeholders and should be based on the following principles:

1. Clearly defined key terms and reporting thresholds.

Definitions that are unambiguous help reduce uncertainty for operators in determining when a situation may require notification to CISA of a **confirmed** cyber incident. In particular, the definition of a 'covered cyber incident' is the touchstone that establishes which types of compromises are reportable. Regulations mandating **cyber incident reporting must clearly define the threshold for a cyber incident under each network environment**, i.e., information technology ("IT") and operational technology ("OT").

Specific to distinguishing between IT and OT, consumer data breach carries a different consequence regime than a breach in critical OT infrastructure. Requirements addressing reporting incidents of OT breaches should be designed to promote safety, transparency, and accountability, while protecting the reporting entity's identity. Relative to threshold, reportable instances should be exploitations and distributed denial of service ("DDoS") attacks, as opposed to a downloaded malware that was killed, a phish, a scan, a scam, or a vulnerability. Effective incident reporting policy bases the notification trigger on potential for harm to public safety, including potential impacts to critical services and national security.

a. *Covered Entities.*

CIRCIA states that the definition of a "covered entity" will be consistent with the definition of critical infrastructure provided in section 2240(5) of the Homeland Security Act of 2002[4] and based on: 1) consequences that disruption to or compromise of the entity could cause to national security, economic security, or public health and safety; 2) the likelihood that such an entity may be targeted by a malicious cyber actor, including a foreign country; and 3) the extent to which damage, disruption, or unauthorized access to such an entity, including the accessing of sensitive cybersecurity vulnerability information or penetration testing tools or techniques, will likely enable the disruption of the reliable operation of critical infrastructure.[5]

Exelon supports this framework but note that it is in CISA's interest to take a methodological approach to determining covered entities; such an approach should be risk based and should take into consideration the existing risk methodology utilized by other security regulatory programs[6]. CISA should likewise avoid imposing reporting standards that are difficult to apply or are overly subjective (such as provisions that excuse reporting only in cases where another law provides greater protection or at least as thorough disclosure requirements, or only in situations in which the entity complies with both jurisdictional requirements).

Regardless of the scope of what is considered a covered entity, CISA *must* develop and implement a robust outreach process to clearly inform entities of their responsibilities and requirements under the final regulation.

b. *Covered Cyber Incident*.

Reporting thresholds should depend on the significance of the breach and the corresponding impacts and harm. Exelon believes that CISA should consider covered cyber incidents to be those **substantial incidents,**

[4] PL 107-296, title XXII (Nov. 25, 2002).
[5] PL 117-103 (Mar. 15, 2022), § 2242(c)(1).
[6] Including, but not limited to: The Transportation Security Administration's ("TSA") Pipeline Security Guidelines and critical facilities list, the U.S. Coast Guard's ("USCG") Maritime Transportation Security Act, and CISA's Chemical Facility Antiterrorism Standards.

as defined in the legislation, that directly impact or could directly impact the operational capabilities of the critical infrastructure entity, as determined by the entity. The more explicit CISA is on this definition, the fewer instances of over-reporting or reporting incidents that do not have an impact on U.S. economic and national security, as envisioned in the legislation. This will help ensure that CISA receives the credible cyber incident data needed to mitigate the potential impact of incidents to U.S. economic and national security.

Further, for those companies with international operations, covered incidents should be limited to those which directly impact the companies' domestic operations. CISA should also consider scoping the rule to exclude non-malicious physical incidents that might impact cybersecurity infrastructure, such as accidental damage or damage caused by extreme weather events.

c. *Reasonable Belief.*

CISA's requirements for reporting should be confined to **confirmed** cyber incidents, as determined by the covered entity. In other words, a covered entity *reasonably believes* a covered cyber incident has occurred when they have *confirmed*, based on their policies and procedures, a cyber incident that directly impacts or could directly impact operations. Clarity in reporting requirements is essential for regulatory compliance and minimizing undue burden to covered entities and in particular to the agency receiving the report. Potential incidents that are investigated and found to be non-incidents or non-material provide no useful information to stakeholders or the government, nor do they ultimately impact U.S. economic and national security.

d. *Reporting Requirements.*

The final rule should likewise maintain a prompt reporting timeline of not less than 72 hours after confirming a covered cyber incident. Exelon believes a 72-hour deadline reflects an appropriate standard for notifying CISA about significant cyber incidents. Covered entities need time to investigate an intrusion before reporting to the government; they should not be required to report an incident until after conducting initial mitigation and response efforts to a confirmed incident. Even relatively minor cyber incidents can absorb hundreds of personnel hours to accurately assess. The final rule should also recognize timelines of existing cyber incident reporting requirements (*e.g.*, TSA and NERC), and clarify whether DHS supersedes such.

Exelon believes that, in both initial reporting and in any supplemental reports, **a covered entity should not be required to disclose anything that, if compromised, could put the company at additional risk** (*e.g.*, network mappings and system architecture, identification of security controls and protocols, security tools in place, software versions deployed in the environment). The **required disclosures should be limited to indicators of compromise, relevant internet protocol ("IP") addresses, and other artifacts necessary for CISA to understand the attack.** CISA should likewise not be empowered to utilize any information provided in reporting as a basis for investigation into the effectiveness of a covered entities' security controls.

Similarly, CISA should consider allowing covered entities the discretion in determining when an incident is resolved for purposes of supplemental reporting. Each incident, depending on the operational impact and attack vector, is different and has different timelines for recovery. If a covered entity, for example, is

able to isolate an incident and fully operate their critical services, then CISA should consider the incident resolved for purposes of supplemental reporting.

e. *Ransom Payments and Ransomware Attacks.*

Exelon agrees with the definitions of ransom payment[7] and ransomware attack[8] included in CIRCIA and supports the inclusion of ransomware and ransomware payments as reportable incidents. We further appreciate the shortened timeframe for reporting ransomware incidents, with the intent to support quick recovery and restitution of ransom payments. In this regard, **reporting of a ransomware incident should be required within 24 hours *after* the payment is made**. Any reporting made prior to payment may be inaccurate and premature as ransomware incidents can develop and evolve rapidly. Additionally, where a ransom payment is made and a ransomware attack is reported, it is imperative that law enforcement agencies are engaged early. Exelon strongly encourages CISA, within the framework of the CIRCIA rulemaking, to establish a formal reciprocal information sharing program with the Federal Bureau of Investigation ("FBI") and other relevant agencies within the Department of Justice ("DOJ") to ensure that the intent of recovery and restitution is met.

f. *Supply Chain Compromise.*

Exelon appreciates CISA's inclusion of a supply chain compromise[9] in the rule and agree with the definition within CIRCIA. Given the potential breadth of impact of a supply chain compromise, CISA must **very clearly define the responsible party for reporting any such compromise**. Exelon believes that each covered entity directly impacted by a supply chain compromise should be the party responsible for reporting their own and only their own incident. It should not be the responsibility of the supplier to report all customers who use their devices or software in order to protect the identity of the covered entity or consumer. Furthermore, CISA should not require covered entities to report the use of any such supply chain component that has been compromised if their own systems have not been affected by the supply chain compromise incident.

When considering the reporting requirements of a supply chain compromise, CISA should consider that a company affected by a supply chain compromise might not have all relevant data available for a complete report. In this vein, covered entities should only be required to disclose the information made available to them by the compromised vendor, and CISA must also understand that covered entities may be limited in their disclosures based on contractual obligations and rights with the vendor (*e.g.* confidentiality obligations).

g. *Third Parties.*

Exelon appreciates the inclusion of third parties to submit reporting on behalf of covered entities. We believe that CISA is including this provision to allow for covered entities to focus internal resources on response and recovery during a cybersecurity incident. With that said, CISA should **clarify the types of third parties authorized to submit reporting on behalf of a covered entity**. For example, many critical infrastructure operators use third-party firms for cybersecurity projects, including SCADA and other OT monitoring. Exelon believes that such project management contractor services should not be authorized

[7] PL 107–296, title XXII, § 2240 (13).
[8] PL 107–296, title XXII, § 2240 (14).
[9] PL 107–296, title XXII, § 2240 (17).

for reporting covered cyber incidents affecting a covered entity, but rather firms such as those handling incident management, regulatory compliance, and a covered entity's external legal representatives are the types of third parties that CISA should authorize to submit reporting on a covered entities behalf.

2. Harmonization of requirements and, where possible, a single, national point of contact for the operator to report all cyber incidents.

There already exists multiple cyber incident reporting laws or expectations on certain critical infrastructure sectors. In the energy sector, for example, TSA's Security Directive Pipeline-2021-01B requires reporting within 24-hours ""as soon as an incident is identified and requires entities to develop a Cybersecurity Incident Response Plan to mitigate operational risk and disruptions.[10]" the North American Electric Reliability Corporation ("NERC") is "one hour within determination of a reportable incident;[11]" and the Nuclear Regulatory Commission ("NRC") mandates reporting anywhere between one hour and 24 hours after discovery of an incident[12], depending on the criticality of the attack. These examples do not take into consideration existing state-level expectations.

Recognizing that a national reporting center like CISA has the capability to disseminate to all appropriate Federal and state entities, CISA's policy mandating additional cyber incident reporting needs to provide clear direction to operators subject to multiple regulatory authorities and to offer appropriate preemption. CISA must recognize existing hierarchies of compliance obligations and promote a mechanism that simplifies mass government notification and avoids competing reporting demands on the operator. To ameliorate some of these concerns, CISA is encouraged to establish agreements with the various federal government agencies that have existing critical infrastructure reporting requirements to facilitate sharing cyber incident report(s) with CISA, assuming appropriate information and data protection provisions are in place, and for that sharing to satisfy the obligation of the operator to report to CISA for those incidents.

Exelon stands ready to support this long-overdue harmonization effort and understand that reporting harmonization does not mean purely aligned requirements across critical infrastructure sectors.

3. Reporting requirements must not undermine existing public-private partnerships and should include reciprocal information sharing.

Many in the private sector have long-established collaborative partnerships with relevant federal agencies in sharing cybersecurity vulnerability and threat information. For example, DHS CyberSentry and the Cyber Information Sharing and Collaboration Program ("CISCP") functions as an actionable, relevant, and timely unclassified information exchange across all critical infrastructure sectors. Similarly, the Department of Energy ("DOE") Cybersecurity Risk Information Sharing Program ("CRISP") facilitates bi-directional sharing of unclassified and classified threat information for sectoral situational awareness. Natural gas utilities additionally work with their state partners in voluntary information sharing as well mandated cyber incident reporting. These programs, and others, improve the ability of the sector to protect against and respond to cybersecurity threats. Any incident reporting requirements must be careful not to damage or

[10] *See* Security Directive Pipeline-2021-01B (May 29, 2022): https://www.tsa.gov/sites/default/files/sd_pipeline-2021-01b_05-29-2022.pdf.
[11] *See* NERC CIP-008-06: https://www.nerc.com/pa/Stand/Reliability%20Standards/CIP-008-6.pdf.
[12] *See* 10 CFR, "Physical Protection of Plants and Materials," Part 73, (Ref. 1), § 73.77: https://www.nrc.gov/docs/ML1426/ML14269A388.pdf.

undermine these existing and proven information sharing regimes. Similarly, any reporting regime must be reciprocal, and under the same timelines, for federal entities experiencing a reportable incident.

4. Incident reporting requirements must include strong data security protections for reporting entities.

Reportable information can be quickly and easily accessed and made public. Any incident reporting regime must ensure that all company-specific information is anonymized, protected, and retained in accordance with, *for example*, existing protected critical infrastructure information ("PCII") protections, including exemption from: Freedom of Information Act ("FOIA") requests; state, local, tribal, and territorial disclosure laws; use in regulatory actions; and use in civil litigation. Likewise, incident reporting requirements must include a safe harbor for personal data that is securely encrypted, exempting an entity from providing notification of a breach of encrypted data to the extent the encryption has not been compromised. It also should include exceptions for personal data that has been adequately de-identified, pseudonymized or truncated, and for information that is publicly available.

Furthermore, CISA should address how the reported information will be used, analyzed, stored, and destroyed. Such processes and mechanisms clearly laid out in advance will determine the value output of the compiled information. Ensuring an efficient and effective reporting regime that maintains the confidentiality of the covered entity and its data, and that achieves our shared goals of strengthening the cybersecurity of U.S. critical infrastructure, is a top priority for Exelon and it's operating companies. We appreciate the opportunity to provide comments on this RFI and look forward to future engagement throughout the rulemaking process.

Sincerely,

Steven J. Foley