

COMMENTS FROM EXELON ON REQUEST FOR INFORMATION:

Evaluating and Improving NIST Cybersecurity Resources: The Cybersecurity Framework and Cybersecurity Supply Chain Risk Management

Docket No. 2022-03642

April 25, 2022

We commend the National Institute for Standards and Technology (NIST) for releasing a Request for Information (RFI) to gather stakeholder input regarding strategies for improving its Cybersecurity Framework (CSF) and advancing cybersecurity supply chain risk management. The information systems that support our nation's critical infrastructure must adapt to meet new societal goals and customers' needs. These critical cyber assets are also subject to ever-evolving and increasing threats. The tools and approaches we use to combat those threats and manage supply risks must also evolve.

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 supports the general comments made by EEI, but because of the extensive and rewarding use of the NIST CSF as the underpinning for Exelon's Security Controls Program, it is critical for Exelon to respond about the positive impact the framework has had on our program. We offer some insights that we hope NIST will consider as it redesigns the CSF and considers approaches to manage cybersecurity supply chain risk.

Section 1: Use of the NIST Cybersecurity Framework

1. The usefulness of the NIST Cybersecurity Framework for aiding organizations in organizing cybersecurity efforts via the five functions in the Framework and actively managing risks using those five functions.

Exelon has had enormous benefit from the use of the NIST Cybersecurity Framework ("CSF"). The electric industry is highly regulated as there are multiple mandatory compliance frameworks that guide us on how to protect our most critical assets. For those assets not controlled by an over-arching mandatory standard, such as NERC CIP, Exelon has voluntarily built an internal Security Controls Program based on the NIST Cybersecurity Framework. This internal Security Controls Program is multi-faceted and touches nearly every organization and system that impacts the company's cybersecurity program. By leveraging the NIST CSF, we were able to use an established, comprehensive and flexible model to build our controls program and implement the NIST CSF's five core functions of Identify, Protect, Detect, Respond, Recover.

Applying the CSF has also benefitted Exelon to help foster a culture of security through our organization. Our security control documents explicitly reference NIST controls. On an annual basis the Exelon Corporate and Information Security Services ("CISS") team leads an effort to obtain attestations from the control owners that certifies successful adherence. In addition, Exelon updates and reviews the Security Controls policy and procedure documents in

an annual effort we refer to as “NIST Week”. During this weeklong effort, the CISS team coordinates a review of all the company security documents that are based on the NIST controls and gathers stakeholders from across the organization to review, comment, and improve our security program. With the state of evolving threats to our industry, it is essential that we are meeting to review and update our documentation. The cross-company subject matter experts, stakeholders and compliance contacts work collaboratively to review and improve these documents and the controls we use to implement them.

The annual attestation and NIST Week review are also effective ways to inform Risk management and long-range planning. If there are controls in the annual attestation process where an exception is taken, it is tracked as a risk. In the NIST Week process, if there is a control that we identify that presents challenges, we also identify this as a risk. Any risk identified through either process is then used in our broader CISS Risk Management planning, and appropriate remediation actions are developed, documented and tracked. The identified risks are also prepared and taken to long-range planning conversations with senior leadership to develop organizational strategy for the coming years.

The NIST CSF has become an essential part of how we secure our infrastructure at Exelon. Providing some of how we use the CSF every day and in annual planning should exhibit how important these are to our program. By using the NIST CSF as the foundation for our security controls program, we give our program weight and consistency and process to improve.

2. Current benefits of using the NIST Cybersecurity Framework. Are communications improved within and between organizations and entities (e.g., supply chain partners, customers, or insurers)? Does the Framework allow for better assessment of risks, more effective management of risks, and/or increase the number of potential ways to manage risks? What might be relevant metrics for improvements to cybersecurity as a result of implementation of the Framework?

The NIST CSF has always been valuable because it is a flexible, risk-based framework that can be implemented voluntarily. Any change to the NIST CSF that maintains those components will add to its use and value.

Metrics have become an essential part of how private industry communicates to leadership. Cybersecurity controls do not easily lend themselves to clean metrics. Suggested metrics for each of the core functions could be a great addition for the use of the NIST CSF. Companies may have examples that could be provided for potential use. As cybersecurity expertise continues to become a need in leadership teams and boards, standardizing the way that companies communicate about cybersecurity metrics would be beneficial.

Development of metrics also prioritizes the components of a cybersecurity program. For a team in an early stage, focusing on just metric-topics could be an effective way to establish a program and grow it for years to come. Meaningful metrics can be developed in a collaborative public/private partnership.

3. Challenges that may prevent organizations from using the NIST Cybersecurity Framework or using it more easily or extensively (e.g., resource considerations, information sharing restrictions, organizational factors, workforce gaps, or complexity).

Implementation of the NIST CSF requires internal expertise and cost to develop a security controls program. Exelon understands that these are challenges for any organization, regardless of size.

It would be beneficial if there was a more wide-spread adoption of the NIST CSF within the vendor community. A successful adoption of the NIST CSF gives a baseline to discussions cybersecurity between vendors and industry. Currently, our Security Risk Assessment (“SRA”) process does some fact-finding on what controls a vendor currently has in-place, and in this process we explicitly ask about the NIST CSF.

There has been a general increase in the controls placed on private industry on identifying supply chain components, subcomponents and this has led to industry increasing contractual controls with our vendors. When the vendors have a NIST-based program, or at least an adherence to the Five Core Functions, the discussion is more collaborative. Having supplier specific resources or outreach to the vendor community to let them know about the great resources NIST has available could lead to better controls between vendors and industry.

Cost and expertise are still a major hurdle for some companies, especially small and medium-sized businesses. In the event there are grants at the federal, state or local level of

government to mature a cybersecurity program, it would be helpful if these efforts leveraged the NIST CSF.

In addition to some of the challenges of implementing a NIST CSF based controls framework, there are also some regulatory complications to consider. Regulators at both federal and state levels are currently imposing substantive cybersecurity requirements that are not completely consistent with the guidance in the NIST CSF. Businesses are then required to evaluate and compare current controls with the newly developed controls and determine if there is similarity. It would be far less disruptive for businesses and less of a burden on limited security resources if the NIST CSF was more consistency adopted by other federal agencies and used as the basis for any new substantive requirement.

For example, most recently the Department of Homeland Security (“DHS”) developed a Security Directive for critical operators of natural gas. In some cases, specific requirements of these directives aligned to the NIST CSF, but in others it was in conflict with NIST guidance. It places a risk on companies who have to shift resources to implement new security measures that are not necessarily more protective in their approach. Critical Infrastructure owners may find themselves deciding between frameworks for implementation. To help industry make those implementation decisions, it would be beneficial if NIST coordinated outreach to federal agencies to ensure consistency with the widely accepted NIST guidelines. This outreach could be done proactively, or when it is evident that an agency is working on a new substantive security requirement.

- 4. Any features of the NIST Cybersecurity Framework that should be changed, added, or removed. These might include additions or modifications of: Functions, Categories, or Subcategories; Tiers; Profile Templates; references to standards, frameworks, models, and guidelines; guidance on how to use the Cybersecurity Framework; or references to critical infrastructure versus the Framework's broader use.**

In addition to the proposal for metrics in the response to Question 2, there is one other key feature that could be added: model Incident Reporting language.

The five functions of the NIST CSF Identify, Protect, Detect, Respond, Recover are designed in a way that helps organizations deal with preparing for and responding to a cyber incident. In the past two years, there has been a significant increase in the number of governing bodies that are developing a mandatory incident reporting requirement. It would be incredibly helpful if NIST could work with the private sector to develop a “model” incident reporting requirement that could be leveraged by federal, state and local government partners.

The current patchwork regulatory landscape for incident reporting creates a burden on private industry. Exelon, and many in the private sector understand the inherent value in sharing information with our government partners, but it has to be done so in a mutually beneficial and secure manner. The authors of the NIST CSF understand that incident response is complicated, involves many subject matter experts and senior leaders, and often has a lengthy deliberation process from discovery to recovery. It would be helpful to develop an Incident Reporting Requirement that met all stakeholder needs to aid in quicker recovery.

Developing a model incident reporting requirement that is flexible and allows time for industry to confirm the extent of a potential breach and meets the government information sharing needs would be an incredible asset to the private/public partnership.

5. Impact to the usability and backward compatibility of the NIST Cybersecurity Framework if the structure of the framework such as Functions, Categories, Subcategories, etc. is modified or changed.

As provided in the response to Question 2, The NIST CSF has always been valuable because it is a flexible, risk-based framework that can be implemented voluntarily. Any change to the NIST CSF that maintains those components will add to its use and value.

Since the last version of the NIST CSF was developed in 2018, the threat landscape has evolved exponentially. The NIST CSF should be updated as the threats continue to change.

Section 2: Relationship of the NIST Cybersecurity Framework to Other Risk Management Resources

7. Suggestions for improving alignment or integration of the Cybersecurity Framework with other NIST risk management resources. As part of the response, please indicate benefits and challenges of using these resources alone or in conjunction with the Cybersecurity Framework. These resources include:

- **Risk management resources such as the NIST Risk Management Framework, the NIST Privacy Framework, and Integrating Cybersecurity and Enterprise Risk Management (NISTIR 8286).**
- **Trustworthy technology resources such as the NIST Secure Software Development Framework, the NIST Internet of Things (IoT) Cybersecurity Capabilities Baseline, and the Guide to Industrial Control System Cybersecurity.**
- **Workforce management resources such as the National Initiative for Cybersecurity Education (NICE) Workforce Framework for Cybersecurity.**

The National Initiative for Cybersecurity Education (NICE) Workforce Framework for Cybersecurity has been an incredible asset to industry. Exelon has leveraged and used the NICE Framework as the basis for job descriptions within our cybersecurity organization. It has made our postings competitive and attractive for prospective job applicants. It has also helped establish the different specialties and expand the potential job offerings within the cybersecurity team for both internal promotion and external new hires.

Aligning those job descriptions and team designations to the Core Functions of the NIST CSF could be an effective way for new programs to understand how to implement controls effectively.

8. Use of non-NIST frameworks or approaches in conjunction with the NIST Cybersecurity Framework. Are there commonalities or conflicts between the NIST framework and other voluntary, consensus resources? Are there commonalities or conflicts between the NIST framework and cybersecurity-related mandates or resources from government agencies? Are there ways to improve alignment or integration of the NIST framework with other frameworks, such as international approaches like the ISO/IEC 27000-series, including ISO/IEC TS 27110?

One way to improve alignment with other existing frameworks is to develop a way to compare controls across them at the same time. In the electric industry, we use the NIST CSF as the baseline for our security controls, we also complete maturity assessments and compare those NIST-based controls to frameworks like the DoE's C2M2¹.

Mapping the NIST CSF to other resources developed by the federal government could help cement the perceived usefulness of implementing the NIST CSF controls. It would become a de facto implementation guide for private companies to understand how successful evidence of

¹ https://www.energy.gov/sites/default/files/2021-07/C2M2%20Version%202.0%20July%202021_508.pdf

a control could be used as evidence of compliance for another framework. Many private sector companies have developed these internally as a way to track their own process and avoid duplication of cost and effort.

10. References that should be considered for inclusion within NIST's Online Informative References Program. This program is an effort to define standardized relationships between NIST and industry resources and elements of documents, products, and services and various NIST documents such as the NIST Cybersecurity Framework, NIST Privacy Framework, Security and Privacy Controls for Information Systems and Organizations (NIST Special Publication 800-53), NIST Secure Software Development Framework, and the NIST Internet of Things (IoT) Cybersecurity Capabilities Baseline.

As the NIST CSF continues to be used by critical infrastructure owner and operators references to other existing frameworks would be beneficial. For example, the mapping of the NIST CSF to the NERC CIP standards could be helpful for transmission owner / operators.² Even lessons learned from these efforts can help inform the strategy used in decision making within private sector.

Additionally, if there are certification opportunities for vendors that leverage the NIST CSF from reputable trade organizations, it would be helpful to know that there is a certification process similar to what the Better Business Bureau (“BBB”) offers for Vendor Privacy Program Certification³. These efforts can help vendors take credit for their own complex cybersecurity programs.

Section 3: Cybersecurity Supply Chain Risk Management

11. National Initiative for Improving Cybersecurity in Supply Chains (NIICS). What are the greatest challenges related to the cybersecurity aspects of supply chain risk management that the NIICS could address? How can NIST build on its current work on supply chain security, including software security work stemming from [E.O. 14028](#), to increase trust and assurance in technology products, devices, and services?

One of the greatest challenges for utilities is identifying component and subcomponent parts of vendor products and services. Utilities have each begun to develop their own programs

² [Benefits of an Updated Mapping between the NIST Cybersecurity Framework and the NERC Critical Infrastructure Protection Standards | CSRC](#)

³ [Vendor Privacy Program | BBB National Programs \(bbbprograms.org\)](#)

to complete an evaluation for unwanted influence on component and subcomponent parts. As the industry shares many of the same vendors, this means that there are multiple evaluations that a single vendor needs to complete to conduct business. This is overly burdensome on the electric industry and its vendors as it lacks standardization.

One of the ways Exelon leverages the NIST CSF and other NIST resources in the vendor risk assessment process is through the Exelon's Security Risk Assessment ("SRA") program. This program for Exelon's vendors was developed to screen vendors and thereby ensure they meet basic security hygiene requirements. The SRA covers a broad range of questions, including for example, assessing whether a vendor has implemented:

- an industry recognized Information Security Policy, such as the NIST CSF or ISO-27001;
- the use of anti-malware to secure devices and ensure malware signatures are regularly updated;
- a practice of conducting employee background investigations, including criminal checks;
- an information access management process;
- steps to protect data at rest, in use, and in transit;
- a program to properly dispose of data;
- a program to define and test business continuity and disaster recovery measures;
- a security incident handling program, which includes customer notification and coordination;
- programs to ensure customer notice and mitigation of vulnerabilities that impact vendor products or services;
- baseline security configuration management;
- security logging and monitoring;
- cyber vulnerability management and patching programs to protect vendor assets;
- a vendor asset management program;
- vendor network protections;
- vendor physical security protections;
- remote access controls on vendor systems; and
- security controls over third-party and fourth party (*i.e.*, sub-tier vendor) engagements.

With respect to this last area of vendor implementation of security controls governing sub-tier vendors, Exelon's SRA program specifically assesses and determines in advance whether a prospective vendor will use subcontractors in delivering materials or providing services to Exelon. If subcontractors are used, vendors must confirm whether the prospective vendor will:

- purchase materials or services from companies (or their affiliates) that are not prohibited from doing business with the United States federal government;⁴
- require subcontractors to comply with the vendor's industry accepted Information Security Policy, such as, NIST CSF or ISO 27001;
- apply and enforce the same or more stringent security controls that the vendor is held to in its contract with Exelon.

A subset of Exelon's SRA questions, including the above sub-tier vendor questions, are non-negotiable "gating" questions and if a prospective vendor provides an unacceptable answer to these questions, Exelon will not do business with them. Based on SRA responses, Exelon maintains metrics in a security profile of its vendors and uses those metrics to identify and minimize security risks as well as to guide its future procurement decisions.

While this approach has been successful in enhancing Exelon's supply chain cybersecurity and weeding out unsuitable vendors, such as vendors unable or unwilling to provide this information, this is Exelon's unique approach. It would be more cost-effective for industry and vendors alike if a single vendor could complete a single common security risk assessment and if that assessment was accessible by any potential utility buyer. As new standards are developed, many of them based directly on the NIST CSF, NIST could inform the conversation by helping vendors understand that the cyber practices covered in the NIST CSF are going to be the baseline for cyber security practices and by adopting them now, they will position themselves to be safe, secure and reliable for their customers.

The electric industry has made some significant progress on an industry common Security Risk Assessment⁵ developed through the North American Transmission Forum ("NATF"). Adoption of the form is not yet widespread enough to reduce the amount of

⁴ Exelon currently excludes any vendor who obtains products or services from Kaspersky, Huawei Technologies Company, ZTE Corporation, Hytera Communications, Hangzhou Hikvision Digital Technology Company, and Dahua Technology Company, or affiliates of these companies.

⁵ <https://www.natf.net/industry-initiatives/supply-chain-industry-coordination>

duplicative work that is placed on industry vendors. A standardized approach to understanding vendor risk can be even further simplified if the vendor and industry populations continue to agree and use the NIST CSF as the basis for effective security controls. By having targeted sections for vendor use, there could be further adoption of the NIST CSF, simplifying the risk assessment process.

12. Approaches, tools, standards, guidelines, or other resources necessary for managing cybersecurity-related risks in supply chains. NIST welcomes input on such resources in narrowly defined areas (e.g. pieces of hardware or software assurance or assured services, or specific to only one or two sectors) that may be useful to utilize more broadly; potential low risk, high reward resources that could be facilitated across diverse disciplines, sectors, or stakeholders; as well as large-scale and extremely difficult areas.

The most critical devices to the electric sector require a long lead time for development, and the industry has developed programs to combat and handle “urgent” or “just in time” inventory via mutual assistance programs, as well as spare asset sharing programs. By fully implementing a Security Controls program based on the Identify, Protect, Detect, Respond, Recover, Exelon believes that others would be able to identify the devices and assets that are critical and would require extensive replacement planning.

13. Are there gaps observed in existing cybersecurity supply chain risk management guidance and resources, including how they apply to information and communications technology, operational technology, IoT, and industrial IoT? In addition, do NIST software and supply chain guidance and resources appropriately address cybersecurity challenges associated with open-source software? Are there additional approaches, tools, standards, guidelines, or other resources that NIST should consider to achieve greater assurance throughout the software supply chain, including for open-source software?

There is a gap with timely and effective information sharing. The goal would be to share timely actionable intelligence. There are still significant hurdles to sharing sensitive information about vendors with other partners in the event of a significant breach. Some of the recent federal incident reporting requirements will require reporting to a centralized agency in the federal government, but this does not get actionable information into the hands of the defenders who need to Identify and Detect within their own systems through any certified channel unless the individual company pursues it via controls in an existing contract. This is a more significant gap

that likely needs to be approached in a larger, collaborative cross-sector effort, but since the NIST CSF is based on preparing for and responding to cyber events and is the baseline accepted approach to cybersecurity, it may be the best place to lead the discussion.

A centralized approach to identifying and assessing vendor risk information would be a huge benefit to the private sector. This effort would take time to develop, but using the NIST CSF as a baseline would be necessary for it to be successful.


14. Integration of Framework and Cybersecurity Supply Chain Risk Management Guidance. Whether and how cybersecurity supply chain risk management considerations might be further integrated into an updated NIST Cybersecurity Framework—or whether and how a new and separate framework focused on cybersecurity supply chain risk management might be valuable and more appropriately be developed by NIST.

By leveraging some of the key themes above, NIST could integrate some supply chain risk management guidance into the NIST CSF. There are already several industry-specific supply chain requirements⁶, some of which include mandatory controls. Exelon would recommend that any NIST integration of supply chain not interfere or conflict with existing compliance frameworks.

Thank you for the invitation to submit comments.

Contact:

Joseph Quinn
Exelon Corporation


1310 Point Street
Baltimore, MD 21231

⁶ Such as NERC CIP-013