COMMENTS OF EXELON CORPORATION

March 3, 20223

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, 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 the NIST CSF update independently. Below, we have offered some insights that we hope NIST CSF will consider as it restructures the Framework.

General Comments

1. *CSF 2.0 will explicitly recognize the CSF's broad use to clarify its potential applications*

Exelon Corporation recognizes the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) as a foundational resource for cybersecurity guidance for

organizations. NIST CSF has been an invaluable tool for organizations looking to protect themselves from cyber threats. As technology becomes more interconnected, the security measures must evolve to reflect the constantly changing landscape of cyber threats.

Exelon recognizes the importance of a comprehensive cybersecurity framework and fully supports the recent update by NIST to the CSF. By expanding the global reach and working with international organizations, the CSF provides valuable guidance and best practices for organizations to effectively implement cybersecurity strategies and measure progress over time. Additionally, the expansion of the framework provides a set of guidelines for third parties that partner with utilities to implement rigorous security protocols that are recognized across the industry.

2. ***CSF 2.0 will remain a framework, providing context and connections to existing standards and resources.***

NIST CSF 2.0 has proposed a more integrated framework approach which will allow for referencing and mapping of other NIST frameworks. Exelon recognizes that the NIST CSF mapping and references to other frameworks will allow for better alignment with security protocols and established standards. This will also help identify gaps and ensure compliance with NIST CSF requirements and support organizational efforts to maintain their security posture.

NIST CSF 2.0 is also expected to release an update to the NIST CSF website which should make it easier to access resource documents and increase confidence that they are appropriately updated. Exelon supports the online update, as organizations should be able to rely on NIST online references when implementing controls or making changes to existing controls.

Additionally, the NIST CSF 2.0 update is expected to maintain the current level of detail in the functional domain areas. Exelon understands the importance of providing comprehensive guidance on baseline controls and compliance with established standards andwe support NIST CSF 2.0 maintaining the current level of detail.

NIST has also requested feedback on enhancing the respond and recover domains. Exelon finds that both domains offer sufficient guidance. However, a decision-making framework could be useful to help define decision-making authority during an incident. This could increase efficiently and decrease decision-making delays. Incident documentation guidance could be helpful in ensuring that relevant details regarding the incident are captured. This may help organizations with legal compliance and post-incident reviews.

3. ***NIST CSF 2.0 will include updated and expanded guidance on framework implementation***

The NIST CSF 2.0 update has proposed adding examples within the subcategories to offer additional guidance on implementation. Exelon supports additional examples to the functional domains provided they are not prescriptive. Any examples should serve assuggestions on how the controls could be implemented.

In addition to the subcategory examples, the NIST CSF 2.0 also recommends the use of NIST CSF profile templates. There may be value in using the template to define mission critical assets and business objectives to help align the security posture to an organization's goals.

4. ***CSF 2.0 will emphasize the importance of cybersecurity governance***

Exelon recognizes the value in a sixth domain for cybersecurity governance. to create a framework for organizations to maintain effective governance and compliance with security policies, standards and regulations. Exelon supports the new domain if it will help manage security operations and establish industry best practices.

5. ***CSF 2.0 will emphasize the importance of cybersecurity supply chain risk management***

The Supply Chain Risk Management is a critical component of NIST CSF 2.0. A robust, comprehensive supply chain management system can help identify, monitor, and mitigate thr eats to safety. Exelon supports NIST CSF providing additional guidance to reduce theimpacts from supply-chain incidents. Exelon recommends that such guidance would be more effective if provided in the functional domain areas rather than creating a stand-alone domain. Integrating supply chain guidance in each domain area would address weaknesses and vulnerabilities in the supply chain security controls without the increased burden of supporting an additional domain.

6. ***CSF will advance understanding of cybersecurity measurement and assessment of cybersecurity programs***

Exelon supports NIST CSF 2.0 providing guidance to help organizations identify their current level of cybersecurity maturity, understand their security posture, and develop strategies for improving their security programs. The proposed assessment model should provide organizations with a structured approach for assessing the cybersecurity program and practices and for implementing additional measures to improve security posture.